الجمهوريـــة الجزائريـــة الديمقراطيـــة الشعبيـــة
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE HADJ LAKHDAR

BATNA (ALGERIE)

THESE

Présentée à la Faculté des Sciences
Département de Mathématiques
pour l'obtention du diplôme de

DOCTORAT EN SCIENCES

Option: Mathématiques

Par

CHERIF MIHOUBI

THEME

CLASSIFICATION DES CODES LINEAIRES TERTIAIRES OPTIMAUX [n, n/2]

Soutenue le : 03/07/2012

Devant le jury d'examen :

Mr. L. NOUI	Prof.	Université de Batna	Président
Mr. A. AMROUNE	Prof.	Université de M'sila	Rapporteur
Mr. H. BELOUADAH	Prof.	Université de M'sila	Examinateur
Mr. A. BOUDAOUD	Prof.	Université de M'sila	Examinateur
Mr. S E. REBIAI	Prof.	Université de Batna	Examinateur
Mr. N. TRABELSSI	Prof.	Université de Sétif	Examinateur

RESUME:

Dans ce travail on considère les codes cycliques de rendement 1/2 sur les corps finis GF(3) et GF(5) et on accentue notre étude sur ceux iso-duaux. Le problème central dans la théorie du codage est trouver la meilleure distance minimum dq pour laquelle un code de paramètres [n, k, d] sur Fq existe. Dans ce contexte nous avons réussi à optimiser cette distance pour les codes cycliques de taux 1/2 sur GF(3) et GF(5) en allant jusqu'à la longueur 74 pour les codes ternaires et 42 pour ceux sur GF(5). Nous avons aussi réussi à construire sept classes de codes cycliques iso-duaux sur le corps fini à 3 éléments et trois classes de codes cycliques iso-duaux sur le corps fini à 5 éléments.

En considérant les polynômes sur le corps fini de Galois à deux éléments GF(2), notre intention portait sur la divisibilité des trinômes $x^{am} + x^{bs} + 1$... (1), pour $m > s \geq 1$ par un polynôme irréductible de degré r sur GF(2), pour cela, nous avons réalisé le résultat suivant:

- S'il existe m, s des entiers positifs tels que le trinôme $x^{am} + x^{bs} + 1$ soit divisible par un polynôme irréductible T de degré r sur GF(2), alors a et b ne sont pas divisibles par (2^r-1).

MOTS CLES: *Corps finis, Codes cycliques, Distance minimum, Codes iso-duaux, Polynômes irréductibles, Divisibilité.*

ABSTRACT:

In this work we consider the cyclic codes of rate 1/2 over the finite fields GF(3) and GF(5) and we check our study over whose are isodual. 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 Fq exists. In this context we have successfully optimize this distance for the cyclic codes of rate 1/2 over GF(3) et GF(5) up to length 74 for the ternary cyclic codes and 42 for whose over GF(5) . We have also successful to construct seven classes of isodual cyclic codes over the field of 3 elements and three classes over the field of 5 elements.

Considering polynomials over the Galois finite fields for two elements GF(2). Our intention stand over the divisibility of the trinomials $x^{am} + x^{bs} + 1$...(1), for $m > s \geq 1$ by an irreducible polynomial T of degree r over GF(2).

Finally, considering the polynomials of type (1) over GF(2), we contribute to the result:

- If there exist positive integers m, s such that the trinomial $x^{am} + x^{bs} + 1$ is divisible by an irreducible polynomial T of degree r over GF(2), then a and b are not divisible by (2^r-1).

KEY WORDS: *Finite fields, Cyclic codes, Minimum distance, Isodual codes, Irreducible polynomials, Divisibility.*

UNIVERSITE HADJ LAKHDAR BATNA

THESE

présentée pour obtenir le grade de docteur

Spécialité: Mathématiques

CHERIF MIHOUBI

Classification des Codes Linéaires Tertiaires Optimaux [n, n/2]

Devant le Jury:

Mr, NOUI Lemnouar	**Président**	**Pr**	**U. de Batna**
Mr, AMROUNE Abdelaziz	**Rapporteur**	**Pr**	**U. de M'sila**
Mr, BELOUADAH Hocine	**Examinateur**	**Pr**	**U. de M'sila**
Mr, BOUDAOUD Abdelmadjid	**Examinateur**	**Pr**	**U. de M'sila**
Mr, REBIAI Salah eddine	**Examinateur**	**Pr**	**U. de Batna**
Mr, TRABELSSI Nadir	**Examinateur**	**Pr**	**U. de Setif**

REMERCIEMENTS

Je tiens à remercier Monsieur Abdelaziz Amroune d'avoir accepté de diriger ce travail et de créer autour de moi un environnement de recherche par ses conseils et son soutien permanent.

Comme je remercie Monsieur Noui Lemnouar, pour avoir accepté de présider ce jury et de ne cesser de me donner des conseils et des suggestions.

Je remercie également Messieurs Boudaoud Abdelmadjid, Salah eddine Rebiai, Nadir Trabelssi et Hocine Belouadah, pour avoir accepté de juger ce travail et de faire partie du jury.

Je ne peux oublier de remercier le Professeur Paul Zimmermann du Loria-Nancy France, pour toutes ses aides précieuses ainsi que ses conseils durant mon passage en septembre- octobre 2007 et Monsieur Patrick Solé directeur de recherche au CNRS pour son soutien permanent, sa gentillesse et ses précieuses directives durant mon stage à l'université Sophia Antipolis à Nice en mars-avril 2009.

Enfin, je remercie Mr Hassane Aissaoui , responsable exploitation au laboratoire informatique à L'Enst Paris, pour l'amélioration du programme informatique de recherche de la distance minimum des codes cycliques ternaires $C[26, 13]_3$ ainsi que tous les agents de la bibliothèque par leur disponibilité et leur soutien.

NOTATIONS

(a, b) : p gcd(a, b)

$|G|$: l'ordre de G

$\cong$: isomorphe

Deg p : degré de p

(p) : idéal engendré par p

$\overline{p}$: fonction polynômiale induite par p

$\ker \Psi$: noyau de Ψ

car$F$: caractéristique de F

$[K : F]$: dimension de K sur F

$f\,'$: polynôme dérivé de f

F^* : $F \setminus \{0\}$

$a \mid b$: a divise b

$a \equiv b (\mathrm{mod}\, n)$: $(a - b)$ divisible par n

F_q : corps fini d'ordre q

$n!$: factorielle n

$\varphi(n)$: indicateur d'Euler

Q_n : le $n^{ième}$ polynôme cyclotomique

m_α : le polynôme minimal de α

μ : fonction de Mobius

$p^r \mid\mid a$: p^r divise a mais p^{r+1} ne divise pas a (p premier)

A : anneau des polynômes

I : idéal de A

$F_q[x]$: anneau des polynômes à coefficients dans F_q

F_q^n : espace vectoriel des vecteurs de longueur n sur F_q

$F_q[x]/(f)$: anneau des classes modulo $f(x)$

$F_q[X]/(X^n - 1)$: anneau quotient(des classes de polynômes de degré inférieur à n)

$wt(x)$: poids de Hamming de x

d_H : distance de Hamming

$d_{\min}$: distance minimum

$C[n, k, d]$: code de paramètres n, k, d

$c(x)$: mot de code $\in C$

k/n : rendement ou taux d'un code $C[n, k, d]$

$x^{\perp}$: transposé du vecteur x

G : matrice génératrice

H : matrice de parité

σ : pérmutation

S_n : groupe des pérmutations

$g(x)$: polynôme générateur

$C^{\perp}$: code dual de C

$g^{\perp}(x)$: polynôme générateur du code dual

$h(x)$: polynôme de parité

$f^*(x)$: polynôme réciproque de $f(x)$

$d_q(n, k)$: plus grande valeur de d pourque $C[n, k, d]$ existe

d_C : maximale distance minimum d'un code cyclique

d_I : maximale distance minimum d'un code cyclique iso-dual

INTRODUCTION

– Le codage correcteur d'erreur introduit une forme de redondance controlée dans un message à transmettre pour le protéger face aux erreurs de transmission, cette technique joue aujour'hui un rôle fondamental dans les systèmes modernes de transmission et de stockage de l'information numérique. La théorie du codage vise à construire des codes correcteurs performants, opérant au plus proche des limites théoriques établies par la théorie de l'information. Dans ce contexte, la recherche de codes optimaux prend alors tout son sens puisqu'il s'agit de rechercher le code ayant la plus grande capacité de correction d'erreur possible pour une longueur de code et une dimension fixée.

La classification des codes linéaires *ternaires optimaux* de taux $\frac{\mathbf{1}}{\mathbf{2}}$ a été faite jusqu'à la longueur 12 du code par T.A**.** Gulliver et N. Senkevitch [11], de même celle des tous les codes *linéaires optimaux* de paramètres $[n, \frac{n}{2}]$ sur $GF(5)$ et $GF(7)$ a été faite respectivement jusqu'à la longueur 12 et 8 par T.A. Gulliver, P.R.J. Ostergard et N. Senkevitch [12].

- Peut t-on caractériser le polynôme générateur d'un code cyclique iso-dual? cette question reste comme un problème ouvert défiant.

Dans ce travail nous accentuons notre étude sur les codes cycliques sur un corps fini F_p, pour $p = 3, 5$; comme étant des idéaux principaux de l'anneau $F_p[X]/(X^n - 1)$.

- En considérant les codes cycliques de paramètres $[n, \frac{n}{2}]$, pour n pair, non multiple de 3 et de 5 respectivement sur $GF(3)$ et sur $GF(5)$, nous avons construit **sept classes** de codes cycliques iso-duaux de paramètres $[n, \frac{n}{2}]_3$ et **trois classes** de codes cycliques iso-duaux de paramètres $[n, \frac{n}{2}]_5$, et on a contribué à de nouveaux résultats sur l'**optimisation** de la distance minimum d'un code cyclique et sur la **caractérisation** du polynôme générateur d'un code cyclique **iso-dual**.

• Soit $X^n - 1 = (X^m - 1)(X^m + 1)$, $n = 2m$, avec $X^m - 1 = (X - 1)u(X)v(X)$.

– Si $u^* = u$, $v^* = v$ ou $u^* = \varepsilon v$, $v^* = \eta u$ ou $u^*(x) = u(x)$, $v^*(x) = \eta v(-x)$ ou $u^*(x) = \epsilon u(-x)$, $v^*(x) = v(x)$ou $u^*(x) = u(-x)^*$, $v^*(x) = v(x)$ ou $u^*(x) = u(x), v^*(x) = v(-x)^*$ ou $u^*(x) = -v^*(x)$ avec ϵ, $\eta = \pm 1$. Alors le code cyclique de générateur $g(X) = (X-1)u(X)v(-X)$ est **iso-dual** en longueur $2m$ sur $GF(3)$.

– Si $u^* = u$, $v^* = v$ ou $u^* = \varepsilon v$, $v^* = \eta u$ ou $u^*(x) = v^*(-x)$, $v^*(x) = u^*(-x)$ avec ϵ, $\eta = \pm 1$. Alors le code cyclique de générateur $g(X) = (X-1)u(X)v(-X)$ est **iso-dual** en longueur $2m$ sur $GF(5)$.

Notre classification des codes cycliques sur $GF(3)$ et $GF(5)$, est faite respectivement jusqu'à la longueur 74 et 42 du code.

- Résultat [28] qui a fait l'objet d'un article paru en 2011 au journal "Int. J. Open Problems Comp. Maths" pour les codes cycliques iso-duaux sur $GF(5)$ et d'un autre article [29] sur les codes cycliques optimaux et iso-duaux sur $GF(3)$ en cours de parution au journal "Bulletin of Mathematical Sciences",.Springer.

– Les origines de la théorie des corps finis sont apparues au 17ème et 18ème siècles. Les premiers pas sont présentés par Fermat(1601-1665), Euler(1707-1783), Lagrange(1736-1813) et Legendre(1752-1833). Tous travaillaient sur un corps spécial F_p, où p est premier. Dans son papier "*Sur la théorie des nombres* " Evariste Galois marque le début de la théorie des corps finis.

- Que peut-on dire de la divisibilité des trinômes

$$x^{am} + x^{bs} + 1 \quad \text{pour } am > bs \geq 1 \qquad (1)$$

par un polynôme irréductible, de degré r, sur F_2?

- En considérant les polyômes du type (1), sur le corps F_2, on a contribué à un résultats [26] généralisant les travaux de **Golomb** et **Lee** [14]:

• S'il existe m, s des entiers positifs tels que le trinôme $x^{am} + x^{bs} + 1$ soit divisible

par un polynôme irréductible T de degré r sur F_2, alors a et b ne sont pas divisibles par $(2^r - 1)$. Résultat qui a fait l'objet d'un article paru en 2008 au journal "International Journal of Algebra", et qui a été pris comme référence dans l'article [17].

- De telles questions se posent constamment dans la théorie algébrique du codage.

Le présent travail est subdivisé en quatres chapitres:

- Dans le chapitre 1, on donne les propriétés de base des codes linéaires et cycliques sur un corps fini et on présente les principaux codes cycliques sur un tel corps.

- Dans les chapitres 2 et 3, la notion de polynôme réciproque et son utilisation pour la classification des codes cycliques iso-duaux sont présentées, ainsi que les contributions sur l'optimisation de la distance minimum d'un code cyclique, et les résultats originaux sur la caractérisation du polynôme générateur d'un code cyclique iso-dual sur $GF(p)_{p=3,\,5}$.

- Dans le chapitre 4, on évoque les principaux résultats de divisibilité des trinômes $x^m + x^s + 1$ par un polynôme irréductible sur $GF(2)$ et on présente la preuve de la $2^{ème}$ contribution indiquée ci-dessus.

• En annexe I, on donne des rappels sur la théorie des polynômes sur un corps fini, en évoquant la notion de polynôme irréductible sur un tel corps et ses principales propriétés [27].

• En annexe II, on évoque les raffinnements [17] apportés par R. Kim et W. Koepf à nos résultats sur la divisibilité des trinômes $x^{am} + x^{bs} + 1$ par un polynôme irréductible sur F_2 et sur l'extension du Critère de Welch.

CHAPITRE I **Codes Linéaires, Cycliques sur un Corps fini**

1.1 Introduction

Le codage correcteur d'erreurs, dont l'origine remonte à la fin des années 40, permet de transmettre de façon fiable de l'information, codée au moyen de mots d'une longueur donnée, sur des lignes plus ou moins bruitées. La transmission de l'information sur des lignes bruitées présentant un risque d'erreurs variable selon les cas, il s'agit de trouver un moyen de les corriger à la réception de l'information, au prix d'une certaine redondance, tout en minimisant dans chaque situation le temps d'occupation de la ligne. Les premiers travaux sur le sujet ont été menés par Golay, Hamming et Shannon.

Les codes correcteurs d'erreurs sont présents aujourd'hui dans tous les réseaux, à des niveaux techniques plus ou moins complexes. La généralisation de l'usage des satellites de télécommunication dans les réseaux mondiaux augmentant le niveau de bruit, le niveau technique de la correction d'erreurs dans ces réseaux a tendance à augmenter sensiblement. On trouve aussi de la correction d'erreurs à un niveau sophistiqué dans les sondes spatiales, les systèmes de guidage, les lecteurs de disques numériques et de disques compacts.

Voyons schématiquement le problème posé par la transmission sur un canal bruité.
Source $\longrightarrow (u_1, ..., u_k) \longrightarrow$ Encodeur $\longrightarrow (x_1, ..., x_n)$

Canal bruité $(y_1, ..., y_n) \longrightarrow$ Décodeur $\longrightarrow (v_1, ..., v_k)$

L'encodeur transforme le mot transmis en un mot de code. Nous appelons taux de transmission le rapport $= k/n$. La valeur r telle que $n = k + r$ est appelée redondance. Dans le canal bruité, certains symboles peuvent être modifiés. Pouvoir détecter une erreur, c'est pouvoir répondre à la question suivante : le vecteur reçu $(y_1, ..., y_n)$ est-il égal au vecteur $(x_1, ..., x_n)$?

Pouvoir corriger cette erreur, c'est pouvoir, après détection, obtenir par décodage:

$$(v_1, ..., v_k) = (u_1, ..., u_k)$$

1.2 Paramètres d'un code

Poids et distance de Hamming

Introduites par Hamming en 1950, ces notions sont fondamentales pour estimer l'efficacité d'un code.

Définition 1.2.1

Soit $x = (x_1, ..., x_n) \in F_q^n$. *Le poids de Hamming de* x, noté $wt(x)$ *est égal au nombre de coordonnées non nulles de* x.

$$wt(x) := card\{i : 1 \leq i \leq n \mid x_i \neq 0\}.$$

Soit x, $y \in F_q^n$. La distance de Hamming de x et y, notée $d_H(x, y)$ est égale au nombre d'indices i où les coordonnées de x et y différent.

$$d_H(x, y) = wt(x - y) := card\{i : 1 \leq i \leq n \mid x_i \neq y_i\}$$

Le support d'un élément $x \in F_q^n$ est l'ensemble des indices i tels que $x_i \neq 0$. Le poids de x est donc le cardinal de son support. La distance de Hamming, est une vraie distance au sens métrique du terme, c'est à dire qu'elle vérifie les propriétés d'une distance $d(x, y)$:

- $d(x, y) = 0 \Leftrightarrow x = y$
- $d(x, y) = d(y, x)$
- $d(x, z) \leq d(x, y) + d(y, z)$

Définition 1.2.2

Un code C *de longueur* n *est un sous-ensemble de* F_q^n. *La distance minimum de* C, *notée* $d(C)$, *est le minimum des distances entre deux éléments distincts de* C.

$$d(C) = \min_{x,y \in C,\, x \neq y} d_H(x, y).$$

1.3 Codes Linéaires

Pour les codes contenus dans F_q^n, nous allons nous concentrer sur les codes linéaires, c'est-à-dire ceux qui ont une structure d'espaces vectoriels. Les outils de l'algèbre linéaire facilitent dans ce cas les opérations de codage et de décodage.

Définition 1.3.1

Un code C de longueur n est dit linéaire si C est un F_q sous espace vectoriel de F_q^n. Dans ce cas, on note k sa dimension.

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

$$d(C) = wt(C) = min\{wt(x),\ x \in C \backslash \{0\}\}.$$

D'un point de vue algorithmique, le calcul de la distance d'un code quelconque nécessite $|C|^2$ opérations, tandis que pour un code linéaire il n'en faut que $|C|$ (environ).
Si C est un code linéaire, *longueur*, *dimension et distance* sont les paramètres fondamentaux de C et sont notés $[n, k, d]$.

Matrice génératrice, de contrôle de parité

Définitions 1.3.2(Code dual)

Soit C un code linéaire de longueur n et de dimension k. Une matrice génératrice de C est une matrice $k \times n$ dont les lignes forment une base de C. Le code dual du code C est l'orthogonal $C^\perp$ de C pour la forme usuelle $x \cdot y = \sum_{i=1}^{n} x_i y_i$.

$$C^\perp := \{x : x \in F_q^n \mid x \cdot y = 0 \text{ pour tout } y \in C\}.$$

Une matrice de contôle de parité de C est une matrice $(n-k) \times n$ génératrice de $C^{\perp}$. Un code est dit autodual s'il est égal à son dual.

Autrement dit, si C est un $[n, k]-$ code alors $C^{\perp}$ est un $[n, n-k]-$ code.

Proposition 1.3.3

Soit C un code linéaire, de longueur n et de dimension k, soit G une matrice génératrice de C et soit H une matrice de contrôle de parité de C. alors:

- $x \in C \Longleftrightarrow$*Il existe* $u \in F_q^k \mid x = uG$
- $x \in C \Leftrightarrow Hx^t = 0$
- *C contient un mot de poids au plus w, ssi w colonnes de H sont linéairement dépendantes.*

Remarque 1.3.4

Ainsi, un code C est de poids d si et seulement si, il existe d colonnes de sa matrice de contrôle de parité linéairement dépendantes, tandis que $d-1$ colonnes quelconques sont indépendantes. Cette remarque est à la base du processus de construction des codes de Hamming.

Proposition 1.3.5

Soit C un code linéaire de matrice génératrice G. Supposons que G soit de la forme dite canonique ou systématique $G = [I_k = I_k \mid A]$. Alors une matrice de contrôle de parité est $H = [-A^t \mid I_{n-k}]$.

Equivalence de codes

Soit S_n le groupe des permutations de l'ensemble $\{1, 2, ..., n\}$. Ce groupe opère sur F_q^n par permutation des coordonnées:

$$\sigma \in S_n, (x_1, ..., x_n)^{\sigma} := (x_{\sigma(1)}, ..., x_{\sigma(n)}).$$

Toutes les notions introduites sont invariantes par permutation: ainsi, $wt(\sigma(x)) = wt(x)$, $d_H(\sigma(x), \sigma(y)) = d_H(x, y)$, etc, ..., si un code C_1 est l'image d'un code C_2 par une permutation σ, bien que distincts, ces codes auront les mêmes propriétés relativement au problème de correction de l'information. Pour cette raison, on étudie en général les codes à permutation prés.

A toute permutation σ, on associe une matrice M_σ qui est la matrice de la transformation linéaire de F_q^n associée à σ. C'est une matrice $n \times n$, dont toutes les entrées sont nulles, sauf les $(\sigma(i), i)$ où elles sont égales à 1.

On a:

$$x^\sigma = xM_\sigma.$$

Si C est un code linéaire de matrice génératrice G, C^σ est encore un code linéaire, de matrice génératrice GM_σ. Celle-ci est obtenue à partir de G par permutation, suivant σ, des colonnes de G.

Proposition 1.3.6 (et définition.)

Soit C_1, C_2 deux codes linéaires de matrices génératrices respectivement G_1 et G_2. On dit que les codes C_1 et C_2 sont equivalents s'il existe une permutation σ telle que $C_2 = C_1^\sigma$. Cela est équivalent à demander qu'il existe une matrice de permutation M_σ et une matrice $k \times kP$ à coefficients dans F_q et inversible telles que

$$G_2 = PG_1M\sigma$$

Définition 1.3.7

L'ensemble des permutations $\sigma \in S_n$ telles que $\sigma(C) = C$ forme un groupe, appelé le groupe des permutations (ou le groupe des automorphismes) du code C, noté $Aut(C)$.

1.4 Codes Cycliques

Les codes cycliques forment une sous-classe des codes linéaires, et sont les plus utilisés en pratique. Ils conjuguent en effet de nombreux avantages: leur mise en oeuvre

(codage/décodage) est facile, ils offrent une gamme étendue de codes, avec de nombreux choix de paramètres $[n, k, d]$, et enfin permettent de corriger différents types d'erreurs, isolées ou par paquets.

On définit la fonction "décalage" sur F_q^n, qui est une permutation circulaire des coordonnées:

$$\begin{aligned} F_q^n &\rightarrow F_q^n \\ \sigma &: (c_0, c_1, ..., c_{n-1}) \rightarrow (c_{n-1}, c_0, c_1, ..., c_{n-2}) \end{aligned}$$

Définition 1.4.1

Soit C un code linéaire sur F_q^n. On dit que C est cyclique si $\sigma(C) = C$.

La transformation σ est d'ordre n, c'est à dire que n est le plus petit entier tel que $\sigma^n = id$.

Exemple 1.4.2

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

ii) Le code binaire $C = \{0000, 1001, 0110, 1111\}$ n'est pas cyclique. Il est cependant équivalent à un code cyclique (il faut échanger les troisième et quatrième coordonnées).

Lemme 1.4.3

Un code cyclique de F_q^n est un idéal de l'anneau $F_q[x]/(x^n - 1)$.

Preuve

Soit l'application

$$\begin{aligned} \varphi &: F_q^n \rightarrow F_q[x] \rightarrow F_q[x]/(x^n - 1) \\ &: c \rightarrow c(x) \rightarrow c(x) \ mod \ x^n - 1 \end{aligned}$$

qui associe à un mot

$$c = (c_0, c_1, ..., c_{n-1})$$

le polynôme

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x_{n-1}$$

φ est est un isomorphisme de F_q - espaces vectoriels.

Dans $F_q[x]/(x^n - 1)$, la multiplication par x correspond à la permutation circulaire des coefficients. Ainsi, pour tout $u \in F_q^n$, on a

$$\varphi(\sigma(u)) = x\varphi(u)$$

un code C est stable par σ si et seulement si

$$x\varphi(C) = \varphi(C)$$

Comme d'autre part un code linéaire est aussi un F_q - espace vectoriel, il est stable par σ si et seulement si son image par φ est un idéal de $F_q[x]/(x^n - 1)$.

Polynôme générateur

Définition 1.4.4

Le polynôme générateur $g(x)$ du code cyclique C est le polynôme normalisé de plus bas degré contenu dans C.

"Normalisé" signifie que le coefficient du monôme de plus haut degré vaut 1. Cette normalisation garantit l'unicité de $g(x)$.

Théorème 1.4.5

Soit C un idéal de $F_q[x]/(x^n - 1)$, Alors

i) Il existe un et un seul polynôme unitaire $g(x)$ de degré minimal dans C.

ii) C est un idéal principal généré par $g(x)$.

Preuve

i) Soit $g(x)$ le polynôme non nul de C de degré minimal r. Nous pouvons toujours transformer $g(x)$ en un polynôme unitaire en inversant le coefficient dominant. Supposons qu'il existe un deuxième polynôme unitaire $f(x)$ de degré minimal r. La différence $g(x) - f(x)$ appartient à C et a un degré inférieur à r. Ceci contredit le fait que r est minimal. Donc $g(x)$ est unique.

ii) Soit $c(x) \in C$. Par division euclidienne, nous pouvons écrire

$$c(x) = u(x)g(x) + r(x)$$

avec $deg\ r(x) < deg\ g(x)$.

Mais

$$r(x) = c(x) - u(x)g(x)) \in C$$

Ceci est une contradiction sauf si

$$r(x) = 0$$

c'est à dire que C s'écrit $C = \langle g(x) \rangle$ □

Exemple 1.4.6

Sur $F_2[x]$ on a la factorisation

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

Dans $F_2[x]/(x^3 - 1)$, soit C_1, C_2 les codes cycliques générés réspectivement par les polynômes $g_1(x) = 1 + x$, $g_2(x) = 1 + x + x^2$

alors on a:

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

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

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

Lemme 1.4.7

Les mots de C sont les multiples de $g(x)$ dans $F_q[x]/(x^n - 1)$. *Plus précisément, si $d^o g(x) = n - k$,*

$$\forall c(x) \in C,\ \exists!\ a(x) \in F_q[x],\ d^o a(x) < k : c(x) = a(x)g(x)$$

et donc $d^o g(x) + dim C = n$.

En effet, soit $c(x) \in C$. Calculons sa division euclidienne par $g(x)$:

$$c(x) = q(x)g(x) + r(x),\ d^o r(x) < d^o g(x)$$

On sait que tout multiple de $g(x)$ est dans C. Il vient que $r(x) = c(x) - q(x)g(x)$ est dans C, ce qui contredit la définition de $g(x)$ comme étant de degré minimal dans C, sauf si $r(x)$ est *nul*. Le second point du lemme vient en remarquant que $d^o q(x) < k$ car $d^o c(x) < n$. □

Théorème 1.4.8

Soit C un code cyclique de F_q^n, de polynôme générateur

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

alors une matrice génératrice de C est la matrice $(k) \times n$ donnée par:

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

Preuve

Notons au début que $g_0 \neq 0$: Sinon

$$(0,\ g_1,\ g_2,\ ...\ , g_{n-k-1}) \in C$$

ce qui implique que

$$(g_1,\ g_2,\ ...\ , g_{n-k-1},\ 0) \in C$$

C'est à dire que

$$g_1 + g_2 x + ... + g_{n-k-1} x^{n-k-1} \in C$$

Ce qui contredit la minimalité du degré $n-k$ du polynôme générateur. Maintenant, on voit que les k lignes de la matrice G sont linéairement indépendantes du fait de l'échelonnement de $g_o s$ avec 0_s au dessus. Ces k lignes représentent les polynômes $g(x)$, $xg(x)$, $x^2 g(x), ..., x^{k-1} g(x)$. Dans l'ordre de montrer que G est une matrice génératrice de C nous devons montrer que tout mot de code dans C peut s'écrire comme combinaison linéaire de $g(x)$, $xg(x)$, $x^2 g(x), ..., x^{k-1} g(x)$. Le lemme 1.4.7 montre que si $c(x)$ est un mot de code dans C, alors $c(x) = m(x)g(x)$ pour un certain polynôme $m(x)$ de degré inférieur à k dans $F_q[x]$. Ainsi,

$$\begin{aligned} c(x) &= m(x)g(x) \\ &= (m_0 + m_1 x + \cdots + m_{k-1}x^{k-1})g(x) \\ &= m_0 g(x) + m_1 x g(x) + \cdots + m_{k-1}x^{k-1}g(x) \end{aligned}$$

ce qui montre que tout mot de code $c(x)$ dans C peut s'écrire comme combinaison linéaire des mots représentés par les k lignes indépendantes de G. Nous concluons que G est une matrice génératrice de C et que la dimension de C est k. □

Exemple 1.4.9

Determinons tous les codes cycliques *ternaires* et leurs polynômes générateurs pour $n = 4$. La factorisation de $x^4 - 1$ sur $GF(3)$ prend la forme:

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

il y a donc $2^3 = 8$ polynômes générateurs de codes cycliques, à savoir:

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^2-1	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x-1)(x^2+1) = x^3 - x^2 + x - 1$	[-1 1 -1 1]
$(x+1)(x^2+1) = x^3 + x^2 + x + 1$	[1 1 1 1]
$x^4 - 1 = 0$	[0 0 0 0]

Lemme 1.4.10

Soit $g(x)$ le polynôme générateur du code cyclique C dans F_q^n, alors $g(x)$ *est un diviseur* de $x^n - 1$.

Ce résultat nous permettra de construire les codes cycliques à partir des diviseurs de $x^n - 1$. Pour la preuve, on procède de la même façon que le lemme précédent, on calcule la division euclidienne de $x^n - 1$ par $g(x)$ dans $F_q[x]$, et on conclut en passant modulo $x^n - 1$, ce qui donne

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

ainsi

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

donc

$$r(x) = 0 \qquad \square$$

Exemple 1.4.11

Considérons les codes binaires de longueur 7. Nous avons alors la factorisation en facteurs irréductibles suivante:

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

Comme il y a 3 facteurs irréductibles, il y a $2^3 = 8$ codes cycliques (y compris 0 et F_2^7).

Ainsi les 8 polynômes générateurs sont:

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

Remarquons que dans (1) le polynôme 1 est générateur de tout F_2^7. Dans (2) on trouve le code de parité et dans (7) le code de répétition. Comme mentionné avant, dans (8) nous voyons le code 0 de générateur x^7+1. Les polynômes dans (3) et (4) sont de degré 3 ainsi ils sont générateurs des codes [7, 4](appelés codes Hamming).

Dual d'un code cyclique

Théorème 1.4.12

Soit $C[n,k]$ *un code cyclique. Alors son code dual* $C^\perp$ *est cyclique et il est généré par le polynôme*

$$g^\perp(x) = x^k h(x^{-1})$$

où $h(x)$*, de degré* k*, est le polynôme de parité du code* C*.*

Preuve:

Rappelons que $h(x)$ vérifie la relation

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

Dans l'anneau quotient $F_q[x]/(x^n - 1)$, nous avons

$$g(x)h(x) = x^n - 1 = 0$$

Pour tout mot de code $c(x) = u(x)g(x)$, on a

$$c(x)h(x) = u(x)g(x)h(x) = 0$$

Nous obtenons donc un produit de convolution nul

$$\sum_{i=0}^{n-1} c_i h_{j-i} = 0, \qquad pour \qquad j = 0,\ 1, ...,\ n-1$$

Construisons la matrice

$$H = \begin{bmatrix} h_k\ ...\ h_1\ h_0\ 0 \\ \cdots \quad \cdots \\ 0\ h_k\ ...\ h_1\ h_0\ 0 \\ 0\ h_k\ ...\ h_1\ h_0\ 0 \end{bmatrix} = \begin{bmatrix} x^{n-k-1}h(x) \\ \cdots \\ xh(x) \\ h(x) \end{bmatrix}$$

Ce produit se traduit par $cH^t = 0$. Donc H est bien la matrice de parité du code C. En comparant avec la forme de G dans le théorème, nous concluons que $h(x)$ est le polynôme générateur du code dual si les symboles sont lus à l'envers. C'est à dire que $h(x)$ est le polynôme générateur d'un code équivalent à $C^\perp$ et que $C^\perp$ est un code cyclique. Sinon en gardant les symboles du code dans le même ordre mais en inversant les coefficients de $h(x)$, ainsi le code dual $C^\perp$ est généré par le polynôme $x^k h(x^{-1})$. □

Exemple 1.4.13

Les codes [7, 3] dans (5) et (6) (exemple 1.4.11) sont les *duaux* des codes de Hamming.

1.5 Principaux Codes Cycliques

Trois exemples historiques

1.5.1 Le test de parité: un exemple de code détecteur.

Chaque mot de code a un nombre **pair** de bits "1" et il y a un seul bit de redondance:

$$x_n = \sum_{i=0}^{n-1} x_i \bmod 2.$$

Ce code détecte un nombre impair d'erreurs. Ainsi pour $n = 6$:

$$101011 \longrightarrow \begin{cases} 100011 \\ 110011 \end{cases} \quad \begin{matrix} \text{l'erreur est détectée} \\ \text{les erreurs ne sont pas détectées} \end{matrix}$$

Ce code n'est pas correcteur car il ne permet pas de localiser les erreurs.

1.5.2 Le code de répétition

Dans l'encodage, chaque bit du mot-source est répété trois fois (ce qui triple la longueur; donc le taux de transmission est de 1/3). Ce code peut corriger une erreur par décodage majoritaire: chaque groupe de trois bits consécutifs du mot de code est décodé en un 0 (resp. un 1) s'il contient une majorité de 0 (resp. de 1).

1.5.3 Le premier code du mathématicien R.W. Hamming

Ce code, à l'origine "un bricolage", est basé sur le test de parité : Longueur: $n = (t+1)^2$, Information: $k = t^2$, Redondance: $r = 2t + 1$.

Pour voir son fonctionnement regardons un exemple. Ainsi pour $t = 2$, et donc $n = 9$, $k = 4$, $r = 5$. Il s'agit d'un code binaire de longueur 9, corrigeant 1 erreur et en détectant 3.

$$1101 \longrightarrow \overset{\text{ENCODAGE}}{\left\{ \begin{array}{c} 110 \\ 011 \\ 101 \end{array} \right\}} \longrightarrow 110011101$$

(chaque ligne et chaque colonne ont alors un nombre pair de "1")

Le taux de transmission est passé de 1/3, qui était le taux de transmission du code de répétition 1-correcteur, à 4/9. Le deuxième code de Hamming, appelé code de Hamming, aura un taux de 4/7, le meilleur possible pour un code 1-correcteur transmettant des blocs de 4 bits.

CHAPITRE II Codes Cycliques Optimaux, iso-duaux de Rendement $\frac{1}{2}$ sur $\mathbf{F_3}$

2.1 Introduction

La théorie du codage vise à construire des codes correcteurs performants, opérant au plus proche des limites théoriques établies par la théorie de l'information. Dans ce contexte, la recherche de codes optimaux prend alors tout son sens puisqu'il s'agit de rechercher le code ayant la plus grande capacité de correction d'erreur possible pour une longueur de code et une dimension fixée.

2.2 Codes Cycliques Optimaux sur GF(3)

Nous adaptons les notations et définitions indiquées dans [21, 23]. Soit le corps fini de Galois à 3 éléments noté $F_3 = \{0, 1, 2\}$. Un code $C[n, k]$ linéaire ternaire est un sous espace vectoriel de dimension k de F_3^n. Le taux d'un code linéaire $C[n, k]$ est défini par k/n. Deux codes ternaires C et C' sont équivalents si l'un est obtenu à partir de l'autre par une permutation des coordonnées. Soit $g(x)$ le polynôme générateur du code cyclique C, alors son code dual(cyclique) $C^{\perp}$ admet pour polynôme générateur le polynôme réciproque de:

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

où le polynôme réciproque $f^*(x)$ d'un polynôme $f(x)$, de degré r sur F_3, est défini par:

$$f^*(x) = x^r f(\frac{1}{x})$$

Un code C est dit iso-dual si C et $C^{\perp}$ sont équivalents. Les éléments de C sont appelés des mots de code et le poids $wt(x)$ d'un mot de code x est le nombre de positions non nuls dans x. La distance $d(x, y)$ de Hamming entre deux mots de codes est définie par : $d(x, y) = wt(x - y)$. La distance minimale d'un code linéaire C est :

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

Un code linéaire $C[n, k, d]$, sur un corps fini F , est un code $C[n, k]$ de distance minimale d. Pour un code linéaire, la distance minimale est égale au plus petit des poids de tous ses mots de codes non nuls.

Le problème central dans la théorie des codes est d'optimiser un des paramètres n, k et d pour des valeurs données des deux autres, q étant fixé. Une des deux versions 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.

La recherche des codes ternaires optimaux a été initié par Hill et Newton [16]. Ils ont trouvé les valeurs de $n_3(k, d)$ pour $k \leq 4$ pour tout d, et les valeurs de $n_3(5, d)$ pour toutes mais 30 valeurs de d. L'état de l'art et tables pour $n_3(6, d)$ et $d_3(n, 6)$ est dans [15]. Maruta [25] a prouvé l'inexistence de certains codes de dimension 6 sur F_3 et a présenté une nouvelle table pour $n_3(6, d)$ à l'adresse suivante : http://www.geocities.com/mars39.geo/griesmer.html. Grassl [8] maintient à jour une table des bornes supérieures et inférieures de $d_3(n, k)$ pour $n \leq 243$. Des bornes pour des valeurs numériques de $d_3(n, 7)$ ont été améliorées ou établies à travers la construction des codes quasi-cycliques par Gulliver et Ostergard [13].

2.2.1 Codes Cycliques $\mathbf{C[26, 13]_3}$:

Notre recherche est axée sur l'optimisation de la distance minimale des codes cycliques ternaires $C[n, \frac{n}{2}]$, où n est pair non multiple de 3, en particulier le code $[26, 13]$. Pour les codes *linéaires ternaires* $C[n, \frac{n}{2}]_3$, les bornes inférieures et supérieures de d_3 pour $2 \leq n \leq 24$ sont confondues. Pour $n \geq 26$ (voir [8]) les bornes supérieures ne sont pas toujours atteintes. On donne ici la table des bornes de d_3 pour $26 \leq n \leq 74$.

n	**26**	28	32	34	38	40	44	**46**	50
d_3	**8-9**	9-10	10-11	11-12	11-13	12-14	13-15	**14-15**	14-17

n	52	56	58	62	64	**68**	70	**74**
d_3	15-18	16-18	17-19	17-20	18-21	**16-22**	17-23	**18-24**

L'utilisation de L'algorithme de Chen présenté dans l'article [34]: J. F. Voloch, "Computing the minimal distance of cyclic codes" Comp and Applied Mathematics, Vol 24, pp. 393-398, 2005, nous a permis d'obtenir tous les résultats sur les codes cycliques $C[26,13]_3$. En utilisant Mathematica 5.2, la factorisation du polynôme:

$$\begin{aligned} x^{26}-1 = \quad & (1+x)(2+x)(1+2x+x^3)(2+2x+x^3)(2+x^2+x^3)(2+x+x^2+x^3) \\ & (1+2x+x^2+x^3)(1+2x^2+x^3)(1+x+2x^2+x^3)(2+2x+2x^2+x^3) \end{aligned}$$

en facteurs irréductibles sur le corps F_3 donne *huit* polynomes de *degré* $= 3$ et *deux* polynômes de *degré* $= 1$. Ainsi pour avoir un polynôme générateur $g(x)$ de degré 13, il faut choisir 4 polynômes parmis les 8 et en choisir 1 de degré 1, ce qui donne $C_8^4 \times C_2^1 = 140$ choix possibles. Toutes les combinaisons possibles ont été faites, ce qui a donné les poids des mots de code du $C[26,13]_3$ pour chaque polynôme $g(x)$ choisi. On enregistre dans la table 1 les résultats de calcul du poids des mots de code pour certains polynômes générateurs.

Table 1

g(x)	mot de code (a)	$\begin{smallmatrix}u^*(x)= \\ v^*(x)=\end{smallmatrix}$	$[\frac{x^{26}-1}{g(x)}]^* =$	wt(a)
10000000000001	10000000000001000000000000	$\begin{smallmatrix}u^*(x)=v(x) \\ v^*(x)=u(x)\end{smallmatrix}$	$g(-x)$	2
22121212121211	21000000000002100000000000	$\begin{smallmatrix}u^*(x)=v(x) \\ v^*(x)=u(x)\end{smallmatrix}$	$-g(-x)$	4
11220102101001	10100000100001010000010000	$\begin{smallmatrix}u^*(x)=u(x) \\ v^*(x)=-v(-x)\end{smallmatrix}$	$[-g(-x)]^*$	6
20020212210221	22010000000002201000000000	$\begin{smallmatrix}u^*(x)=u(x) \\ v^*(x)=-v(-x)\end{smallmatrix}$	$[-g(-x)]^*$	6
20021002012101	22000010000101002000120000	/	$no-isod$	**8**
20120100020121	12001010000002100202000000	/	$no-isod$	**8**
12112100012111	21000100000000200000000211	/	$no-isod$	7
22000102100211	22200000000102202020000000	/	$no-isod$	**8**
20210211021111	22200000000100100000201001	/	$no-isod$	**8**

g(x)	mot de code (a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{26}-1}{g(x)}]^* =$	wt(a)
10020222110211	12010000000002102000000000	$\begin{bmatrix} u^*(x)=-u(-x) \\ v^*(x)=v(x) \end{bmatrix}$	$[-g(-x)]^*$	6
12011200010121	10100000100001010000010000	$\begin{bmatrix} u^*(x)=u(-x)^* \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	6
20000000000001	10000000000002000000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$-g(-x)$	2
12222222222221	11000000000002200000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$g(-x)$	4
10111211001201	22000000100001100000020000	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	6
21120102202001	10100000100002020000020000	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=-v(-x) \end{bmatrix}$	$[-g(-x)]^*$	6
12121021020221	10200001000002000012000200	/	$no-isod$	7
20121020110101	10210000000002000202200000	/	$no-isod$	7
...	...	...	...	...

Remarque: Il y a exactement 54 codes optimaux parmi les 140 codes cycliques $[26, 13]_3$ existants.

Notons d_C la maximale distance minimum d'un code cyclique, nous résumons alors notre premier résultat par:

Proposition 1:

La distance minimale optimale des codes cycliques ternaires C[26,13]$_3$ est $d_C(26) = 8$.

2.2.2 Codes Cycliques $[34, 17]_3$:

Dans ce cas on a 4 choix seulement pour g(x) et la factorisation de $x^{34} - 1$ en facteurs irréductibles sur F_3 nous donne:

$$\begin{aligned} x^{34} - 1 &= (1+x)(2+x)(1+x+x^2+x^3+...+x^{15}+x^{16}) \\ &\quad (1+2x+x^2+2x^3+...+2x^{15}+x^{16}) \end{aligned}$$

Ainsi on aura les mots de codes et leurs poids respectifs

Table 2

g(x)	mot de code a	$\left[\begin{smallmatrix}u^*=\\v^*=\end{smallmatrix}\right.$	$[\frac{x^{34}-1}{g(x)}]^*=$	wt(a)
2212121212121211	2100000000000000021000000000000000	$\left[\begin{smallmatrix}u^*=u\\v^*=v\end{smallmatrix}\right.$	$-g(-x)$	4
1222222222222221	1100000000000000022000000000000000	$\left[\begin{smallmatrix}u^*=u\\v^*=v\end{smallmatrix}\right.$	$g(-x)$	4
2000000000000001	1000000000000000020000000000000000	$\left[\begin{smallmatrix}u^*=u\\v^*=v\end{smallmatrix}\right.$	$-g(-x)$	2
1000000000000001	1000000000000000010000000000000000	$\left[\begin{smallmatrix}u^*=u\\v^*=v\end{smallmatrix}\right.$	$g(-x)$	2

Remarque: Les 4 codes cycliques de paramètres $[34, 17]_3$ sont **iso-duaux** dont 2 sont optimaux.

Proposition 2:

La distance minimale optimale des codes cycliques ternaires [34,17]$_3$ est $d_C(34)$ =4.

2.2.3 Codes Cycliques $[38, 19]_3$:

De même ici on a 4 choix pour le polynôme générateur du code [38, 19]$_3$:

$$\begin{aligned} x^{38}-1 &= (1+x)(2+x)(1+x+x^2+x^3+...+x^{17}+x^{18}) \\ &\quad (1+2x+x^2+2x^3+...+2x^{17}+x^{18}) \end{aligned}$$

D'où la table des mots de codes et leurs poids correspondant

Table 3

g(x)	mot de code a	$\left[\begin{smallmatrix}u^*=\\v^*=\end{smallmatrix}\right.$	$[\frac{x^{38}-1}{g(x)}]^*=$	wt(a)
1222222222222222221	1100000000000000002200000000000000000	$\left[\begin{smallmatrix}u^*=u\\v^*=v\end{smallmatrix}\right.$	$g(-x)$	4
2000000000000000001	1000000000000000002000000000000000000	$\left[\begin{smallmatrix}u^*=u\\v^*=v\end{smallmatrix}\right.$	$-g(-x)$	2
1000000000000000001	1000000000000000001000000000000000000	$\left[\begin{smallmatrix}u^*=u\\v^*=v\end{smallmatrix}\right.$	$g(-x)$	2
22121212121212121211	2100000000000000000210000000000000000	$\left[\begin{smallmatrix}u^*=u\\v^*=v\end{smallmatrix}\right.$	$-g(-x)$	4

Remarque: Tous les codes cycliques ternaires de paramètres [38, 19]$_3$ sont **iso-duaux**.

Proposition 3 :

La distance minimale optimale des codes cycliques ternaires [38,19]$_3$ est $d_C(38)$ =4.

2.2.4 Codes Cycliques $\mathbf{C}[\mathbf{46}, \mathbf{23}]_3$:

Pour les codes cycliques $C[46, 23]$, la factorisation de $x^{46}-1$ nous donne 12 choix possibles pour le polynôme générateur de degré 23:

$$\begin{aligned} x^{46}-1 &= (1+x)(2+x)(1+2x+x^2+x^3+2x^4+x^6+x^8+x^{11}) \\ &\quad (2+2x+2x^2+x^3+x^4+2x^6+2x^8+x^{11}) \\ &\quad (2+x^3+x^5+2x^7+2x^8+x^9+x^{10}+x^{11}) \\ &\quad (1+x^3+x^5+2x^7+x^8+x^9+2x^{10}+x^{11}) \end{aligned}$$

Et par conséquent on note dans la table(4) tous les mots de code et leurs poids correspondants:

Table 4

g(x)	mot de code(a)	$\left[\begin{smallmatrix} u^*(x)= \\ v^*(x)= \end{smallmatrix}\right.$	$\left[\frac{x^{46}-1}{g(x)}\right]^*=$	wt(a)
22222211110022002200011	10202010000000000000000020002000002010000000020	$u^*(x)=-v^*(x)$	$-g(-x)$	9
20020211212010120020122 1	21110000011000000000000000200010002200002022 00	/	$no-isod$	13
10000000000000000000001	10000000000000000000000100000000000000000000000	$\left[\begin{smallmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{smallmatrix}\right.$	$g(-x)$	2
12222222222222222222221	11000000000000000000000220000000000000000000000	$\left[\begin{smallmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{smallmatrix}\right.$	$g(-x)$	4
21120100120201212210100 1	22121001000000000000002002000000210000010002 1	/	$no-isod$	13
22000011001100222211111 1	10102000100000000000000200010000000020101000	$u^*(x)=-v^*(x)$	$-g(-x)$	9
12121221210012001200002 1	10202010000000000000000020002000002010000000020	$u^*(x)=-v^*(x)$	$g(-x)$	9
11220100220201111220200 1	12222001000000000000002001000000220000020001 1	/	$no-isod$	13
22121212121212121212121 1	21000000000000000000002100000000000000000000	$\left[\begin{smallmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{smallmatrix}\right.$	$-g(-x)$	4
20000000000000000000001	10000000000000000000002000000000000000000000	$\left[\begin{smallmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{smallmatrix}\right.$	$-g(-x)$	2
10020221111020220010221 1	22120000021000000000000000200010002100002021 00	/	$no-isod$	13
12000021002100121221212 1	10102000100000000000000200010000000020101000	$u^*(x)=-v^*(x)$	$g(-x)$	9

Remarques:

- Pour les codes **iso-duaux** de paramètres $[\mathbf{46}, \mathbf{23}]_3$ on a:

soit

$$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix} \text{ ou } \begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$$

ou bien

$$u^*(x) = -v^*(x)$$

Et dans les **2 cas** on a $[\frac{x^{46}-1}{g(x)}]^* = \pm g(-x)$.

- Il y a exactement 8 codes $[46, 23]_3$ iso-duaux et 4 codes optimaux non iso-duaux.

Proposition 4 :

La distance minimale optimale des codes cycliques ternaires C[46, 23]$_3$ est $d_C(46)$ =13.

2.2.5 Codes Cycliques $[\mathbf{50}, \mathbf{25}]_3$:

Pour les codes cycliques $C[50, 25]$, la factorisation de $x^{50}-1$ nous donne 8 choix possibles pour le polynôme générateur de degré 25:

$$\begin{aligned} x^{50}-1 &= (1+x)(2+x)(1+x+x^2+x^3+x^4)(1+2x+x^2+2x^3+x^4) \\ &\quad (1+x^5+x^{10}+x^{15}+x^{20})(1+2x^5+x^{10}+2x^{15}+x^{20}) \end{aligned}$$

Et par conséquent on a la table qui nous donne tous les mots de code et leurs poids correspondants:

Table 5:

g(x)	mot de code a	$\begin{bmatrix} u^*= \\ v^*= \end{bmatrix}$	$[\frac{x^{50}-1}{g(x)}]^* =$	wt(a)
10000000000000000000000001	10.....010.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	2
12222222222222222222222221	110.....0220.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	**4**
20000000000000000000000001	10.....020.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	2
22121212121212121212121211	210.....0210.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	**4**

g(x)	mot de code a	$\begin{smallmatrix}[u^*= \\ [v^*=\end{smallmatrix}$	$[\frac{x^{50}-1}{g(x)}]^* =$	wt(a)
12222011110222201111022221	2000010...20000010...0	$\begin{smallmatrix}[u^*=u \\ [v^*=v\end{smallmatrix}$	$g(-x)$	**4**
10000200002000020000200001	1000010...02000020...0	$\begin{smallmatrix}[u^*=u \\ [v^*=v\end{smallmatrix}$	$g(-x)$	**4**
20000200001000020000100001	2000010...20000010...0	$\begin{smallmatrix}[u^*=u \\ [v^*=v\end{smallmatrix}$	$-g(-x)$	**4**
22121021210212102121021211	1000010...02000020...0	$\begin{smallmatrix}[u^*=u \\ [v^*=v\end{smallmatrix}$	$-g(-x)$	**4**

Remarque: Tous les codes cycliques $[50, 25]_3$ sont **iso-duaux** dont 6 sont optimaux**.**

Proposition 5 :

La distance minimale optimale des codes cycliques ternaires [50, 25]$_3$ est $d_C(50)$ =4.

2.2.6 Codes Cycliques $[58, 29]_3$:

Pour les codes cycliques ternaires $[58, 29]$, la factorisation de $x^{58} - 1$ nous donne 4 choix possibles pour le polynôme générateur de degré 29:

$$\begin{aligned} x^{58} - 1 &= (1+x)(2+x)(1+x+x^2+...+x^{27}+x^{28}) \\ &\quad (1+2x+x^2+2x^3+...+2x^{27}+x^{28}) \end{aligned}$$

Et par conséquent on a la table qui nous donne tous les mots de code et leurs poids correspondants:

Table 6

g(x)	mot de code a	$\begin{smallmatrix}[u^*= \\ [v^*=\end{smallmatrix}$	$[\frac{x^{58}-1}{g(x)}]^* =$	wt(a)
10.....01	10.....010.....0	$\begin{smallmatrix}[u^*=u \\ [v^*=v\end{smallmatrix}$	$g(-x)$	2
12.....21	110...0220...0	$\begin{smallmatrix}[u^*=u \\ [v^*=v\end{smallmatrix}$	$g(-x)$	**4**
20.....01	10.....020.....0	$\begin{smallmatrix}[u^*=u \\ [v^*=v\end{smallmatrix}$	$-g(-x)$	2
2212...1211	210...0210...0	$\begin{smallmatrix}[u^*=u \\ [v^*=v\end{smallmatrix}$	$-g(-x)$	**4**

Remarque: Les codes cycliques de paramètres $[58, 29]_3$ sont **tous** iso-duaux.

Proposition 6 :

La distance minimale optimale des codes cycliques ternaires [58, 29]$_3$ est $d_C(58)$ =4.

2.2.7 Codes Cycliques $[\mathbf{62}, \mathbf{31}]_3$:

De même la factorisation du binôme $x^{62}-1$ nous donne 4 choix du polynôme générateur du code ce qui nous permet de voir exhaustivement tous les poids des mots du code.

$$\begin{aligned} x^{62}-1 &= (1+x)(2+x)(1+x+x^2+\ ...\ +x^{29}+x^{30}) \\ &\quad (1+2x+x^2+\ ...\ +2x^{29}+x^{30}) \end{aligned}$$

Par conséquent, on résume les paramètres du code dans la table qui suit:

Table 7

g(x)	mot de code a	$\begin{bmatrix} u^*= \\ v^*= \end{bmatrix}$	$[\frac{x^{62}-1}{g(x)}]^* =$	wt(a)
10.....01	10.....010.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	2
12.....21	110...0220...0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	**4**
20.....01	10.....020.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	2
2212...1211	210...0210...0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	**4**

Remarque: Tous les codes cycliques $[\mathbf{62}, \mathbf{31}]_3$ sont **iso-duaux**.

Proposition 7:

La distance minimale optimale des codes cycliques ternaires [62, 31]$_3$ est $d_C(62)$ =4.

2.2.8 Codes Cycliques C$[\mathbf{68}, \mathbf{34}]_3$:

De même la factorisation du binôme $x^{68}-1$ nous donne 12 possibilités pour le choix du polynôme générateur du code ce qui nous permet de voir exaustivement tous les poids

des mots du code.

$$\begin{aligned} x^{68}-1 &= (1+x)(2+x)(1+x^2)(1+2x+2x^4+2x^5+2x^6+2x^{10} \\ &\quad +x^{11}+2x^{12}+x^{15}+x^{16})(1+x+x^2+x^3+x^4+x^5+x^6 \\ &\quad +x^7+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}) \\ &\quad (1+x+2x^4+x^5+2x^6+2x^{10}+2x^{11}+2x^{12}+2x^{15}+x^{16}) \\ &\quad (1+2x+x^2+2x^3+x^4+2x^5+x^6+2x^7+x^8+2x^9+x^{10} \\ &\quad +2x^{11}+x^{12}+2x^{13}+x^{14}+2x^{15}+x^{16}) \end{aligned}$$

Ainsi on résume les paramètres du code dans la table 8:

Table 8:

g(x)	mot de code(a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{68}-1}{g(x)}]^*=$	wt(a)
2010122100100102100202112002002012 1	220...0110...0220...0110...0	/	$non-isod$	8
2020102010201020102010201020102010 1	2010....00...02010....00.....0	/	$non-isod$	4
2220100200112202002201002001122020 1	210...0210...0210...0210...0	/	$non-isod$	8
2120100100122101002102002002112020 1	220...0110...0220...0110...0	/	$non-isod$	8
2000000000000000000000000000000000 1	100.....020.....0	/	$non-isod$	2
2010112200100201100101122001002011 1	210...0210...0210...0210...0	/	$non-isod$	8
1010212100201212002120101220210102 1	20.....010....020....010.....0	/	$non-isod$	4
1102022021101022200111102002222010 1	10....010....010.....010.....0	/	$non-isod$	4
1201012022101021200212102001212010 1	20.....010....020...010...0	/	$non-isod$	4
1020202020202020202020202020202020 1	1010.....02020.....0	/	$non-isod$	4
1010222200201111002220101120220201 1	10....010...010.....010....0	/	$non-isod$	4
1000000000000000000000000000000000 1	10.....010.....0	/	$non-isod$	2

Pour ces codes, la factorisation de $x^{68}-1=(x^{34}-1)(x^{34}+1)$ s'écrit:

$$x^{34}-1 = (1+x)(2+x)u(x)u(-x)$$
$$x^{34}+1 = (1+x^2)v(x)v(-x)$$

Si on prend tous les $g(x)$ qui divisent $(x^{68}-1)$, comme c'est indiqué dans table 3, on a **toujours**:

$$[\frac{x^{68}-1}{g(x)}]^* \neq \pm g(-x)$$

et

$$[\frac{x^{68}-1}{g(x)}]^* \neq [\pm g(-x)]^*$$

Ce qui montre qu'il **n'existe pas de codes cycliques iso-duaux** de paramètres $[68, 34]_3$.

Remarque: Il y a exactement 4 codes cycliques optimaux.

Proposition 8:

La distance minimale optimale des codes cycliques ternaires C[68, 34]$_3$ est $d_C(68)$ =8.

2.2.9 Codes Cycliques $[70, 35]_3$:

La factorisation de $x^{70}-1$ nous donne 48 choix possibles pour $g(x)$ de degré 35.

$$\begin{aligned} x^{70}-1 = {} & (1+x)(2+x)(1+x+x^2+x^3+x^4)(1+2x+x^2+2x^3+x^4) \\ & (1+x+x^2+x^3+x^4+x^5+x^6)(1+2x+x^2+2x^3+x^4+2x^5+x^6) \\ & (1+2x+2x^2+x^3+2x^4+x^5+x^7+2x^8+x^{10}+x^{12}) \\ & (1+x+2x^2+2x^3+2x^4+2x^5+2x^7+2x^8+x^{10}+x^{12}) \\ & (1+x^2+2x^4+2x^5+2x^7+2x^8+2x^9+2x^{10}+x^{11}+x^{12}) \\ & (1+x^2+2x^4+x^5+x^7+2x^8+x^9+2x^{10}+2x^{11}+x^{12}) \end{aligned}$$

Pour ces codes on a 3 cas:

soit

$$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix} \quad \text{ou} \quad \begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^*,\ v\ pair \end{bmatrix} \quad \text{avec} \quad [\frac{x^{70}-1}{g(x)}]^* = \pm g(-x)$$

soit

$$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix} \quad \text{avec} \quad [\frac{x^{70}-1}{g(x)}]^* = [-g(-x)]^*$$

Les 2 premiers cas sont vérifiés par les codes de distance minimum $d_C = 2, 4, 8$. Le 3ème cas est vérifié par les codes ayant $d_C = 14$. On note que 50% des codes ayant $d_C = 10$ vérifient les 1er et 2ème cas et que les $\frac{1}{3}$ ayant $d_C = 12$ vérifient le 3ème cas. Dans la dernière colonne de la table 9 suivante, on note les poids minimus des mots correspondants aux générateurs des codes cycliques, d'où les paramètres caractérisant les codes cycliques $[70,35]_3$.

g(x)	mot de code a	$\begin{matrix}u^*(x)=\\v^*(x)=\end{matrix}$	$[\frac{x^{70}-1}{g(x)}]^*=$	w
10211101000002021201210220211000 1101	11110...020...020...010..02220...010..010..020..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)^*\end{matrix}$	$g(-x)$	12
12222011101000202210012222002021 0211	1110...020...010...010...02220...010..020..020..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)\end{matrix}$	$[-g(-x)]^*$	12
12222222222222222222222222222222221	110.....0220.....0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(x)\end{matrix}$	$g(-x)$	4
11201011002221010220101222001101021 1	220...010.....010.....0220.....010...010...0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(x)\end{matrix}$	$g(-x)$	8
11201202002222100122020001011102222 1	1110...020...020..010...02220..010..010..020...0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)\end{matrix}$	$[-g(-x)]^*$	12
10110001120220121021202000001011120 1	1110...020..010...010..02220...010..020..020..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(x)^*\end{matrix}$	$g(-x)$	12
11112112101212012010020121001212001 1	10..010..010..010..010..010..010..010..010..010..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)^*\end{matrix}$	$g(-x)$	10
10000102022020121122011111022222222 1	10..010..010..010..010..010..010..010..010..010..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)\end{matrix}$	$[-g(-x)]^*$	10
10000002000000200000020000002000000 1	10.....01...020...020.....0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(x)\end{matrix}$	$g(-x)$	4
12222011110222201111022220111102222 1	2000010.....02000010.....0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(x)\end{matrix}$	$g(-x)$	4
12222222201111102211210202202010000 1	10..010..010..010..010..010..010..010..010..010..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)\end{matrix}$	$[-g(-x)]^*$	10
11002121001210200102102121012112111 1	10..010..010..010..010..010..010..010..010..010..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)^*\end{matrix}$	$g(-x)$	10
11112002120210101012201012112102001 1	2020..010..010..0100010002000102000 20..010..020..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)^*\end{matrix}$	$g(-x)$	12
10000000020000010022010120021012222 1	10100010100010...0100010..011010...01010100010..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)\end{matrix}$	$[-g(-x)]^*$	14
10000200002000020000200002000020000 1	1000010.....02000020.....0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(x)\end{matrix}$	$g(-x)$	4
12222220111111022222201111110222222 1	20.....010.....020.....010.....0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(x)\end{matrix}$	$g(-x)$	4
12222101200210102200100000200000000 1	101010..010110..0100010..010001010001010..0100	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)\end{matrix}$	$[-g(-x)]^*$	14
11002012112101022101010120212002111 1	101020....020.....01010..02010.....01020002020..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)^*\end{matrix}$	$g(-x)$	12
12122210222220121010121221011222002 1	210..020000200010000021 0.....020000200010..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)^*\end{matrix}$	$g(-x)$	10
11212120110000200200120002100020000 1	210..020000200010000021 0...020000200010..0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)\end{matrix}$	$[-g(-x)]^*$	10
11212011002220210110120222001102121 1	120...010000010.....0210.....020000020...0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(x)\end{matrix}$	$g(-x)$	8
10000000000000000000000000000000001	10.....010.....0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(x)\end{matrix}$	$g(-x)$	2
10000200012000210020020000110212121 1	210...020001000010...0210...020001000010...0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)\end{matrix}$	$[-g(-x)]^*$	10
12002221101221210101210222220122212 1	210...020001000010...0210...020001000010...0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)^*\end{matrix}$	$g(-x)$	10
22221220121210222020222211012212001 1	110...0100002000100000220...020000100020...0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)^*\end{matrix}$	$-g(-x)$	10
20000200011000110010020000210222222 1	220000010002000010...0110000020001000020...0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(-x)\end{matrix}$	$[-g(-x)]^*$	10
20000000000000000000000000000000001	10.....020.....0	$\begin{matrix}u^*(x)=u(x)\\v^*(x)=v(x)\end{matrix}$	$-g(-x)$	2

21111110210000100200220002200010000 1	110...010000200010...0220...020000100020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	10
22001211202211110101110212120112111 1	220000010002000010...0110000020001000020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	10
21211002220220202022102022211102002 1	2020..010...010..0100010002000102000 20..010..020..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	12
22121101100220201200200000100000000 1	101010...010120..010..010..010..01010..01010..0010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	14
22121210212121021212102121210212121 1	100000010.....0200000020.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	4
20000200001000020000100002000010000 1	2000010.....02000010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	4
20000000020000010012010110022022121 1	10100010100010..0100010...021010.....01010100010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	14
21001022211101021101010110111002212 1	101020.....020...01010...02010...01020002020.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	12
21211122202222011020020111002222002 1	10...020...010...020...010...020...010...020...010...020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	10
22121212102121201221110202101020000 1	10...020...010...020...010...020...010...020...010...020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	10
22121021210212102121021210212102121 1	1000010.....02000020.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	4
20000002000000100000020000001000000 1	20.....010.....020.....010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	4
20000102021010222112012121021212121 1	10...020...010...020...010...020...010...020...010...020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	10
21001111002220100102201111011122212 1	10...020...010...020...010...020...010...020...010...020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	10
21111021001210110120220212002102222 1	220.....010000010...0220...010000010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	8
20112101000002022201110210112000210 1	2120.....010...020...010...02120...010...020...010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	12
21102202001212200112020001012102121 1	2120.....010...020...010...02120...010...020...010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	12
21102021001211010210202212002101022 1	120...010.....010...0210...020.....020....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	8
22121212121212121212121212121212121 1	210.....0210.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	4
22121021202000101220011212001011022 1	2120.....010...020...010...02120...010...020...010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	12
20210001220210222011010000020212201 1	2120.....010...020...010...02120...010...020...010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	12

Remarque: Les 48 codes cycliques de paramètres $[70, 35]_3$ sont **tous iso-duaux** dont exactement 4 sont **optimaux**.

Proposition 9:

La distance minimum optimale des codes cycliques ternaires C[70, 35]$_3$ est $d_C(70)$ *=14.*

2.2.10 Codes Cycliques C$[74, 37]_3$:

La recherche de la distance minimale pour ces codes a demandé beaucoup de temps, en

effet, pour certains polyômes générateurs, l'exécution du programme de calcul de cette distance a demande plus 12 heures de travail sur le PC(512 G).

La factorisation de $x^{74}-1$ nous donne aussi 12 choix possibles pour $g(x)$ de degré 37.

$$\begin{aligned} x^{74}-1 &= (1+x)(2+x)(1+2x^2+2x^4+x^5+2x^7+2x^{11}+x^{13}+2x^{14}+2x^{16}+x^{18}) \\ &\quad (1+2x^2+2x^4+2x^5+x^7+x^{11}+2x^{13}+2x^{14}+2x^{16}+x^{18}) \\ &\quad (1+x+2x^2+2x^3+x^4+2x^5+2x^6+2x^8+2x^9+2x^{10}+2x^{12}+2x^{13}+ \\ &\quad x^{14}+2x^{15}+2x^{16}+x^{17}+x^{18})(1+2x+2x^2+x^3+x^4+x^5+2x^6+2x^8+ \\ &\quad x^9+2x^{10}+2x^{12}+x^{13}+x^{14}+x^{15}+2x^{16}+2x^{17}+x^{18}) \end{aligned}$$

Par conséquent on a tous les mots de codes et leurs poids dans la table 10.

Table 10:

n°	g(x)	mot de code(a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{74}-1}{g(x)}]^*=$	wt(a)
1	1111222211222200222222002222211222221111	10102000200010...010.....010.....01010...020...020	/	$no-isod$	11
2	12222100020220200222200202202000122221	210..020..02001020..010..010..02010020..0200012	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	14
3	10000000000000000000000000000000000001	10.....010.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	2
4	12222222222222222222222222222222222221	110.....0220.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	4
5	10000100012002100111100120021000100001	110020020....0200200110020....0110....110...0200	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	14
6	11002200222200110000001100222200220011	2010100020.....010....02000101020...010....010...0	/	$no-isod$	11
7	21211212211212001212120012122112122121	10102000200010....010...010....01010....020....020	/	$no-isod$	11
8	20000100011002200121200110022000200001	120020010...0200100120020....0210....0210...0100	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	14
9	22121212121212121212121212121212121211	210.....0210.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	4
10	20000000000000000000000000000000000001	10.....020.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	2
11	22121100020210100212100202101000221211	1100020..02002010..010..020..02010010..0100022	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	14
12	21001200121200210000002100121200120021	2010100020.....010...02000101020....010....010...0	/	$no-isod$	11

Remarque: il y a exactement 8 codes $[74,37]_3$ *iso-duaux* dont 4 sont *optimaux*.

Proposition 10 :

La distance minimale optimale des codes cycliques ternaires C[74, 37]$_3$ est $d_C(74)$ =14.

Note: La distance minimale de ces codes cycliques ternaires depasse la borne BCH [10].

2.3 Table des valeurs de $d_I(n)$ et $d_C(n)$:

Notons $d_I(n)$ la maximale distance minimum d'un code cyclique *iso-dual*. Nous résumons alors les différentes valeurs prises par $d_I(n)$ et $d_C(n)$ des codes de paramètres $[n, \frac{n}{2}]_3$ selon la longueur du code.

n	26	34	38	46	50	58	62	68	70	74
$d_I(n)$	6	4	4	9	4	4	4	∄	14	14
$d_C(n)$	8	4	4	13	4	4	4	8	14	14

Remarque: On constate que pour $n = 34, 38, 50, 58, 62, 70, 74$; le code iso-dual est autant performant(au sens de la distance minimum) que le code cyclique.

2.4 Nouvelles Classes de Codes Cycliques Iso-duaux sur GF(3)

2.4.1 Codes Cycliques Iso-Duaux sur GF(3)

Une généralisation pour les codes cycliques $C[n, \frac{n}{2}]$ sur le corps fini F_3, dans le cas où n est pair non multiple de 3 (le cardinal du corps), sur le fait que ces derniers sont iso-duaux. L'utilisation de la notion de polynôme réciproque nous a permis de trouver une propriété concernant l'iso-dualité de ces codes cycliques pour $n = 26, 34, \ldots, 74$. Cette iso-dualité est réalisée par le fait que le polynôme réciproque du complément du générateur $g(X)$ d'un tel code cyclique vérifie la propriété suivante:

Sachant que pour $n = 2m$, on a:

$$X^n - 1 = (X^m - 1)(X^m + 1)$$

on pose

$$X^m - 1 = (X-1)u(X)v(X) \quad \text{et} \quad X^m + 1 = (X+1)u(-X)v(-X)$$

avec la condition que les polynômes u et v soient auto-réciproques c.a.d:

$$u^* = u \qquad \text{et} \qquad v^* = v$$

soit $g(X) = (X-1)u(X)v(-X)$ alors:

$$\frac{X^n - 1}{g(X)} = (X+1)u(-X)v(X)$$

d'où

$$\begin{aligned} (\frac{X^n - 1}{g(X)})^* &= (X+1)u(-X)v(X) \\ &= -(-X-1)u(-X)v(X) \\ &= -g(-X) \end{aligned}$$

Ainsi le code cyclique de générateur le polynôme $g(X)$ est iso-dual en longueur $2m$. Nous résumons ce résultat par:

Proposition 2.4.1.1:
Soit $X^m - 1 = (X-1)u(X)v(X)$ avec m impair et $u^* = u$, $v^* = v$. Alors le code cyclique ternaire généré par le polynôme $g(X) = (X-1)u(X)v(-X)$ est iso-dual en longueur $2m$.

2.4.2 Nouvelles Classes de Codes Cycliques Iso-Duaux sur GF(3)

Nous donnons *sept constructions* de code cycliques iso-duaux sur le corps fini F_3. On suppose que $n = 2m$ avec m impair et n non multiple de 3. Dans ce cas la factorisation

$$x^m - 1 = (x-1)u(x)v(x)$$

donne, en changeant x par $-x$, la factorisation

$$x^m + 1 = (x+1)u(-x)v(-x).$$

On choisit

$$g(x) = (x-1)u(x)v(-x)$$

Nous considérons les sept cas suivants:

1. $u^*(x) = u(x)$, $v^*(x) = v(x)$
2. $u^*(x) = \epsilon v(x)$, $v^*(x) = \eta u(x)$
3. $u^*(x) = -v^*(x)$
4. $u^*(x) = u(x)$, $v^*(x) = v(-x)^*$
5. $u^*(x) = u(-x)^*$, $v^*(x) = v(x)$
6. $u^*(x) = u(x)$, $v^*(x) = \eta v(-x)$
7. $u^*(x) = \epsilon u(-x)$, $v^*(x) = v(x)$

avec ϵ, $\eta = \pm 1$.

Proposition 2.4.2.1 : *Prenant la notation précédente. Dans les sept cas, le code cyclique de générateur $g(x)$ est iso-dual sur F_3.*

Preuve: Dans chaque cas nous calculons le polynôme générateur du code dual. Premièrement on a:

$$(x^n - 1)/g(x) = (x+1)u(-x)v(x).$$

Prenant les réciproques des deux côtés, nous obtenons dans les cinq premiers cas $\pm g(-x)$, et dans les deux derniers cas $[-g(-x)]^*$. Le résultat s'ensuit. □

CHAPITRE III Codes Cycliques Optimaux, iso-duaux de Rendement $\frac{1}{2}$ sur $\mathbf{F_5}$

3.1 Introduction

Soit le corps fini de Galois à 5 éléments noté $F_5 = \{0, 1, 2, 3, 4\}$. Un code $C[n, k]_5$ linéaire est un sous espace vectoriel de dimension k de F_5^n. Le taux d'un code linéaire $C[n, k]$ est défini par k/n. Deux codes linéaires C et C' sont équivalents si l'un est obtenu à partir de l'autre par une permutation des coordonnées. Soit $g(x)$ le polynôme générateur du code cyclique C, alors son code dual(cyclique) $C^{\perp}$ admet pour polynôme générateur le polynôme réciproque de:

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

où le polynôme réciproque $f^*(x)$ d'un polynôme $f(x)$, de degré r sur F_5, est défini par:

$$f^*(x) = x^r f(\frac{1}{x})$$

Un code C est dit *iso-dual* si C et $C^{\perp}$ sont équivalents. Les éléments de C sont appelés des mots de code et le poids $wt(x)$ d'un mot de code x est le nombre de positions non nuls dans x. La distance $d(x, y)$ de Hamming entre deux mots de codes est définie par : $d(x, y) = wt(x - y)$. La distance minimale d'un code linéaire C est :

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

Un code linéaire $C[n, k, d]$, sur un corps fini F, est un code $C[n, k]$ de distance minimale d. Pour un code linéaire, la distance minimale est égale au plus petit des poids de tous ses mots de code non nuls.

Le problème central dans la théorie des codes est d'optimiser un des paramètres n, k et d pour des valeurs données des deux autres, q étant fixé. Une des deux versions 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.

Ces dernières années, de bons codes linéaires sur $GF(5)$ ont été construits. Dans [5] Daskalov et Gulliver construisent 44 bons codes et présentent une tabe sur les bornes des distances minimus pour $1 \leq k \leq 8$, $1 \leq n \leq 100$. 32 QC et QT codes sont contruits, sur $GF(5)$, dans [4]. Grassl et White présentent dans [9] 55 nouveaux codes. Certains bons codes linéaires incluant la notion de rendement élevé sont présentés dans [3]. Grassl [8] maintient à jour une table electronique(online) sur les bornes de la distance minimale $d_5(n, k)$ des codes linéaires. La classification de tous les codes linéaires optimaux $[n, n/2, d]$ sur F_5 et sur F_7 a été faite respectivement jusqu'à la longueur 12 et 8 [12].

3.2 Codes Cycliques Optimaux sur GF(5)

La table 1 représente les premiers résultats de calcul de la distance minimum optimale des codes cycliques $C[n, k, d]_5$ ayant un nombre restreints de polynômes générateurs pour $n = 2$, 4, 6, 14, 18, 34, 46, 54, 74, 86, 94, 98. (notons que pour $n \geq 6$, ces codes ont la même distance minimale optimale $d_c = 4$).

Table 1:

n	2	4	6	14	18	34	46	54	74	86	94	98
k	1	2	3	7	9	17	23	27	37	43	47	49
nbre de g(x)	2	6	4	4	8	4	4	16	4	4	4	8
d_c	2	3	4	4	4	4	4	4	4	4	4	4
nbre de codes optimaux	2	4	2	2	6	2	2	14	2	2	2	6

Notre recherche est axée sur l'optimisation de la distance minimum des codes cycliques $C[n, \frac{n}{2}]$, n pair non multiple de 5. Pour les **codes linéaires** $C[n, \frac{n}{2}]_5$, n pair, les bornes inférieures et supérieures de d_5 pour $2 \leq n \leq 16$ sont confondues. Pour $n \geq 18$ (voir [8]) les bornes supérieures ne sont pas toujours atteintes. On donne ici la table des bornes

de d_5 pour $18 \leq n \leq 54$.

n	18	**22**	24	**26**	28	32	34	36
d_5	7-8	**8-10**	9-10	**10-11**	11-12	11-13	11-14	12-15

n	**38**	**42**	44	46	48	52	54
d_5	**12-16**	**14-18**	13-19	14-20	15-20	15-21	16-22

L'utilisation de l'algorithme de Chen présenté dans l'article[34], nous a permis d'obtenir tous les résultats sur les codes cycliques de paramètres $[2m, m]_5$, pour $m = 11$, 13, 19 et 21.

3.2.1. Codes Cycliques $\mathbf{C[22, 11]_5}$

La factorisation du polynôme $X^{22} - 1$ en facteurs irréductibles sur le corps F_5 donne 4 polynômes de *degré* $= 5$ et *deux* polynômes de *degré* $= 1$. Ainsi pour avoir un polynôme générateur $g(X)$ de degré 11, il faut choisir 2 polynômes, de degré 5, parmis les 4 et en choisir 1 parmi les 2 de degré 1, ce qui nous donne $C_4^2 \times C_2^1 = 12$ choix possibles. Toutes les combinaisons ont été faites, ce qui donne, pour chaque polynôme $g(X)$ choisi, le poids minimum du mot de code $C[22, 11]_5$. Tous les résultats possibles sont enregistés dans la table 2.

$$\begin{aligned} x^{22} - 1 \;&=\; (1+x)(4+x)(1+3x+4x^2+4x^3+x^4+x^5)(4+x+x^2+4x^3+2x^4 \\ &\quad +x^5)(1+x+4x^2+4x^3+3x^4+x^5)(4+3x+x^2+4x^3+4x^4+x^5) \end{aligned}$$

Table 2:

n°	g(x)	mot de code (a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{22}-1}{g(x)}]^* =$	wt(a)
1	423233112341	3203100000000230040001	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$[-g(-x)]^*$	**8**
2	100000000001	10000000000100000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$g(-x)$	2
3	441111442211	2020100000004000400020	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$-g(-x)$	6

n°	g(x)	mot de code (a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{22}-1}{g(x)}]^* =$	wt(a)
4	443311444411	2010100000000010300020	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$-g(-x)$	6
5	122222222221	1100000000044000000000	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$g(-x)$	4
6	412344223231	2302010000000004100014	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$[-g(-x)]^*$	**8**
7	113314322221	3302010000000004400044	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$[-g(-x)]^*$	**8**
8	423232323231	4100000000041000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$-g(-x)$	4
9	144141143241	2020100000004000400020	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$g(-x)$	6
10	142341141441	2010100000000010300020	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$g(-x)$	6
11	400000000001	1000000000040000000000	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$-g(-x)$	2
12	122223413311	3302100000000330010004	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$[-g(-x)]^*$	**8**

Remarque: Les 12 codes cycliques $C[22,11]_5$ sont tous iso-duaux dont exactement 4 sont *optimaux*.

Nous résumons notre premier résultat par:

Proposition 1:

La distance minimale optimale des codes cycliques C[22,11]$_5$ est $d_C(22)$ *=8.*

3.2.2. Codes Cycliques $\mathbf{C[26,13]_5}$:

On a: $\binom{2}{1} \times \binom{6}{3} = 40$ choix possibles pour le polynôme générateur d'un code cyclique $C[26,13]_5$, ces codes ont une spécificité particulière du fait que tous les générateurs $g(X)$, de degré 13, nous donnent une *même distance minimale optimale* à l'excéption des générateurs triviaux, à savoir $1+X^{13}$ et $4+X^{13}$, et les deux codes générés par les polynômes dont les coefficients sont : 12222222222221 et 42323232323231. Nous résumons les résultats de toutes les combinaisons possibles dans la table 3.

$$\begin{aligned} x^{26}-1 &= (1+x)(4+x)(1+x+4x^2+x^3+x^4)(1+2x+2x^3+x^4)(1+2x+x^2+2x^3 \\ &\quad +x^4)(1+3x+3x^3+x^4)(1+3x+x^2+3x^3+x^4)(1+4x+4x^2+4x^3+x^4) \end{aligned}$$

Table 3:

n°	g(x)	mot de code (a)	$\begin{bmatrix} u^*= \\ v^*= \end{bmatrix}$	$\left[\frac{x^{26}-1}{g(x)}\right]^*=$	wt(a)
1	11314011041311	120030010...040020034000	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	8
2	41202223330341	41200010...0143000400...0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	8
3	12121433412121	103040...010204000302000	/	$non\ isodual$	8
4	40133423122401	41200010...014300040...00	/	$non\ isodual$	8
5	12210100101221	221000010.....0400004330	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	8
6	40010423104001	221000010.....0400004330	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	8
7	13433300333431	130400010..0130400010..0	/	$non\ isodual$	8
8	44014123414011	32040.....01032040.....010	/	$non\ iso-dual$	8
9	12222222222221	110.....0440.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	4
10	40000000000001	10.....040.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	2
11	12312144121321	2404000010....0100004042	/	$non\ isodual$	8
12	40431023042101	2202010.....03303040.....0	/	$non\ isodual$	8
13	13040011004031	22040.....01033010.....040	/	$non\ isodual$	8
14	44422314233111	430400010..0120100040..0	/	$non\ isodual$	8
15	13240244204231	122000010.....0100002210	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	8
16	44213032024311	2202010.....03303040.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	8
17	14011133111041	22040.....01033010.....040	/	$non\ isodual$	8
18	43132300232421	43040..010..012010..040..0	/	$non\ isodual$	8
19	14123344332141	130400010..0130400010..0	/	$non\ isodual$	8
20	43040041001021	32040.....01032040.....010	/	$non\ isodual$	8
21	13410111101431	310....0110...01300400400	/	$non\ isodual$	8
22	44033141422011	41200010...014300040....0	/	$non\ isodual$	8

n°	g(x)	mots de code (a)	$\begin{bmatrix} u^*= \\ v^*= \end{bmatrix}$	$[\frac{x^{26}-1}{g(x)}]^*=$	wt(a)
23	13014222241031	3202010.....03202010....0	/	$non\ isodual$	8
24	44402000030111	2340010.....0100432000	/	$non\ iso-dual$	8
25	14312022021341	3202010.....03202010.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	8
26	43340214301221	4230...010.....010....03240	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	8
27	14032111123041	44200010....044200010...0	/	$non\ isodual$	8
28	43110141404421	210.....410....04300100400	/	$non\ isodual$	8
29	10432433423401	44200010...044200010....0	/	$non\ isodual$	8
30	42424423113131	103040..0102040..03020..0	/	$non\ isodual$	8
31	10000000000001	10.....010.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	2
32	42323232323231	410.....0410.....0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	4
33	14103000030141	3310010.....0100133000	/	$non\ isodual$	8
34	43011232344021	2202010.....03303040.....0	/	$non\ isodual$	8
35	10010433401001	3240.....010....040....01320	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	8
36	42310100404231	3240....010.....0400001320	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	8
37	10134033043101	3202010.....03202010.....0	/	$non\ isodual$	8
38	42213114424331	21010....010...0400004043	/	$non\ isodual$	8
39	11303233230311	44200010....044200010...0	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	8
40	41211041044341	420020010..040030031000	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	8

Remarques:

- Il y a exactement 36 codes cycliques *optimaux* de paramètres $[26, 13]_5$.

- 40% des codes cycliques $C[26, 13]_5$ sont *iso-duaux*, en effet on a 12 *codes optimaux iso-duaux* ($d_C = 8$) et 4 codes iso-duaux dont 2 sont de générateurs les polynômes triviaux $1 + X^{13}$, $4 + X^{13}$ et de distance minimale $d_C = 2$, les 2 autres ont pour générateurs 12222222222221, 42323232323231 et de distance minimale $d_C = 4$.

Proposition 2:

La distance minimale optimale des codes cycliques C[26, 13]$_5$ est $d_C(26)$ =8.

3.2.3 Codes Cycliques $\mathbf{C[38,19]_5}$:

Pour les codes cycliques $C[38,19]_5$, la factorisation de $X^{38}-1$ en polynômes irréductibles sur F_5 nous donne aussi 12 choix possibles pour le polynôme générateur de degré 19, par conséquent on note dans la table 4, pour chaque générateur, le poids minimum du mot de code.

$$\begin{aligned} x^{38}-1 &= (1+x)(4+x)(4+4x+2x^2+4x^3+2x^4+2x^5+2x^6+ \\ &\quad 3x^7+x^9)(1+4x+3x^2+4x^3+3x^4+2x^5+3x^6+3x^7 \\ &\quad +x^9)(4+2x^2+3x^3+3x^4+3x^5+x^6+3x^7+x^8+x^9) \\ &\quad (1+3x^2+3x^3+2x^4+3x^5+4x^6+3x^7+4x^8+x^9) \end{aligned}$$

Table 4:

n°	g(x)	mot de code (a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{38}-1}{g(x)}]^* =$	wt(a)
1	44002233333311331111	40304010..000000..01000203020....0	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$-g(-x)$	8
2	12222222222222222221	110.....0440....0000000.....0	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$g(-x)$	4
3	43321324124303204001	120010..01010..03010..010101010..0	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$[-g(-x)]^*$	11
4	40010320213413243221	1030001010..01002100010101010..0	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$[-g(-x)]^*$	11
5	10000000000000000001	10.....010.....0	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$g(-x)$	2
6	44442244222222330011	2030200010.....010403040...0	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$-g(-x)$	8
7	14003223232341234141	40304010.....010.....0203020...0	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$g(-x)$	8
8	40000000000000000001	10.....040.....0	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$-g(-x)$	2
9	10010330312443342231	1030001010..01003100010101010..0	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$[-g(-x)]^*$	11
10	13224334421303301001	130010..01010003010..01010101000	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$[-g(-x)]^*$	11
11	42323232323232323231	410.....0410.....0	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$-g(-x)$	4
12	14143214323232230041	2030200010.....0104030400000	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$g(-x)$	8

Remarque: Tous les codes cycliques de paramètres $[38, 19]_5$ sont iso-duaux dont exactement 4 sont *optimaux.*

Proposition 3 :

La distance minimale optimale des codes cycliques C[38, 19]$_5$ *est* $d_C(38)$ *=11.*

3.2.4 Codes Cycliques $\mathbf{C[42, 21]_5}$:

La décomposition de $X^{42} - 1$ en facteurs irréductibles nous donne 80 possibilités pour le choix du polynôme générateur, de degré 21, du code. Ce qui nous permet de voir exhaustivement, pour chaque générateur, le poids minimum du mot de code $C[42, 21]_5$. Dans la table 5 on note seulement les paramètres des *codes cycliques optimaux.*

$$\begin{aligned} x^{42}-1 &= (1+x)(4+x)(1+x+x^2)(1+4x+x^2)(1+2x^2+2x^3+2x^4 \\ &\quad +x^6)(1+2x^2+3x^3+2x^4+x^6)(1+x+x^2+x^3+x^4+x^5 \\ &\quad +x^6)(1+x+3x^2+4x^3+3x^4+x^5+x^6)(1+4x+x^2+4x^3 \\ &\quad +x^4+4x^5+x^6)(1+4x+3x^2+x^3+3x^4+4x^5+x^6) \end{aligned}$$

Table 5: pour les codes iso-duaux on a toujours: ($u^* = u$ et $v^* = v$)

n°	g(x)	mot de code (a)	$[\frac{x^{42}-1}{g(x)}]^* =$	wt(a)
1	1343441034004301443431	4334000040...0100001221000010...040000	$non\ isodual$	12
2	1101434141441414341011	1301010.....0110.....0300001002020...0302	$non\ isodual$	12
3	4101131111144444244041	1204040.....0410...0200001003030.....0203	$non\ isodual$	12
4	4313144024001301142421	4231000040...0100004231000040...010000	$non\ isodual$	12
5	1434433001441003344341	33210030...0100000022340020...04000000	$g(-x)$	12
6	4233122324411323342231	4231000040...0100004231000040...010000	$-g(-x)$	12

n°	g(x)	mot de code (a)	$[\frac{x^{42}-1}{g(x)}]^* =$	wt(a)
7	1223423334114333243221	4334000040...0100001221000010...040000	$g(-x)$	12
8	4424132001144003241311	32240030...0100000032240030...01000000	$-g(-x)$	12
9	1301323321441233231031	33210030...0100000022340020...04000000	*non isodual*	12
10	1112441241001421442111	22000320000010..0100000230022020..020	*non isodual*	12
11	4142144211004431143141	32000330...040...010...02200032020....030	*non isodual*	12
12	4301222331144223334021	32240030...0100000032240030...01000000	*non isodual*	12

Remarque:

Il y a exactement 12 codes *optimaux* de paramètres $[42, 21]_5$ parmi les 80 codes cycliques existants.

Proposition 4:

La distance minimale optimale des codes cycliques C[42, 21]$_5$ est $d_C(42)$ =12.

3.2.5 Table des valeurs de $d_I(n)$ et $d_C(n)$:

Dans cette table on résume les différentes valeurs prises par $d_I(n)$ et $d_C(n)$ selon la longueur n du code.

n	22	26	38	42
$d_I(n)$	8	8	11	12
$d_C(n)$	8	8	11	12

Notons que pour $n = 22, 26, 38, 42$ les codes cycliques iso-duaux sont autant efficaces que les cycliques sur F_5.

3.3 Nouvelles Classes de Codes Cycliques Iso-duaux sur GF(5)

3.3.1 Codes Cycliques Iso-Duaux sur GF(5)

Une généralisation pour les codes cycliques $C[n, \frac{n}{2}]$ sur le corps fini F_5, dans le cas où n est pair non multiple de 5, sur le fait que ces derniers sont iso-duaux. L'utilisation de la

notion de polynôme réciproque nous a permis de trouver une propriété concernant l'iso-dualité de ces codes cycliques. Cette iso-dualité est réalisée par le fait que le polynôme générateur du code dual $C^{\perp}$, qui est le polynôme réciproque du complément du générateur $g(X)$ du code C, vérifie la propriété suivante:

Sachant que pour $n = 2m$ on a:

$$X^n - 1 = (X^m - 1)(X^m + 1)$$

On pose

$$X^m - 1 = (4 + X)u(X)v(X) \quad \text{et} \quad X^m + 1 = (1 + X)u(-X)v(-X)$$

Avec la condition que les polynômes u et v soient auto-réciproques c.a.d:

$$u^* = u \qquad \text{et} \qquad v^* = v$$

soit $g(X) = (1 + X)u(X)v(-X)$ alors:

$$\frac{X^n - 1}{g(X)} = (4 + X)u(-X)v(X)$$

d'où

$$\begin{aligned} [\frac{X^n - 1}{g(X)}]^* &= (1 + 4X)u(-X)v(X) \\ &= (1 - X)u(-X)v(X) \\ &= g(X)^{\perp} \\ &= g(-X) \end{aligned}$$

Ainsi le code cyclique de générateur le polynôme réciproque du complément de $g(X)$ est

iso-dual en longueur $2m$.

Les codes $C[26,13]_5$, $C[42,21]_5$ vérifient ce cas (tables 3 et 5).

Proposition 3.3.2:

Soit $X^m-1=(4+X)u(X)v(X)$ *avec* m *impair et* $u^*=u$, $v^*=v$. *Alors le code cyclique, sur* F_5, *généré par le polynôme* $g(X)=(1+X)u(X)v(-X)$ *est iso-dual en longueur* $2m$.

Exemple 3.3.3:

Pour les codes cycliques $\mathbf{C}[\mathbf{18},\mathbf{9}]_5$, dont la distance minimale optimale est $d_5=4$, on sait que:

$$X^{18}-1=(X^9-1)(X^9+1)$$

et

$$\begin{aligned} X^9-1 &= (4+X)(1+X+X^2)(1+X^3+X^6) \\ X^9+1 &= (1+X)(1+4X+X^2)(1+4X^3+X^6) \end{aligned}$$

Soit

$$\begin{aligned} g(X) &= (1+X)(1+4X+X^2)(1+X^3+X^6) \\ &= 1+2X^3+2X^6+X^9 \end{aligned}$$

Avec

$$u(X)=1+4X+X^2 \quad \text{et} \quad v(X)=1+4X^3+X^6$$

Vérifiant

$$u^*=u \quad et \quad v^*=v$$

Alors:

$$\begin{aligned}\frac{X^{18}-1}{g(X)} &= (4+X)u(-X)v(X)\\ &= (4+X)(1+X+X^2)(1+4X^3+X^6)\\ &= 4+2X^3+3X^6+X^9\end{aligned}$$

d'où:

$$\begin{aligned}(\frac{X^{18}-1}{g(X)})^* &= X^9(4+\frac{2}{X^3}+\frac{3}{X^6}+\frac{1}{X^9})\\ &= 1+3X^3+2X^6+4X^9\\ &= -[\frac{X^{18}-1}{g(X)}]\\ &= g(X)^{\perp}\\ &= g(-X)\end{aligned}$$

Donc le code $\mathbf{C}[\mathbf{18},\mathbf{9}]_5$ est bien iso-dual en longueur 18.

Exemple 3.3.4:

Pour les codes cycliques $\mathbf{C}[\mathbf{22},\mathbf{11}]_5$, dont la distance minimale optimale est $d_5 = 8$, on sait que:

$$X^{22}-1 = (X^{11}-1)(X^{11}+1)$$

et

$$\begin{aligned}X^{11}-1 &= (4+X)(4+X+X^2+4X^3+2X^4+X^5)(4+3X+X^2+4X^3+4X^4+X^5)\\ X^{11}+1 &= (1+X)(1+3X+4X^2+4X^3+X^4+X^5)(1+X+4X^2+4X^3+3X^4+X^5)\end{aligned}$$

Soit

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

Avec

$$u(X) = (1+3X+4X^2+4X^3+X^4+X^5) \text{ et } v(X) = (1+X+4X^2+4X^3+3X^4+X^5)$$

Vérifiant

$$u^* = v \quad et \quad v^* = u$$

Alors:

$$\begin{aligned} \frac{X^{22}-1}{g(X)} &= (1+X)(4+X+X^2+4X^3+2X^4+X^5)(4+3X+X^2+4X^3+4X^4+X^5) \\ &= 1+2X+2X^2+2X^3+2X^4+2X^5+2X^6+2X^7+2X^8+2X^9+2X^{10}+X^{11} \end{aligned}$$

d'où:

$$\begin{aligned} (\frac{X^{22}-1}{g(X)})^* &= 1+2X+2X^2+2X^3+2X^4+2X^5+2X^6+2X^7+2X^8+2X^9+2X^{10}+X^{11} \\ &= \frac{X^{22}-1}{g(X)} \\ &= g(X)^{\perp} \\ &= -g(-X) \end{aligned}$$

Donc le code $\mathbf{C}[\mathbf{22},\mathbf{11}]_5$ est bien iso-dual en longueur 22.

Remarque: Notons que la meilleure distance minimale connue pour un code autodual de longueur 42 est 12 [10, tables de P. Gaborit], c'est à dire de même distance minimale optimale que celui iso-dual $C[42,21]_5$ qu'on a trouvé (voir table 5).

3.3.5 Nouvelles classes de Codes cycliques iso-daux sur GF(5)

Nous donnons *trois constructions* de codes cycliques iso-duaux. On suppose que $n = 2m$ avec m impair et n non multiple de 5. Dans ce cas la factorisation

$$x^m - 1 = (x-1)u(x)v(x)$$

donne, en changeant x par $-x$, la factorisation

$$x^m + 1 = (x+1)u(-x)v(-x).$$

On choisit

$$g(x) = (x-1)u(x)v(-x)$$

Nou considérons les trois cas suivants:

1. $u^*(x) = u(x)$, $v^*(x) = v(x)$
2. $u^*(x) = \epsilon v(x)$, $v^*(x) = \eta u(x)$
3. $u^*(x) = v^*(-x)$, $v^*(x) = u^*(-x)$

avec ϵ, $\eta = \pm 1$.

Proposition 3.3.6 : *Prenant la notation précédente. Dans les trois cas, le code cyclique de générateur $g(x)$ est iso-dual sur F_5.*

Preuve: Dans chaque cas nous calculons le polynôme générateur du code dual. Premièrement on a:

$$(x^n - 1)/g(x) = (x+1)u(-x)v(x).$$

Prenant les réciproques des deux côtés, nous obtenons dans les trois cas: $\pm g(-x)$ ou $[-g(-x)]^*$. Le résultat s'ensuit. □

Programme de recherche de la distance minimum d'un code cyclique sur GF(p), p=3, 5.

/* Recherche de la distance minimale d'un code cyclique sur GF(p)

La recherche se fait en utilisant l'algorithme de Chen (1969) 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. Aucune optimization particulière n'est mise en oeuvre.

Il faut renseigner la longueur N du code, le degré DEG_G de son polynôme générateur, ainsi que les DEG_G+1 coefficients de ce polynôme. Il faut également indiquer une borne inférieure w_0 sur la distance minimale estimée du code (prendre w_0 =1 si aucune borne plus précise n'est disponible).

Principe de l'algorithme: si le code possède un mot de poids w, alors il existe forcément un décalage cyclique de ce même mot possédant r = floor(w*k/n) coordonnées non nulles sur la partie information. Il suffit donc de générer tous les mots ayant un poids d'information égal à r, et de vérifier si l'un de ces mots possède un poids total de w (auquel cas dmin = w).

La recherche se fait par ordre de poids w croissant.

Pour compiler sous Linux/Unix:

gcc -O2 dmin_f3 -o dmin_f3

*/

```
#include <stdio.h>
#include <stdlib.h>
/* — Renseigner ici les paramètres du code — */
#define     N           62          /* longueur du code */
#define     DEG_G       31          /* degré du générateur */
#define     W0          1           /* borne inf sur dmin */
/* Tableau des coefficients du polynôme générateur
dans l'ordre g_0, g_1, ..., g_{N-K} */
```

```
int G[DEG_G+1] = {2, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1,
2, 1, 2, 1, 2, 1, 1};
/* ---------------------------------- */
#define      K          (N-DEG_G)
int pos_nz[K];
int val_nz[K];
int message[K];
int parite[N-K];
/* Génère toutes les combinaisons de k éléments parmi
n dans l'ordre lexicographique */
int next_comb (int n, int k, int *c)
{
     int i, j;
     j = k-1;
     while ( j >= 0 && c[j] == (n-k+j) ) j--;
     if (j == -1) return 0;
     c[j]++;
     for (i = j+1; i < k; i++)
          c[i] = c[i-1] + 1;
     return 1;
}
/* Réalise l'encodage cyclique d'un message */
void encode (int *data, int *parity)
{
     int i, t;
     for (i = 0; i < N-K; i++)
          parity[i] = 0;
     for (t = 0; t < K; t++)
```

```
    {
        int feedback = (parity[0] + data[t]) % 3;
        for (i = 0; i < N-K-1; i++)
        {
            int j = (feedback * (3-G[N-K-1-i])) % 3;
            parity[i] = (parity[i+1] + j) % 3;
        }
        parity[N-K-1] = (feedback * (3-G[0])) % 3;
}
}
/* Programme principal */
int main ()
{
    int i, w;
    /* Affiche quelques infos sur le code */
    printf("Code cyclique (%d,%d) sur GF(3)\n", N, K);
    printf("Polynôme générateur G = ");
    for (i = 0; i <= DEG_G; i++)
        printf("%d", G[i]);
    printf("\n");
    printf("Borne inférieure sur dmin: %d\n\n", W0);
    /* Initialise le message d'info à zéro */
    for (i = 0; i < K; i++)
        message[i] = 0;
    for (i = 0; i < N-K; i++)
        parite[i] = 0;
    /* Boucle infinie sur les poids w croissants */
    for (w = W0; ; w++)
```

```
{
    int weight, r;
    /* Calcul du poids r sur la partie info */
    r = (w*K)/N;
    printf("Recherche de mots de poids w=%d (r=%d)\n", w, r);
    fflush(stdout);
    if (r != 0)
    {
        /* Boucle sur les combinaisons de r éléments non nuls parmi K */
        for (i = 0; i < r; i++)
            pos_nz[i] = i;
        do
        {
            /* Boucle sur les différents messages possibles */
            for (i = 0; i < r; i++)
                val_nz[i] = 1;
            do {
                /* Encodage d'un message */
                for (i = 0; i < r; i++)
                    message[ pos_nz[i] ] = val_nz[i];
                encode(message, parite);

                /* Calcul du poids du mot */
                weight = r;
                for (i = 0; i < N-K; i++)
                    if (parite[i] != 0)
                        weight++;
                /* C'est terminé si on obtient le poids recherché. */
```

```
            if (weight == w)
            {
                printf("Un mot de poids w=%d a été trouvé\n", w);
                /* Affiche le mot dans l'ordre c_{n-1}, ..., c_0 */
                printf("Mot: ");
                for (i = 0; i < K; i++)
                    printf("%d", message[i]);
                for (i = 0; i < N-K; i++)
                    printf("%d", (3-parite[i]) % 3);
                printf("\n");
                return 0;
            }
            /* Génère le message suivant (s'il en reste) */
            val_nz[0] = (val_nz[0] + 1) % 3;
            i = 0;
            while (i < r && val_nz[i] == 0)
            {
                val_nz[i] = 1;
                if (i < r-1)
                    val_nz[i+1] = (val_nz[i+1] + 1) % 3;
                i++;
            }
        } while (i != r);
        /* Sinon, on continue en remettant le message à zéro */
        for (i = 0; i < r; i++)
            message[ pos_nz[i] ] = 0;
    } while (next_comb(K, r, pos_nz) != 0);
}
```

```
            /* Augmente le poids w si nécessaire */
            printf("Aucun mot de poids w=%d n'a été trouvé\n\n", w);
        }
        return 0;
}
```

CHAPITRE IV

Divisibilité des trinômes $x^{am}+x^{bs}+1$ par un polynôme irréductible sur F_2

4.1 Introduction

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. Les trinômes irréductibles présentent un grand défi pour les chercheurs malgré les résultats qui paraissent régulièrement. Dans cette partie on s'intéresse à la divisibilité des trinômes du type

$$x^{am} + x^{bs} + 1$$

par un polynôme irréductible de degré r, sur le corps fini F_2, pour a, b des entiers quelconques et m, s des entiers à déterminer.

4.2 Primitivité d'un polynôme irréductible sur un corsps fini

Définition 4.2.1:

Soit T un polynôme irréductible de degré $r > 1$ sur F_2. La primitivité de T est le plus petit entier positif t tel que T divise $x^t - 1$.

Exemple 4.2.2:

Considérons le polynôme $T = x^4 + x^3 + x^2 + x + 1$ irréductible sur F_2 et faisons les divisions succéssives de $x^t - 1$ par T pour $t = 2, 3, 4, 5, ...$, sur F_2.

$x^2 + 1 \equiv x^2 + 1 \mod (T)$

$x^3 + 1 \equiv x^3 + 1 \mod (T)$

$x^4 + 1 \equiv x^3 + x^2 + x \mod (T)$

$x^5 + 1 \equiv (x+1)(x^4 + x^3 + x^2 + x + 1)$

$x^5 + 1 \equiv 0 \bmod (T)$

Ainsi la primitivité du polynôme T est $t = 5$.

4.3 Théorèmes de base sur la divisibilité des trinômes x^m+x^s+1 par un polynôme irréductible sur F_2

Théorème 4.3.1[14]:

Soit T un polynôme irréductible de degré $r > 1$ sur F_2, ayant α comme racine dans une extension. T divise un certain trinôme si et seulement si ils existent des entiers distincts i et j tels que $\alpha^i + \alpha^j = 1$.

Preuve:

Le trinôme $h(x) = x^i + x^j + 1$ est divisible par T si et seulement si $h(\alpha) = \alpha^i + \alpha^j + 1 = 0$, c'est à dire $\alpha^i + \alpha^j = 1$. □

Théorème 4.3.2[14]:

Soit T un polynôme irréductible de degré $r > 1$ sur F_2 et de primitivité t, ayant α comme racine dans une extension. Si T divise un trinôme quelconque, alors il divise infiniment des trinômes.

Preuve:

Supposons que le polynôme T, de primitivité t, divise le trinôme $x^m + x^s + 1$. Alors T divise aussi la famille des trinômes $x^{m+\mu t} + x^{s+\nu t} + 1$ pour tous les entiers positifs μ et ν. □

Théorème 4.3.3[14]:

Soit T un polynôme irréductible de degré $r > 1$ sur F_2, ayant α comme racine dans une extension. Si T divise des trinômes quelconques, alors il divise un certain trinôme de degré $< t$.

Preuve:

Si T divise $x^m + x^s + 1$, nous avons $\alpha^m + \alpha^s + 1 = 0$. Comme $\alpha^t = 1$, ce qui donne $\alpha^{m'} + \alpha^{s'} + 1 = 0$ où $m \equiv m'(\mathrm{mod}\, t)$ et $s \equiv s'(\mathrm{mod}\, t)$, pour lequels m' et s' sont dans l'ensemble $\{0,\ 1,\ ...,\ t-1\}$. Alors T doit diviser un certain trinôme $x^{m'} + x^{s'} + 1$ de degré $< t$.□

4.4 Polynômes cyclotomiques et divisibilité des trinomes x^m+x^s+1 sur F_2

Pour tout entier quelconque impair $t > 3$, soit

$$\Phi_t(x) = f_1(x)f_2(x)...f_r(x)$$

la factorisation sur F_2 du $t^{ième}$ polynôme cyclotomique en polynômes irréductibles. On sait que tous les $f_i(x)$ sont de même degré (supposons le n) et ont la même primitivité t(voir 14, W. Golomb and P-F Lee).

Théorème 4.4.1[14]:

Si un seul des polynômes $f_i(x)$ divise un trinôme, alors tous les r polynômes $f_i(x)$ divisent des trinômes.

Preuve:

Collectivement, les racines des polynômes $f_1(x), f_2(x), ..., f_r(x)$, dans une extension, sont toutes les puissances $\alpha, \alpha^2, \alpha^3, ..., \alpha^{t-1}$, d'une racine simple α de $\Phi_t(x)$, qui peut être prise comme racine de n'importe lequel des polynômes $f_i(x)$. En plus, les racines de $\alpha^t = 1$ forment toujours un groupe multiplicative cyclique. Si α est une racine primitive de $\alpha^t = 1$, alors toute autre racine primitive est une puissance de α. supposons que $f_i(x)$ divise le trinôme $x^m + x^s + 1$. Alors

$$\alpha^m + \alpha^s + 1 = 0$$

où on selectionne α telle qu'elle soit racine de $f_i(x)$. Pour tout autre polynôme $f_j(x)$ de l'ensemble des diviseurs de $\Phi_t(x)$, supposons que l'une des ces racines soit $\beta = \alpha^u$, avec $pgcd(t, u) = 1$(c'est à dire: $rt + vu = 1$ pour certains entiers r, v). Alors nous avons $\alpha = \beta^v$ pour $1 \leq v \leq t - 1$ pour lequel

$$(\beta^v)^m + (\beta^v)^s + 1 = \beta^{vm} + \beta^{vs} + 1 = 0$$

Par conséquent $f_j(x)$ divise le polynôme $x^{vm} + x^{vs} + 1$. □

Spécialement, si un polynôme quelconque des $f_i(x)$ est toujours un trinôme, alors tous les $f_i(x)$ divisent des trinômes. Le théorème précise que pour tout entier impair $t > 3$, soit que tous les $f_i(x)$ divisent des trinômes ou ne divisent pas des trinômes.

Théorème 4.4.2(Critère de Welch) [14]:
Pour tout entier impair t, les polynômes irréductibles de primitivité t divisent des trinômes si et seulement si le $pgcd[1 + x^t, 1 + (1 + x)^t]$ est de degré supérieur à 1.

Preuve:
Soit

$$c_t(x) = \frac{x^t - 1}{x - 1} = f_1(x)f_2(x)...f_r(x)$$

(non nécéssairement le $t^{ième}$ polynôme cyclotomique) la factorisation de $c_t(x)$ en facteurs irréductibles. Alors

$$(1 + x^t) = (1 + x)c_t(x)$$

(sur F_2 bien sûr)
et

$$[1 + (1 + x)^t] = xc_t(1 + x)$$

Ainsi, excepté pour des facteurs linéaires possibles,

$$pgcd[1+x^t, 1+(1+x)^t] = pgcd[c_t(x), c_t(1+x)]$$

Alors collectivement les racines de $f_1(x), f_2(x), ..., f_r(x)$ sont:

$$\alpha, \alpha^2, \alpha^3, ..., \alpha^{t-1}$$

où $\alpha \neq 1$ et $\alpha^t = 1$.
Par conséquent, les racines des facteurs irréductibles de $c_t(1+x)$ sont:

$$1+\alpha, 1+\alpha^2, 1+\alpha^3, ..., 1+\alpha^{t-1}$$

Ainsi, le pgcd en question est de degré supérieur à 1 si et seulement si les racines $1+\alpha^j$ de $c_t(1+x)$ sont égales aux racines α^i de $c_t(x)$, c'est à dire

$$1+\alpha^j = \alpha^i$$

Qui est précisement la condition qu'un facteur de $c_t(x)$ ayant α comme racine divise le trinôme $x^i + x^j + 1$. □

Exemple 4.4.3:
Considérons le polynôme $T = x^4 + x^3 + x^2 + x + 1$ irréductible sur F_2 et de primitivité 5, le calcul du pgcd$[1+x^t, 1+(1+x)^t]$ pour $t = 5$ donne:

$$\text{pgcd}[1+x^5, 1+(1+x)^5), \text{mod}\, 2] = 1$$

Ce qui explique bien que ce polynôme ne divise pas des trinômes sur F_2.

4.5 Polynômes réciproques et divisibilité des trinômes x^m+x^s+1 sur F_2

Définition 4.5.1:

Soit $f(x)$ un polynôme irréductible de degré n. Le polynôme réciproque de $f(x)$ est défini par:

$$f^*(x) = x^n f(\frac{1}{x})$$

Si $f^*(x) = f(x)$, alors on dit que $f(x)$ est un polynôme auto-réciproque(c.a.d, si α est une racine de $f(x)$, alors α^{-1} est aussi une racine de $f(x)$).

Lemme 4.5.2:

Pour les valeurs premiers p avec

$$\Phi(p) = \frac{(x^p - 1)}{(x - 1)} = f_1(x)f_2(x) \ ... \ f_r(x)$$

comme produit de $r > 1$ polynômes irréductibles, si un seul des $f_i(x)$ est auto-réciproque, alors $f_i(x)$ ne peut être un trinôme.

Preuve:

Comme $f_i(x)$ est auto-réciproque, on a:

$$f_i(x) = x^{(p-1)/r} f_i(\frac{1}{x})$$

Si $f_i(x)$ est un trinôme, il doit être $x^{(p-1)/r} + x^{(p-1)/2r} + 1$, qui divise $x^{3(p-1)/2r} + 1$, par conséquent $\alpha^{3(p-1)/2r} = 1$, mais $3(p-1)/2r < p$ pour tout $r > 1$, qui contredit la primitivité de p le plus petit exposent verifiant $\alpha^p = 1$. □

4.6 Condition nécessaire de divisibilité des trinômes $x^{am}+x^{bs}+1$ par un polynôme irréductible de degré r sur F_2

4.6.1. Etude des familles $F(a, b)$ telles que $x^a + x^b + 1$ soit irréductible sur F_2

Considérant la famille de polynômes $F(a, b) = \{x^{am} + x^{bs} + 1,\ 0 < bs < am\}$ avec a, b des entiers positifs et m, s des entiers à déterminer tels que le trinôme $x^a + x^b + 1$ soit

irréductible sur le corps fini F_2. Soit $\pi\mathrm{M}(a,b)$ le cardinal de l'ensemble des trinômes T irréductibles de la famille $F(a,b)$ tels que le degré de T soit inférieur ou égal à une borne déterminée M.

1^{er} cas F(3,2) :

Le trinôme x^3+x^2+1 étant irréductible sur le corps fini F_2, on va étudier la famille

$$F(3,2)=\{x^{3m}+x^{2s}+1, 0<2s<3m\}$$

avec m,s des entiers positifs. Le calcul systématique de la densité de ces trinômes irréductibles et l'estimation du rapport $\pi\mathrm{M}(3,2)/\pi\mathrm{M}(1,1)$ pour M=100, 200, 300, 500, 700, 900, 1000, 1500, 2000 a donné les résultats suivants :

M	$\pi\mathrm{M}(3,2)$	$\pi\mathrm{M}(1,1)$	$\pi\mathrm{M}(3,2)/\pi\mathrm{M}(1,1)$
100	27	276	0,098
200	58	589	0,098
300	102	937	0,11
500	162	1490	0,11
700	218	2082	0,10
900	283	2732	0,10
1000	321	3020	0,11
1500	466	4575	0,10
2000	635	6031	0,11

$2^{ème}$ cas F(5,3) :

Pour le trinôme x^5+x^3+1, irréductible sur le corps fini F_2, on fait l'étude sur la famille

$$F(5,3)=\{x^{5m}+x^{3s}+1, \quad 0<3s<5m\}$$

avec m,s des entiers positifs. Le même calcul systématique de la densité et l'estimation

du rapport πM$(5,3)/\ \pi$M$(1,1)$ pour M=100,200,300,500,700,900,1000,1500,2000 a donné :

M	πM$(5,3)$	πM$(1,1)$	πM$(5,3)/\pi$M$(1,1)$
100	26	276	0,09
200	54	589	0,09
300	86	937	0,09
500	141	1490	0,09
700	191	2082	0,09
900	257	2732	0,09
1000	265	3020	0,09
1500	428	4575	0,09
2000	582	6031	0,1

3ème cas F(7,3) :

Le même calcul pour la famille des trinômes

$$F(7,3) = \{x^{7m} + x^{3s} + 1, \quad 0 < 3s < 7m\}$$

avec $x^7 + x^3 + 1$ irréductible sur F_2 donne :

M	πM$(7,3)$	πM$(1,1)$	πM$(7,3)/\pi$M$(1,1)$
100	20	276	0,07
200	40	589	0,07
300	69	937	0,07
500	112	1490	0,08
700	160	2082	0,08
900	227	2732	0,08
1000	238	3020	0,08
1500	345	4575	0,08
2000	446	6031	0,07

$4^{ème}$ cas F(7,5) :

Pour faire la comparaison de ces résultats avec ce que donne un polynôme réductible, on a choisi le trinôme $x^7 + x^5 + 1$(non irréductible sur F_2), et le calcul dans la famille

$$F(7,5) = \{x^{7m} + x^{5s} + 1, \quad 0 < 5s < 7m\}$$

a donné les résultats suivants sur lequels on remarque que la densité est doublement faible, d'où l'intéret du choix d'un polynôme irréductible.

M	πM$(7,5)$	πM$(1,1)$	πM$(7,5)/\pi$M$(1,1)$
100	12	276	0,04
200	21	589	0,04
300	43	937	0,05
500	70	1490	0,05
700	102	2082	0,05
900	131	2732	0,05
1000	141	3020	0,05
1500	215	4575	0,05
2000	288	6031	0,05

• **Soit la fonction F: M** $\rightarrow$ π**M(a, b)**/π **M(1, 1)**

Pour **M**=100, 200, 300, 500, 700, 900, 1000, 1500, 2000
Avec $(a = 3, b = 2)$, $(a = 5, b = 3)$, $(a = 7, b = 3)$, $(a = 7, b = 5)$
on a respectivement

1) **F(M)**= 0,098; 0,098; 0,11; 0,11; 0,10; 0,10; 0,11; 0,10; 0,11.
2) **F(M)**= 0,09; 0,09; 0,09; 0,09; 0,09; 0,09; 0,09; 0,09; 0,1.
3) **F(M)**= 0,07; 0,07; 0,07; 0,08; 0,08; 0,08; 0,08; 0,08; 0,07.
4) **F(M)**= 0,04; 0,04; 0,05; 0,0 5; 0,05; 0,05; 0,05; 0,05; 0,05.

On constate que si on prends un polynôme irréductible sur F_2, les valeurs de **F**(**M**) (c'est à dire la densité de probabilité pour qu'un trinôme $x^{am} + x^{bs} + 1$ soit irréductible sur F_2 par rapport à la famille $F(1, 1)$), est nettement supérieure à celle lorsqu'on choisit un polynôme non irréductible(voir 4ème cas).

4.6.2 Condition nécessaire de divisibilité des trinômes $x^{am} + x^{bs} + 1$ par un polynôme irréductible sur F_2 pour $0 < bs < am$.

4.6.2.1 Concepts généraux

Soit le corps fini à deux éléments noté F_2. Si le polynôme T, de degré r, est irréductible (sur F_2), il divise le binôme $(x^{2^r-1}+1)$ [21]. Soit T un polynôme irréductible de degré $r>1$ sur F_2 ayant α comme racine, dans une extension, et de primitivité t (c.a.d que t est le plus petit entier tel que T divise le binôme x^t-1)). Le théorème suivant du à Swan est un important résultat sur la non-existance, dans certains cas, de trinômes irréductibles sur F_2.

4.6.2.2 Théorème de Swan[14]

Soit $n>m>0$ et supposons exactement qu'un seul n, m soit impair. Alors le trinôme x^n+x^m+1 admet un nombre pair de facteurs irréductibles sur F_2 si et seulement si

(i) n est pair, m est impair, $n\neq 2m$, et $nm/2\equiv 0,1 (\mathrm{mod}\, 4)$

(ii) *n est impair, m est pair, $m\nmid 2n$, et $n\equiv \pm 3 (\mathrm{mod}\, 4)$*

(iii) *n est impair, m est pair, $m\mid 2n$, et $n\equiv \pm 1 (\mathrm{mod}\, 8)$*

4.6.2.3 Résultats obtenus

Notre étude est axée sur la recherche de familles de polynômes creux (i.e., à petit nombre de termes) sur le corps fini F_2 qui produisent une grande proportion de polynômes irréductibles. Une recherche expérimentale des trinômes irréductibles sur F_2 a été faite, en particulier sur les trinômes du type $\mathrm{x}^{5m}+\mathrm{x}^{3s}+1$, $\mathrm{x}^{7m}+\mathrm{x}^{3s}+1$ ou $\mathrm{x}^{7m}+\mathrm{x}^{5s}+1$, ce qui a exploré plusieurs pistes.

Le calcul systématique de la densité des trinômes irréductibles de la forme

$$x^{am}+x^{bs}+1, \qquad 0<bs<am\leq M$$

pour a,b entiers positifs, et M une borne fixée, $M=100,300,500,1000$, a été fait et fut comparée à la densité des trinômes quelconques (i.e., $a=b=1$) ce qui a donné les résultats suivants :

1) Pour M = 100

a b p nb total nb/total

1	1	2	276	4950	0,05575757576
2	1	2	126	2500	0,05400000000
1	2	2	75	2450	0,03061224490
3	1	2	113	1650	0,06848484848
3	2	2	27	817	0,033047735562
3	3	2	31	528	0,05871212121
1	3	2	112	1617	0,06926406926
2	3	2	64	817	0,078335337332
4	1	2	78	1275	0,06117647059
4	2	2	0	625	0,00000000000
4	3	2	37	417	0,08872901679
4	4	2	0	300	0,00000000000
1	4	2	33	1200	0,02750000000
2	4	2	0	600	0,00000000000
3	4	2	14	400	0,03500000000
5	1	2	60	1030	0,05825242718
5	2	2	13	510	0,02549019608
5	3	2	26	337	0,07715133531
5	4	2	06	250	0,02400000000
5	5	2	08	190	0,04210526316
1	5	2	57	950	0,06000000000
2	5	2	29	480	0,06041666667
3	5	2	25	317	0,078864355331
4	5	2	21	245	0,08571428571
6	1	2	59	800	0,07375000000
6	2	2	0	392	0,00000000000
6	3	2	31	250	**0,1210937500**
6	4	2	0	192	0,00000000000

6	5	2	13	154	0,08441558442
6	6	2	0	120	0,00000000000
1	6	2	23	784	0,02933673469
2	6	2	0	392	0,00000000000
3	6	2	0	256	0,00000000000
4	6	2	0	200	0,00000000000
5	6	2	6	163	0,03680981595
6	6	2	0	120	0,00000000000
7	1	2	58	721	0,08844382802
7	2	2	14	357	0,03921568627
7	3	2	20	236	0,08474576271
7	4	2	6	175	0,03428571429
7	5	2	12	139	0,08633093525
7	6	2	2	115	0,01739130435
7	7	2	8	91	0,08791208791
1	7	2	56	665	0,08421052632
2	7	2	26	336	0,07738095238
3	7	2	25	222	**0,11261261261**
4	7	2	13	172	0,07558139535
5	7	2	11	139	0,07913669065
6	7	2	12	107	**0,1121495327**
7	7	2	8	91	0,08791208791
8	1	2	0	612	0,00000000000
8	2	2	0	300	0,00000000000
8	3	2	0	200	0,00000000000
8	4	2	0	144	0,00000000000
8	5	2	0	118	0,00000000000
8	6	2	0	96	0,00000000000

8	7	2	0	83	0,00000000000
8	8	2	0	66	0,00000000000
1	8	2	13	576	0,02256944444
2	8	2	0	288	0,00000000000
3	8	2	6	192	0,03125000000
4	8	2	0	144	0,00000000000
5	8	2	4	120	0,03333333333
6	8	2	0	92	0,00000000000
7	8	2	2	84	0,02380952381
9	1	2	38	583	0,06518010292
9	2	2	10	289	0,03460207612
9	3	2	14	187	0,07486631016
9	4	2	7	142	0,04929577465
9	5	2	9	112	0,08035714286
9	6	2	0	91	0,00000000000
9	7	2	8	79	**0,1012658228**
9	8	2	3	69	0,04347826087
9	9	2	8	55	**0,1454545455**
1	9	2	42	506	0,08300395257
2	9	2	26	256	**0,1015625000**
3	9	2	16	165	0,09696969697
4	9	2	14	131	**0,1068702290**
5	9	2	9	106	0,08490566038
6	9	2	16	80	**0,2000000000**
7	9	2	9	74	**0,1216216216**
8	9	2	0	62	0,00000000000
10	1	2	34	540	0,06296296296
10	2	2	0	265	0,00000000000

10	3	2	16	177	0,09039548023
10	4	2	0	130	0,00000000000
10	5	2	8	100	0,0800000000
10	6	2	0	85	0,00000000000
10	7	2	6	73	0,08219178082
10	8	2	0	63	0,00000000000
10	9	2	7	56	**0,1250000000**
10	10	2	0	45	0,00000000000
1	10	2	9	450	0,0200000000
2	10	2	0	225	0,00000000000
3	10	2	3	150	0,0200000000
4	10	2	0	115	0,00000000000
5	10	2	0	90	0,00000000000
6	10	2	0	72	0,00000000000
7	10	2	1	66	**0,1515151515**
8	10	2	0	55	0,00000000000
9	10	2	0	53	0,00000000000

2) **Pour M = 300, 500**

Pour les mêmes trinômes, on a poursuivi le calcul pour $M = 300,500$ en faisant comparer la densité avec celle des trinômes quelconques P(1, 1, M).

3) **Pour M = 1000**

a	b	nb	total	nb/total	(nb/total)/P(1,1,M)
1	1	3020	499500	0.006046046046	1
6	3	355	27556	0,01288285673	2.130790376
3	7	357	23643	0,01509960665	2.497434941
6	7	187	11786	0,01586628203	2.624241018
9	7	140	7929	0,01765670324	2.920371943
9	9	116	6105	0,01900081900	3.142685129
2	9	298	27556	0,01081434170	1.788663470
6	9	194	9310	0,02124863089	3.514467261
4	9	181	13806	0,01311024192	2.168399284
7	9	99	7818	0,01266308519	2.094440746
10	9	77	5556	0,01385889129	2.292223907
7	10	24	7029	0,003414425950	0.5647370073

On a montré que les trinômes de la famille $x^{am} + x^{bs} + 1$ ne sont pas divisibles par les premiers polynômes irréductibles sur F_2, à savoir $x^2 + x + 1$, $x^3 + x + 1$ et $x^3 + x^2 + 1$, pour (a *mod* 3 et b *mod* 3), (a *mod* 7 et b *mod* 7) respectivement, (notons que x, $x + 1$, ne divisent pas les trinômes en question, car 0 et 1 qui en sont des racines, n'annulent pas les trinômes de la famille) . Nous généralisons ce fait par le résultat suivant:

Théorème 4.6.2.4[26] :

Soit T un polynôme irréductible de degré $r >1$ sur F_2 et soient a, b des entiers non nuls. S'ils existent m, s des entiers positifs tels que T divise $x^{am} + x^{bs} + 1$, alors a et b ne sont pas divisibles par $(2^r - 1)$.

Preuve:

En effet, supposons que a ou b soit divisible par $(2^r - 1)$ et montrons que T, irréductible de degré r, ne divise pas $x^{am} + x^{bs} + 1$ quelques soient m, s entiers.

1^{er} cas: Si $a \equiv 0\ mod(2^r - 1)$, a s'écrit $a \equiv a_1\ (2^r - 1)$ et sachant que $(x^{2^r-1} + 1) \equiv 0$

$mod(T)$ alors $x^{2^r-1} \equiv 1\ mod(T)$ d'où $(x^{2^r-1})^{a_1 m} \equiv (1)^{a_1 m}\ mod(T) \equiv 1\ mod(T)$, c'est-à-dire que $(x^{2^r-1})^{a_1 m} + 1 \equiv 0\ mod(T)$. Mais le polynôme T ne divise pas le monôme x^{bs} $(r > 1)$, ainsi le polynôme T ne divise pas le trinôme $x^{am} + x^{bs} + 1$ quelques soient m, s entiers.

$2^{ème}$ cas: Si $b \equiv 0\ mod(2^r - 1)$, b s'écrit $b \equiv b_1\ (2^r - 1)$, alors $(x^{2^r-1})^{b_1 s} + 1 \equiv 0\ mod(T)$. Mais le polynôme T ne divise pas le monôme x^{am} $(r > 1)$, ainsi le polynôme T ne divise pas le trinôme $x^{am} + x^{bs} + 1$ quelques soient m, s entiers.

Donc le polynôme T ne divise pas le trinôme $x^{am} + x^{bs} + 1$ quelques soient m et s si a ou b est divisible par $(2^r - 1)$.

Remarque:
L'implication inverse est fausse, d'après le théorème 4.3.3, si on prend $T = x^4 + x^3 + x^2 + x + 1$, irréductible sur F_2 et de primitivité $t = 5$, on n'en trouve pas de trinômes de degré strictement inférieur à 5 qui soient divisibles par T (les seuls trinômes de degré 4, sur F_2, et qui ne sont pas divisibles par T sont $x^4 + x^3 + 1$, $x^4 + x^2 + 1$ et $x^4 + x + 1$).

Maintenant essayons d'alléger les conditions sur le Théorème 4.6.2.4 pour avoir l'implication inverse.

Proposition 4.6.2.5[26]:
Soient r, a, b des entiers non nuls. S'il existe un polynôme T irréductible sur F_2 de degré r et s'ils existent m, s entiers positifs tels que T divise $x^{am} + x^{bs} + 1$ alors a et b ne sont divisibles par $(2^r - 1)$.

Preuve:
La preuve de la proposition 4.6.2.5 est identique à celle du théorème 4.6.2.4. Mais la réciproque est vraie pour les deux cas spéciaux suivants:

- Pour $r = 2 \times 3^k$, k un entier positif, il existe un polynomial $T = x^r + x^{r/2} + 1$ *irreducible*

sur F_2 [32, Th 1.1.28] et ils existent $(m = 2r, s = r)$ tels que le polynomial T divise le trinôme $P = x^{2r} + x^r + 1$ (ici $a = b = 1$) et $P = T^2$.

- De même d'après le théorème 4.3.2, T qui divise le trinôme $x^{2r}+x^r+1$, il divise infiniment les trinômes $x^{2r+\mu t} + x^{r+\nu t} + 1$ où t est la primitivité de T et μ, ν sont des entiers positifs. Si on pose $(a = 1 + \mu t,\ b = 1 + \nu t)$ alors T divise le trinôme $x^{2r(1+\mu t)} + x^{r(1+\nu t)} + 1$, c'est à dire le trinôme $x^{am} + x^{bs} + 1$ pour $(m = 2r,\ s = r)$.

4.6.3 **Recherche pratique de trinômes irréductibles suivant les différentes valeurs de** a, b **et** M.

Voici le programme Maple de recherche des **trinômes irréductibles sur** F_2 pour des valeurs de a, b et M une borne fixée.

```
> search3 := proc(a,b,p,M)
> local m,s,nb,total,f,B;
> nb := 0;
> total := 0;
> for m from 1 while a*m <= M do
  > for s from 1 while b*s < a*m do
    > f := x^(a*m) + x^(b*s) + 1;
     > B := Irreduc(f) mod p;
      > total := total + 1;
        > if B=true then nb:=nb+1 fi;
    > od
   > od;
  > nb, total, evalf(nb/total)
> end:
```

Résultats pratiques:

search3(7, 3, 2, 100)	search3(3, 5, 2, 80)	search3(7, 5, 2, 150)	search3(1,1,2,10)
$x^7 + x^3 + 1$	$x^6 + x^5 + 1$	$x^{14} + x^5 + 1$	$x^2 + x + 1$
$x^7 + x^6 + 1$	$x^9 + x^5 + 1$	$x^{28} + x^{15} + 1$	$x^3 + x + 1$
$x^{14} + x^9 + 1$	$x^{12} + x^5 + 1$	$x^{28} + x^{25} + 1$	$x^3 + x^2 + 1$
$x^{28} + x^3 + 1$	$x^{18} + x^{15} + 1$	$x^{42} + x^{35} + 1$	$x^4 + x + 1$
$x^{28} + x^9 + 1$	$x^{33} + x^{10} + 1$	$x^{49} + x^{15} + 1$	$x^4 + x^3 + 1$
$x^{28} + x^{15} + 1$	$x^{33} + x^{20} + 1$	$x^{49} + x^{40} + 1$	$x^5 + x^2 + 1$
$x^{28} + x^{27} + 1$	$x^{36} + x^{15} + 1$	$x^{63} + x^5 + 1$	$x^5 + x^3 + 1$
$x^{35} + x^{33} + 1$	$x^{36} + x^{25} + 1$	$x^{63} + x^{35} + 1$	$x^6 + x + 1$
$x^{49} + x^9 + 1$	$x^{39} + x^{25} + 1$	$x^{84} + x^5 + 1$	$x^6 + x^3 + 1$
$x^{49} + x^{12} + 1$	$x^{39} + x^{35} + 1$	$x^{84} + x^{35} + 1$	$x^6 + x^5 + 1$
$x^{49} + x^{15} + 1$	$x^{42} + x^{35} + 1$	$x^{84} + x^{45} + 1$	$x^7 + x + 1$
$x^{49} + x^{27} + 1$	$x^{54} + x^{45} + 1$	$x^{84} + x^{75} + 1$	$x^7 + x^3 + 1$
$x^{84} + x^9 + 1$	$x^{57} + x^{25} + 1$	$x^{126} + x^{105} + 1$	$x^7 + x^4 + 1$
$x^{84} + x^{27} + 1$	$x^{57} + x^{35} + 1$	$x^{140} + x^{15} + 1$	$x^7 + x^6 + 1$
$x^{84} + x^{39} + 1$	$x^{57} + x^{50} + 1$	$x^{140} + x^{45} + 1$	$x^9 + x + 1$
$x^{84} + x^{45} + 1$	$x^{60} + x^{15} + 1$	$x^{140} + x^{65} + 1$	$x^9 + x^4 + 1$
$x^{84} + x^{57} + 1$	$x^{60} + x^{45} + 1$	$x^{140} + x^{75} + 1$	$x^9 + x^5 + 1$
$x^{84} + x^{75} + 1$	$x^{63} + x^5 + 1$	$x^{140} + x^{95} + 1$	$x^9 + x^8 + 1$
$x^{98} + x^{27} + 1$	$x^{63} + x^{35} + 1$	$x^{140} + x^{125} + 1$	$x^{10} + x^3 + 1$
$x^{98} + x^{87} + 1$			$x^{10} + x^7 + 1$
$20, 236, 0.08474576$	$19, 195, 0.09743590$	$19, 311, 0.06109325$	$20, 45, 0.44444444$

ANNEXE I Résultats Fondamentaux sur les Corps finis et les Polynômes Irréductibles

1. Introduction

Le vingthième siècle fut le temps des applications des corps finis dues à l'apparition des ordinateurs. Les domaines les plus importants dans cette application sont la crytographie et la théorie des codes. Mais l'application des corps finis ne s'arrête pas là, elle s'étend à d'autres domaines tels que la géométrie progective, combinatoire, la théorie spectrale, transformation de Fourier discrete, ... , Nous présentons dans cette section les principaux résultats sur la théorie des corps finis et les propriétés de base des polynômes irréductibles sur tels corps. Signalons qu'un corps fini est commutatif(Théorème de Wedderburn) [21].

2. Principaux résultats sur les corps finis

(1) *Dans tout corps fini F_q le nombre d'éléments est une puissance d'un nombre premier, et ce premier est la caractéristique du corps(fini).*

(2) *Si p est un nombre premier et m un entier positif, alors il y a un corps fini d'ordre p^m qui est unique à un isomorphisme prés.*

(3) *Le groupe multiplicatif F_q^* des éléments non nuls du corps fini F_q est cyclique. Tout élément générateur est un élément primitif de F_q.*

(4) *Soit $q = p^m$. Alors, tout sous corps de F_q admet pour ordre p^d, où d est entier positif diviseur de m. Inversement si $d \mid m$, alors il existe exactement un seul sous corps de F_q d'ordre p^d.*

(5) *Tout élément $x \in F_q$ satisfait l'équation $x^q - x = 0$.*

(6) *Un corps fini F_q est isomorphe au corps de decomposition de $x^q - x$ sur F_q, où $q = p^m$.*

3. L'anneau A[x] des Polynômes

3.1 Définitions de base

On appelle anneau tout ensemble A muni de deux opérations binaires + et ., l'une est une loi de groupe abélien l'autre associative et doublement distributive par rapport à la première. On note additivement la loi de groupe et multiplicativement l'autre loi. L'anneau est dit unitaire si la seconde loi admet un élément neutre et commutatif si la loi est commutative. Un anneau A est dit intégre s'il est distinct de $\{0\}$ et n'admet pas de diviseurs de zéro. Un corps est un anneau unitaire où tout élément non nul admet un inverse pour la loi (.).

3.2 Idéal d'un anneau

Definition 3.2.1

Un ensemble non vide I de A est dit idéal si :

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

Exemple 3.2.2

Les idéaux de Z sont de la forme nZ où $n \in N$.

Definitions 3.2.3

L'ensemble des classes résiduèlles d'un anneu A modulo un idéal I forme un anneau noté A/I dont les deux opérations sont définies par :

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

3.3. Anneau des polynômes

Definition 3.3.1

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 $A[x]$.

Si $f = (a_0, a_{1, \dots}, a_n, 0, 0, ...) \in A[x]$ on notera $f = (a_0, a_{1, \dots}, a_n)$.

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 $(0, 0, ...) = -\infty$, les polynômes de degré $= 0$ sont les constantes.

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

$$(a_0, a_{1, \dots}) + (b_0, b_{1, \dots}) = (a_0 + b_0, a_1 + b_{1, \dots})$$

$$(a_0, a_{1, \dots})(b_0, b_{1, \dots}) = (c_0, c_{1, \dots}) \text{ où } c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

Notons que si A est intégre on a : $\deg fg = \deg f + \deg g$.

Muni des deux opérations + et . , $A[x]$ est anneau commutatif avec unité $(1, 0, 0, ...)$.

$(A[x], +, .)$ est appelé l'anneau des polynômes sur A.

Dans $A[x]$, on définit : $x = (0, 1, 0, 0, ...)$, $x^2 = (0, 0, 1, 0, ...)$, ...avec $x^0 = (1, 0, 0, ...)$ ce qui permet d'écrire tout polynôme P de degré n comme **:**

$$P = a_0 + a_1 x + ... + a_n x^n$$

Soit $f, g \in A[x]$, avec deg $f > 0$. On dit que f divise g noté $(f \mid g)$ si $g = fh$ pour $h \in A[x]$ et $\deg f < \deg g$, f est alors appelé un diviseur propre de g.

Définition 3.3.2

L'anneau des polynômes $F_q[x]$(ou $K[x]$ *en général, K* corps*) est l'ensemble des polyômes $f(x)$ à coefficients dans F_q (qui satisfait les propriétés d'un anneau).*

Définition 3.3.3(Idéal principal)

Soit I un idéal de $F_q[x]$. On dit queI un idéal principal s'il existe un polynôme P dans $F_q[x]$ tel que $I = (P)$.

Notons que (P), l'idéal engendré par le polynôme P, est défini par:

$$(P) = \{A \in F_q[x] \mid (\exists Q \in F_q[x]])\ A = PQ\}$$

Théorème 3.3.4:

Soit K un corps, alors l'anneau des polynômes $K[x]$ est principal.

Preuve:

On va montrer que tout idéal dans $K[x]$ est *principal*.

Soit I un idéal de $K[X]$. Si $I = \{0\}$, alors $I = (0)$.

Supposons $I \neq \{0\}$. Alors, $I - \{0\} \neq \emptyset$.Soit G un polynôme de $I - \{0\}$ vérifiant

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

Sachant que $G \in I$ équivaut à $(G) \subset I$. Soit $A \in I$, par la division Euclidienne, il existe un unique couple

de polynômes (Q, R) tel que :

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

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

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

De

$$R \in I,\ deg(G) = min\{deg(P) \in N \mid P \in I - \{0\}\}$$

et

$$deg(R) < deg(G)$$

on déduit :

$$R = 0$$

D'où

$$A = GQ$$

et donc $I \subset (G)$. Comme, d'autre part, $(G) \subset I$, on obtient :

$$I = (G)$$

Un anneau intègre dont tout idéal est principal s'appelle un anneau principal. Nous avons donc prouvé que $K[X]$ est *principal.* □

Théorème de la factorisation unique

Définition 3.3.5

Un polynôme f de deg ≥ 1 qui n'admet pas de diviseurs propres(autres que l'identité et f) est appelé un polynôme irréductible.

Théorème 3.3.6 [21]

Soit F_q un corps. Alors tout polynôme $f \in F_q[x]$ a une représentation unique (à l'ordre prés) de la forme:

$$f = rp_1p_2...p_k.$$

où $r \in F_q$ et $p_1,\ p_{2,...,}p_k$ sont des polynômes unitaires irréductibles sur F_q.

Ce théorème affirme donc l'existence de l'écriture unique d'un polynôme comme produit de polynômes unitaires irréductibles.

4. Principales propriétés des polynômes irréductibles dans $\mathbf{F_q[x]}$

- Les irréductibles sont les éléments premiers des polynômes. Ils jouent le même rôle que

les éléments premiers des nombres. Pour les nombres entiers on a

$$Z/(p) \textit{ est un corps ssi } p \textit{ est premier.}$$

Le théorème (4.2) suivant garantit que le même est vrai pour les polynômes sur un corps fini.

Corollaire 4.1

Soit $f(x)$ *un polynôme de degré* > 1 *sur le corps* F_q et

$$F_q[x]/(f(x)) = \{r(x) \in F_q[x] \mid deg\ r(x) < deg\ f(x)\}.$$

Alors $F_q[x]/(f(x))$ est un anneau muni des deux opérations $+$ et $\cdot$ définies comme suit: Pour tout $r_1(x)$, $r_2(x) \in F_q[x]/(f(x))$

$$\begin{aligned} r_1(x) + r_2(x) &= [r_1(x) + r_2(x)]_{mod\ f(x)} \\ r_1(x) \cdot r_2(x) &= [r_1(x) \cdot r_2(x)]_{mod\ f(x)} \end{aligned}$$

Théorème 4.2 [21]:

Pour $f(x) \in F_q[x]$, *l'anneau des classes résiduelles* $F_q[x](f(x))$ *est un corps si et seulement si* $f(x)$*est irréductible.*

Exemple 4.3: Considérons le polynôme $x^2 + x + 1 \in F_2[x]$, nous avons la table de la loi $(\cdot)$

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

Dans ce cas on a bien un corps car le polynôme x^2+x+1 est irréductible sur le corps fini F_2. Par contre si on prend le polynôme $f = x^2+1$, qui est réductible sur F_2(1 est une racine de f), l'anneau $F_2[x](f)$ n'accède pas à la structure de corps par le fait que l'élément $(1+x) \in F_2[x](x^2+1)$ n'admet pas un inverse.

Notons que si f est un polynôme **unitaire irréductible** de degré n sur F_p, alors le nombre d'éléments de $F_q[x](f)$ est p^n. Par conséquent $F_q[x](f)$ est aussi un corps fini.

4.4 Pourquoi le choix d'un polynôme irréductible?

La réductibilité d'un polynôme f sur un corps F, c'est à dire la possibilité de sa représentation sous la forme $f = f_1.f_2$ où $f_1,\ f_2 \in F[x]$ et $0 < \deg f_i < \deg f$ pour $i = 1,2$ entraine dans $F[x]/(f)$ l'éxistence de diviseurs non triviaux de zéro, à savoir $\overline{f_i} \neq \overline{0}$, $i = 1,2$ mais

$$\overline{f_1}.\overline{f_2} = \overline{f_1.f_2} = \overline{f} = \overline{0}$$

c'est à dire que dans ce cas $F[x]/(f)$ ne peut être un corps car il est non intégre. C'est pour cela qu'on choisit un polynôme irréductible f sur F pour que l'anneau $F[x]/(f)$ des classes résiduelles modulo f accède à la structure de corps. Ainsi si f est irréductible et $g \neq 0$ un polynôme tel que $\deg g < \deg f$ alors le $p\gcd(f,g) = 1$ et ils existent $u, v \in F[x]$ avec: $uf + vg = 1$ d'où $\overline{uf+vg} = \overline{uf} + \overline{vg} = \overline{1}$ et comme $uf \in (f)$ on a : $\overline{uf} = \overline{0}$ et par la suite $\overline{vg} = \overline{vg} = \overline{1}$ ce qui signifie que tout $\overline{g} \neq \overline{0}$ admet dans $F[x]/(f)$ un inverse $\overline{v} = \overline{g}^{-1}$. Cette remarque montre que dans le cas où le polynôme f est irréductible,

l'anneau quotient $F[x]/(f)$ est un corps contenant un sous corps isomorphe à F à savoir l'ensemble (corps premier) des éléments $\overline{a}$, pour $a \in F$.

Rappelons qu'un polynôme f sur F de degré non nul est dit irréductible (ou premier) dans $F[x]$ s'il n'est divisible par aucun polynôme $g \in F[x]$ tel que $0 < \deg g < \deg f$. En particulier tout polynôme de $\deg = 1$ est irréductible.

On sait maintenant que le corps de décomposition d'un polynôme irréductible de degré k sur le corps fini F_q est F_{q^k}.

Lemme 4.5

Soit f un polynôme irréductible sur F_q, et α une racine de f dans une extension de F_q. Alors si $g \in F_q[x]$, on a $g(\alpha) = 0$ si et seulement si $f \mid g$.

Preuve.

Soit $g \in F_q[x]$ avec $g(\alpha) = 0$, en faisant la division euclidienne de g par f on a: $g(x) = f(x).h(x) + r(x)$ avec $\deg r < \deg f$. Comme $g(\alpha) = 0$, alors $f(\alpha).h(\alpha) + r(\alpha) = 0$, mais $f(\alpha) = 0$ ce qui donne $r(\alpha) = 0$ donc le polynôme r doit diviser f, contradiction avec la fait que f est irréductible, d'où $r = 0$ c'est à dire $g = f.h$ par conséquent f divise g. Invérsement, supposons que f divise g alors $g(x) = f(x).h(x)$ ainsi $g(\alpha) = f(\alpha).h(\alpha) = 0$ et comme α est racine de f on a $g(\alpha) = 0$ d'où le résultat. □

Exemple 4.6

Soient $f(x) = x^2 + x + 1$, irréductible sur F_2, et $g(x) = x^5 + x^4 + 1 \in F_2[x]$. Soit α une racine de f dans F_{2^2}, c'est à dire $\alpha^2 + \alpha + 1 = 0$, d'où $\alpha^2 = \alpha + 1$ ainsi : $g(\alpha) = \alpha^5 + \alpha^4 + 1$ mais

$$\alpha^3 = \alpha^2.\alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha = (\alpha + 1) + \alpha = 2\alpha + 1 = 1.$$

Et $\alpha^4 = \alpha^3.\alpha = \alpha$, d'où $\alpha^5 = \alpha^2 = \alpha + 1 = \alpha^4 + 1$, ce qui donne $\alpha^5 + \alpha^4 + 1 = 0$.

C'est à dire que α est racine du polynôme g et on a $f \mid g$ car $g(x) = f(x).(x^3 + x + 1)$. Inversement si $f \mid g$ et $f(\alpha) = 0$ on a directement $g(\alpha) = 0$.

Théorème 4.7 [21]

Pour tout corps fini F_q, et un entier positif k, il existe un polynôme irréductible f de degré k surF_q.

En effet, soit β un élément primitif de F_{q^k} . Alors $F_q(\beta) = F_{q^k}$, et comme

$$[F_q(\beta) : F_q] = \left[F_{q^k} : F_q\right] = k$$

alors le polynôme minimal de β, irréductible sur F_q, doit être de degré k.

Théorème 4.8 [21]

Un polynôme irréductible f sur F_q, de degré k, divise $x^{q^n} - x$ si et seulement si $k \mid n$.

Exemple 4.9

Soit $f(x) = x^2 + x + 2$, irréductible sur F_3, et comme $2 \mid 2$ on déduit que $f \mid x^{3^2} - x$, en effet dans F_3 on a $-1 = 2$ et $x^9 + 2x = (x^2 + x + 2)(x^7 + 2x^6 + 2x^5 + 2x^3 + x^2 + x)$.

Théorème 4.10 [21]

Si α est une racine d'un polynôme irréductible f de degré k, sur F_q, alors toutes les racines sont données par $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{k-1}}$, appelés les conjuguées de α. En plus, k est le plus petit entier pour lequel $\alpha^{q^k} = \alpha$.

Preuve

Soit $f = a_0 + a_1x + ... + a_kx^k$, où $a_i \in F_q$. Si α est racine de f alors:

$$f(\alpha) = a_0 + a_1\alpha + ... + a_k\alpha^k = 0$$

Comme F_q est de caractéristique p, p premier, on a: $a_i^q = a_i$ pour tout $a_i \in F_q$. Et ainsi:

$$\begin{aligned} f(\alpha^q) &= a_0 + a_1\alpha^q + ... + a_k\alpha^{q^k} \\ &= a_0^q + a_1^q\alpha^q + ... + a_k^q\alpha^{q^k} \\ &= a_0^q + (a_1\alpha)^q + ... + (a_k\alpha^{^k})^q \\ &= (a_0 + a_1\alpha + ... + a_k\alpha^k)^q \\ &= [f(\alpha)]^q = 0 \end{aligned}$$

Donc si α est racine de f, α^q est aussi racine de f. Montrons maintenant que ces racines sont distinctes, ce qui complète la liste des racines de f. Si $\alpha^{q^i} = \alpha^{q^j}$, où $i < j$ alors prenons q^{k-j} comme puissance des deux côtes de l'égalité, on trouve $\alpha^{q^{k+i-j}} = \alpha^{q^k} = \alpha$. Et ainsi α est racine du polynôme $x^{q^{k+i-j}} - x$ le lemme (4.5) implique $f \mid x^{q^{k+i-j}} - x$, qui est en contradiction avec le théorème (4.8), par conséquent les racines de f sont distinctes. C'est à dire que k est le plus petit entier positif pour lequel $\alpha^{q^k} = \alpha$. □

Exemple 4.11

Soit $f(x) = x^4 + x + 1$, irréductible sur F_2, et α une racine de f dans un extension de F_2, ainsi $\alpha^4 + \alpha + 1 = 0$ c'est à dire $\alpha^4 = \alpha + 1$. Calculons $f(\alpha^2)$, $f(\alpha^{2^2})$ et $f(\alpha^{2^3})$.

- $f(\alpha^2) = \alpha^8 + \alpha^2 + 1 = (\alpha^4)^2 + \alpha^2 + 1 = (\alpha + 1)^2 + \alpha^2 + 1 = (\alpha^2 + 1) + \alpha^2 + 1 = 0.$
- $f(\alpha^4) = (\alpha^4)^4 + \alpha^4 + 1 = (\alpha + 1)^4 + (\alpha + 1) + 1 = (\alpha^4 + 1) + (\alpha + 1) + 1 = 0.$
- $f(\alpha^8) = (\alpha^8)^4 + \alpha^8 + 1 = (\alpha^4)^8 + (\alpha^4)^2 + 1 = (\alpha + 1)^8 + (\alpha + 1)^2 + 1$
  $= (\alpha^8 + 1) + (\alpha^2 + 1) + 1 = \alpha^8 + \alpha^2 + 1 = f(\alpha^2) = 0.$

Et on a $\alpha^{2^4} = \alpha^{16} = (\alpha^4)^4 = (\alpha + 1)^4 = \alpha^4 + 1 = (\alpha + 1) + 1 = \alpha$.

Le théorème (4.10) a des conséquences importantes:

Corollaire 4.12

Soit $f \in F_q[x]$ irréductible, de degré k, alors toutes les racines de f, dans son corps de décomposition, sont simples et ont le même ordre multiplicatif.

Preuve

Soit K le corps de décomposition de f, le cardinal de K est q^k, et ceci résulte du fait que le cardinal de K^* est $q^k - 1$ qui est premier avec q^i pour tout i. □

Théorème 4.13

$x^{q^n} - x = \prod_i f_i$, *où le produit est étendu sur tous les polynômes unitaires irréductibles distincts sur* F_q, *dont le degré est diviseur de* n.

Preuve

Si f_i et f_j sont deux polynômes unitaires irréductibles distincts sur F_q dont le degré divise n, alors f_i et f_j sont premiers entre eux et par conséquent $f_i.\ f_j \mid x^{q^n} - x$. Et le théorème se déduit du théorème (4.8), car $x^{q^n} - x = x(\ x^{q^n-1} - 1)$, et le fait que le polynôme $x^{q^n} - x$ a toutes ses racines simples dans son corps de décompositon sur F_q. □

5. Polynômes Cyclotomiques

5.1 Racines n^{ièmes} de l'unité

Définitions 5.1.1

Soit F *un corps . Une racine de* $x^n - 1$ *dans* $F[x]$ *est appelée une racine* n^{ieme} *de l'unité. L'ordre d'une racine* n^{ieme} α *de l'unité est le plus petit entier positif* k *tel que :* $\alpha^k = 1$. *Une racine* n^{ieme} *de l'unité d'ordre* n *est dite primitive, le corps de décomposition* S_n *de* $x^n - 1$ *est appelé le corps cyclotomique associé.*

Dans la suite on aura besoin de la fonction φ de N dans N, dite d'Euler, qui est définie par :

$$\varphi(n) = |\{\ m\ /\ 1 \leq m \leq n \text{ et } (m,n) = 1\}|$$

pour m, n des entiers positifs. Si $n = p_1^{t_1} \ldots p_k^{t_k}$ où les p_i sont des entiers premiers distincts, alors :

$$\varphi(n) = n(1 - \frac{1}{p_1}) \ ... \ (1 - \frac{1}{p_k}).$$

Théorème 5.1.2 [21]

Soit n un entier positif et F un corps dont la caractéristique ne divise pas n.

i) Il y a une extension finie K de F qui contient une racine primitive n^{ieme}de l'unité.

ii) Soit α une racine primitive n^{ieme} de l'unité, alors $F(\alpha)$ est le corps de décomposition de $f = x^n - 1$ sur F.

iii) Le polynome $x^n - 1$ admet exactement n racines distinctes dans $F(\alpha)$. Ces racines forment un groupe cyclique, l'ordre d'une racine $n^{ième}$ de l'unité α est juste l'ordre de α dans ce groupe. Les racines primitives n^{iemes} de l'unité dans $F(\alpha)$ sont précisement les générateurs de ce groupe. Il ya $\varphi(n)$ racines primitives n^{iemes} de l'unité, qui peuvent s'obtenir à partir de l'une d'entres elles α avec α^k tel que le pgcd $(k, n) = 1$ et $k < n$.

5.2 Polynômes cyclotomiques

Définition 5.2.1

Soit n un entier positif et F un corps dont la caractéristique ne divise pas n, et α une racine primitive $n^{ième}$de l'unité. Le polynôme:

$$Q_n = (x - \alpha_1)...(x - \alpha_{\varphi(n)}) \in F(\alpha)[x]$$

où $\alpha_1, ..., \alpha_{\varphi(n)}$ sont les racines primitives $n^{ièmes}$ de l'unité dans $F(\alpha)$, est appelé le $n^{ième}$ polynôme cyclotomique sur F.

Remarque 5.2.2

Le polynôme Q_n ne dépend pas de α.

Exemple 5.2.3

Soit $n = 8$ et $F = F_3$. Comme $n = 3^2 - 1$, n n'est pas divisible par 3, et considérons le polynôme $x^2 + x + 2$ qui est irréductible sur F_3, pour cela il suffit de voir que tous les éléments de F_3 ne sont pas des racines de ce polynôme. On se donne la peine de trouver une racine primitive huitième de l'unité dans $F_9 = F_3[x]/(x^2 + x + 2)$, soit α une racine du polynôme $x^2 + x + 2$ c'est àdire $\alpha^2 + \alpha + 2 = 0$, d'où sur F_3, $\alpha^2 = 2\alpha + 1$. calculons α^k pour $k = 3, 4, ..., 8$.

$\alpha^3 = \alpha^2.\alpha = (2\alpha + 1).\alpha = 2\alpha^2 + \alpha = 2(2\alpha + 1) + \alpha = 2\alpha + 2.$

$\alpha^4 = \alpha^3.\alpha = (2\alpha + 2).\alpha = 2\alpha^2 + 2\alpha = 2(2\alpha + 1) + 2\alpha = 2.$

$\alpha^5 = \alpha^4.\alpha = 2\alpha.$

$\alpha^6 = \alpha^5.\alpha = 2\alpha^2 = 2(2\alpha + 1) = \alpha + 2.$

$\alpha^7 = \alpha^6.\alpha = (\alpha + 2).\alpha = \alpha^2 + 2\alpha = (2\alpha + 1) + 2\alpha = \alpha + 1.$

$\alpha^8 = \alpha^7.\alpha = (\alpha + 1).\alpha = \alpha^2 + \alpha = (2\alpha + 1) + \alpha = 1.$

Ainsi $F_9 = \{ 0,\ 1,\ 2,\ \alpha,\ 2\alpha,\ 1 + \alpha, 1 + 2\alpha,\ 2 + \alpha,\ 2 + 2\alpha\}$

$F_9 = \{ 0,\ 1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6,\ \alpha^7\}.$

Donc α est une racine primitive huitième de l'unité . Et comme

$\varphi(8) = |\{m \in N \ / \leq 1 \leq m \leq 8 \text{ et } (m,8) = 1\}| = |\{1,3,5,7\}| = 4.$
Les autres racines primitives huitième de l'unité sont α^3, α^5, et α^7. Ainsi on trouve:

$$Q_8 = (x - \alpha^1)(x - \alpha^3)(x - \alpha^5)(x - \alpha^7).$$

En developpant ceci et en tenant compte que la multiplication dans F_9, en sa représentation en puissance de α, se fait en observant que:

$$\alpha^i.\alpha^j = \alpha^{i+j(\mathrm{mod}\,8)}$$

on trouve que $Q_8 = x^4 + 1$. Par la suite Q_8 n'est pas dans F_9 mais dans $F_3[x]$.

C'est à dire que Q_n a ses coéfficients dans F_p [21]. Soit α une racine primitive $n^{ième}$ de l'unité, alors il résulte que:

$$Q_n = \prod_i (x - \alpha^i)$$

où le produit est formé pour tout i avec $pgcd(i,n) = 1$. Le plynôme Q_n est degré $\varphi(n)$. Soit $n = kd$ ainsi α^k est d'ordre d, car $(\alpha^k)^d = \alpha^{kd} = \alpha^n = 1$, et est une racine primitive d^{ieme} de l'unité. Le d^{ieme} polynôme cyclotomique est de la forme :

$$Q_d = \prod_{p\,\mathrm{gcd}(i,d)=1} (x - \alpha^{ik}).$$

Toute racine $n^{ième}$ de l'unité est une racine primitive $d^{ième}$ de l'unité pour exactement un seul d. Par conséquent, on peut regrouper les racines $n^{ièmes}$ de l'unité ensemble et on obtient le résultat suivant:

Théorème 5.2.4 [21]

$$x^n - 1 = \prod_{d/n} Q_d \ \ (\textit{décomposition cyclotomique})$$

Un résultat important se déduit pour le polynôme cyclotomique Q_{p^m}, pour p premier et m un entier positif, à savoir:

Corollaire 5.2.5

$$Q_{p^m} = 1 + x^{p^{m-1}} + ... + x^{(p-1)\ p^{m-1}}.$$

En effet, du théorème précédent et sachant que les diviseurs de p^m, p premier, sont 1, p, $p^2, ..., p^m$ alors:

$$\begin{aligned} x^{p^m} - 1 &= \prod_{d/p^m} Q_d = Q_{1.} Q_P ... Q_{P^m} \\ Q_{P^m} &= \frac{x^{p^m} - 1}{Q_{1.} Q_P ... Q_{P^{m-1}}} \\ &= \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} \\ &= 1 + x^{p^{m-1}} + ... + x^{(p-1)\ p^{m-1}}. \end{aligned}$$

Exemple 5.2.6

Soit dans F_2, le polynôme $x^{15} - 1$, donnons sa décomposition cyclotomique. Comme les diviseurs de 15 sont: $1, 3, 5, 15$, on a

$$x^{15} - 1 = \prod_{d/15} Q_d = Q_1 Q_3 Q_5 Q_{15}$$

Où $Q_1 = x+1$, $Q_3 = x^2+x+1$, $Q_5 = x^4+x^3+x^2+x+1$ et $Q_{15} = x^8+x^7+x^5+x^4+x^3+x+1$.
En effet, de la formule $Q_n = \prod_i (x - \alpha^i)$, où $p \gcd(i, n) = 1$, avec $1 \leq i \leq n$, et comme
$\varphi(15) = |\{m \in N \ / \ 1 \leq m \leq 15 \text{ et } (m, 15) = 1\}| = |\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$.
Et la caracteristique 2 de F_2 ne divise pas 1, 3, 5 et 15 on a d'aprés le corollaire (5.2.5)
$\deg Q_1 = \varphi(1) = 1$ et $Q_1 = x + 1$.
$\deg Q_3 = \varphi(3) = 2$, et

$$Q_3 = \frac{x^{3^1} - 1}{x^{3^{1-1}} - 1}$$

$$= \frac{x^3 - 1}{x - 1}$$
$$= x^2 + x + 1.$$

$\deg Q_5 = \varphi(5) = 4$, et

$$Q_5 = \frac{x^{5^1} - 1}{x^{5^{1-1}} - 1}$$

$$= \frac{x^5 - 1}{x - 1}$$
$$= x^4 + x^3 + x^2 + x + 1.$$

Q_1, Q_3, Q_5 sont irréductibles sur F_2. Comme $15 \mid (2^4 - 1)$ et $\deg Q_{15} = \varphi(15) = 8$, on conclut que Q_{15} est le produit de deux polynômes irréductibles de $deg = 4$ à savoir:

$$Q_{15} = (x^4 + x + 1)(x^4 + x^3 + 1)$$

D'où l'écriture du polynôme $x^{15} - 1$ en produit de polynômes irréductibles sur F_2.

A coté du degré d'un polynôme, il y a un important entier naturèl appelé *l'ordre* d'un polynôme.

Definition 5.2.7

Soit $0 \neq f \in F_q[x]$. *Si* $f(0) \neq 0$, *alors le plus petit entier naturel* e *tel que* f *divise* $(x^e - 1)$ *est appelé l'ordre de* f.

Théorème 5.2.8 [21]

Soit $f \in F_q[x]$ *un polynôme irréductible sur* F_q *de* $\deg = m \geq 2$. *Alors l'ordre de* f *est égal à l'ordre de toute racine de* f *dans* F_q.

Corollaire 5.2.9 [20]

Si $f \in F_q[x]$ *est irréductible sur* F_q *de degré* m, *alors l'ordre de* f *divise* $q^m - 1$.

Lemme 5.2.10 [21]

$Q_n[x] \in F_q[x]$ *est irréductible si, et seulement si l'ordre multiplicatif de* q *modulo* n *est* $\varphi(n)$, *c'est à dire si* $q^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$.

ANNEXE II Raffinements apportés à nos résultats sur la divisibilté des trinômes $x^{am}+x^{bs}+1$ sur F_2

Pour garder le texte intégral des raffinements rapportés à notre résultat, j'ai laissé le texte original(en anglais).

We extend Welch's criterion for testing if an irreducible polynomial divides trinomials $x^m + x^s + 1$ to the trinomials $x^{am} + x^{bs} + 1$. We give a refinement of a necessary condition for divisibility of trinomials $x^{am} + x^{bs} + 1$ by a given irreducible polynomial [26].

1. Divisibility of trinomials $x^{am} + x^{bs} + 1$

In this section we consider the conditions for divisibility of trinomials $x^{am} + x^{bs} + 1$ by a given irreducible polynomial over F_2. Let f be an irreducible polynomial of degree n over F_2 and a and b be positive integers. In [26] it was proved that if there exist positive integers m and s such that f divides $x^{am} + x^{bs} + 1$, then a and b are not divisible by $2^n - 1$. Below we give a refinement of this result.

2. Theorem[5, 17]: *Let f be an irreducible polynomial of order $e > 1$ over F_2 and a and b be positive integers. If there exist positive integers m and s such that f divides trinomial $x^{am} + x^{bs} + 1$ $(am > bs)$, then am, bs and $am - bs$ are not divisible by e.*

Proof: Let α be any root of f in a certain extension of F_2. If am is divided by e, then $\alpha^{am} = 1$, so f divides a polynomial $x^{am} + 1$. Since $e > 1$, $f(0) \neq 0$ and thus f does not divide x^{bs}. Therefore f can not divide the trinomial $x^{am} + x^{bs} + 1$. The case where bs is divided by e is very similar. Suppose $am - bs$ is divided by e. Then in the same way as above we see easily that $x^{am-bs} + 1$ is divided by f and thus $x^{am} + x^{bs} + 1 = x^{bs}(x^{am-bs} + 1) + 1$ is not divisible by f. □

If f is an irreducible polynomial of order e and degree n over F_2, then e is a divisor of $2^n - 1$. Thus the above theorem derives directly the result in [26].

Finally we consider the criterion for testing if an irreducible polynomial divides trinomials of type $x^{am} + x^{bs} + 1$ over F_2.

Theorem [6, 17] *Let f be an irreducible polynomial of order e and degree n over F_2 and a and b be positive integers. Then f divides trinomials $x^{am} + x^{bs} + 1$ if and only if $gcd(1 + x^{e_1}, 1 + (1 + x)^{e_2})$ has degree greater than 1, where*

$$e_1 = \frac{e}{gcd(a, e)}, \ e_2 = \frac{e}{gcd(b, e)}.$$

Proof. Let α be any root of f. Then the order of α in the multiplicative group $F_{q^n}^*$ is e and 1, α, α^2,$\cdots$, α^{e-1} are distinct roots of $x^e - 1$. Since

$$x^e - 1 = \prod_{d/e} Q_d$$

for every $i(0 \leq i \leq e - 1)$, α^i is a root of an irreducible polynomial whose order is a divisor of e. In particular, α^a has order $e_1 = \frac{e}{gcd(a,e)}$ and α^a, α^{2a}, $\cdots$, $\alpha^{(e-1)a}$ are all roots of $C_{e_1}(x) := \frac{x^{e_1}-1}{x-1}$. Similarly α^b, α^{2b}, $\cdots$, $\alpha^{(e_2-1)b}$ are all roots of $C_{e_2}(x) := \frac{x^{e_2}-1}{x-1}$ and thus $1 + \alpha^b, 1 + \alpha^{2b}$, $\cdots$, $1 + \alpha^{(e_2-1)b}$ are all roots of $C_{e_2}(x + 1)$. Hence α is a root of trinomial $x^{am} + x^{bs} + 1$ if and only if $C_{e_1}(x)$ and $C_{e_2}(x + 1)$ have common root. This is equivalent to the fact that $gcd(1 + x^{e_1}, 1 + (1 + x)^{e_2})$ has degree greater than 1. □

Put $a = b = 1$ in Theorem 6. Then we have Welch's criterion.

Problèmes Ouverts:

En perspéctives nous proposons les problèmes ouverts suivants:

Question 1: Peut-on généraliser la **caractérisation** du polynôme générateur d'un code cyclique **iso-dual** sur d'autres corps finis F_p, pour $p = 7, 11, 13, ..., ?$

Question 2: Peut-on estimer la **densité de probabilité**, en fonction de a et b, pour qu'un trinôme $x^{am} + x^{bs} + 1$ soit irréductible sur F_2 par rapport à la famille $F(1, 1)$?

Question 3: Peut-on étendre nos résultats sur la divisibilité des trinômes sur F_2 pour les **quadrinômes** $x^{am} + x^{bs} + x^{ct} + 1$ sur le corps fini F_3?

Conclusion:

- La **caractérisation** du polynôme générateur d'un code **cyclique iso-dual** est un problème ouvert défiant et nous avons réussi, dans ce contexte, à construire **sept classes** de codes cycliques **iso-duaux** sur $GF(3)$ et **trois classes** de codes cycliques **iso-duaux** sur $GF(5)$.

Pour les codes cycliques $C[n, \frac{n}{2}]$ sur $GF(p)$, avec $p = 3$ ou 5, dans le cas où n est pair non multiple respectivement de 3 et 5, nous avons trouvé de nouveaux résultats sur **l'optimisation** de la distance minimum de ces codes où la longueur n peut atteindre 74 pour les codes cycliques **ternaires** et 42 pour les codes cycliques sur $GF(5)$. Notant que la distance minimum optimale des codes cycliques $C[42, 21]_5$ iso-duaux qu'on a trouvé est identique à celle du code auto-dual de même paramètres(tables de P. Gaborit) [10].

- Malgré que le nombre de polynômes irréductibles de degré fixé n sur un corps fini F_q est connu, on ne peut pas en général, les expliciter tous si les deux entiers positifs n et q deviènnent assez grand. Mais nous avons pu sur F_2 trouver de **nouvelles générations** de polynômes irréductibles de la forme $x^{am} + x^{bs} + 1$ avec a, b fixés et m, s à déterminer en allant jusqu'à **2000** comme degré du polynôme et nous avons prouvé une propriété généralisant les résultats de **Golomb** et **Lee** [14] sur la divisibilité de ces trinômes par un polynôme irréductible sur F_2. Notons que ce résultat a fait l'objet d'une référence dans l'article [17] " R. Kim, W. Koepf, v 3, 2009, no 4, 189-197. IJA."

BIBLIOGRAPHIE

[1] **N. Bourbaki,** *"Algèbre. Eléments de Mathématique*s", Masson, Paris, 1981.

[2] **H. Cohen,** "*A Course In Computational Algebraic NumberTheory "*, Springer-Verlag, Berlin Heidelberg, 1993.

[3] **R. Daskalov,** "*Some high-rate linear codes over GF(5) and GF(7)*", Probl. Pered. Inform, vol 43, 2, pp. 65-73, 2007.

[4] **R. Daskalov, P. Hristov**, **E. Metodieva**, "*New minimum distance bounds for linear codes over GF(5)*", Discrete. Mathematics, vol. 275, pp.97-110, 2004.

[5] **R. Daskalov, T. Gulliver**, "*Bounds on minimum distance for linear codes over GF(5)*", AAECC 9, pp. 521-546, 1999.

[6] **Jean-Pierre Escofier:** *Théorie de Galois* ($2^{ème}$ édition), Dunod, Paris, 2000.

[7] **M.V. Eupen and P. Lisonek** "*Classification of Some Optimal Ternary Linear Codes of Small Length* " Designs, Codes and Cryptography, vol 10, pp. 63-84, 1997.

[8] **M. Grassl**, "*Bounds on the minimum distance of linear codes* ", [Electronic table; online], http://www.codetables.de.

[9] **M. Grassl, G. White**, "*New codes from chains of quasi-cyclic codes*", Proc. ISIT2005, Adelaide, Australia, pp. 2095-2099, 2005.

[10] **P. Gaborit**, "*Table of Self-Dual Codes over GF(3) and GF(5)* ", [tables; online], http://www.unilim.fr/pages_perso/philippe.gaborit/SD/GF5.htm.

[11] **T. A. Gulliver, N. Senkevitch** "*Optimal Ternary linear rate 1/2 codes* ". Designs, Codes and Cryptography vol 23, pp. 167-171, 2001.

[12] **T. A. Gulliver, P. R. J. Ostergard and N. Senkevitch** "*Optimal linear rate 1/2 codes over* F_5 *and* F_7". Discrete Mathematics, vol 265, pp. 59-70, 2003.

[13] **T. A. Gulliver and Patric. R. J. Ostergard**, "*Improved Bounds for Ternary Linear Codes of Dimension 7* ". IEEE. Trans. Inform. Theory, vol. 43, pp. 1377-1381, 1997.

[14] **W. Golomb and Pey-Feng Lee.** *Irreducible Polynomials Which Divide Trinomials Over GF(2), IEEE Vol. 53. pp.768-774. 2007.*

[**15**] **N. Hamada and Y. Watamori**, "*The nonexistence of ternary linear codes of dimension 6 and the bounds for n (6, d) , 1 d 243* " Math. Japon., vol 43, pp. 577-593, 1996.

[**16**] **R. Hill, D.E. Newton**, "*Optimal ternary linear codes"*, Designs Codes Cryptogr., vol. 2, pp.137-157, 1992.

[**17**] **R. Kim, W. Koepf**. *Divisibility of Trinomials by Irreducible Polynomials over* F_2", International Journal of Algebra,.vol 3, no 4, 189-197, 2009.

[**18**] **A. Kostrikin**: *Introduction à L'algèbre-Edition Mir*, Traduction française, 1981.

[**19**] **A. Kuroch:** *Algèbre Supérieur (TA)*- Edition Mir, 1977.

[**20**] **R. Lidl & H. Niederreiter:** *Finite Fields*-Addison-wesley Publishing Company, 1983.

[**21**] **R. Lidl & G. Pilz:** *Applied Abstract Algebra*-Springer-Verlag. New York, 1998.

[**22**] **Larry Joel Goldstein:** *Abstract Algebra. A First Course*-Printice-Hall, Inc, Englewood Cliffs, New Jersey, 1973.

[**23**] **F. J. MacWilliams and N. J. A. Sloane**, "*The Theory OF Error-Correcting codes*". North-Holland, Amsterdam, 1977.

[**24**] **C. Mangalo:** *Algèbre 1. De la théorie de Galois*-Edicef-Pusaf, Paris.1987.

[**25**] **T.Maruta**, Personal communication, 2002.

[**26**] **C. Mihoubi.** "*A Necessary Condition of the Divisibility of Trinomials* $x^{am}+x^{bs}+1$ *by any Irreducible Polynomial of degree r over GF(2)",* International Journal of Algebra, *vol. 2, No. 13, pp.645-648. 2008.*

[**27**] **C. Mihoubi.** "*Etude sur l'irréductibilité des polynômes* $x^m + x^s + 1$ *sur un corps fini*". Thèse de Magister, Université de M'sila, 2001.

[**28**] **C. Mihoubi.** "*Isodual Cyclic Codes of rate* $\frac{1}{2}$ *over GF(5)",* Int. J. Open Problems Comp. Maths., *vol 4, No 4, pp.33-39. 2011.*

[**29**] **C. Mihoubi and P. Solé.** "*Optimal and Isodual Ternary Cyclic Codes of rate* $\frac{1}{2}$ ", à paraitre dans le journal, Bulletion of Mathematical Sciences, Springer.

[**30**] **E. M. Rains and N. J. A. Sloane**, "*Self-dual codes, Handbook of Coding Theory*

" (V. S. Pless and W. C. Huffman, eds.), Elsevier, Amsterdam (1998).

[31] Steven Roman, "*Coding and Information Theory",* Springer Verlag 1992.

[32] R. Swan. "*Factorisation of polynomials over finite fields",* Pacific Journal of Mathematics, Vol 12 pp. 1099-1106.1962.

[33] J.H. Van Lint, *"Introduction to Coding Theory",* Springer-Verlag New York Inc,1982.

[34] J. F. Voloch, "*Computing the minimal distance of cyclic codes*", Comp and Applied Mathematics, Vol 24, pp.393-398, 2005.

ملخص الرسالة باللغة العربية

تصنيف الشفرات الخطية الدائرية الأفضلية [n, n/2] على الحقلين المنتهيين GF(3) و GF(5)

في هذا العمل نعتبر الشفرات الخطية ذات المردود 1/2 على الحقلين المنتهيين المذكورين ونركز اهتمامنا على الشفرات الدائرية المتكافئة منها. المشكل الرئيسي في نظرية التشفير هي إيجاد أحسن مسافة أصغريه التي من اجلها توجد الشفرة ذات الخصائص

$[n, k, d]$ على Fq

في هذا الإطار تمكنا من تقدير هذه المسافة بالنسبة للشفرات الدائرية ذات المردود 1/2 على الحقلين المنتهيين سالفي الذكر بحيث وصلنا إلى الطول 74 من اجل الشفرات الدائرية على الحقل المنتهي GF(3) و إلى الطول 42 من اجل هذه الشفرات على الحقل المنتهي GF(5).

كما تمكنا أيضا من بناء 7 أقسام من الشفرات الدائرية المتكافئة على الحقل المنتهي ذو ثلاثة عناصر و 3 أقسام من الشفرات الدائرية المتكافئة على الحقل المنتهي ذو خمسة عناصر.

و نعتبر أيضا كثيرات الحدود على الحقل المنتهي GF(2) التي لها استعمالات كثيرة و خاصة في نظرية التشفير الجبري.

اهتماماتنا تخص قابلية قسمة ثلاثي الحدود $X^{am}+X^{bs}+1$ من اجل $m > s \geq 1$ على كثير حدود T غير قابل للتحليل درجته r على الحقل المنتهي GF(2).

و في الأخير توصلنا إلى النتيجة التالية :

إذا وجد عددان طبيعيان m, s حيث ثلاثي الحدود $X^{am}+X^{bs}+1$ يكون قابلا للقسمة على كثير حدود T غير قابل للتحليل درجته r على GF(2) فإن a و b غير قابلين للقسمة على $(2^r -1)$.