

Trinômes irréductibles sur F2 et codes cycliques ternaires de rendements 1/2

Cherif Mihoubi

▶ **To cite this version:**

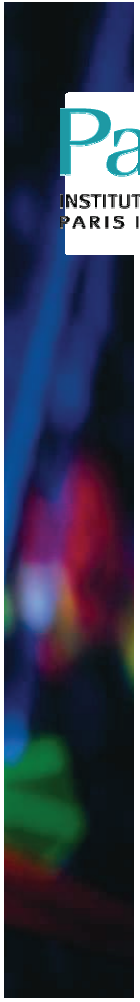
Cherif Mihoubi. Trinômes irréductibles sur F2 et codes cycliques ternaires de rendements 1/2. Mathématiques générales [math.GM]. Télécom ParisTech, 2012. Français. NNT : 2012ENST0084 . tel-01145440

HAL Id: tel-01145440
https://pastel.hal.science/tel-01145440

Submitted on 24 Apr 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2012-ENST-0084

EDITE ED 130

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

Télécom ParisTech

présentée et soutenue publiquement par

Cherif Mihoubi

21 décembre 2012

Trinômes Irréductibles sur F2 et Codes Cycliques Ternaires de Rendement 1/2

Directeur de thèse : **Patrick Solé**

Jury

M. Gérard Cohen,	Président, Télécom ParisTech	Professeur
Mme. Sihem Mesnager,	Examinatrice, Université Paris 8	Maître de conférences
M. Jean Francis Michon,	Rapporteur, Université de Rouen	Professeur
M. Abdelkader Necer,	Rapporteur, Université de Limoges	Maître de conférences
M. Hugues Randriam,	Examinateur, Télécom ParisTech	Maître de conférences
M. Patrick Solé,	Directeur de thèse, Télécom ParisTech	Directeur de recherche

T H È S E

Télécom ParisTech
Ecole de l'Institut Télécom – membre de ParisTech
46, rue Barrault – 75634 Paris Cedex 13 – Tél. + 33 (0)1 45 81 77 77 – www.telecom-paristech.fr

Résumé

– En considérant les polynômes sur le corps fini de Galois à deux éléments, notre intention porte sur la divisibilité des trinômes $x^{am}+x^{bs}+1$, pour $m > s \geq 1$ par un polynôme irréductible de degré r, pour cela, nous avons réalisé le résultat : *S'il existe m, s des entiers positifs tels que le trinôme $x^{am}+x^{bs}+1$ soit divisible par un polynôme irréductible de degré r sur $\mathbb{F}_2$, alors a et b ne sont pas divisibles par* (2^r-1).

Pour ce type de trinômes nous conjecturons que le rapport $\pi_M(a,b)/\pi_M(1,1)$ tend vers une limite finie (dépendant de a et b) quand M tend vers l'infini.

– Notre recherche porte ensuite sur les codes cycliques de rendement $\frac{1}{2}$ sur les deux corps finis $\mathbb{F}_3$ et $\mathbb{F}_5$ et nous accentuons notre recherche sur ceux iso duaux. Le problème central dans la théorie du codage est trouver la plus grande distance minimum d_q pour laquelle un code de paramètres $[n,k,d]$ sur $\mathbb{F}_q$ existe.
Dans ce contexte nous avons réussi à optimiser cette distance pour les codes cycliques de taux $\frac{1}{2}$ sur $\mathbb{F}_3$ et $\mathbb{F}_5$ en allant jusqu'à la longueur 74 pour les codes ternaires et 42 pour ceux sur $\mathbb{F}_5$. 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.

Mots clés : Polynômes irréductibles, Divisibilité, Corps finis, Codes cycliques, Distance minimum, Codes iso-duaux.

Abstract

– Considering polynomials over the Galois finite fields for two elements, our intention stand over the divisibility of the trinomials $x^{am}+x^{bs}+1$, for $m > s \geq 1$ by an irreducible polynomial of degree r, for this, 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 of degree r over $\mathbb{F}_2$, then a and b are not divisible by* (2^r-1).

For this type of trinomials we conjectured that the ratios $\pi_M(a,b)/\pi_M(1,1)$ tend to a finite limit (dependently of a and b) when M tend to infinity.

– Our research stand at sequel on the cyclic codes of rate $\frac{1}{2}$ over the two finite fields $\mathbb{F}_3$ and $\mathbb{F}_5$ and we check our research over whose are isodual.
The so-called fundamental problem in coding theory is finding the largest value of d_q for which a code of parameters $[n,k,d]$ over $\mathbb{F}_q$ exists.
In this context we have successfully optimize this distance for the cyclic codes of rate $\frac{1}{2}$ over $\mathbb{F}_3$ and $\mathbb{F}_5$ up to length 74 for the ternary cyclic codes and 42 for whose over $\mathbb{F}_5$. 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.

Key words : Irreducible polynomials, Divisibility, Finite fields, Cyclic codes, Minimum distance, Isodual codes.

Thèse

Présentée pour obtenir le grade de docteur de l'Ecole Nationale Supérieure des Télécommunications

Spécialité : Communications et Electronique

Cherif Mihoubi

Trinômes Irréductibles sur F_2 et Codes Cycliques Ternaires de Rendement 1/2

Soutenue le : 21/12/2012

Devant le jury composé de :

M. Gérard Cohen	**Président**	**Professeur**
Mme. Sihem Mesnager	**Examinatrice**	**Maître de conférences**
M. Jean Francis Michon	**Rapporteur**	**Professeur**
M. Abdelkader Necer	**Rapporteur**	**Maître de conférences**
M. Hugues Randriam	**Examinateur**	**Maître de conférences**
M. Patrick Solé	**Directeur de thèse**	**Directeur de recherche**

Remerciements

Je tiens à exprimer toute ma gratitude aux personnes qui m'ont aidé, encouragé, soutenu, pour mener à bien ce travail de thèse.

Je tiens à remercier M. Patrick Solé d'avoir accepté de diriger ce travail et de créer autour de moi un environnement de recherche par ses conseils, ses encouragements et son soutien permanent.

Comme je remercie M. Gérard Cohen, pour avoir accepté de présider ce jury et de ne cesser de me donner des conseils et des suggestions.

Je remercie également Mme Sihem Mesnager, Messieurs Jean Francis Michon, Abdelkader Necer et Hugues Randriam, pour avoir accepté de juger ce travail et de faire partie du jury.

Mes remerciements vont encore une fois à M. G. Cohen pour m'avoir dédié, en 2008, le livre "*Codes Correcteurs d'Erreurs*" et à Messieurs A. Necer et J. F. Michon pour leur lecture attentive, de mon manuscrit, leurs corrections proposées et leurs remarques constructives, sans lesquelles, le manuscrit ne peut être dans son état actuel.

Je ne peux oublier de remercier M. R. Le Bidan enseignant chercheur à l'enst Brest, avec qui j'ai fait mes débuts en théorie du codage, pour son soutien permanent, sa gentillesse et ses précieuses directives durant mon stage au département signal et communications en juin 2007 ainsi que M. P. Zimmermann du Loria-Nancy France, pour toutes ses aides précieuses et ses conseils durant mon passage en septembre- octobre 2007.

Un très grand merci à Mmes Florence Besnard et Chantal Cadiat pour leur aide apportée, leur patience et leur grande gentillesse.

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

Table des matières

Remerciements....2

Notations....5

Introduction générale....7

Chapitre 1 Divisibilité des trinômes $x^{am}+x^{bs}+1$ par un polynôme irréductible sur $\mathbb{F}_2$

1.1 Introduction....10

1.2 Théorèmes de base sur la divisibilité des trinômes $x^m + x^s + 1$ par un polynôme irréductible sur $\mathbb{F}_2$....12

1.3 Polynômes cyclotomiques et divisibilité des trinômes $x^m + x^s + 1$ sur $\mathbb{F}_2$....13

1.4 Polynômes réciproques et divisibilité des trinômes $x^m + x^s + 1$ sur $\mathbb{F}_2$....16

1.5 Condition nécessaire de divisibilité des trinômes $x^{am} + x^{bs} + 1$ par un polynôme irréductible sur $\mathbb{F}_2$....17

1.6 Conjecture....22

1.7 Généralisations apportées à notre résultat sur les trinômes $x^{am}+x^{bs}+1$....25

Chapitre 2 Codes linéaires, codes cycliques sur corps fini

2.1 Introduction....27

2.2 Paramètres d'un code....27

2.3 Codes linéaires sur $\mathbb{F}_q$....28

2.4 Codes cycliques sur $\mathbb{F}_q$....31

2.5 Exemples historiques de codes correcteurs....40

Chapitre 3 Codes cycliques optimaux, iso-duaux sur $\mathbb{F}_3$

3.1 Introduction....42

3.2 Codes cycliques iso-duaux sur $\mathbb{F}_3$....42

3.3 Codes cycliques optimaux sur $\mathbb{F}_3$.....45
3.4 Table des valeurs de $d_I(n)$ et $d_C(n)$ 59

Chapitre 4 Codes cycliques optimaux, iso-duaux sur $\mathbb{F}_5$
4.1 Introduction.....60
4.2 Codes cycliques iso-duaux sur $\mathbb{F}_5$.....60
4.3 Codes cycliques optimaux sur $\mathbb{F}_5$.....65
4.4 Table des valeurs de $d_I(n)$ et $d_C(n)$.....72

Annexe 1 Calcul de la densité des trinômes $x^{am}+x^{bs}+1$ sur $\mathbb{F}_2$...74

Annexe 2 Programme de recherche de la distance minimum..80

Conclusion.....86

Bibliographie.....87

Notations

(a, b) : pgcd(a, b)

$|G|$: l'ordre de G

$\cong$: isomorphe

deg p : degré de p

(p) : idéal engendré par p

$\overline{p}$: fonction polynomiale 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

$\mathbb{F}_q$: corps fini d'ordre q

$n!$: factorielle de n

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

Φ_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)

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

I : idéal de A

$\mathbb{F}_q[x]$: anneau des polynômes à coefficients dans $\mathbb{F}_q$

$\mathbb{F}_q^n$: espace vectoriel des vecteurs de longueur n sur $\mathbb{F}_q$

$\mathbb{F}_q[x]/(f)$: anneau des classes modulo $f(x)$

$\mathbb{F}_q[x]/(x^n - 1)$: 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 d'un code de paramètres $[n, k, d]$

x^t : transposé du vecteur x

G : matrice génératrice

H : matrice de parité

σ : permutation

S_n : groupe des permutations

$g(x)$: 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 pourqu'un code $[n, k, d]$ existe

$n_q(k, d)$: plus petite valeur de n pourqu'un code $[n, k, d]$ existe

d_C : maximale distance minimum d'un code cyclique

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

d_F : maximale distance minimum d'un code formellement auto-dual

Introduction générale

Les origines de la théorie des corps finis sont apparues au XVII^{e} et XVIII^{e} 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 $\mathbb{F}_p$, où p est premier. Dans son papier "*Sur la théorie des nombres*" E. Galois [56] marque le début de la théorie des corps finis et conçoit une construction d'une extension de corps de $\mathbb{F}_p$, et utilisa une racine imaginaire i d'un polynôme irréductible sur $\mathbb{F}_p$, de degré n, et montre que l'ensemble des polynômes

$$a_0 + a_1 i + \ ... \ + a_{n-1} i^{n-1}, \text{ où pour } k \in \{0,\ 1,\ ... \ , n-1\}\,,\ a_k \in \mathbb{F}_p$$

est un corps de p^n éléments.

Golomb et Lee [28] développent la théorie des polynômes irréductibles qui divisent, ou ne divisent pas, des trinômes sur $\mathbb{F}_2$ et considèrent certaines familles de polynômes de degré $p > 3$ premier qui ne divisent pas des trinômes.

Dans leur papier [39], Kim et Koepf considèrent certaines conditions pour lesquelles des polynômes irréductibles divisent des trinômes sur $\mathbb{F}_2$. En ce sens, une condition de divisibilité des trinômes auto-réciproques par un polynôme irréductible est établie et l'extension du critère de Welch pour tester si un polynôme irréductible divise les trinômes $x^{am} + x^{bs} + 1$ est faite.

- Soit $(a, b) \in \mathbb{N}^2$, $(m, n) \in \mathbb{N}^2$, en considérant les trinômes du type $x^{am} + x^{bs} + 1$, sur le corps $\mathbb{F}_2$, nous avons étendu un résultat dû à **Golomb** et **Lee** [28] :

• *S'il existe m, s des entiers positifs tels que le trinôme $x^{am} + x^{bs} + 1$ soit divisible par un polynôme irréductible 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 [49] paru en 2008 et qui a été pris comme référence dans l'article [39].

Soit $F(a,b)$ =$\{x^{am}+x^{bs}+1,\ 0<bs<am\}$, où a,b sont des entiers positifs tels que le trinôme x^a+x^b+1 soit irréductible sur $\mathbb{F}_2$, et $\pi_M(a,b)$ le nombre des trinômes T irréductibles de la famille $F(a,b)$ de degré $\leqslant M$. Alors, nous conjecturons que le rapport $\frac{\pi_M(a,b)}{\pi_M(1,1)}$ tend vers une limite $L(a,b)$ finie quand M tend vers l'infini.

La théorie des codes s'est développée pour répondre au problème de correction des erreurs introduites dans un système de transmission de l'information. A l'origine développée par des ingénieurs en électronique, elle constitue maintenant une branche des mathématiques discrètes. Cette théorie et ces trois domaines d'application que sont la compression, la détection/ correction d'erreurs et la cryptographie utilisent la théorie des corps finis.

Une classe importante de codes est celle des codes auto-duaux [60], à cause de ses liens avec la théorie des invariants, des designs combinatoire, et des formes modulaires. Cette classe est une sous-classe des codes formellement auto-duaux [16]. Dans ce travail, nous considérons les codes cycliques de rendement 1/2 sur les deux corps finis $\mathbb{F}_3$ et $\mathbb{F}_5$. Une partie importante de ces codes est celle des codes cycliques iso-duaux, c'est à dire les codes cycliques qui sont équivalents à leurs duaux. Les codes iso-duaux sont en particulier formellement auto-duaux.
La question qu'on se pose sur les codes iso-duaux est un problème ouvert original et récent :

Peut-t-on caractériser le polynôme générateur d'un code cyclique iso-dual ?

Notre étude porte sur les codes cycliques sur un corps fini $\mathbb{F}_p$, pour $p=3,\ 5$; comme étant des idéaux principaux de l'anneau $\mathbb{F}_p[x]/(x^n-1)$.
- En considérant les codes cycliques de paramètres $[n,\ \frac{n}{2}]$, pour n pair, non multiple de 3 et de 5 respectivement sur $\mathbb{F}_3$ et sur $\mathbb{F}_5$, nous avons contribué à de nouveaux résultats sur l'**optimisation** de la distance minimum d'un code cyclique et sur la **construction** du polynôme générateur d'un code cyclique **iso-dual**. A cet effet**,** nous avons réussi à construire **sept** classes de codes cycliques iso-duaux de paramètres $[n,\ \frac{n}{2}]_3$ et **trois** classes

de codes cycliques iso-duaux de paramètres $[n, \frac{n}{2}]_5$.

Notre construction des codes cycliques iso-duaux sur $\mathbb{F}_3$ et $\mathbb{F}_5$, est faite respectivement jusqu'à la longueur 74 et 42.

- Résultat qui a fait l'objet d'un article [51] paru en 2011 au journal "Int. J. Open Problems Comp. Maths" pour les codes cycliques iso-duaux sur $\mathbb{F}_5$ et d'un autre article avec P. Solé [52] sur les codes cycliques optimaux et iso-duaux sur $\mathbb{F}_3$ paru en juillet 2012 au journal "Bulletin of Mathematical Sciences".

Le présent travail est subdivisé en quatre chapitres :

- Dans le chapitre 1, nous évoquons les principaux résultats sur la divisibilité des trinômes $x^m + x^s + 1$ par un polynôme irréductible sur $\mathbb{F}_2$ et nous présentons la preuve de notre contribution indiquée ci-dessus.
- Dans le chapitre 2, nous présentons quelques préliminaires sur les codes cycliques sur un corps fini que nous en aurons besoin dans la suite.
- Dans les chapitres 3 et 4 , après avoir présenté une caractérisation des codes cycliques iso-duaux, nous exposons notre principale contribution sur l'optimisation de la distance minimum d'un code cyclique, et les résultats originaux sur la construction du polynôme générateur d'un code cyclique iso-dual sur $\mathbb{F}_p$, $p = 3, 5$.
- En annexe 1, nous présentons le calcul de la densité des trinômes $x^{am} + x^{bs} + 1$ sur $\mathbb{F}_2$ dont le degré est borné par une constante entière M.
- En annexe 2, nous présentons le programme de recherche de la distance minimum d'un code cyclique sur les deux corps finis $\mathbb{F}_3$ et $\mathbb{F}_5$.

Chapitre 1 **Divisibilité des trinômes $x^{am}+x^{bs}+1$ par un polynôme irréductible sur $\mathbb{F}_2$**

1.1 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 et la cryptographie. Les trinômes irréductibles continuent à présenter une grande difficulté pour les chercheurs malgré les résultats qui paraissent régulièrement.

Motivé par les travaux de I. F. Blake, S. Gao et R. J. Lambert [2], R. Brent et P. Zimmermann [5] définissent le trinôme presque primitif (irréductible), qui est le trinôme avec un facteur primitif, et proposent des algorithmes pour rechercher les trinômes presque primitifs. Doche [15] appelle ces trinômes "trinômes presque irréductibles", comme trinômes redondants.

De nombreux résultats sont connus concernant les polynômes irréductibles auto-réciproques, dans cette démarche, J. L. Yucas et J. L. Mullen [68] étudient en détail l'ordre des polynômes irréductibles auto-réciproques sur des corps finis. Dans [42], il est mentionné que si f est un polynôme irréductible de degré n sur $\mathbb{F}_q$ avec $f(0) \neq 0$, alors l'ordre de f , qui divise $q^n - 1$, est égal l'ordre de toute racine de f dans le groupe multiplicatif $\mathbb{F}_q^{*n}$. Dans le cas $q = 2$, l'ordre de f est toujours un entier impair [39]. De même nous pouvons voir dans [42], qu'un polynôme f irréductible et auto-réciproque divise des trinômes dans $\mathbb{F}_2[x]$ ssi l'ordre de f est un multiple de 3.

Golomb et Lee [28] développent la théorie des polynômes irréductibles qui divisent, ou ne divisent pas, des trinômes sur $\mathbb{F}_2$ et considèrent certaines familles de polynômes qui ne divisent pas des trinômes. En effet, ils ont prouvé que pour un entier premier $p > 3$, s'il existe un polynôme irréductible d'ordre p, alors tous les polynômes irréductibles ayant le même ordre ne divisent pas des trinômes.

Kim et Koepf [39] considèrent certaines conditions pour lesquelles des polynômes irréductibles divisent des trinômes sur $\mathbb{F}_2$. En ce sens, une condition de divisibilité des trinômes auto-réciproques par un polynôme irréductible est établie, ils donnent une description de cette condition et présentent leur résultat principal : Soit f un polynôme irréductible sur $\mathbb{F}_2$, f divise des trinômes auto-réciproques ssi l'ordre de f est un multiple de 3. Exposent ensuite leur extension du critère de Welch pour tester si un polynôme irréductible divise les trinômes $x^{am} + x^{bs} + 1$.

Soit a, b, m et s dans $\mathbb{N}$. Nous nous intéressons à la divisibilité du trinôme de la forme

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

par un polynôme irréductible, sur le corps fini $\mathbb{F}_2$.

1.2 Primitivité d'un polynôme irréductible sur un corps fini

Définition 1.2.1

Soit T un polynôme irréductible de degré $r > 1$ sur $\mathbb{F}_2$. La primitivité de T est le plus petit entier positif t tel que T divise $x^t - 1$.

Certains auteurs appellent la primitivité de T l'exposant ou l'ordre.
La primitivité de $T(x)$ peut être définie comme étant l'ordre de x dans le groupe multiplicatif $\mathbb{F}_2[x]/(T(x))$.

Exemple 1.2.2

Considérons le polynôme $T = x^4 + x^3 + x^2 + x + 1$ irréductible sur $\mathbb{F}_2$ et faisons les divisions successives de $x^t - 1$ par T pour $t = 2, 3, 4, 5, ...,$ sur $\mathbb{F}_2$.

$$
\begin{aligned}
x^2+1 &\equiv x^2+1 \bmod (T)\\
x^3+1 &\equiv x^3+1 \bmod (T)\\
x^4+1 &\equiv x^3+x^2+x \bmod (T)\\
x^5+1 &\equiv (x+1)(x^4+x^3+x^2+x+1) \bmod (T)\\
x^5+1 &\equiv 0 \bmod (T)
\end{aligned}
$$

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

1.3 Théorèmes de base sur la divisibilité des trinômes x^m+x^s+1 par un polynôme irréductible sur $\mathbb{F}_2$

Théorème 1.3.1 [28]

Soit T un polynôme irréductible de degré $r > 1$ sur $\mathbb{F}_2$, ayant α comme racine dans une extension de $\mathbb{F}_2$. Le polynôme T divise un trinôme si et seulement s'il existe des entiers i et j tels que $\alpha^i + \alpha^j = 1$.

Théorème 1.3.2 [28]

Soit $r \in \mathbb{N}$ $(r > 1)$. Soit *T un polynôme irréductible de degré r sur $\mathbb{F}_2$. Si T divise un trinôme quelconque, alors il divise une infinité de trinômes.*

Preuve

Supposons que le polynôme T, de primitivité t, divise le trinôme $x^m + x^s + 1$.
De $\alpha^m + \alpha^s = 1$ et $\alpha^t = 1$ nous avons alors $\alpha^{\mu t} = 1$ et $\alpha^{\nu t} = 1$ et par conséquent $\alpha^{m+\mu t} + \alpha^{s+\nu t} = 1$. D'où le polynôme T divise la famille des trinômes $x^{m+\mu t} + x^{s+\nu t} + 1$ pour tous les entiers positifs μ et ν. □

Théorème 1.3.3 [28]

Soit $r \in \mathbb{N}$ $(r > 1)$. *Soit T un polynôme irréductible de degré r sur $\mathbb{F}_2$ et de primitivité*

t. Si T divise un trinôme quelconque, alors il divise un trinôme de degré $< t$.

Preuve

Nous supposons que $m > s \geq 1$ et que $m > t$. Il existe alors $m^{'}$ et $s^{'}$ dans $\{0,\ 1,\ ...,\ t-1\}$ tels que : $m = qt + m^{'}$, $s = q^{'}t + s^{'}$. Comme $\alpha^t = 1$ et $\alpha^m + \alpha^s = 1$, il vient $\alpha^{m^{'}} + \alpha^{s^{'}} = 1$. Par conséquent T divise un certain trinôme $x^{m^{'}} + x^{s^{'}} + 1$ de degré strictement inférieur à t. $\square$

1.4 Polynômes cyclotomiques et divisibilité des trinômes x^m+x^s+1 sur $\mathbb{F}_2$

Soit t un entier impair strictement supérieur à 3. Soit $\Phi_t(x)$ le t-ième polynôme cyclotomique. Nous savons d'après W. Golomb et P. F. Lee [28] que : il existe $r \in \mathbb{N}^*$ et f_1, f_2, ..., f_r des polynômes irréductibles de même degré tels que :

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

De plus les facteurs ont la même primitivité t.

Dans la suite nous noterons n le degré des facteurs de Φ_t et t leur primitivité commune.

Théorème 1.4.1 [28]

Si un des facteurs de Φ_t divise un trinôme, alors tous les facteurs 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 $x^t - 1$ forment toujours un groupe multiplicative cyclique. Si α est une racine primitive de $x^t - 1$, alors toute autre racine primitive est une puissance de α. Supposons que $f_i(x)$ divise le trinôme $x^m + x^s + 1$ alors, pour α racine d'un certain facteur,

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

Pour tout autre polynôme $f_j(x)$ de l'ensemble des diviseurs de $\Phi_t(x)$, supposons que l'une de 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 $x^{vm} + x^{vs} + 1$. □

En particulier, si un des $f_i(x)$ est 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 1.4.2 (Critère de Welch) [28]

Pour tout entier impair t, les polynômes irréductibles de $\mathbb{F}_2[x]$ et 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

$$c_t(x) = \frac{x^t - 1}{x - 1} = g_1(x)g_2(x)...g_r(x)$$

(non nécessairement le t-ième polynôme cyclotomique) la factorisation de $c_t(x)$ en facteurs irréductibles. Alors

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

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 $g_1(x)$, $g_2(x)$, ..., $g_r(x)$ sont :

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

où α est une racine primitive t-ième de l'unité.
Par conséquent, les racines des facteurs irréductibles de $c_t(1+x)$ sont :

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

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

Exemple 1.4.3
Considérons le polynôme $T = x^4 + x^3 + x^2 + x + 1$ irréductible sur $\mathbb{F}_2$ et de primitivité 5, le calcul du pgcd$[1+x^t, 1+(1+x)^t]$ pour $t = 5$ donne :

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

Ce qui explique bien que ce polynôme ne divise pas de trinômes sur $\mathbb{F}_2$.

1.5 Polynômes réciproques et divisibilité des trinômes x^m+x^s+1 sur $\mathbb{F}_2$

Définition 1.5.1

Soit $n \in \mathbb{N}^*$. *Soit f un polynôme de degré $n > 1$. Le polynôme réciproque de f est défini par :*

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

Si $f^*(x) = f(x)$, alors on dit que f est un polynôme auto-réciproque.

Remarque

Si α est une racine de $f(x)$, alors α^{-1} est aussi racine de $f(x)$.

Lemme 1.5.2 [28]

Soit p un nombre premier, $\Phi_p(x)$ le p^{e} polynôme cyclotomique dans $\mathbb{F}_2[x]$. Soit $r \in \mathbb{N}$ et

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

la décomposition de $\Phi_p(x)$ en facteurs irréductibles. Si l'un des facteurs irréductibles de $\Phi_p(x)$ est auto-réciproque, alors il ne divise pas un trinôme.

Preuve

Comme $f_i(x)$ est auto-réciproque, nous avons :

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

Si $f_i(x)$ est un trinôme, il s'écrit $x^{(p-1)/r} + x^{(p-1)/2r} + 1$, 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 exposant tel que $\alpha^p = 1$. □

1.6 Condition nécessaire de divisibilité des trinômes par un polynôme irréductible

1.6.1 Etude des familles $F(a,b)$ telles que $x^a + x^b + 1$ soit irréductible sur $\mathbb{F}_2$

Soit $(a,\ b) \in \mathbb{N}^2$, nous considérons 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 tels que le trinôme $x^a + x^b + 1$ soit irréductible sur le corps fini $\mathbb{F}_2$. Soit $\pi_M(a,b)$ le nombre de trinômes T irréductibles de la famille $F(a,b)$ de degré $\leqslant M$.

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

Le trinôme $x^3 + x^2 + 1$ étant irréductible sur le corps fini $\mathbb{F}_2$, nous allons étudier la famille

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

avec m, s des entiers positifs. Le calcul systématique, sur machine en utilisant Maple 10, de la densité de ces trinômes irréductibles et l'estimation du rapport $\pi_M(3,2)/\pi_M(1,1)$ pour $M = 100,\ 200,\ 300,\ 500,\ 700,\ 900,\ 1000,\ 1500,\ 2000$ a donné les résultats suivants :

M	$\pi_M(3,2)$	$\pi_M(1,1)$	$\pi_M(3,2)/\pi_M(1,1)$
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

2e cas F(5,3)

Pour le trinôme $x^5 + x^3 + 1$, irréductible sur le corps fini $\mathbb{F}_2$, nous faisons 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 $\pi_M(5,3)/\ \pi_M(1,1)$ pour $M = 100$, 200, 300, 500, 700, 900, 1000, 1500, 2000 donne :

M	$\pi_M(5,3)$	$\pi_M(1,1)$	$\pi_M(5,3)/\pi_M(1,1)$
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

3e 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 $\mathbb{F}_2$ donne :

M	$\pi_M(7,3)$	$\pi_M(1,1)$	$\pi_M(7,3)/\pi_M(1,1)$
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^{e} cas F(7,5)

Pour faire la comparaison de ces résultats avec ce que donne un polynôme réductible, nous choisissons le trinôme $x^7 + x^5 + 1$(non irréductible sur $\mathbb{F}_2$), et le calcul dans la famille

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

a donné les résultats suivants sur lesquels nous avons remarqué que la densité est doublement faible, d'où l'intérêt du choix d'un polynôme irréductible.

M	$\pi_M(7,5)$	$\pi_M(1,1)$	$\pi_M(7,5)/\pi_M(1,1)$
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** $\rightarrow \pi_M(\mathbf{a},\mathbf{b})/\pi_M(\mathbf{1},\mathbf{1})$

Pour M= 100, 200, 300, 500, 700, 900, 1000, 1500, 2000

Avec $(a = 3, b = 2)$, $(a = 5, b = 3)$, $(a = 7, b = 3)$, $(a = 7, b = 5)$ nous avons :

(a, b)\M	100	200	300	500	700	900	1000	1500	2000
(3, 2)	0,098	0,098	0,11	0,11	0,10	0,10	0,11	0,10	0,11
(5, 3)	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,1
(7, 3)	0,07	0,07	0,07	0,08	0,08	0,08	0,08	0,08	0,07
(7, 5)	0,04	0,04	0,05	0,05	0,05	0,05	0,05	0,05	0,05

Nous remarquons que le rapport $\pi_M(a,b)/\pi_M(1,1)$ a tendance à se fixer vers un nombre bien déterminé et que la densité est nettement supérieure si nous choisissons le trinôme $x^a + x^b + 1$ irréductible, que celle où le trinôme n'est pas irréductible.

1.6.2 Condition nécessaire de divisibilité des trinômes par un polynôme irréductible

1.6.2.1 Concepts généraux

Le théorème suivant dû à Swan est un important résultat sur la non-existence, dans certains cas, de trinômes irréductibles sur F_2.

1.6.2.2 Théorème de Swan [65]

Soit $n > m > 0$ et supposons que soit n est impair, soit m est impair. Alors le trinôme $x^n + x^m + 1$ admet un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$ si et seulement si, nous sommes dans l'une des situations suivantes :

(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 $n \equiv \pm 1 (\mathrm{mod}\, 8)$*

Maintenant nous allons faire une recherche expérimentale des trinômes irréductibles sur $\mathbb{F}_2$ de la forme $x^{am} + x^{bs} + 1$ pour tous les couples d'entiers $(a,\ b)$ tels que $a \leq 10$ et $b \leq 10$.

1.6.2.3. Résultats obtenus

Notre étude est axée sur la recherche de familles de trinômes sur le corps fini $\mathbb{F}_2$ qui produisent une grande proportion de polynômes irréductibles. Une recherche expérimentale a été faite, en particulier sur les trinômes du type $x^{5m} + x^{3s} + 1$, $x^{7m} + x^{3s} + 1$ ou $x^{7m} + x^{5s} + 1$, ce qui a permis d'explorer plusieurs pistes.

Le calcul systématique de la densité, c'est-à-dire le rapport du nombre de trinômes irréductibles au nombre de trinômes quelconques (i.e., $a = b = 1$) de la forme

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

pour a, b entiers positifs, et M une borne fixée, $M = 100, 300, 500$ a été fait (voir tableau en annexe 1), ce qui a donné les résultats suivants où nb représente le nombre de trinômes irréductibles et *total* indique le nombre de trinômes quelconques de la famille $F(a, b)$.

Pour M = 1000

Nous reprenons le même calcul, mais avec les couples (a, b) dont le rapport $nb/total$ est signifiant, c'est à dire dont la densité est importante (en caractères gras dans le précédent tableau).

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

Après tous ces calculs, nous constatons que le rapport $\frac{\pi_M(a,b)}{\pi_M(1,1)}$ tend vers une limite finie, dépendant de a et b, quand M tend vers l'infini. Nous proposons alors la conjecture suivante :

Conjecture

Soit $F(a,b) = \{x^{am} + x^{bs} + 1,\ 0 < bs < am\}$ *avec* a, b *des entiers positifs, tels que le trinôme* $x^a + x^b + 1$ *soit irréductible sur* $\mathbb{F}_2$ *et* $\pi_M(a,b)$ *le nombre de trinômes* T *irréductibles de la famille* $F(a,b)$ *tels que le degré de* T *soit inférieur ou égal à une borne déterminée* M*. Alors le rapport* $\frac{\pi_M(a,b)}{\pi_M(1,1)}$ *tend vers une limite* $L(a,b)$ *finie quand* M *tend vers l'infini.*

Nous avons montré que les trinômes de la famille $x^{am} + x^{bs} + 1$ ne sont pas divisibles par les premiers polynômes irréductibles sur $\mathbb{F}_2$, 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, pour tous les couples entiers (a, b) avec $a \leqslant 10$ et $b \leqslant 10$, (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 1.6.2.4 [49]
Soit T un polynôme irréductible de degré $r > 1$ sur $\mathbb{F}_2$ et soient a, b des entiers non nuls. S'il existe 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 positifs.

1^{er} cas : Si $a \equiv 0\ mod(2^r - 1)$, a s'écrit $a = a_1\ (2^r - 1)$ 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 positifs.

2^e cas : Si $b \equiv 0\ mod(2^r - 1)$, la démonstration est identique à celle du 1^{er} cas.

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

Remarque :
La réciproque de ce théorème est fausse. D'après le théorème 1.3.3, si nous prenons $T = x^4 + x^3 + x^2 + x + 1$, irréductible sur $\mathbb{F}_2$ et de primitivité $t = 5$ (exemple 1.2.2) nous

ne trouvons pas de trinômes de degré strictement inférieur à 5 et qui soient divisibles par T (les seuls trinômes de degré 4, sur $\mathbb{F}_2$ 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 de relâcher les conditions sur le Théorème 1.6.2.4 pour avoir l'implication inverse.

Proposition 1.6.2.5 [49]
Soient r, a, b des entiers non nuls. S'il existe un polynôme T irréductible sur $\mathbb{F}_2$ de degré r et s'il existe 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
La preuve de la proposition 1.6.2.5 est identique à celle du théorème 1.6.2.4. Mais la réciproque est vraie pour les deux cas spéciaux suivants.

Remarque
- Pour $r = 2\times 3^k$, k un entier positif, il existe un polynôme $T = x^r+x^{r/2}+1$ *irréductible* sur $\mathbb{F}_2$ [10] et il existe $(m = 2r, s = r)$ tels que le polynôme T divise le trinôme $P = x^{2r}+x^r+1$ (ici $a = b = 1$) et $P = T^2$.

- De même d'après le théorème 1.3.2, 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 $(m = 2r,\ s = r)$. □

1.7 Généralisations apportées à notre résultat sur la divisibilité des trinômes

En voici le texte intégral des raffinements apportées à notre résultat sur la divisibilité des trinômes $x^{am} + x^{bs} + 1$ sur $\mathbb{F}_2$ et la présentation de l'extension du critère de Welch pour ce type de trinômes :

Nous allons faire l'extension du critère de Welch [28] pour tester si un polynôme irréductible sur $\mathbb{F}_2$ divise les trinômes $x^{am} + x^{bs} + 1$. Nous donnons un raffinement de la condition nécessaire de divisibilité des trinômes $x^{am}+x^{bs}+1$ par un polynôme irréductible quelconque présentée dans [49].

1.7.1 Divisibilité des trinômes $x^{am} + x^{bs} + 1$

Dans cette section nous considérons les conditions de divisibilité des trinômes $x^{am}+x^{bs}+1$ par un polynôme irréductible. Soit f un polynôme irréductible de degré n sur $\mathbb{F}_2$ et a, b des entiers positifs. Dans [49] il a été prouvé que s'ils existent des entiers positifs m et s tel que f divise $x^{am} + x^{bs} + 1$, alors a et b ne sont pas divisible par $2^n - 1$. Dans ce qui suit nous donnons un raffinement de ce résultat.

1.7.2 Théorème [5, 39]

Soit f un polynôme irréductible d'ordre $e > 1$ sur $\mathbb{F}_2$ et a, b des entiers positifs. S'ils existent des entiers positifs m et s tel que f divise le trinôme $x^{am} + x^{bs} + 1$ $(am > bs)$, alors *am, bs et $am - bs$ ne sont pas divisibles par e.*

Preuve

Soit α une racine quelconque de f dans une certaine extension de $\mathbb{F}_2$. Si am est divisible par e, alors $\alpha^{am} = 1$, ainsi f divise le polynôme $x^{am} + 1$. Comme $e > 1$, $f(0) \neq 0$ alors f ne divise pas x^{bs}. Par conséquent f ne divise pas le trinôme $x^{am} + x^{bs} + 1$. Le cas où bs est divisible par e est exactement similaire. Supposons que $am - bs$ est divisible par e. Alors de la même manière que précédemment, nous voyons facilement que $x^{am-bs} + 1$ est

divisible par f, et ainsi $x^{am} + x^{bs} + 1 = x^{bs}(x^{am-bs} + 1) + 1$ n'est pas divisible par$f$. □

Si f est un polynôme irréductible d'ordre e et de degré n sur $\mathbb{F}_2$, alors e est un diviseur de $2^n - 1$. Ainsi le théorème précédent dérive directement du résultat dans [49].

Finalement nous considérons le critère pour tester si un polynôme irréductible divise les trinômes du type $x^{am} + x^{bs} + 1$ sur $\mathbb{F}_2$.

1.7.3 Théorème [6, 39]

Soit f un polynôme irréductible d'ordre e et de degré n sur $\mathbb{F}_2$ et a, b entiers positifs. Alors f divise les trinômes $x^{am} + x^{bs} + 1$ si et seulement si $gcd(1 + x^{e_1}, 1 + (1 + x)^{e_2})$ a un degré supérieur à 1, où

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

Preuve

Soit α une racine quelconque de f. Alors l'ordre de α dans le groupe multiplicatif $\mathbb{F}_{q^n}^*$ est e et 1, α, α^2,$\cdots$, α^{e-1} sont les racines distinctes de $x^e - 1$. Ainsi

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

pour tout i $(0 \leq i \leq e-1)$, α^i est une racine d'un polynôme irréductible dont l'ordre est un diviseur de e. En particulier, α^a a pour ordre $e_1 = \frac{e}{gcd(a,\ e)}$ et α^a, α^{2a}, $\cdots$, $\alpha^{(e-1)a}$ sont toutes les racines de $C_{e_1}(x) := \frac{x^{e_1}-1}{x-1}$. Similairement α^b, α^{2b}, $\cdots$, $\alpha^{(e_2-1)b}$ sont toutes les racines de $C_{e_2}(x) := \frac{x^{e_2}-1}{x-1}$ et ainsi $1 + \alpha^b, 1 + \alpha^{2b}$, $\cdots$, $1 + \alpha^{(e_2-1)b}$ sont toutes les racines de $C_{e_2}(x + 1)$. D'où α est une racine du trinôme $x^{am} + x^{bs} + 1$ si et seulement si $C_{e_1}(x)$ et $C_{e_2}(x + 1)$ ont une racine commune. Ce qui est équivalent au fait que $gcd(1 + x^{e_1}$, $1 + (1 + x)^{e_2})$ a un degré supérieur à 1. □

Posons $a = b = 1$ dans le théorème 6 [39]. Nous avons alors Le critère de Welch.

Chapitre 2 Codes linéaires, codes cycliques sur un corps fini

2.1 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.

2.2 Paramètres d'un code

Poids et distance de Hamming [1]

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

Définition 2.2.1

Soit $n \in \mathbb{N}$. Soit p un nombre premier et q une puissance de p. Soit $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$. Le poids de Hamming de x, noté $wt(x)$, *est le nombre de coordonnées non nulles de x.*

Nous avons :

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

Soit x, $y \in \mathbb{F}_q^n$. La distance de Hamming entre x et y, notée $d_H(x, y)$ est par définition le nombre d'indices i tels que $x_i \neq y_i$.

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

Le support d'un élément $x \in \mathbb{F}_q^n$ 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 $d(x, y)$.
$\forall x$, $y \in \mathbb{F}_q^n$:

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

Définition 2.2.2 [1]

Un code C de longueur n est un sous-ensemble de $\mathbb{F}_q^n$. La distance minimum de C, notée $d(C)$, est le minimum des distances entre deux éléments distincts de C.

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

2.3 Codes linéaires sur $\mathbb{F}_q$

Pour les codes contenus dans $\mathbb{F}_q^n$, 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 2.3.1 [1]

Soit $n \in \mathbb{N}$. Soit q une puissance d'un nombre premier. Un code C de longueur n

est dit linéaire si C est un $\mathbb{F}_q-$ sous espace vectoriel de $\mathbb{F}_q^n$. 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, nous avons :

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

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 du code et nous écrivons C de paramètres $[n,k,d]$ ou bien C est un $[n,k,d]$-code.

Matrice génératrice, matrice de contrôle ou de parité

Définition 2.3.2 [1]

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 bilinéaire usuelle $x \cdot y = \sum_{i=1}^{n} x_i y_i$.

$$C^\perp := \{x \in \mathbb{F}_q^n \mid \forall y \in \mathbb{F}_q^n,\ x \cdot y = 0\}.$$

Une matrice de contrôle de parité de C est une matrice $(n-k) \times n$ génératrice de $C^\perp$. Un code est dit auto-dual 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 2.3.3 [1]

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 C, alors :

• $\forall x \in \mathbb{F}_q^n$, $x \in C \Longleftrightarrow \exists u \in F_q^k \mid x = uG$

• $\forall x \in \mathbb{F}_q^n$, $x \in C \Leftrightarrow Hx^t = 0$

• *C contient un mot de poids au plus w, ssi w colonnes de H sont linéairement dépendantes.*

Remarque 2.3.4 [1]

Ainsi, un code C est de poids d si et seulement si, il existe d colonnes de sa matrice de contrôle 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 2.3.5 [1]

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

Equivalence de codes [1]

Soit S_n le groupe des permutations de l'ensemble $\{1, 2, ..., n\}$. Ce groupe opère sur $\mathbb{F}_q^n$ 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, $wt(\sigma(x)) = wt(x)$, $\sigma(x) \cdot \sigma(y) = x \cdot y$, $d_H(\sigma(x), \sigma(y)) = d_H(x, y)$, 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, nous étudions 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 $\mathbb{F}_q^n$ 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.
Nous avons :

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

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 2.3.6 (et définition) [1]
Soit C_1, C_2 deux codes linéaires de matrices génératrices respectives G_1, G_2. On dit que les codes C_1 et C_2 sont équivalents s'il existe une permutation σ telle que $C_2 = C_1^\sigma$. Ce qui équivaut à l'existence d'une matrice de permutation M_σ et une matrice $k \times k$ P à coefficients dans F_q et inversible telles que

$$G_2 = PG_1M_\sigma$$

Nous utilisons aussi la notion *d'équivalence monomiale.* Deux codes sont dits monomialement équivalents s'ils sont échangés par une transformation monomiale, où une transformation monomiale est du type :

$$(x_1, ..., x_n) \longrightarrow (a_1 x_{\sigma(1)}, ..., a_n x_{\sigma(n)}), \text{ où pour tout } i,\ a_i \in \mathbb{F}_q^*$$

Définition 2.3.7 [1]
Soit $n \in \mathbb{N}^*$. Soit S_n le groupe des permutations σ telles que $\sigma(C) = C$. Ce groupe est appelé le groupe des automorphismes du code C, noté $Aut(C)$.

2.4 Codes cycliques sur $\mathbb{F}_q$

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 $\mathbb{F}_q^n$, qui est une permutation circulaire σ des coordonnées, par :

$$\begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (c_0, c_1, ..., c_{n-1}) & \to & (c_{n-1}, c_0, c_1, ..., c_{n-2}) \end{array}$$

Définition 2.4.1 [1]
Soit C un code linéaire sur $\mathbb{F}_q^n$. On dit que C est cyclique si $\sigma(C) = C$.

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

Exemple 2.4.2
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 troisièmes et quatrièmes coordonnées).

Lemme 2.4.3 [1]
Un code cyclique de $\mathbb{F}_q^n$ peut être identifié à un idéal de l'anneau $\mathbb{F}_q[x]/(x^n - 1)$.

Preuve
Soit l'application

$$\begin{array}{rcl} \varphi & : & \mathbb{F}_q^n \to \mathbb{F}_q[x] \to \mathbb{F}_q[x]/(x^n - 1) \\ c & \to & c(x) \to c(x)\ mod\ x^n - 1 \end{array}$$

qui associe à un mot de $\mathbb{F}_q^n$

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

le polynôme de $\mathbb{F}_q[x]$

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

φ est est un isomorphisme de $\mathbb{F}_q$ - espaces vectoriels.

Dans $\mathbb{F}_q[x]/(x^n - 1)$, la multiplication par x correspond à la permutation circulaire des coefficients. Ainsi, pour tout $u \in \mathbb{F}_q^n$, nous avons

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

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 $\mathbb{F}_q$ - espace vectoriel, il est stable par σ si et seulement si son image par φ est un idéal de $\mathbb{F}_q[x]/(x^n - 1)$. □

Polynôme générateur

Définition 2.4.4 [1]

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

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

Théorème 2.4.5 [4]

Soit C un idéal de $\mathbb{F}_q[x]/(x^n - 1)$, Alors

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

ii) C est un idéal principal engendré 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 $degr(x) < degg(x)$.

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 2.4.6

Dans $\mathbb{F}_2[x]$ nous avons la factorisation

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

Dans $\mathbb{F}_2[x]/(x^3 - 1)$, soit C_1, C_2 les codes cycliques engendrés respectivement par les polynômes $g_1(x) = 1 + x$, $g_2(x) = 1 + x + x^2$.

Alors nous avons :

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

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

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

Lemme 2.4.7 [4]
Les mots de C sont les multiples de $g(x)$ dans $\mathbb{F}_q[x]/(x^n - 1)$. *Plus précisément, si $deg(g(x)) = n - k$,*

$$\forall c(x) \in C,\ \exists!\ a(x) \in \mathbb{F}_q[x],\ dega(x) < k : c(x) = a(x)g(x)$$

et donc $deg(g(x)) + dimC = n$.

En effet, soit $c(x) \in C$. Effectuons la division euclidienne de $c(x)$ par $g(x)$:

$$c(x) = q(x)g(x) + r(x),\ deg\ r(x) < deg\ g(x)$$

Nous savons 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 $degq(x) < k$ car $degc(x) < n$. □

Théorème 2.4.8 [64]
Soit C un code cyclique de $\mathbb{F}_q^n$, de polynôme générateur

$$g(x) = g_0 + g_1x + ... + g_{n-k}x^{n-k}$$

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

$$g_1 + g_2x + ... + g_{n-k-1}x^{n-k-1} \in C$$

Ce qui contredit la minimalité du degré $n-k$ du polynôme générateur. Maintenant, nous voyons que les k lignes de la matrice G sont linéairement indépendantes du fait de l'échelonnement de g_os avec 0_s au dessus. Ces k lignes représentent les polynômes $g(x)$, $xg(x)$, $x^2g(x), ..., x^{k-1}g(x)$. 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 $g(x)$, $xg(x)$, $x^2g(x), ..., x^{k-1}g(x)$. Le lemme 2.4.7 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 2.4.9

Déterminons tous les codes cycliques *ternaires* et leurs polynômes générateurs pour $n = 4$. La factorisation de $x^4 - 1$ sur $\mathbb{F}_3$ 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 2.4.10 [1]
Soit $g(x)$ le polynôme générateur du code cyclique C dans $\mathbb{F}_q^n$, alors $g(x)$ *est un diviseur* de $x^n - 1$.

Ce résultat nous permettra de construire des codes cycliques à partir des diviseurs de $x^n - 1$. Pour la preuve, nous procédons de la même façon que le lemme précédent, nous faisons la division euclidienne de $x^n - 1$ par $g(x)$ dans $\mathbb{F}_q[x]$, et nous concluons 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

$$r(x) = 0$$

Dual d'un code cyclique

Théorème 2.4.11 [4]
Soit $C[n,k]$ *un code cyclique. Alors son code dual $C^{\perp}$ est cyclique et il est engendré 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 $\mathbb{F}_q[x]/(x^n - 1)$, nous avons

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

Pour tout mot de code $c(x) = u(x)g(x)$, nous aurons

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

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 engendré par le polynôme $x^k h(x^{-1})$. □

2.5 Exemples historiques de codes correcteurs

2.5.1 Le test de parité : un exemple de code détecteur [7]

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 $n = 6$:

$$101011 \longrightarrow \begin{array}{cc} 100011 & \text{l'erreur est détectée} \\ 110011 & \text{les erreurs ne sont pas détectées} \end{array}$$

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

2.5.2 Le code de répétition [7]

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).

2.5.3 Le premier code du mathématicien R.W. Hamming [7]

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 détectant 3.

$$\begin{array}{rcll} & & \text{Encodage} & \\ & & 110 & \\ 1101 & \longrightarrow & 011 \longrightarrow & 110011101 \\ & & 101 & \end{array}$$

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

$$\begin{array}{rcll} & & \text{Décodage} & \\ & & 110 & \\ 110\underline{0}01101 & \longrightarrow & 0\underline{0}1 \longrightarrow & 110011101 \\ & & 101 & \end{array}$$

Le taux de transmission est passé de $1/3 = 0,33$, qui était le taux de transmission du code de répétition 1-correcteur, à $4/9 = 0,44$. Le deuxième code, appelé code de Hamming, aura un taux de $4/7 = 0,55$, le meilleur possible pour un code 1-correcteur transmettant des blocs de 4 bits.

Chapitre 3 Codes cycliques optimaux, iso-duaux de rendement $\frac{1}{2}$ sur $\mathbb{F}_3$

3.1 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.

3.2 Codes cycliques iso-duaux

3.2.1 Codes cycliques iso-duaux sur $\mathbb{F}_3$ [52]

Soit le corps de Galois à 3 éléments noté $\mathbb{F}_3 = \{0, 1, 2\}$. Un code $C[n, k]$ linéaire ternaire est un sous espace vectoriel de dimension k de $\mathbb{F}_3^n$. Le rendement 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 monomiale des coordonnées. Soit $g(x)$ le polynôme générateur(unitaire) du code cyclique C, alors son code dual (cyclique) $C^\perp$ admet pour polynôme générateur le polynôme réciproque (unitaire) de :

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

Proposition 3.2.1.1 [1]

Un code C est iso-dual si et seulement si $C^\perp$ s'obtient par permutation des coordonnées de C avec changement de signe éventuel.

Soit n un entier pair non multiple de 3. Nous présentons une généralisation, pour les codes cycliques de paramètres $[n, \frac{n}{2}]$ sur le corps fini $\mathbb{F}_3$, sur le fait que ces derniers sont iso-duaux (i.e., équivalents à leurs duaux). L'utilisation de la notion de polynôme réciproque nous a permis de trouver une construction 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 $n = 2m$, le binôme $x^n - 1$ s'écrit :

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

Avec $x^m - 1$ et $x^m + 1$ qui s'écrivent

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

Où les polynômes u et v existent toujours et leur unicité dépend de n.
Supposons que u et v soient auto-réciproques c-a-d,

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

Soit $g(x) = (x - 1)u(x)v(-x)$, alors :

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

D'où

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

Ainsi le code dual $C^\top$du code cyclique C a pour générateur $g^\top(x) = -g(-x)$, c-a-d que C et $C^\top$sont monomialement équivalents [1] et par conséquent le code cyclique de générateur $g(x)$ est iso-dual en longueur $2m$. Nous résumons ce résultat par :

Proposition 3.2.1.2 [52]

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

3.2.2 Nouvelles classes de codes cycliques iso-duaux sur $\mathbb{F}_3$ [52]

Nous donnons *sept constructions* de code cycliques iso-duaux sur le corps fini $\mathbb{F}_3$. Nous supposons 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

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

Nous choisissons

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

Nous considérons les sept cas suivants :

Soit ϵ, η dans $\{\pm 1\}$

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. $u^*(x) = \epsilon u(-x)$, $v^*(x) = v(x)$

Proposition 3.2.2 [52] **:** *Avec les notations précédentes. Dans les sept cas, le code cyclique de générateur $g(x)$ est iso-dual sur $\mathbb{F}_3$.*

Preuve

Dans chaque cas nous calculons le polynôme générateur du code dual. Premièrement nous avons :

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

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. □

3.3 Codes cycliques optimaux sur $\mathbb{F}_3$ [52]

Nous adaptons les notations et définitions indiquées dans [42, 46]. 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 $\mathbb{F}$, 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 initiée par Hill et Newton [37]. 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 30 valeurs de d. L'état de l'art et tables pour $n_3(6, d)$ et $d_3(n, 6)$ est dans [34]. Maruta [48] 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 [26] 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(multi-cycliques) par Gulliver et Ostergard [32].

3.3.1 Codes cycliques $[\mathbf{26},\mathbf{13}]_3$ [52]

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 [26]) les bornes supérieures ne sont pas toujours atteintes. Nous donnons ici la table des bornes de d_3 pour $26 \leq n \leq 74$ et $k = \frac{n}{2}$.

n	26	28	32	34	38	40	44	46	50
$d_3(n,\frac{n}{2})$	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
$d_3(n,\frac{n}{2})$	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 [66] nous a permis d'obtenir tous les résultats sur les codes cycliques de paramètres $[26,13]_3$. La factorisation du polynôme :

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

en facteurs irréductibles sur le corps $\mathbb{F}_3$ donne huit polynômes 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 de degré 3 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 code $[26,13]_3$ pour chaque polynôme $g(x)$ choisi. Nous enregistrons

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			**8**
20120100020121	12001010000002100202000000			**8**
12112100012111	21000100000000200000000211			7
22000102100211	22200000000102202020000000			**8**
20210211021111	22200000000100100000201001			**8**
10020222110211	12010000000002102000000000	$\begin{smallmatrix}u^*(x)=-u(-x)\\v^*(x)=v(x)\end{smallmatrix}$	$[-g(-x)]^*$	6
12011200010121	10100000100001010000010000	$\begin{smallmatrix}u^*(x)=u(-x)^*\\v^*(x)=v(x)\end{smallmatrix}$	$g(-x)$	6
20000000000001	10000000000002000000000000	$\begin{smallmatrix}u^*(x)=v(x)\\v^*(x)=u(x)\end{smallmatrix}$	$-g(-x)$	2
12222222222221	11000000000002200000000000	$\begin{smallmatrix}u^*(x)=v(x)\\v^*(x)=u(x)\end{smallmatrix}$	$g(-x)$	4
10111211001201	22000000100001100000020000	$\begin{smallmatrix}u^*(x)=u(x)\\v^*(x)=v(-x)^*\end{smallmatrix}$	$g(-x)$	6
21120102202001	10100000100002020000020000	$\begin{smallmatrix}u^*(x)=u(x)\\v^*(x)=-v(-x)\end{smallmatrix}$	$[-g(-x)]^*$	6
...	...	...	...	...

Remarque [52] : Il y a exactement 54 codes optimaux parmi les 140 codes cycliques $[26, 13]_3$ existants.

Notons $d_C(n)$ la plus grande distance minimum d'un code cyclique de longueur n, nous résumons alors notre premier résultat par :

Proposition 3.3.1 [52]

La plus grande distance minimum des codes cycliques ternaires [26,13]$_3$ est $d_C(26)=8$.

3.3.2 Codes Cycliques $[\mathbf{34}, \mathbf{17}]_3$ [52]

Dans ce cas nous avons seulement 4 choix possibles pour le polynôme générateur $g(x)$ du code, et la factorisation de $x^{34} - 1$ en facteurs irréductibles sur $\mathbb{F}_3$ 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 nous aurons les mots de codes et leurs poids respectifs

Table 2

g(x)	mot de code a	$\begin{bmatrix} u^*= \\ v^*= \end{bmatrix}$	$\left[\frac{x^{34}-1}{g(x)}\right]^*=$	wt(a)
221212121212121211	210000000000000002100000000000000	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	4
122222222222222221	110000000000000002200000000000000	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	4
200000000000000001	100000000000000002000000000000000	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	2
100000000000000001	100000000000000001000000000000000	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	2

Remarque [52]

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

Proposition 3.3.2 [52]

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

3.3.3 Codes cycliques $[\mathbf{38}, \mathbf{19}]_3$ [52]

De même ici nous avons 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 correspondants.

Table 3

g(x)	mot de code a	$\begin{bmatrix} u^*= \\ v^*= \end{bmatrix}$	$[\frac{x^{38}-1}{g(x)}]^*=$	wt(a)
12222222222222222221	11000000000000000002200000000000000000	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	4
20000000000000000001	10000000000000000002000000000000000000	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	2
10000000000000000001	10000000000000000001000000000000000000	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$g(-x)$	2
22121212121212121211	21000000000000000002100000000000000000	$\begin{bmatrix} u^*=u \\ v^*=v \end{bmatrix}$	$-g(-x)$	4

Remarque [52]

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

Proposition 3.3.3 [52]

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

3.3.4 Codes cycliques $[\mathbf{46}, \mathbf{23}]_3$ [52]

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

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

Par conséquent nous enregistrons dans la table 4 qui suit tous les mots de code et leurs poids correspondants :

g(x)	mot de code(a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{46}-1}{g(x)}]^*=$	wt(a)
22222211110022002200011	10202010000000000000000020002000002010000000020	$u^*(x)=-v^*(x)$	$-g(-x)$	9
20020211212010120020122 1	21110000011000000000000000200010002200002022 00			13
10000000000000000000001	10000000000000000000001000000000000000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$g(-x)$	2
12222222222222222222221	11000000000000000000002200000000000000000000	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$g(-x)$	4

Table 4 suite

g(x)	mot de code(a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{46}-1}{g(x)}]^*=$	wt(a)
211201001202012122101001	221210010000000000000002002000002100000100021			13
220000110011002222111111	101020001000000000000000200010000000020101000	$u^*(x)=-v^*(x)$	$-g(-x)$	9
121212212100120012000021	102020100000000000000000200020000201000000020	$u^*(x)=-v^*(x)$	$g(-x)$	9
112201002202011112202001	122220010000000000000002001000002200000200011			13
221212121212121212121211	210000000000000000000002100000000000000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$-g(-x)$	4
200000000000000000000001	100000000000000000000002000000000000000000000	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$-g(-x)$	2
100202211110202200102211	221200000210000000000000002000100021000020210 0			13
120000210021001212212121	101020001000000000000000200010000000020101000	$u^*(x)=-v^*(x)$	$g(-x)$	9

Remarques [52]

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

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** nous avons $\left(\frac{x^{46}-1}{g(x)}\right)^* = \pm g(-x)$.

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

Proposition 3.3.4 [52]

La plus grande distance minimum des codes cycliques ternaires [46, 23]$_3$ est $d_C(46)$=13.

3.3.5 Codes cycliques $[\mathbf{50}, \mathbf{25}]_3$ [52]

Pour les codes cycliques $[50, 25]_3$, 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 nous avons la table qui nous donne tous les mots de code et leurs poids correspondants :

Table 5

g(x)	mot de code a	$\left[\begin{smallmatrix}u^*= \\ v^*=\end{smallmatrix}\right.$	$[\frac{x^{50}-1}{g(x)}]^* =$	wt(a)
10000000000000000000000001	10.....010.....0	$\left[\begin{smallmatrix}u^*=u \\ v^*=v\end{smallmatrix}\right.$	$g(-x)$	2
12222222222222222222222221	110.....0220.....0	$\left[\begin{smallmatrix}u^*=u \\ v^*=v\end{smallmatrix}\right.$	$g(-x)$	**4**
20000000000000000000000001	10.....020.....0	$\left[\begin{smallmatrix}u^*=u \\ v^*=v\end{smallmatrix}\right.$	$-g(-x)$	2
22121212121212121212121211	210.....0210.....0	$\left[\begin{smallmatrix}u^*=u \\ v^*=v\end{smallmatrix}\right.$	$-g(-x)$	**4**
12222011110222201111022221	2000010...20000010...0	$\left[\begin{smallmatrix}u^*=u \\ v^*=v\end{smallmatrix}\right.$	$g(-x)$	**4**
10000200002000020000200001	1000010...02000020...0	$\left[\begin{smallmatrix}u^*=u \\ v^*=v\end{smallmatrix}\right.$	$g(-x)$	**4**
20000200001000020000100001	2000010...20000010...0	$\left[\begin{smallmatrix}u^*=u \\ v^*=v\end{smallmatrix}\right.$	$-g(-x)$	**4**
22121021210212102121021211	1000010...02000020...0	$\left[\begin{smallmatrix}u^*=u \\ v^*=v\end{smallmatrix}\right.$	$-g(-x)$	**4**

Remarque [52]

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

Proposition 3.3.5 [52]

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

3.3.6 Codes cycliques $[\mathbf{58}, \mathbf{29}]_3$ [52]

Pour les codes cycliques ternaires de paramètres $[58, 29]$, 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 nous avons la table qui nous donne tous les mots de code et leurs poids correspondants :

Table 6

g(x)	mot de code a	$\begin{bmatrix} u^*= \\ v^*= \end{bmatrix}$	$[\frac{x^{58}-1}{g(x)}]^* =$	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 [52]

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

Proposition 3.3.6 [52]

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

3.3.7 Codes cycliques $[\mathbf{62}, \mathbf{31}]_3$ [52]

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 [52]

Tous les codes cycliques $[62, 31]_3$ sont **iso-duaux**.

Proposition 3.3.7 [52]

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

3.3.8 Codes cycliques $[68, 34]_3$ [52]

De même la factorisation du binôme $x^{68} - 1$, sur $\mathbb{F}_3$, nous donne 12 possibilités pour le choix du polynôme générateur du code ce qui nous permet de voir exhaustivement tous les poids des mots du code.

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

Ainsi nous résumons les paramètres du code dans la table 8 :

Table 8

g(x)	mot de code(a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$\left[\frac{x^{68}-1}{g(x)}\right]^*=$	wt(a)
2010122100100102100202112002002012 1	220...0110...0220...0110...0			8
2020102010201020102010201020101	2010....00...02010....00.....0			4
2220100200112202002201002001122020 1	210...0210...0210...0210...0			8
2120100100122101002102002002112020 1	220...0110...0220...0110...0			8
2000000000000000000000000000000001	100.....020.....0			2
2010112200100201100101122001002011 1	210...0210...0210...0210...0			8
1010212100201212002120101220210102 1	20.....010....020....010.....0			4
1102022021101022200111102002222010 1	10....010....010.....010.....0			4

Table 8 suite

g(x)	mot de code(a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$\left[\frac{x^{68}-1}{g(x)}\right]^*=$	wt(a)
120101202210102120021210200121201 01	20.....010....020...010...0			4
102020202020202020202020202020201	1010.....02020.....0			4
101022220020111100222010112022020 11	10....010...010.....010....0			4
100000000000000000000000000000001	10.....010.....0			2

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

$$\begin{aligned} x^{34}-1 &= (1+x)(2+x)u(x)u(-x) \\ x^{34}+1 &= (1+x^2)v(x)v(-x) \end{aligned}$$

Si nous prenons tous les $g(x)$ qui divisent $(x^{68}-1)$, comme c'est indiqué dans table 8, nous aurons toujours :

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

et

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

Dans ce cas nous nous pouvons rien affirmer s'il existe ou n'existe pas de codes cycliques iso-duaux de paramètres $[68,34]_3$.

Remarque [52]

Il y a exactement 4 codes cycliques optimaux de paramètres $[68,34]_3$.

Proposition 3.3.8 [52]

La plus grande distance minimum des codes cycliques ternaires [68, 34]$_3$ est $d_C(68)$=8.

3.3.9 Codes cycliques $[\mathbf{70,35}]_3$ [52]

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 nous avons 3 cas :

soit

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

soit

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

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

Table 9

g(x)	mot de code a	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$\left[\frac{x^{70}-1}{g(x)}\right]^*=$	w
10211101000002021201210220211000110 1	11110...020...020...010..02220...010..010..020..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	12
12222011101000202210012222002021021 1	1110...020...010...010...02220...010..020..020..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	12
12222222222222222222222222222222221	110.....0220.....0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	4
11201011002221010220101222001101021 1	220...010.....010.....0220.....010...010...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	8
11201202002222100122020001011102222 1	1110...020...020..010...02220..010..010..020...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	12

Table 9 suite 1

10110001120220121021202000001011120l	1110...020..010...010..02220...010..020..020..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x)^* \end{cases}$	$g(-x)$	12
11112112101212012010020121001212001l	10..010..010..010..010..010..010..010..010..010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$g(-x)$	10
10000102022020121122011111022222222l	10..010..010..010..010..010..010..010..010..010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	10
10000002000000200000020000002000000l	10.....01...020...020.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$g(-x)$	4
12222011110222201111022220111102222l	2000010.....02000010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$g(-x)$	4
12222222201111102211210202202010000l	10..010..010..010..010..010..010..010..010..010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	10
11002121001210200102102121012112111l	10..010..010..010..010..010..010..010..010..010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$g(-x)$	10
11112002120210101012201012112102001l	2020..010..010..0100010002000102000020..010..020..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$g(-x)$	12
10000000020000010022010120021012222l	10100010100010...0100010..011010...01010100010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	14
10000200002000020000200002000020000l	1000010.....02000020.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$g(-x)$	4
12222220111111022222201111110222222l	20.....010.....020.....010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$g(-x)$	4
12222101200210102200100000200000000l	101010..010110..0100010..0100010100010l0..0100	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	14
11002012112101022101010120212002111l	101020....020.....01010..02010.....01020002020..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$g(-x)$	12
12122210222220121010121221011220021l	210..0200002000100000210.....020000200010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$g(-x)$	10
11212120110000200200120002100020000l	210..0200002000100000210...020000200010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	10
11212011002220210110120222001102121l	120...010000010.....0210.....020000020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$g(-x)$	8
10000000000000000000000000000000001	10.....010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$g(-x)$	2
10000200012000210020020000110212121l	210...020001000010...0210...020001000010...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	10
12002221101221210101210222220122212l	210...020001000010...0210...020001000010...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$g(-x)$	10
22221220121210222020222211012212001l	110...0100002000100000220...020000100020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	10
20000200011000110010020000210222222l	220000010002000010...0110000020001000020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	10
20000000000000000000000000000000001	10.....020.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	2
21111110210000100200220002200010000l	110...010000200010...0220...020000100020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	10
22001211202211110101110212121011211l	220000010002000010...0110000020001000020...0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	10
21211002220220202022102022211102002l	2020..010...010..0100010002000102000020..010..020..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	12

Table 9 suite 2

2212110110022020120020000010000000001	101010...010120..010..010..010..01010..01010..0010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	14
2212121021212102121210212121021212111	100000010.....0200000020.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	4
2000020000100002000010000200001000001	2000010.....02000010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	4
2000000002000001001201011002202212111	10100010100010..0100010...021010.....01010100010..0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	14
2100102221110102110101011011100221211	101020.....020...01010...02010...01020002020.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	12
2121112220222201102002011100222200211	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
2212121210212120122111020210102000011	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
2212102121021210212102121021210211211	1000010.....02000020.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	4
2000000200000010000002000000100000011	20.....010.....020.....010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	4
2000010202101022211201212102121211211	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
2100111100222010010220111101112221211	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
2111102100121011012022021200210222211	220.....010000010...0220...010000010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	8
2011210100000202220111021011200021011	2120.....010...020...010...02120...010...020...010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{cases}$	$-g(-x)$	12
2110220200121220011202000101210212111	2120.....010...020...010...02120...010...020...010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	12
2110202100121101021020221200210102211	120...010.....010...0210...020.....020....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	8
2212121212121212121212121212121212111	210.....0210.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(x) \end{cases}$	$-g(-x)$	4
2212102120200010122001121200101102211	2120.....010...020...010...02120...010...020...010.....0	$\begin{cases} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{cases}$	$[-g(-x)]^*$	12
2021000122021022201110100000202122011	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 [52]

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

Proposition 3.3.9 [52]

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

3.3.10 Codes cycliques $[\mathbf{74}, \mathbf{37}]_3$ [52]

La recherche de la distance minimale pour ces codes a demandé beaucoup de temps, en effet, pour certains polynômes 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 nous avons 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	1111222211222200222222002222211222211111	10102000200010...010.....010.....01010...020...020			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			11
7	21211212211212001212120012122112122121	10102000200010....010...010....01010....020....020			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			11

Remarque [52]

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

Proposition 3.3.10 [52]

La plus grande distance minimum des codes cycliques ternaires [74, 37]$_3$ est $d_C(74)$=14.

Note [52]

La distance minimale de ces codes cycliques ternaires dépasse la borne BCH [21].

3.4 Table des valeurs de $d_I(n)$ et $d_C(n)$ [52]

Notons $d_I(n)$ la plus grande 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 ternaires de paramètres $[n, \frac{n}{2}]$ selon la longueur n 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 [52]

Nous constatons que pour $n = 34, 38, 50, 58, 62, 70, 74$; le code iso-dual est aussi performant (au sens de la distance minimum) que le code cyclique.

Chapitre 4 Codes cycliques optimaux, iso-duaux de rendement $\frac{1}{2}$ sur $\mathbb{F}_5$

4.1 Introduction

Soit le corps fini de Galois à 5 éléments noté $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. Un code $C[n, k]_5$ linéaire est un sous espace vectoriel de dimension k de $\mathbb{F}_5^n$. Ces dernières années, de bons codes linéaires sur F_5 ont été construits. Dans [14] Daskalov et Gulliver construisent 44 bons codes et présentent une table sur les bornes des distances minimums pour $1 \leq k \leq 8$, $1 \leq n \leq 100$. 32 quasi-cycliques (QC) et quasi-twisted (QT) codes sont construits, sur $\mathbb{F}_5$, dans [13]. Grassl et White présentent dans [27] 55 nouveaux codes. Certains bons codes linéaires incluant la notion de rendement élevé sont présentés dans [12]. Grassl [26] maintient à jour une table électronique 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 $\mathbb{F}_5$ et sur $\mathbb{F}_7$ a été faite respectivement jusqu'à la longueur 12 et 8 [31].

4.2 Codes cycliques iso-duaux

4.2.1 Codes cycliques iso-duaux sur $\mathbb{F}_5$ [51]

Le même travail que celui sur $\mathbb{F}_3$ est repris pour les codes cycliques $C[n, \frac{n}{2}]$ sur le corps fini $\mathbb{F}_5$, dans le cas où n est pair non multiple de 5, sur le fait que ces derniers sont iso-duaux. Cette iso-dualité est réalisée par le fait que le polynôme générateur (unitaire) du code dual $C^{\perp}$, vérifie la propriété suivante :

Sachant que pour $n = 2m$, le binôme $x^n - 1$s'écrit :

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

Avec $x^m - 1$ et $x^m + 1$ qui s'écrivent

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

Supposons que les polynômes u et v soient auto-réciproques c-a-d :

$$u^*(x) = u(x) \quad \text{et} \quad v^*(x) = v(x)$$

Choisissons $g(x) = (1+x)u(x)v(-x)$, alors

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

D'où

$$\begin{aligned}\left(\frac{x^n-1}{g(x)}\right)^* &= (1+4x)u(-x)v(x) \\ &= (1-x)u(-x)v(x) \\ &= g(x)^{\perp} \\ &= g(-x)\end{aligned}$$

Ainsi le code cyclique de générateur le polynôme réciproque du complément de $g(x)$ est iso-dual en longueur $2m$.

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

Proposition 4.2.2 [51]
Soit $x^m - 1 = (4+x)u(x)v(x)$ avec m impair et $u^* = u$, $v^* = v$. Alors le code cyclique, sur $\mathbb{F}_5$, engendré par le polynôme $g(x) = (1+x)u(x)v(-x)$ est iso-dual en longueur $2m$.

Exemple 4.2.3 [51]

Pour les codes cycliques $[18, 9]_5$, dont la plus grande distance minimum est $d_C(18) = 4$, nous savons 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

$$u(x) = 1 + 4x + x^2 \quad et \quad v(x) = 1 + 4x^3 + x^6$$

Vérifiant

$$u^*(x) = u(x) \quad \text{et} \quad v^*(x) = v(x)$$

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

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

Donc le code cyclique de paramètres $[18,9]_5$ est bien iso-dual en longueur 18.

Exemple 4.2.4 [51]

Pour les codes cycliques $[22,11]_5$, dont la plus grande distance minimum est $d_C(22)=8$, nous savons 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

$$u^*(x) = u(x) \quad \text{et} \quad v^*(x) = v(x)$$

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 :

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

Ainsi le code cyclique de paramètres $[22, 11]_5$ est bien iso-dual en longueur 22.

4.2.5 Nouvelles classes de codes cycliques iso-daux sur $\mathbb{F}_5$ [51]

Nous donnons *trois constructions* de codes cycliques iso-duaux. Nous supposons 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

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

Nous choisissons

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

Nous considérons les trois cas suivants :

Soit ϵ, η dans $\{\pm 1\}$

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

Proposition 4.2.6 [51]

Dans les trois cas précédents, le code cyclique de générateur $g(x)$ est iso-dual en longueur $2m$ sur $\mathbb{F}_5$.

Preuve

Dans chaque cas nous calculons le polynôme générateur du code dual. Premièrement nous avons :

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

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

4.3 Codes cycliques optimaux sur $\mathbb{F}_5$ [51]

La table 1 représente les premiers résultats de calcul de la plus grande distance minimum des codes cycliques de paramètres $[n, k, d]_5$ 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 plus grande distance minimum $d_C = 4$).

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
$d_C(n)$	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 [26]) les bornes supérieures ne sont pas toujours atteintes. Nous donnons ici la table des bornes de d_5 pour $18 \leq n \leq 54$.

n	18	22	24	26	28	32	34	36
$d_5(n, \frac{n}{2})$	7-8	8-10	9-10	10-11	11-12	11-13	11-14	12-15

n	38	42	44	46	48	52	54
$d_5(n, \frac{n}{2})$	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 [66], nous a permis d'obtenir tous les résultats sur les codes cycliques de paramètres $[2m, m]_5$, pour $m = 11$, 13, 19 et 21.

4.3.1 Codes cycliques $[\mathbf{22}, \mathbf{11}]_{\mathbf{5}}$ [51]

La factorisation du polynôme $x^{22} - 1$ en facteurs irréductibles sur le corps $\mathbb{F}_5$ 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 parmi 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 enregistrés dans la table 2.

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

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	1000000000010000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$g(-x)$	2
3	441111442211	2020100000004000400020	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$-g(-x)$	6
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 [51]

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

Nous résumons notre premier résultat par :

Proposition 4.3.1 [51]

La plus grande distance minimum des codes cycliques [22,11]$_5$ *est* $d_C(22)=8$.

4.3.2 Codes cycliques $[\mathbf{26}, \mathbf{13}]_5$ [51]

Nous avons : $\binom{2}{1} \times \binom{6}{3} = 40$ choix possibles pour le polynôme générateur d'un code cyclique de paramètres $[26, 13]_5$, ces codes ont une spécificité particulière du fait que tous les générateurs $g(x)$, de degré 13, nous donnent une *même plus grande distance minimum* à l'exception 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 alors les résultats de toutes les combinaisons possibles dans la table 3.

$$x^{26}-1 = (1+x)(4+x)(1+x+4x^2+x^3+x^4)(1+2x+2x^3+x^4)(1+2x+x^2+2x^3 +x^4)(1+3x+3x^3+x^4)(1+3x+x^2+3x^3+x^4)(1+4x+4x^2+4x^3+x^4)$$

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			8
4	40133423122401	41200010...014300040...00			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			8
8	44014123414011	32040.....01032040.....010			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			8
12	40431023042101	2202010.....03303040.....0			8
13	13040011004031	22040.....01033010.....040			8
14	44422314233111	430400010..0120100040..0			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			8
18	43132300232421	43040..010..012010..040..0			8
19	14123344332141	130400010..0130400010..0			8
20	43040041001021	32040.....01032040.....010			8

Table 3 suite

n°	g(x)	mots de code (a)	$\begin{bmatrix} u^*= \\ v^*= \end{bmatrix}$	$[\frac{x^{26}-1}{g(x)}]^*=$	wt(a)
21	13410111101431	310....0110...01300400400			8
22	44033141422011	41200010...014300040....0			8
23	13014222241031	3202010.....03202010....0			8
24	44402000030111	2340010.....0100432000			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			8
28	43110141404421	210.....410....04300100400			8
29	10432433423401	44200010...044200010....0			8
30	42424423113131	103040..0102040..03020..0			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			8
34	43011232344021	2202010.....03303040.....0			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			8
38	42213114424331	21010....010...0400004043			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 [51]

- 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 nous avons 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 minimum $d_C = 2$, les 2 autres ont pour générateurs

12222222222221, 42323232323231 et de distance minimum $d_C = 4$.

Proposition 4.3.2 [51]

La plus grande distance minimum des codes cycliques [26, 13]$_5$ est $d_C(26)$=8.

4.3.3 Codes cycliques $[38, 19]_5$ [51]

Pour les codes cycliques $[38, 19]_5$, la factorisation de $x^{38} - 1$ en polynômes irréductibles sur $\mathbb{F}_5$ nous donne aussi 12 choix possibles pour le polynôme générateur de degré 19, par conséquent nous notons 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

Table 4 suite

n°	g(x)	mot de code (a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{38}-1}{g(x)}]^* =$	wt(a)
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 [51]

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

Proposition 4.3.3 [51]

La plus grande distance minimum des codes cycliques [38, 19]$_5$ *est* $d_C(38)$*=11.*

4.3.4 Codes cycliques $[42, 21]_5$ [51]

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 $[42, 21]_5$. Dans la table 5 nous notons 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 nous avons 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		12
2	1101434141441414341011	1301010.....0110.....0300001002020...0302		12
3	4101131111144444244041	1204040.....0410...0200001003030.....0203		12
4	4313144024001301142421	4231000040...0100004231000040...010000		12
5	1434433001441003344341	33210030...0100000022340020...04000000	$g(-x)$	12
6	4233122324411323342231	4231000040...0100004231000040...010000	$-g(-x)$	12
7	1223423334114333243221	4334000040...0100001221000010...040000	$g(-x)$	12
8	4424132001144003241311	32240030...0100000032240030...01000000	$-g(-x)$	12
9	1301323321441233231031	33210030...0100000022340020...04000000		12
10	1112441241001421442111	22000320000010..0100000230022020..020		12
11	4142144211004431143141	32000330...040...010...02200032020....030		12
12	4301222331144223334021	32240030...0100000032240030...01000000		12

Remarque [51]

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

Proposition 4.3.4 [51]

La plus grande distance minimum des codes cycliques [42, 21]$_5$ est $d_C(42)$=12.

Remarque [51]

Notons que la meilleure distance minimum connue pour un code autodual de longueur 42 est 12 [22, tables de P. Gaborit], c'est à dire identique à celle du code iso-dual de paramètres $[42, 21]_5$ que nous avons trouvé.

4.3.5 Table des valeurs de $d_I(n)$ et $d_C(n)$ [51]

Dans cette table nous résumons 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 aussi efficaces que les codes cycliques sur $\mathbb{F}_5$.

Annexe 1 Calcul de la densité des trinômes $x^{am}+x^{bs}+1$ sur $\mathbb{F}_2$

1) Pour M = 100

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

a	b	nb	total	nb/total
6	2	0	392	0,00000000000
6	3	31	250	**0,1210937500**
6	4	0	192	0,00000000000
6	5	13	154	0,08441558442
6	6	0	120	0,00000000000
1	6	23	784	0,02933673469
2	6	0	392	0,00000000000
3	6	0	256	0,00000000000
4	6	0	200	0,00000000000
5	6	6	163	0,03680981595
6	6	0	120	0,00000000000
7	1	58	721	0,08844382802
7	2	14	357	0,03921568627
7	3	20	236	0,08474576271
7	4	6	175	0,03428571429
7	5	12	139	0,08633093525
7	6	2	115	0,01739130435
7	7	8	91	0,08791208791
1	7	56	665	0,08421052632
2	7	26	336	0,07738095238
3	7	25	222	**0,11261261261**
4	7	13	172	0,07558139535
5	7	11	139	0,07913669065
6	7	12	107	**0,1121495327**
7	7	8	91	0,08791208791
8	1	0	612	0,00000000000
8	2	0	300	0,00000000000

a	b	nb	total	nb/total
8	3	0	200	0,00000000000
8	4	0	144	0,00000000000
8	5	0	118	0,00000000000
8	6	0	96	0,00000000000
8	7	0	83	0,00000000000
8	8	0	66	0,00000000000
1	8	13	576	0,02256944444
2	8	0	288	0,00000000000
3	8	6	192	0,03125000000
4	8	0	144	0,00000000000
5	8	4	120	0,03333333333
6	8	0	92	0,00000000000
7	8	2	84	0,02380952381
9	1	38	583	0,06518010292
9	2	10	289	0,03460207612
9	3	14	187	0,07486631016
9	4	7	142	0,04929577465
9	5	9	112	0,08035714286
9	6	0	91	0,00000000000
9	7	8	79	**0,1012658228**
9	8	3	69	0,04347826087
9	9	8	55	**0,1454545455**
1	9	42	506	0,08300395257
2	9	26	256	**0,1015625000**
3	9	16	165	0,09696969697
4	9	14	131	**0,1068702290**
5	9	9	106	0,08490566038

a	b	nb	total	nb/total
6	9	16	80	**0,2000000000**
7	9	9	74	**0,1216216216**
8	9	0	62	0,00000000000
10	1	34	540	0,06296296296
10	2	0	265	0,00000000000
10	3	16	177	0,09039548023
10	4	0	130	0,00000000000
10	5	8	100	0,0800000000
10	6	0	85	0,00000000000
10	7	6	73	0,08219178082
10	8	0	63	0,00000000000
10	9	7	56	**0,1250000000**
10	10	0	45	0,00000000000
1	10	9	450	0,0200000000
2	10	0	225	0,00000000000
3	10	3	150	0,0200000000
4	10	0	115	0,00000000000
5	10	0	90	0,00000000000
6	10	0	72	0,00000000000
7	10	1	66	**0,1515151515**
8	10	0	55	0,00000000000
9	10	0	53	0,00000000000

2) Pour M = 300, 500

Pour les mêmes trinômes, nous poursuivons le calcul pour $M = 300, 500$ en faisant comparer la densité avec celle des trinômes quelconques P(1, 1, M). Comme les résultats sont presque du même ordre de grandeur que pour le cas $M = 100$, j'ai préféré, et pour voir mieux, passer directement au cas $M = 1000$.

3) Recherche pratique de trinômes irréductibles suivant les différentes valeurs de a, b et M [49]

3.1 Programme

En voici le programme Maple de recherche des trinômes irréductibles sur $\mathbb{F}_2$ pour des valeurs de a et 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:
```

3.2 Résultats pratiques

Dans chacune des colonnes suivantes, la procédure recherche les trinômes irréductibles dans la famille $F(a, b)$ suivant les différentes valeurs du couple $(a,\ b)$, et recense, à la fin, le nombre de trinômes irréductibles par rapport aux trinômes quelconques ($i.e.$, $a = 1$ et $b = 1$) ce qui donne la densité (nb/total).

search3(7, 3, 2, 100)	search3(3, 5, 2, 80)	search3(7, 5, 2, 150)	search3(1,1,2,10)
$x^7 + x^3 + 1$	$x^6 + x^5 + 1$	$x^{14} + x^5 + 1$	$x^2 + x + 1$
$x^7 + x^6 + 1$	$x^9 + x^5 + 1$	$x^{28} + x^{15} + 1$	$x^3 + x + 1$
$x^{14} + x^9 + 1$	$x^{12} + x^5 + 1$	$x^{28} + x^{25} + 1$	$x^3 + x^2 + 1$
$x^{28} + x^3 + 1$	$x^{18} + x^{15} + 1$	$x^{42} + x^{35} + 1$	$x^4 + x + 1$
$x^{28} + x^9 + 1$	$x^{33} + x^{10} + 1$	$x^{49} + x^{15} + 1$	$x^4 + x^3 + 1$
$x^{28} + x^{15} + 1$	$x^{33} + x^{20} + 1$	$x^{49} + x^{40} + 1$	$x^5 + x^2 + 1$
$x^{28} + x^{27} + 1$	$x^{36} + x^{15} + 1$	$x^{63} + x^5 + 1$	$x^5 + x^3 + 1$
$x^{35} + x^{33} + 1$	$x^{36} + x^{25} + 1$	$x^{63} + x^{35} + 1$	$x^6 + x + 1$
$x^{49} + x^9 + 1$	$x^{39} + x^{25} + 1$	$x^{84} + x^5 + 1$	$x^6 + x^3 + 1$
$x^{49} + x^{12} + 1$	$x^{39} + x^{35} + 1$	$x^{84} + x^{35} + 1$	$x^6 + x^5 + 1$
$x^{49} + x^{15} + 1$	$x^{42} + x^{35} + 1$	$x^{84} + x^{45} + 1$	$x^7 + x + 1$
$x^{49} + x^{27} + 1$	$x^{54} + x^{45} + 1$	$x^{84} + x^{75} + 1$	$x^7 + x^3 + 1$
$x^{84} + x^9 + 1$	$x^{57} + x^{25} + 1$	$x^{126} + x^{105} + 1$	$x^7 + x^4 + 1$
$x^{84} + x^{27} + 1$	$x^{57} + x^{35} + 1$	$x^{140} + x^{15} + 1$	$x^7 + x^6 + 1$
$x^{84} + x^{39} + 1$	$x^{57} + x^{50} + 1$	$x^{140} + x^{45} + 1$	$x^9 + x + 1$
$x^{84} + x^{45} + 1$	$x^{60} + x^{15} + 1$	$x^{140} + x^{65} + 1$	$x^9 + x^4 + 1$
$x^{84} + x^{57} + 1$	$x^{60} + x^{45} + 1$	$x^{140} + x^{75} + 1$	$x^9 + x^5 + 1$
$x^{84} + x^{75} + 1$	$x^{63} + x^5 + 1$	$x^{140} + x^{95} + 1$	$x^9 + x^8 + 1$
$x^{98} + x^{27} + 1$	$x^{63} + x^{35} + 1$	$x^{140} + x^{125} + 1$	$x^{10} + x^3 + 1$
$x^{98} + x^{87} + 1$			$x^{10} + x^7 + 1$
$20, 236, 0.08474576$	$19, 195, 0.09743590$	$19, 311, 0.06109325$	$20, 45, 0.4444444444$

Annexe 2 Programme de recherche de la distance minimum

Nous donnons, dans cet annexe, le programme détaillé, décrit dans l'article [66], de recherche de la distance minimum d'un code cyclique sur les deux corps finis $\mathbb{F}_3$ et $\mathbb{F}_5$. Notons que le calcul de la distance minimum d'un code linéaire en général, sur un corps fini , et d'un code cyclique en particulier, est un problème NP complet. Dans le corps fini $\mathbb{F}_7$, nous nous sommes lancés dans les calculs de la distance minimum, et nous avons réalisé un résultat sur les codes iso-duaux, qui fera très prochainement un projet d'article.

Programme de recherche de la distance minimum d'un code cyclique sur $\mathbb{F}_p$, $p = 3, 5$ [66]

```
/* 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", Com-
putational & Applied Mathematics, vol. 24, n°3, pp. 393-398, 2005. Aucune optimisation
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 w0 sur la distance minimale estimée du code (prendre w0 =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, 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;
}
```

Conclusion

- Malgré le nombre connu de polynômes irréductibles de degré fixé n sur un corps fini $\mathbb{F}_q$, on ne peut pas en général, les expliciter tous si les deux entiers positifs n et q deviennent assez grand. Mais nous avons pu, sur $\mathbb{F}_2$, trouver de **nouvelles familles** de polynômes irréductibles de la forme $x^{am}+x^{bs}+1$ avec a, b des entiers fixés et m, s des entiers positifs en allant jusqu'à **2000** comme degré du polynôme et nous avons étendu un résultat dû à **Golomb** et **Lee** [28] sur la divisibilité de ces trinômes par un polynôme irréductible sur $\mathbb{F}_2$. Notons que ce résultat a fait l'objet d'une référence dans l'article [39].

- La **caractérisation** du polynôme générateur d'un code **cyclique iso-dual** est un problème ouvert difficile et nous avons réussi, dans ce contexte, à construire **sept classes** de codes cycliques **iso-duaux** sur $\mathbb{F}_3$ et **trois classes** de codes cycliques **iso-duaux** sur $\mathbb{F}_5$. Pour les codes cycliques de paramètres $[n, \frac{n}{2}]$ sur $\mathbb{F}_p$, 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 $\mathbb{F}_5$. Notant que la meilleure distance minimum des codes cycliques $[42, 21]_5$ iso-duaux qu'on a trouvé est identique à celle du code auto-dual de même paramètres (voir tables de P. Gaborit) [22]. En perspectives nous proposons les problèmes ouverts suivants :

Question 1

- 1. Peut-on prouver l'existence d'une limite du rapport $\frac{\pi_M(a,b)}{\pi_M(1,1)}$, quand M tend vers l'infini ?

- 2. Peut-on estimer la limite du rapport $\frac{\pi_M(a,b)}{\pi_M(1,1)}$, si elle existe, en fonction de a et b ?

Question 2 Peut-on généraliser la **caractérisation** du polynôme générateur d'un code cyclique iso-dual sur d'autres corps finis $\mathbb{F}_p$?, pour $p = 7, 11, 13, ...$

Question 3 Peut-on étendre les résultats sur $\mathbb{F}_2$ pour les **quadrinômes** $x^{am}+x^{bs}+x^{ct}+1$ sur $\mathbb{F}_3$?

Bibliographie

[1] C. Bachoc, "*Cours de codes",* (UE Codes/Signal), Master CSI 2, 2004-2005. U de Bordeaux I.

[2] I. F. Blake, S. Gao and R. J. Lambert, "*Construction and distribution, problems for irreducible trinomials over finite fields, in Applications of, Finite Fields"*, (D. Gollmann, ed.), Oxford, Clarendon Press, 1996, 19-32.

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

[4] J. Boutros, "*Techniques modernes de codage*", Ecole Nationale Supérieure des Télécommunications, 2004. Extrait d'un livre sur les Communications Radiomobiles, édité par Hermes sous la direction de Xavier Lagrange.

[5] R. Brent and P. Zimmermann, "*Algorithms for finding almost irreducible, and almost primitive trinomials, Primes and Misdemeanours*" : Lectures in Honour of the Sixtieth Birthday of Hugh Cowie Williams, The Fields Institute, Toronto, 2004, 91-102.

[6] A. Canteaut, "*Programmation en langage C*", Cours de DEA de Limoges, 2000.

[7] C. Carlet, "*Cours de Codes Correcteurs d'Erreurs et (fonctions booléennes)*", D.E.A de mathématiques et d'informatique, Bamako, 2007.

[8] P. Charpin, "*Open problems on cyclic codes*", Handbook of Coding Theory, V. S. Pless and W. C. Hu man, Eds., Elsevier Science, North-Holland, 1998.

[9] G. Cohen, P. Godlewski and J.L. Dornstetter, "*Codes correcteurs d'erreurs"*, Télécom Paris. Masson, 1992.

[10] H. Cohen, "*A Course In Computational Algebraic Number Theory "*, Springer-Verlag, Berlin Heidelberg, 1993.

[11] J. H. Conway and N. J. A. Sloane, "*A New Upper Bound on the Minimal Distance of Self-Dual Codes*", IEEE Trans. Inform. Theory, vol. 36, no. 6, pp. 1319 1333, Nov. 1990.

[12] R. Daskalov, "*Some high-rate linear codes over* $\mathbb{F}_5$ *and* $\mathbb{F}_7$", Probl. Pered. Inform, vol 43, 2, pp. 65-73, 2007.

[13] R. Daskalov, P. Hristov and E. Metodieva, "*New minimum distance bounds for linear*

codes over $\mathbb{F}_5$", Discrete Mathematics, vol. 275, pp.97-110, 2004.

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

[15] C. Doche, "*Redundant trinomials for finite fields of characteristic 2*", Proceedings of ACISP 05, LNCS 3574, 2005, 122-133.

[16] S. T. Dougherty, T. A. Gulliver and M. Harada, "*Optimal Ternary Formally-Self dual Codes*", Discrete Mathematics, 196, 117-135, 1999.

[17] S. T. Dougherty and M. Harada, "*Shadow Optimal Self-Dual Codes*", Kyushu J. Math, vol. 53, pp. 223 227, 1999.

[18] J. P. Escofier, *"Théorie de Galois",* 2^{e} édition, Dunod, Paris, 2000.

[19] 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.

[20] J. E. Fields, P. Gaborit and W.C. Hufman and V. Pless, "*On the classification of extremal even formally self-dual codes*", Des. Codes and Cryptogr. 18, 1999, 125-148.

[21] J. E. Fields, P. Gaborit, W.C. Hufman and V. Pless, "*On the classication of extremal even formally self-dual codes of lengths 20 and 22*", Discrete Appl. Math. 111 2001, 75-86.

[22] P. Gaborit, "*Table of Self-Dual Codes over* $\mathbb{F}_3$ *and* $\mathbb{F}_5$ ", [tables; online], http://www.unilim.fr/pages_perso/philippe.gaborit/SD/GF5.htm.

[23] P. Gaborit, "*Quadratic Double Circulant Codes over Fields*", J. Combin. Theory Ser. A, vol. 97, pp. 85 107, 2002.

[24] P. Gaborit, C. S. Nedeloaia and A. Wassermann, "*Weight Enumerators of Duadic and Quadratic Residue Codes*", ISIT'04, Chicago, USA, 27 juin - 2 juillet 2004, p. 485.

[25] P. Gaborit, C. S. Nedeloaia and A. Wassermann, "*On the Weight Enumerators of Duadic and Quadratic Residue Codes*", IEEE Trans. Inform. Theory, vol. 51, no. 1, pp. 402 407, Jan. 2005.

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

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

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

[29] L. J. Goldstein, "*Abstract Algebra A First Course"* Printice-Hall, Inc, Englewood Cliffs, New Jersey, 1973.

[30] T. A. Gulliver and M. Harada, "*Classification of extremal double circulant formally self-dual even codes*", Des. Codes Cryptogr. 11 1997, 25-35.

[31] T. A. Gulliver, P. R. J. Ostergard and N. Senkevitch, "*Optimal linear rate 1/2 codes over* $\mathbb{F}_5$ *and* $\mathbb{F}_7$". Discrete Mathematics, vol 265, pp. 59-70, 2003.

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

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

[34] 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.

[35] M. Harada and P.R.J. Ä Ostergard, "*Classification of extremal formally self-dual even codes of length 22*", Graphs Combin. 18, 2002, 507-516.

[36] M. Harada and K. Waki, "*New Extremal Formally Self-Dual Even Codes of Length 30*", 2009.

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

[38] D. B. Jafe, "*Optimal binary linear codes of length 30*", Discrete Math. 226, 2001, 51-70.

[39] R. Kim and W. Koepf, "*Divisibility of Trinomials by Irreducible Polynomials over* $\mathbb{F}_2$", vol 3, no 4, 189-197, 2009. International Journal of Algebra, Vol. 3, 2009, no. 4, 189 - 197.

[40] A. Kostrikin, "*Introduction à L'algèbre",* Edition Mir, Traduction française, 1981.

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

[42] R. Lidl and H. Niederreiter, "*Finite Fields",* Addison-wesley Publishing Company, 1983.

[43] R. Lidl and G. Pilz, "*Applied Abstract Algebra"* Springer-Verlag. New York, 1998.

[44] J. H. van Lint, "*Repeated-Root Cyclic Codes*", IEEE Trans. Inform. Theory, vol. 37, no. 2, pp. 343 345, Mar. 1991.

[45] J. H. van Lint and R. M. Wilson, "*On the Minimum Distance of Cyclic Codes*", IEEE Trans. Inform. Theory, vol. 32, no. 1, pp. 23 40, Jan. 1986.

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

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

[48] T. Maruta, "*Personal communication"*, 2002.

[49] 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.*

[50] 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.

[51] 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.*

[52] C. Mihoubi and P. Solé, "*Optimal and Isodual Ternary Cyclic Codes of rate* $\mathbf{\frac{1}{2}}$*",* Bulletion of Mathematical Sciences, Springer. 2012, 2:343–357/DOI 10.1007/s13373-012-0027-6.

[53] C. S. Nedeloaia, "*On Weight Distributions of Cyclic Self-Dual Codes*", ISIT'02, Lausanne, Suisse, juin-juillet 2002, p. 232.

[54] C. S. Nedeloaia, "*Weight Distributions of Cyclic Self-Dual Codes*", IEEE Trans. Inform. Theory, vol. 49, no. 6, pp. 1582 1591, June 2003.

[55] C. S. Nedeloaia, "*Upper Bounds on the Dual Distances of EBCH Codes*", Rapport de recherche no. 5477, INRIA Rocquencourt, 14 pages, Jan. 2005.

[56] D. Panario, "*A Minicourse in Finite Fields and Applications",* Séptimo Coloquio National de Códigos, Criptografía y Área Relacionadas, part : History of finite fields, page 8, June 2006.

[57] O. Papini and J. Wolfmann "*Algèbre discrète et codes correcteurs*", Mathématiques et Applications, Collection de la SMAI, Springer-Verlag, 1995.

[58] V. Pless and W.C. Hufman "*Handbook of Coding Theory*", North-Holland, 1998.

[59] V. Pless, "*Introduction to the Theory of Error Correcting Codes*", 3rd ed., Wiley, New York, 1998.

[60] 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.

[61] S. Roman, "*Coding and Information Theory",* Springer Verlag 1992.

[62] T. Schaub, "*A linear complexity approach to cyclic codes*", dissertation, Swiss Federal Institute of Technology, Zurich, 1988.

[63] N. J. A. Sloane and J. G. Thompson, "*Cyclic Self-Dual Codes*", IEEE Trans. Inform. Theory, vol. IT-29, no. 3, pp. 364 366, May 1983.

[64] S. A. Spence, "*Introduction to Algebraic Coding Theory*", Supplementary material for Math 336 Cornell University.

[65] R. Swan, "*Factorisation of polynomials over finite fields",* Pacific Journal of Mathematics, Vol 12 pp. 1099-1106, 1962.

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

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

[68] J. L. Yucas and G. L. Mullen, "*Self reciprocal irreducible polynomials over finite fields*", Design, Codes and Cryptography 33, 2004, 275-281.

[69] G. Zémor, "*Corps finis et Applications*", Master CSI, Arithmétique 1, décembre 2006.