REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
****

UNIVERSITE DE YAOUNDE I
ECOLE NORMALE SUPERIEURE
DEPARTEMENT DE MATHEMATIQUES
****

REPUBLIC OF CAMEROUN
Peace – Work – Fatherland
****

UNIVERSITY OF YAOUNDE I
HIGHER TEACHER TRAINING COLLEGE
DEPARTMENT OF MATHEMATICS
****

CODES DANS DES ALGEBRES DE GROUPES

Présentée en vue de l'obtention du Diplôme de Professeur de l'Enseignement Secondaire deuxième grade
Mémoire de D.I.P.E.S II

Par :

NJOUPOUAMIMCHE Chouaibou
Licencié en mathématiques

Sous la direction
Pr MOUAHA Christophe
Maitre de Conférences

Année Académique
2015-2016

DÉDICACE

Je dédie ce mémoire à :

ma feue mère Mme Nzié oussénatou.

REMERCIEMENTS

Je saisis l'occasion qui m'est offerte pour adresser mes vifs remerciements au **Pr. MOUAHA Christophe**, qui au delà de ses multiples occupations m'a attribué un sujet et a guidé mes premiers pas dans la recherche.

Je tiens également à remercier les enseignants de l'École Normale Supérieure de Yaoundé qui m'ont suivi tout au long de ma formation académique

Mes vifs remerciements vont également à :

- ☞ Mon papa M. NGOUMBE Arouna qui m'a toujours soutenu du début jusqu'à la fin et qui continuera à me soutenir
- ☞ Mes parents M.Ndam Amadou et Me DOUYOU JOUERETOU pour leurs soutiens moral, financier et leurs amour sans faille qui ont su me donner la force d'affronter mes défis quotidiens.
- ☞ Merci à toute la famille NDAM pour leur grande affection et leur soutient moral
- ☞ Merci également à tous mes frères et sœurs surtout à mon grand frère Njankouo Amidou qui n'a cessé de m'encourager tout au long de ma formation

RÉSUMÉ

Dans ce mémoire, nous étudions les codes de Reed-Muller qui constituent une des familles de codes les plus étudiés. Ils ont une très bonne représentation dans les algèbres de groupes. Notre travail consiste à étudier la structure des codes de Reed-Muller dans les algèbres de groupes et de montrer qu'ils sont puissance du radical de ces algèbres de groupes

ABSTRACT

In this dissertation, we are studying Reed-Muller code which constitutes one of the most used codes family. they a good representation on group algebra. Our work consists on studying of Reed-Muller codes on group algebra

Table des matières

INTRODUCTION

La théorie de code correcteur d'erreurs, dont l'origine remonte à la fin des années 40 permet de transmettre de façon fiable l'information, codée au moyen de mots binaires d'une longueur donnée, sur des lignes plus ou moins bruitées. La transmission de l'information présente un risque d'erreurs selon les cas.

Les codes correcteur d'erreurs sont présents aujourd'hui dans les domaines de télécommunication. Comme exemple, le code de Reed-Muller R(1,5) a été utilisé par la NASA pour la transmission d'image de la planète Mars via le satellite Mariner 9.

Les codes de Reed-Muller sont très utilisés et très connus. Une étude détaillée des codes de Reed-Muller binaires se trouve dans l'ouvrage de F.J. MacWilliams et N.J.A.Sloane([5], chap. 13 à 15). Ils sont aussi des sous-ensembles d'une algèbre de groupe additif fini.

Ce travail s'étend sur trois chapitres constitués comme suit :

- Le premier chapitre s'intéresse aux généralités sur les structures (groupe, anneaux, corps, codes linaires)
- Dans le deuxième chapitre, nous donnerons la construction des algèbres de groupes sur un corps fini. Nous donnerons ensuite la définition de la puissance du radical de l'algèbre ainsi que ses propriétés
- •• Dans le troisième et le dernier chapitre, nous définirons les codes de Reed-Muller dans l'algèbre de groupe et on étudiera les codes de Reed-Muller vu comme puissance du radical

Chapitre Un

PRELIMINAIRES

1.1 Structures algébriques

1.1.1 Groupes

Définition 1.1.1 *On dit qu'un ensemble non vide G muni d'une loi de composition interne $*$ est un groupe si :*

- *$*$ est associative*

  $\forall x, y, z \in G, (x * y) * z = x * (y * z)$

- *G admet un élément neutre pour $*$*

  $\exists e \in G$ *tel que* $\forall x \in G, e * x = x * e = x$

- *Tout élément de G admet un symétrique pour $*$*

  $\forall x \in G, \exists y \in G$ *tel que* $x * y = e$

Si de plus $*$ est commutative,on dit que G est un groupe abélien

Définition 1.1.2 *Soit $(G, *)$ un groupe, H une partie non vide de G.On dit que H est un sous groupe de G si et seulement si :*

- *H est stable pour $*$*
- *H est un groupe pour la loi induite par la loi $*$ de G*

Proposition 1.1.1 *Une partie non vide H d'un groupe G est un sous groupe de G si :*

- $e \in H$
- $\forall (x, y) \in H^2, x * y^{-1} \in H$

(où e est le neutre de G)

Proposition 1.1.2 *Soit $(G, *)$ un groupe, $(H_i)_{i \in I}$ une famille de sous-groupes de G. Alors $\bigcap_{i \in I} H_i$ est un sous groupe de G*

Définition 1.1.3 *Soit $(G,*)$ un groupe , A une partie non vide de G. L'intersection de tous les sous groupes de G contenant A est un sous groupe de G,appelé* ***sous groupe engendré*** *par A, et noté $< A >$*

Proposition 1.1.3 *Soit $(G,*)$ un groupe, A une partie non vide de G, $< A >$ est (au sens de l'inclusion) le plus petit sous groupe de G contenant A*

Définition 1.1.4 *1 Un groupe G est dit* ***monogène*** *$\exists a \in G$ tel que $G =< a >$*

2 Si G est un groupe monogène,on appelle ***générateur*** *de G tout élément a de G tel que $G =< a >$*

3 Un groupe G est dit ***cyclique*** *si et seulement s'il est monogène et fini*

Définition 1.1.5 *Soient $(G_1,*)$ et $(G_2,.)$ des groupes et f une application de G_1 dans G_2.*
f est un ***morphisme*** *de $(G_1,*)$ dans $(G_2,.)$ quand $\forall (x,y) \in G_1^2, f(x*y) = f(x).f(y)$*

1.1.2 Anneaux

Définition 1.1.6 *Un anneau $(A,+,\times)$ est la donnée d'un ensemble A muni de deux lois internes + et $\times$ et vérifiant :*

- *$(A,+)$ est un groupe abélien*
- *La multiplication $\times$ est associative c'est-à-dire $\forall x,y,z \in A$,*
  on a, $x \times (y \times z) = (x \times y) \times z$
- *La multiplication $\times$ est distributive sur l'addition + c'est à dire que $\forall x,y,z \in A$,*
  on a, $x \times (y+z) = x \times y + x \times z$ et $(y+z) \times x = y \times x + z \times x$

Si la multiplication est commutative, on dit que l'anneau A est commutatif. S'il existe un élément $1 \in A$ tel que $\forall a \in A, 1 \times a = a \times 1 = a$ (élément neutre pour la multiplication noté 1_A), alors l'anneau A est commutatif ou unitaire

Définition 1.1.7 *Soit A un anneau. On appelle idéal de A toute partie I de A telle que :*

- $I \neq \varnothing$
- $\forall x,y \in I, x-y \in I$
- $\forall a \in A, \forall x \in I, ax \in I$

Définition 1.1.8 *Soit A un anneau commutatif , $a \in A$ et b A*

i) L'élément a est un diviseur de zéro si $a \neq 0_A$ et s'il existe $x \neq 0_A$ tel que $ax = 0_A$

ii) A est intègre s'il n'admet pas de diviseur de zéro

iii) L'élément b divise a si $a \in bA$

iv) Si 1_A existe , un élément a est dit inversible de A si $1_A \in aA$, dans ce cas on note $A^\times = \mu(A)$ l'ensemble des unités de A

v) L'élément $a \in A$ est dit nilpotent s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$

vi) L'élément $a \in A$ est dit régulier si $a \neq 0_A$ et pour tout $x, y \in A, ax = ay$ implique $x = y$

vii) L'entier $n = min\{k \in \mathbb{N}^* | a^k = 0_A\}$ est l'indice de nilpotence de a.

On note $\eta(A)$ l'ensemble des éléments nilpotents de A.

viii) Un idéal I de A est premier si $\forall a, b \in I$ tel que $ab = 0$, alors $a = 0$ où $b = 0$

Proposition 1.1.4 *Soit A un anneau commutatif unitaire et intègre. Alors :*

i) Tout élément nilpotent de A est un diviseur de zéro

ii) Si A est fini, alors tout élément a de A est inversible si et seulement s'il est régulier

iii) $\eta(A)$ est un idéal de A

iv) $\eta(A)$ est l'intersection de tous les idéaux premiers de A

Preuve:

i) Soit $a \in A$ un élément nilpotent, alors $a \neq 0_A$ et il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$, on a $aa^{n-1} = 0_A$. Si $a^{n-1} = 0_A$ alors, cela contredirait la minimalité de l'indice de nilpotence de a. Ainsi, $a^{n-1} \neq 0_A$, $a \neq 0_A$ et $aa^{n-1} = 0_A$. Donc a est un diviseur de zéro

ii) Supposons que A est fini.

$\Longrightarrow$) Soit $a \in A$ un élément inversible de A. On a $a \neq 0_A$ car 0_A n'est pas inversible. Pour tout $x, y \in A$ tel que $ax = ay$, on a :

$$x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = y.$$

D'où a est régulier.

$\Longleftarrow$) Soit $a \in A$ un élément régulier. Montrons que a est inversible.

Considérons l'application $g_a : A \longrightarrow A$ telle que $g_a(x) = ax$. g_a dispose de deux identités à savoir $g_a(x + y) = g_a(x) + g_a(y)$ et $bg_a(x) = g_a(xb)$ pour tous $x, y, b \in A$. Ces deux identités font de $g_a(A)$ un idéal de A. En outre, g_a est une application

injective. En effet, soit $x, y \in A$ tel que $g_a(x) = g_a(y)$. On a $ax = ay$ se qui implique $x = y$ car a est un élément régulier de A. De ce fait, $g_a(A)$ est un idéal de A isomorphe à A, se qui donne $g_a(A) = A$. Or $g_a(A) = aA$, par suite, $aA = A$. Comme $1_A \in A = aA$ alors $1_A = ax, x \in A$ se qui fait que a est un élément inversible

iii) $\eta(A) \neq \varnothing$ car $0_A \in \eta(A)$.

Soit $x, y \in \eta(A)$. Alors, il existe $n, m \in \mathbb{N}^*$ tels que $x^n = 0_A$ et $y^m = 0_A$. On a :

$$(x-y)^{n+m+1} =$$

$$\sum_{k=0}^{n+m+1} C_{n+m+1}^k (-1)^k x^k y^{n+m+1-k} = \sum_{k=0}^{n} C_{n+m+1}^k (-1)^k x^k y^{n+m+1-k} + \sum_{k=n+1}^{n+m+1} C_{n+m+1}^k (-1)^k x^k y^{n+m+1-k}$$

. Or :

$\forall k = 0, ..., n, n+m+1-k \geqslant m$ donc $y^{n+m+1-k} = 0$. D'où $\sum_{k=0}^{n} C_{n+m+1}^k (-1)^k x^k y^{n+m+1-k}$.

Par ailleurs, $\forall k = n+1, ..., n+m+1$ on a $k \geqslant n$ donc $x^k = 0$. D'où $\sum_{k=0}^{n+1} C_{n+m+1}^k (-1)^k x^k y^{n+m+1-k} = 0$.

On en déduit que $(x-y)^{n+m+1} = 0_A$ c'est-à-dire $x - y \in \eta(A)$.

Soient $a \in \eta(A)$. Alors il existe $n \in \mathbb{N}^*$ tel $a^n = 0_A$. Ainsi, $\forall x \in A, (xa)^n = x^n a^n = 0_A$ car A commutatif. D'où $\forall x \in A, xa \in \eta(A)$.

iv) Désignons par $\mathcal{P}$ l'ensemble des idéaux premiers et montrons $\eta(A) = \bigcap_{I \in \mathcal{P}} I$.

Soit $a \in \eta(A)$. Alors il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$. Soit I un idéal premier de A. Montrons que $a \in I$.

Supposons que $a \notin I$. On a $a^{n-1}a = 0_A \in I$ c'est-à-dire $a^{n-1}a \in I$. Comme I est premier et $a \notin I$, on a $a^{n-1} \in I$.

$a^{n-2}a = a^{n-1} \in I$. D'où $a^{n-2} \in I$ car I premier et $a \notin I$. Ainsi de suite on trouve $a \in I$ se qui est absurde. D'où $a \in I$, on obtient donc $a \in \bigcap_{I \in \mathcal{P}} I$. D'où $\eta(A) \subseteq \bigcap_{I \in \mathcal{P}} I$.

Montrons que $\bigcap_{I \in \mathcal{P}} I \subseteq \eta(A)$.

$\eta(A)$ est un idéal de A. Soit $x, y \in A$ tel que $xy \in \eta(A)$. Alors il existe $m \in \mathbb{N}^*$ tel que $(xy)^m = 0_A$, c'est-à-dire $x^m y^m = 0_A$ car A est commutatif d'où $x^m = 0_A$ ou $y^m = 0_A$ car A intègre c'est-à-dire $x \in \eta(A)$ ou $y \in \eta(A)$ donc $\eta(A) \in \mathcal{P}$. D'où $\bigcap_{I \in \mathcal{P}} I \subseteq \eta(A)$. ■

Définition 1.1.9 *Soit A un anneau commutatif et unitaire. On appelle caractéristique de A notée caract(A), l'ordre additif du neutre multiplicatif* 1_A

Exemple 1.1.1

Pour tout entier naturel n, caract$(\mathbb{Z}_{)} = n$

Définition 1.1.10 *Soit A un anneau commutatif et unitaire et I un idéal de A. Alors l'idéal I est maximal parmi les idéaux de A si* $I \neq A$ *et pour tout idéal K tel que* $I \subseteq K \subseteq A$, *on a* $I = K$ *ou* $K = A$

Corollaire 1.1.1 *Soit A un anneau commutatif unitaire. Pour qu'un élément de A soit inversible, il faut et il suffit qu'il n'appartient à aucun idéal maximal*

Preuve:

$\Longrightarrow$) Soit $a \in A$ un élément inversible. Il existe $b \in A$ tel que $ab = 1_A$. Si M est un idéal maximal de A contenant a on aurait $1_A = ab \in M$ car M est un idéal d'où $M = A$ se qui contredit le fait que M soit un idéal maximale de A. Donc a n'appartient à aucun idéal maximal de A.

$\Longleftarrow$) Soit a un élément de A qui n'appartient à aucun idéal maximal de A. Si on suppose que a n'est pas inversible, alors $aA \neq A$ (sinon avec $aA = A$, comme $1_A \in A = aA$ alors $1_A = ax, x \in A$ se qui ferait de a un élément inversible). Or avec $aA \neq A$ il vient que aA est un idéal de A distinct de A d'où $aA \subseteq M$ où M est un idéal maximal de A (car d'après Krull, si est A est un anneau commutatif unitaire alors, tout idéal de A distinct de A est contenu dans un idéal maximal de A). Par conséquent $a \in M$ puisqu'en particulier $1_A \in A, a = a1_A \in M$ se qui contredit le fait que $a \notin T$ pour tout T idéal maximal de A. D'où a est inversible ■

Définition 1.1.11 *Un anneau commutatif unitaire est dit local s'il possède un unique idéal maximal*

Notation 1.1.1. Si A est un anneau local on désigne par m_A son idéal maximal

Proposition 1.1.5 *Si A est un anneau local fini, alors* $m_A = \eta(A)$

Preuve:

Soit P un idéal premier de A (P existe car tout idéal maximal est premier). Alors A/P est intègre et fini d'où A/P est un corps. Ainsi, $P = m_A$ car m_A est l'unique idéal maximal. Puisque $\eta(A)$ est l'intersection de tous les idéaux premiers de A, on a :

$\eta(A) = m_A \cap m_A \cap ... \cap m_A = m_A$ ■

1.1.3 Corps

Définition 1.1.12 *Un corps est un anneau unitaire dans lequel tout élément non nul est inversible*

Remarque 1.1.1

Lorsque la cardinalité d'un corps est fini, on parle de corps de Galois ou de corps fini

Notation 1.1.2 : Le corps fini de cardinal q est noté F_q ou GF(q) (Galois field)

Théorème 1.1.1 *Soit $\mathbb{K}$ un corps fini commutatif d'élément unité 1. Il existe un entier positif p premier tel que :*

i) $\mathbb{K}$ contient un sous corps Π_p isomorphe à $\mathbb{K}$

ii) Π_p est l'ensemble des éléments de $\mathbb{K}$ de la forme $\pm(n.1)$ avec $n \in \mathbb{N}$ et $n.1 = \overbrace{1 + 1 + ... + 1}^{n\ fois}$

iii) p est le plus petit des entiers strictement positifs n tel que $n.1 = 0$

Preuve:

On définit une application π de $\mathbb{Z}$ dans $\mathbb{K}$ de la manière suivante :

$$\pi(a) = \begin{cases} 0 \text{ si } a = 0 \\ \overbrace{1 + ... + 1}^{a\ fois} \text{ si } a > 0 \\ -\overbrace{(1 + ... + 1)}^{a\ fois} \text{ si } a < 0 \end{cases}$$

Pour rappeler la définition, on désignera provisoirement $\pi(a)$ par $a.1$. On montre facilement que π est un morphisme d'anneaux. D'après le premier théorème d'isomorphisme, l'image $\pi(\mathbb{Z})$ est isomorphe à $\mathbb{Z}/ker(\pi)$, avec $ker(\pi) = \{a \in \mathbb{Z}/a.1 = 0\}$. On sait que $ker(\pi)$ est un idéal de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ avec $p \in \mathbb{N}$. Puisque $\mathbb{K}$ est fini, il en est de même pour $\pi(\mathbb{Z})$. L'application π ne peut être injective car sinon l'ensemble fini $\pi(\mathbb{Z})$ serait en bijection avec l'ensemble infini $\mathbb{Z}$. En conséquence $ker(\pi) \neq 0$ et donc :

(1) $p \neq 0$.

$ker(\pi)$ ne peut être égal à $\mathbb{Z}$ car $\pi(1) = 1$, et donc :

(2) $p \neq 1$.

Puisque $ker(\pi) \neq 0$, alors d'après une propriété des idéaux de $\mathbb{Z}$, p est le plus petit élément strictement positif de $ker(\pi)$. C'est-à-dire :

(3) p est le plus petit entier $n > 0$ tels que $n.1 = 0$.

Soient p_1 et p_2 deux entiers tels que $p = p_1p_2$. On voit facilement que $p.1 = (p_1p_2).1 =$

$(p_1.1)(p_2.1)$. Puisque $p.1 = 0$ et $\mathbb{K}$ intègre ($\mathbb{K}$ est un corps), on en déduit que $p_1.1 = 0$ ou $p_2.1 = 0$. Les deux facteurs p_1 et p_2 étants inférieurs à p, la seule possibilité compatible avec (1) et (3) est que l'un de ces facteurs soit égal à p et l'autre à 1. Autrement dit et d'après (2) :

(4) p est un nombre premier.

En conséquence, $\mathbb{Z}/ker(\pi) = \mathbb{Z}/p\mathbb{Z}$ est le corps F_p. l'image ${}_pi(\mathbb{Z})$ étant isomorphe à $\mathbb{Z}/ker(\pi)$, on obtient :

(5) $\pi(\mathbb{Z})$ est un corps isomorphe au corps premier F_p

Définition 1.1.13 *Le sous corps Π_p du théorème précédent s'appelle le sous corps premier de $\mathbb{K}$.*

Le nombre p de ce même théorème s'appelle la caractéristique de $\mathbb{K}$

Proposition 1.1.6 *Si p est la caractéristique d'un corps commutatif fini $\mathbb{K}$, alors le cardinal de $\mathbb{K}$ est une puissance de p*

Preuve:

$\mathbb{K}$ est un espace vectoriel sur F_p. Puisse $\mathbb{K}$ est fini , cet espace vectoriel est de dimension finie. Si r est cette dimension , alors $\mathbb{K}$ est isomorphe en tant qu'espace vectoriel à $(F_p)^r$. Le cardinal de $\mathbb{K}$ est donc $|(F_p)^r| = |F_p|^r = p^r$ ■

Proposition 1.1.7 *Si $\mathbb{K}$ est un corps commutatif fini donc le cardinal est p^r, alors :*
$\forall x \in \mathbb{K}, \quad x^{p^r} = x$

Preuve:

i) Si $x = 0$, alors $x^{p^r} = x$

ii) Si $|\mathbb{K}| = p^r$, alors le cardinal du groupe multiplicatif de $\mathbb{K}$ est $|\mathbb{K}\backslash\{0\}| = p^{r-1}$. Donc pour $x \neq 0$, on obtient $x^{p^r-1} = 1$ se qui implique $x^{p^r} = x$ ■

Définition 1.1.14 *Un générateur du groupe multiplicatif d'un corps $\mathbb{K}$ fini s'appelle une racine primitive de $\mathbb{K}$ ou un élément primitif*

Proposition 1.1.8 *Soit $\mathbb{K}$ un corps commutatif fini de caractéristique p, et soit $\beta \in \mathbb{K}$. L'ensemble I_β des polynômes à coefficients dans F_p ayant β comme racine dans $\mathbb{K}$ est un idéal de $F_p[x]$*

Définition 1.1.15 *Le générateur de l'idéal I_β de $F_P[x]$ s'appelle le polynôme minimal de β*

Théorème 1.1.2 *Soit $\mathbb{K}$ un corps fini de caractéristique p. Si α est une racine primitive de $\mathbb{K}$, alors $\mathbb{K} = F_p(\alpha)$.*

Preuve:

Si α est une racine primitive de $\mathbb{K}$, alors tout élément de $\mathbb{K}$ est de la forme $u = \alpha^i$ avec $0 \leq i \leq |\mathbb{K}| - 2$ car le cardinal de $\mathbb{K}^*$ est $|\mathbb{K}| - 1$. Si $f(x) = x^i$, alors $u = f(\alpha)$, se qui montre que $u \in F_p(\alpha)$. Ceci prouve que $\mathbb{K} = F_p(\alpha)$ ■

Exemple 2.1.1 (Construction de F_4) Puisque $4 = 2^2$ on a besoin d'un polynôme unitaire de degré 2, irréductible sur F_2. Soit $f(x) = x^2 + x + 2$. Puisque $f(0) = 1$ et $f(1) = 1$ (calcul dans F_2), on voit que $f(x)$ n'a pas de racine dans F_2 et donc pas de diviseur de degré 1 sur F_2. Il est donc irréductible sur F_2. Si α est une racine primitive dont $f(x)$ est le polynôme minimal , alors $f(\alpha) = 0$, soit $\alpha^2 = \alpha + 1 = 0$, donc $\alpha^2 = \alpha + 1$.

On en déduit que $\alpha^3 = \alpha^2 + \alpha = 1$.

Finalement $F_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$

Définition 1.1.16 *Un automorphisme d'un corps $\mathbb{K}$ est un isomorphisme de $\mathbb{K}$ dans $\mathbb{K}$*

Proposition 1.1.9 *Soit $\mathbb{K}$ un corps fini de caractéristique p, et soit γ un automorphisme d'un corps $\mathbb{K}$, alors :*

$\forall u \in F_p, \quad \gamma(u) = u.$

On dit qu'un automorphisme fixe chaque élément du sous corps premier.

Preuve:

Si γ est un automorphisme de $\mathbb{K}$, alors c'est un morphisme pour les groupes additif et multiplicatif de $\mathbb{K}$. Par conséquent, $\gamma(0) = 0, \gamma(1) = 1$. De plus, si $u \in F_p \backslash \{0\,1\}$, alors $u = \overbrace{1 + 1 + ... + 1}^{u fois}$ et on a :

$$\begin{aligned} \gamma(u) &= \gamma(1) + \gamma(1) + ... + \gamma(1) \\ &= 1 + 1 + ... + 1 \\ &= u \end{aligned}$$

■

Proposition et définition 1.1.1 Soit $\mathbb{K}$ un corps de caractéristique p. L'application Φ de $\mathbb{K}$ dans $\mathbb{K}$ définie par $\Phi(x) = x^p$ est un automorphisme de $\mathbb{K}$. Cette application s'appelle l'automorphisme de Frobenius de $\mathbb{K}$ (sur F_p)

Preuve:

On a $\Phi(x+y) = (x+y)^p = x^p + y^p = \Phi(x) + \Phi(y)$.

De plus, $\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y)$.

Si $\Phi(x) = \Phi(y)$, alors $x^p = y^p$ ou encore $x^p - y^p = 0$. On en déduit que $(x-y)^p = 0$, et finalement $x = y$. L'application Φ est donc injective et, puisque $\mathbb{K}$ est fini, elle est aussi bijective. ■

Définition 1.1.17 *Les automorphismes de Galois de $\mathbb{K}$ (sur F_p) sont les puissances (au sens de la composition des applications) de l'automorphisme de Frobenius.*
L'ensemble des automorphismes de Galois de $\mathbb{K}$ est donc le groupe cyclique engendré par Φ dans le groupe des permutations de $\mathbb{K}$. On l'appelle groupe de Galois de $\mathbb{K}$ (sur F_p)

Théorème 1.1.3 *Si $\mathbb{K}$ est un corps fini de cardinal p^n, alors l'ordre du groupe de Galois de $\mathbb{K}$ (sur F_p) est n*

Preuve:

Soit α une racine primitive de $\mathbb{K}$, et soit Φ l'automorphisme de Galois sur $\mathbb{K}$. Nous savons que $\forall x \in \mathbb{K}$, $\Phi^n(x) = x^{p^n} = x$, et donc $\Phi^n = Id_{\mathbb{K}}$.

Soit un entier tel que $1 \leq s \leq n$ et $\Phi^s = Id_{\mathbb{K}}$, alors $\forall x \in \mathbb{K}$, $\Phi^s(x) = x$. En particulier , si α est une racine primitive de $\mathbb{K}$: $\Phi^s(\alpha) = \alpha$, c'est-à- dire $\alpha^{p^s-1} = 1$.

L'ordre de α dans le groupe multiplicatif de $\mathbb{K}$ étant $p^n - 1$ on en déduit que $p^n - 1$ divise $p^s - 1$, et donc $n \leq s$. Mais $s \leq n$, d'ou $n = s$.

L'entier n est le plus petit des entiers strictement positif r tel que $\Phi^r = Id_{\mathbb{K}}$. L'ordre de Φ est donc n ■

Corollaire 1.1.2 *Si $\mathbb{K}$ est un corps fini de cardinal p^n et si Φ est l'automorphisme de Frobenius de $\mathbb{K}$, alors les éléments du groupe de Galois de $\mathbb{K}$ sont les Φ^i avec $0 \leq i \leq n-1$*

1.2 Codes linéaires

Soit A un ensemble fini et $n \in \mathbb{N}, n \geq 2$

Theoreme et definition 1.2.1 L'application :

$$\begin{aligned} d_H : \quad A^n \times A^n &\longrightarrow \mathbb{N} \\ (x, y) &\longmapsto card\{i \in \{1, ..., n\} | x_i \neq y_i\} \end{aligned}$$

où $x = (x_1, ..., x_n)$, et $y = (y_1, ..., y_n)$

est une distance appelée **distance de Hammimg**

Preuve:

La symétrie et la séparation sont immédiats.

Montrons l'inégalité triangulaire.

Soient $x = (x_1, ..., x_n)$, $y = (y_1, ..., y_n), z = (z_1, ..., z_n) \in A^n$. Montrons que

$d_H(x, z) \leq d_H(x, y) + d_H(y, z)$.

Posons $A = \{i = 1, ..., n | x_i \neq z_i\}$, $B = \{i = 1, ..., n | x_i \neq y_i\}$ et $C = \{i = 1, ..., n | y_i \neq z_i\}$.

Montons $A \subseteq B \cup C$.

Soit $i \in A$ tel que $i \notin B \cup C$. On a :

$x_i \neq z_i$ et $i \notin B$, $i \notin C$

$x_i \neq z_i$ et $x_i = y_i$, $y_i = z_i$.

$x_i \neq z_i$ et $x_i = z_i$.

Ainsi $A \subseteq B \cup C$ et on a $|A| \leq |B \cup C| \leq |B| + |C|$

Définition 1.2.1 *On appelle code sur A de longueur n,tout sous ensemble non vide de A^n (muni de la distance de Hamming)*

Dans la suite l'alphabet A sera un corps de Galois $\mathbb{F}_q$ où $q = p^m$ est une puissance d'un nombre premier

Définition 1.2.2 *L'application*

$$\begin{array}{rccc} w_H : & (\mathbb{F}_q)^n & \longrightarrow & \mathbb{N} \\ & (x_1, ..., x_n) & \longmapsto & w_H(x) = card(\{i \in \{1, ..., n\} | x_i \neq 0\}) \end{array}$$

est appelé poids de Hamming de $(x_1, ..., x_n)$

Remarque 1.2.1

$\forall x, y \in (\mathbb{F}_q)^n, d_H(x, y) = w_H(x - y)$

Définition 1.2.3 *Soient $k, n \in \mathbb{N}$ avec $k \leq n$.*

Un code linéaire de longueur n et de dimension k est un sous espace vectoriel de dimension k de $(\mathbb{F}_q)^n$.

Un tel object sera alors appelé un $[n, k]-$ code ou un $[n, k]-$ code sur $\mathbb{F}_q$

Définition 1.2.4 *Soit C un* $[n,k]-$ *code sur* $\mathbb{F}_q$.
On définit la distance minimale de C par

$$d_{min}(C) = \min_{c,c' \in C, c \neq c'} d_H(c,c') = \min_{c \in C, c \neq 0} w_H(c)$$

Cette distance est habituellement noté d et ainsi, on parlera d'un $[n,k,d]$-code sur $\mathbb{F}_q$
La distance minimale d'un code est une quantité primordiale puisqu'elle caractérise la capacité de correction de code

1.2.1 Matrice génératrice et codes équivalents

Soit C un $[n,k]-$ code sur $\mathbb{F}_q$. Comme C est un sous espace vectoriel de $\mathbb{F}_q^n$ de dimension k,on peut le représenter par une de ses $\mathbb{F}_q$-bases $(c_1,....,c_k)$

Définition 1.2.5 *Soit C un* $[n,k]$*-code sur* $\mathbb{F}_q$*.Soit* $(c_1,....,c_k)$ *une base de C. Alors la matrice* $G = \begin{pmatrix} c_1 \\ c_2 \\ . \\ . \\ . \\ c_k \end{pmatrix}$
est appelée une matrice génératrice de C.

Définition 1.2.6 *Soit* $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ *une application. On dit que f est une transformation monomiale s'il existe* $(a_1,...,a_n) \in \mathbb{F}_q^{*n}$ *et il existe* $\sigma \in S_n$ *tel que :*

$$\forall x = (x_1,...,x_n) \in \mathbb{F}_q^n, f(x) = (a_1 x_{\sigma(1)},...,a_n x_{\sigma(n)})$$

Définition 1.2.7 *Deux codes linéaire C et C' sont dits équivalents s'il existe une transformation monomiale f telle que :*

$$C' = f(C) \quad où \quad f(C) = \{f(x), x \in C\}$$

Remarque 1.2.2

Un code reste inchangé si on permute les lignes de sa matrice génératrice ou si on remplace une ligne par une combinaison linéaire de cette ligne avec d'autres lignes de cette matrice. En effectuant ces opérations sur les colonnes d'une matrice génératrice d'un code, on obtient un code qui lui est équivalent.

Définition 1.2.8 *Soient C un $[n,k]$-code et G une matrice génératrice de C. On dit que G est sous forme systématique si elle est de la forme*
$G = (I_k|R)$ *où* $R \in M_{k,n-k}(\mathbb{F}_q)$.

Proposition 1.2.1 *Tout code linéaire est équivalent à un code systématique.*

Preuve:

Soit C un $[n,k,d]$-code de matrice génératrice G. Comme G est de rang k, on peut permuter les colonnes de G de façon à obtenir une matrice $G' = [P \mid A]$ où P est une matrice $k \times k$ et A une matrice $k \times n-k$. la matrice G' engendre un code C' équivalent à C d'après la remarque précédente. On multiplie maintenant la matrice G' par P^{-1} pour avoir une matrice $G'' = [I_k \mid A']$. Le code engendré par la matrice G" est équivalent au code C car multiplier par P^{-1} revient à effectuer des opérations élémentaires sur les lignes de G'(se qui laisse inchangé le code C') de façon à obtenir une matrice $k \times k$ et ensuite multiplier chaque ligne par un scalaire particulier(se qui permet d'avoir un code équivalent à C') pour avoir une matrice génératrice ■

Exemple 1.2.1

Soit C le code linéaire binaire ayant pour matrice génératrice

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

Si on prend $S = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, *alors* $G' = SG = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$ *est une forme systématique*

Proposition 1.2.2 *(Borne de Singleton)*

Soit C un code de paramètre $[n,k,d]$.Alors :

$d \leq n-k+1$

Preuve:

Soit C un $[n,k,d]$-code dont sa matrice génératrice G est sous forme systématique c'est-à-dire $G = (I_k|R)$ où $R \in M_{k,n-k}(\mathbb{F}_q)$. Soit c_1 le mot de C. Alors $w_H(c_1) \leq n-(k-1) = n-k+1$. Or $d \leq w_H(c_1) \leq n-k+1$. D'où $d \leq n-k+1$ ■

Lorsque cette borne est atteinte,c'est à dire quand $d = n-k+1$, on parle de code MDS (Maximum Distance Séparable)

Exemple 1.2.2

Prenons comme exemple le code binaire de longueur 4.

$C = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$ *il a pour dimension 3 et a bien pour distance minimale* $2 = 4 - 3 + 1$

1.2.2 Dual d'un code linéaire

Un code étant un sous-espace vectoriel d'un certain $(\mathbb{F}_q^n)$, on peut s'intéresser à son espace dual.

Définition 1.2.9 *Soient* $c = (c_1, ..., c_n)$ *et* $d = (d_1, ..., d_n)$ *des vecteurs de* $(\mathbb{F}_q^n)$. *On appelle produit scalaire entre c et d la quantité*

$$< c, d >= \sum_{i=1}^{n} c_i d_i$$

Remarquons que le terme de produit scalaire est en fait un abus de langage (cette application bilinéaire n'est pas définie positive).

Définition 1.2.10 *Soit C un* $[n, k]$*-code sur* $\mathbb{F}_q$. *On définit son code dual noté* $C^\perp$ *par*

$$C^\perp = \{d \in (\mathbb{F}_q^n) \mid \forall c \in C, \ < c, d >= 0\}$$

Ainsi, $C^\perp$ est un $[n, n-k]$-code sur $\mathbb{F}_q$.

De la même manière que pour la matrice génératrice d'un code, on peut définir une matrice générant le code dual.

Définition 1.2.11 *Soit C un* $[n, k]$*-code sur* $\mathbb{F}_q$. *On appelle matrice de parité de C toute matrice génératrice H de son code dual* $C^\perp$.

On a donc :

$$\forall c \in C, H^t c = 0$$

Ainsi, si G est une matrice génératrice de C, on a :

$$G^t H = 0$$

Il est donc facile de construire une matrice de parité d'un code à partir d'une matrice génératrice de ce code.

Proposition 1.2.3 *Soient C un $[n,k]$-code et G une matrice génératrice de C sous forme systématique $G = (I_k|R)$ où $R \in M_{k,n-k}(\mathbb{F}_q)$*

Alors la matrice

$$H = (-{}^tR|I_{n-k})$$

est une matrice de parité de C

Exemple 1.2.3

Prenons pour exemple le code de Hamming de longueur 7. Les codes de Hamming forment une famille de codes linéaires de longueur $2^m - 1$, de dimension $2^m - m - 1$ et de distance minimal 3. Ils permettent ainsi de corriger des erreurs de poids 1. Une matrice de parité de ces codes est obtenu en listant sur les colonnes tous les vecteurs binaires de longueur m non nul.

Dans notre exemple il s'agit d'un code de paramètres $[7,4,3]$.

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

Et ainsi C possède une matrice génératrice de la forme :

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

ALGEBRES DE GROUPES

2.1 Algèbres de groupes

Soit F un coprs fini

G un groupe additif fini.

$F[G]$ est l'ensemble des applications de G vers F.

Pour tout $g \in G$ X^g est la fonction caractéristique de $\{g\}$ c'est-à-dire :

$$\begin{array}{cccc} X^g & G & \longrightarrow & F \\ & h & \longmapsto & X^g(h) = \begin{cases} 1 & si \quad g = h \\ 0 & si \quad g \neq h \end{cases} \end{array}$$

Posons $F[G] = \{\sum_{g \in G} x_g X^g, x_g \in F\}$

Un élément de $F[G]$ est un polynôme et les opérations dans $F[G]$ sont celles usuelles d'addition et de multiplication de polynômes ;le polynôme nul est l'élément neutre pour l'addition,et le polynôme X^0 ,noté aussi 1 est l'élément neutre pour la multiplication

2.1.1 Construction de l'algèbres F[G]

On définissons sur $F[G]$ les opérations suivantes :

L'addition :

$$\begin{array}{cccc} (+): & F[G] \times F[G] & \longrightarrow & F[G] \\ & (x, y) & \longmapsto & x + y \end{array}$$

Où $\forall g \in G \quad x = \sum_{g \in G} x_g X^g \quad$ et $\quad y = \sum_{h \in G} x_h X^h$

$$(x+y)(g) = \sum_{g\in G}(x_g + y_g)X^g$$

Le produit

$$\begin{array}{rccc}(\times): & F[G]\times F[G] & \longrightarrow & F[G]\\ & (x,y) & \longmapsto & xy\end{array}$$

$$(x\times y)(g) = \sum_{g\in G} x_g X^g . \sum_{h\in G} x_h X^h = \sum_{h\in G}(\sum_{g\in G} x_g y_{h-g} X^h)$$

Produit par un scalaire

$$\begin{array}{rccc}(.): & F\times F[G] & \longrightarrow & F[G]\\ & (\lambda,x) & \longmapsto & \lambda.x\end{array}$$

Où $\forall g \in G ; (\lambda x)(g) = \sum_{g\in G} \lambda x_g X^g = \lambda \sum_{g\in G} x_g X^g = \lambda x(g)$

Muni de ces trois lois, $(F[G], +, ., \times)$ est une F-algèbre associative et unitaire d'unité X^e (e étant l'élément neutre de G) c'est-à-dire :

a) $(F[G], +, .)$ est un espace vectoriel sur F

b) $(F[G], +, \times)$ est un anneau

c)$\forall x \in F$, $\forall a, b \in G$, $x.(a\times b) = (x.a)\times b = a\times(x.b)$

Remarque 2.1.1

Lorsque G est commutatif , $F[G]$ est une F algèbre commutative

Définition 2.1.1 *$F[G]$ est appelé **algèbre du groupe** G*

Dans toute la suite ;$\forall x, y \in G$ et $g \in G$ nous noterons $x\times y$, $\lambda.x$ et $x(g)$ par xy , λx ,et x_g

Exemple 2.1.1

Soit $m \in \mathbb{N}^*$, $m \geq 1$, $F_2[F_{2^m}]$ est la F_2- algèbre du groupe F_{2^m}

Si G est un groupe d'ordre n, $G =< x >$,$x \in G$ alors $F[G] = \sum_{i=0}^{n-1} \alpha_i x^i$ et $F[G] \cong \dfrac{F[G]}{(X^n - 1)}$

Définition 2.1.2

- *Une sous algèbre de $F[G]$ est une partie non vide de $F[G]$ stable par les opérations de $F[G]$*
- *Une sous-algèbre $\boldsymbol{I}$ de $F[G]$ est un idéal si $\forall x \in \boldsymbol{I}, \forall y \in F[G]$ on a $xy \in \boldsymbol{I}$*

Définition 2.1.3 *Soit $h \in G$. Alors :*

L'application

$$\begin{array}{rccc} \sigma_h : & F[G] & \longrightarrow & F[G] \\ & \sum_{g\in G} x_g X^g & \longmapsto & \sum_{g\in G} x_g X^{g+h} \end{array}$$

est appelé h-translation de $F[G]$

Proposition 2.1.1 *Un sous espace de $F[G]$ est un idéal de $F[G]$ si et seulement s'il est stable par chaque translation $\sigma_h, h \in G$*

Preuve:

Soit $\mathbf{I}$ un idéal de $F[G]$. Alors :

$\forall h \in G, \forall x \in \mathbf{I}, x = \sum_{g\in G} x_g X^g$

$$\begin{aligned} \sigma_h(x) &= \sum_{g\in G} x_g X^{g+h} \\ &= X^h(\sum_{g\in G} x_g X^g) \\ &= X^h x \in \mathbf{I} \end{aligned}$$

Donc $\mathbf{I}$ est stable par toutes les translations $\sigma_h, h \in G$.

Réciproquement,supposons que $\mathbf{I}$ est un sous espace vectoriel de $F[G]$ stable par chaque translation.

Soient $x = \sum_{g\in G} x_g X^g \in \mathbf{I}$ et $y = \sum_{h\in G} u_h X^h \in F[G]$.On a :

$$\begin{aligned} xy &= \sum_{h\in G} x_h(\sum_{g\in G} x_g X^{g+h}) \\ &= \sum_{h\in G} x_h \sigma_h(x) \end{aligned}$$

Comme $\mathbf{I}$ est un sous espace vectoriel de $F[G]$ stable par chaque translation,on en déduit que $xy \in \mathbf{I}$ et par suite,$\mathbf{I}$ est un idéal de $F[G]$

Proposition 2.1.2 $dim_F F[G] = |G|$

Preuve:

Soit $x \in F[G]$ et $h \in G$. Alors $x = \sum_{g\in G} x_g X^g(h) = \sum_{g\in G} x_g X^g(h) = x(h)$.

Se qui montre que $x = \sum_{g\in G} x_g X^g$. D'où la famille $\{X^g, g \in G\}$ est une famille génératrice de $F[G]$.

Soit $(a_g)_{g\in G}$ une famille d'éléments de F telle que : $\sum_{g\in G} a_g X^g = 0$. Alors $\forall h \in G$, on a : $\sum_{g\in G} a_g X^g(h) = a_h = 0$. Ainsi, $\{X^g, g \in G\}$ est en plus une famille libre de $F[G]$; c'est donc une base de $F[G]$.

Par conséquent, $dim_F(F[G]) = \text{card}(\{X^g, g \in G\}) = |\, G \,|$

Cas particulier où $F = F_p$ et $G = F_{p^m}$, p nombre premier

Lemme 2.1 *. Soit $x \in F_p[F_{p^m}]$. Alors x est soit nilpotent soit inversible (où une unité)*

Preuve:

On a :

$$\begin{aligned} x &= \sum_{g \in F_{p^m}} x_g X^g \text{ . D'où :} \\ x^p &= (\sum_{g \in F_{p^m}} x_g X^g)^p \\ &= \sum_{g \in F_{p^m}} x_g^p X^{pg} \\ &= \sum_{g \in F_{p^m}} x_g^p \\ &= (\sum_{g \in F_{p^m}} x_g)^p \end{aligned}$$

- $\sum_{g \in F_{p^m}} x_g = 0$, alors $x^p = 0$ donc x est nilpotent
- $\sum_{g \in F_{p^m}} x_g \neq 0$

, alors $x^p \neq 0$; donc il existe $u \in F_{p^m}$ tel que $x^p u = 1$, cet à dire, $x(x^{p-1}u) = 1$, et x est une unité ■

Lemme 2.2 *L'application :*

$$\begin{array}{rccc} \theta_0 : & F_p[F_{p^m}] & \longrightarrow & F_p \\ & x = \sum_{g \in F_{p^m}} x_g X^g & \longmapsto & \sum_{g \in F_{p^m}} x_g \end{array}$$

est un homomorphisme de F_p-algèbres.

Preuve:

Soient $x = \sum_{g \in F_{p^m}} x_g X^g$, $y = \sum_{g \in F_{p^m}} y_g X^g \in F_p[F_{p^m}]$.

On a : $x + y = \sum_{g \in F_{p^m}} (x_g + y_g) X^g$ et $x.y = \sum_{g \in F_{p^m}} (\sum_{u+v=g} x_u y_v) X^g$.

Ainsi $\theta_0(x + y) = \sum_{g \in F_{p^m}} x_g + \sum_{g \in F_{p^m}} y_g = \theta_0(x) + \theta_0(y)$.

Et $\theta_0(x.y) = \sum_{g \in F_{p^m}} (\sum_{u+v=g} x_u y_v) = \sum_{u \in F_{p^m}} x_u \sum_{v \in F_{p^m}} y_v = \theta_0(x)\theta_0(y)$.

Notation1 $M = Ker\theta_0$

Proposition 2.1.3 *Soit $m \in \mathbb{N}^*$. L'algèbre $F_p[F_{p^m}]$ est un anneau local.*

Preuve:

Il suffit de montrer que $F_p[F_{p^m}]$ possède un unique idéal maximal.

Soit $x = \sum_{g \in F_{p^m}} x_g X^g$ un élément de $F_p[F_{p^m}]$.

Alors $x \in M$ équivaut à $\sum_{g \in F_{p^m}} x_g = 0$. D'après le lemme1, x est nilpotent. Donc $M = Ker\theta_0$ est un idéal de $F_p[F_{p^m}]$, et c'est l'unique idéal maximal de $F_p[F_{p^m}]$ car x est soit nilpotent ou inversible. ■

Remarque 2.1.2

L'application

$$\begin{array}{rccc} f: & F_p[F_{p^m}] & \longrightarrow & F_p^{p^m} \\ & x = \sum_{g \in F_{p^m}} x_g X^g & \longmapsto & (x_g)_{g \in Fp^m} \end{array}$$

est un isomorphisme d'espaces vectoriels sur F_p

car $dim_{F_p} F[G] = |G|$ d'où $F[G] \cong F_p^{|G|}$

Définition 2.1.4 *Soient $x = \sum_{g \in F_{p^m}} x_g X^g$ et $y = \sum_{g \in F_{p^m}} y_g X^g$ deux éléments de $F_p[F_{p^m}]$*

1. *On définit le produit scalaire de x et y noté $< x, y >$ par $< x, y >= \sum_{g \in F_{p^m}} x_g y_g$*
2. *Le complémentaire orthogonal d'un idéal $\boldsymbol{I}$ noté $\boldsymbol{I}^\perp$ est défini par :*

   $\boldsymbol{I}^\perp = \{x \in F_p[F_{p^m}] | < x, y >= 0, \forall y \in \boldsymbol{I}\}$
3. *L'annulateur d'un idéal $\boldsymbol{I}$ noté Ann($\boldsymbol{I}$) est défini par :*

   Ann($\boldsymbol{I}$)=$\{x \in F_p[F_{p^m}] | xy = 0, \forall y \in \boldsymbol{I}\}$
4. *Si $x = \sum_{g \in F_{p^m}} x_g X^g$,alors l'opposé de x noté $\widehat{x} = \sum_{g \in F_{p^m}} x_{-g} X^g$, et si I est un idéal de $F_p[F_{p^m}]$,l'opposé de I est le sous ensemble de $F_p[F_{p^m}]$ noté $\widehat{I} = \{\widehat{x}, x \in I\}$*

Lemme 2.3 *Soit $x = \sum_{g \in F_{p^m}} x_g X^g \in F_p[F_{p^m}]$. Alors $\widehat{x} = \sum_{g \in F_{p^m}} x_g X^{-g}$*

Preuve:

Soit $x = \sum_{g \in F_{p^m}} x_g X^g \in F[G]$.

Alors $\widehat{x} = \sum_{g \in F_{p^m}} x_{-g} X^g = \sum_{h \in F_{p^m}} x_h X^{-h} = \sum_{g \in F_{p^m}} x_g X^{-g}$ ■

Proposition 2.1.4 *i) $\widehat{I}$ et AnnI sont des idéaux de $F_p[F_{p^m}]$*

ii)$AnnI = \widehat{I^{\perp}} = (\widehat{I})^{\perp}$

Preuve:

i).$I \neq \varnothing$ car $0 = \sum_{g \in F_{p^m}} 0X^0 = \widehat{0}$ et $0 \in I$

. $\widehat{I} \subseteq F_p[F_{p^m}]$

. Soient $x = \sum_{g \in F_{p^m}} x_g X^g$, $y = \sum_{g \in F_{p^m}} x_g X^g \in F_p[F_{p^m}]$ tels que $\widehat{x} \in \widehat{I}$, $\widehat{y} \in \widehat{I}$

$\widehat{x} - \widehat{y} = \sum_{g \in F_{p^m}} x_{-g} X^g - \sum_{g \in F_{p^m}} y_{-g} X^g = \sum_{g \in F_{p^m}} (x_{-g} - y_{-g}) X^g = \widehat{x - y} \in \widehat{I}$ car $x - y \in I$,(I est un idéal de $F_p[F_{p^m}]$)

$xy = \sum_{l \in F_{p^m}} (\sum_{g \in F_{p^m}} x_g y_{l-g} X^l)$

$\widehat{xy} = \sum_{l \in F_{p^m}} (\sum_{g \in F_{p^m}} x_g y_{l-g} X^{-l}) = \sum_{l \in F_{p^m} l = g+h} (\sum_{g \in F_{p^m}} x_g y_h X^{-g-h})$

$= (\sum_{g \in F_{p^m}} x_g X^{-g})(\sum_{y \in F_{p^m}} y_h X^{-h}) = \widehat{x}.\widehat{y}$. Donc $\widehat{x}.\widehat{y} \in I$ car $xy \in I$.

De même,on montre que si $\widehat{x} \in \widehat{I}$ et $y \in F_p[F_{p^m}]$, alors $\widehat{x}y \in \widehat{I}$.

En effet,$\widehat{x}y = \widehat{x}\widehat{\widehat{y}} = \widehat{x\widehat{y}} \in \widehat{I}$ car $x\widehat{y} \in \widehat{I}$.Donc $\widehat{I}$ est un idéal de $F_p[F_{p^m}]$.

.$AnnI \neq \varnothing$ car $0 = 0y \ \forall y \in I$

.$AnnI \subseteq F_p[F_{p^m}]$

.Soient $x, y, z \in AnnI$ avec $x = \sum_{g \in F_{p^m}} x_g X^g, y = \sum_{g \in F_{p^m}} y_g X^g, z = \sum_{g \in F_{p^m}} z_g X^g$. Soit$x_1 \in I$

$(x - y)x_1 = xx_1 - yx_1 = 0, (xy)x_1 = x(yx_1) = 0, (xz)x_1 = (xx_1)z = 0$. Il en résulte que $AnnI$ est un idéal de $F_p[F_{p^m}]$.

ii) Soient $x \sum_{g\in F_{p^m}} x_g X^g, y = \sum_{g\in F_{p^m}} y_g X^g \in F_p[F_{p^m}]$.

$$\begin{aligned}
x \in AnnI &\Leftrightarrow xy = 0 \ \ \forall y \in I \\
&\Leftrightarrow \sum_{k\in F_{p^m}} (\sum_{g\in F_{p^m}} x_g y_{k-g}) X^{-k} = 0 \ \ \forall y \in I \\
&\Leftrightarrow \forall y \in I, \forall k \in F_{p^m}, \sum_{g\in F_{p^m}} x_g y_{k-g} = 0 \\
&\Leftrightarrow \forall y \in I, \forall k \in F_{p^m}, < \sum_{g\in F_{p^m}} x_g X^g; \sum_{g\in F_{p^m}} y_{k-g} X^g >= 0 \\
&\Leftrightarrow \forall y \in I, \forall k \in F_{p^m}, < x; X^k \sum_{h\in F_{p^m}} y_{-h} X^h \Leftrightarrow >= 0 \\
&\Leftrightarrow \forall y \in I, \forall k \in F_{p^m}, < x; X^u \widehat{y} >= 0 \\
&\Leftrightarrow x \in (\widehat{I})^{\perp} \ \text{ car } \ \widehat{y} \in \widehat{I} \ \text{ qui est un idéal de } \ F_p[F_{p^m}]
\end{aligned}$$

2.1.2 Radical de l'algèbre F[G]

Nous notons $\mathcal{P}$ le radical de l'algèbre F[G] (seul idéal maximal de F[G]) qui est aussi l'ensemble des éléments nilpotents car un élément de F[G] est soit nilpotent soit inversible. Ainsi :

$\mathcal{P} = \{x \in F[G] \ | \sum_{g\in G} x_g = 0\}$

2.1.2.1 Puissance du radical

Définition 2.1.5 *La puissance j^{ime} d'un idéal I est l'idéal engendré par la famille*
$\{\prod_{k=1}^{j} x_k, x_k \in I\}$
Par convention, $I^0 = F[G]$

Proposition 2.1.5 *La suite $(\mathcal{P}^j)_{j\geq \mathbb{N}^*}$ est une suite décroissante*

Preuve:

Soit $j \in \mathbb{N}^*, \forall x = \prod_{k=1}^{j} x_k, x_k \in \mathcal{P}$,on a :

$x = x_j(\prod_{k=1}^{j-1} x_k)$
$= x_j z$
avec $z = \prod_{k=1}^{j-1} x_k, x_k \in \mathcal{P}$. Comme $\mathcal{P}^{j-1}$ est un idéal , $x \in \mathcal{P}^{j-1}$. On en déduit que
$\mathcal{P}^j \subsetneq \mathcal{P}^{j-1}, \forall j \in \mathbb{N}^*$ .Donc la suite $(\mathcal{P}^j)_{j\in\mathbb{N}^*}$ est strictement décroissante ■

2.1.2.2 Complémentaire orthogonal de la puissance du radical

Soit $x \in F[G], x = \sum_{g \in G} x_g X^g$, alors d'après le **lemme1.3**,
$x \in \mathcal{P} \Leftrightarrow \widehat{x} \in \mathcal{P}$ et par suite, $x \in \mathcal{P}^j \Leftrightarrow \widehat{x} \in \mathcal{P}^j$ cet à dire que $\mathcal{P}^j = \widehat{\mathcal{P}^j}$

Proposition 2.1.6 *Posons* $M = m(p-1)$ *. Alors,*$\forall 1 \leq j \leq M, (\mathcal{P}^j)^\perp = \mathcal{P}^{M-j+1}$

Preuve:

Comme $\mathcal{P}^j = \widehat{\mathcal{P}^j}$ et d'après la **Proposition1.2.5**, il suffit de montre que
$Ann(\mathcal{P}^j) = \mathcal{P}^{M-j+1}$.
Comme $(\prod_{k=1}^{j} x_k).(\prod_{t=1}^{M-j+1} x_k) = \prod_{l=1}^{M+1} x_k = 0$, alors $(\prod_{k=1}^{M-j+1} x_k) \subseteq Ann(\mathcal{P}^j)$. On en déduit que $\mathcal{P}^{M-j+1} \subseteq Ann(\mathcal{P}^j)$.

Réciproquement,supposons que $x \notin Ann(\mathcal{P}^j)$.Si x est inversible,alors $x \notin \mathcal{P}^{M-j+1}$.Supposons que x n'est pas inversible.Alors $x \in \mathcal{P}$. Soit s le plus grand entier naturel tel que $x \in \mathcal{P}^t$. Alors x est combinaison linéaire d'élément de la forme $\prod_{k=1}^{s} x_k$. Mais $\forall y \in \mathcal{P}^j, xy = 0$, en particulier, $x \prod_{i=1}^{j} x_i \neq 0$.

Donc pour un certains produit $\prod_{l=1}^{t} x_l$, on a :
$\prod_{l=1}^{t} x_l . \prod_{i=1}^{j} x_i = \prod_{k=1}^{t+j} x_k \neq 0$.
On en déduit que $t + j < M + 1 \Rightarrow t < M - j + 1$. Donc $x \notin \mathcal{P}^{M-j+1}$ ■

2.1.3 Structure d'espace vectoriel de F[G]

D'après la **proposition1.2.2**, la famille $(X^g)_{g \in G}$ est une base de de $F[G]$ et
$dim(F[G]) = |G| = p^m$.
Nous allons maintenant donner une autre base de $F[G]$ qui nous permettra de caractériser les sous espaces $\mathcal{P}^j$.
Soit $e = (e_1, ..., e_m)$ une F_{p^m}-base de G. $\forall g \in G$, on peut écrire $g = \sum_{i=1}^{m} g_i e_i$ avec $0 \leq g_i \leq p^m - 1$.
Donc, $\forall x = \sum_{g \in G} x_g X^g \in F[G]$,
$x = \sum_{g \in G} x_g X^{\sum_{i=1}^{m} g_i e_i} = \sum_{g \in G} x_g \prod_{i=1}^{m} (X^{e_i})^{g_i}$
On en déduit que la famille des p^m éléments,
$B = \{\prod_{i=1}^{m} (X^{e_i})^{g_i}, (g_1, ..., g_m) \in |0, p-1|^m\}$ engendre $F[G]$. C'est donc une base de $F[G]$ car $dim(F[G]) = p^m$.

Considérons l'application :

$$\begin{array}{rccc} \varphi: & F[G] & \longrightarrow & F[G] \\ & x=\sum_{g\in G} x_g \prod_{i=1}^{m}(X_i^{e_i})^{g_i} & \longmapsto & \sum_{g\in G} x_g \prod_{i=1}^{m}(X^{e_i}-1)^{g_i} \end{array}.$$

Alors φ est un automorphisme (car surjective).D'où l'image de la base B ci-dessus est une base de $F[G]$. Posons :

$B(e)=\varphi(B)=\{\prod_{i=1}^{m}(X^{e_i}-1)^{g_i},(g_1,...,g_m)\in[|0;p-1|^m]\}$. On a la propriété suivante

Proposition 2.1.7 *1) B(e) est une base de $F[G]$*

2) $\forall j\in\mathbb{N}\ \ |1\leq j\leq m(p-1)$,

$B_j(e)=\{\prod_{i=1}^{m}(X^{e_i}-1)^{g_i}\in B(e)\ \ |\sum_{i=1}^{m} g_i\geq j\}$ est une base de $\mathcal{P}^j$

Preuve:

1)B(e) est une base de $F[G]$ par construction

2)Procédons par récurrence sur j

- Pour $j=1$:
  Soit $x=\prod_{i=1}^{m}(X^{e_i}-1)^{g_i}\in B_1(e)$, alors $1\leq\sum_{i=1}^{m} g_i$.Donc il existe i_0 tel que $g_{i_0}\neq 0$. On a : $[(X^{e_{i_0}}-1)^{g_{i_0}}]^p=(X^{pe_{i_0}}-1)^{g_{i_0}}=(1-1)^{g_{i_0}}=0$.
  Donc $x^p=\prod[(X^{e_{i_0}}-1)^{g_{i_0}}]^p=0$, se qui implique que $x\in\mathcal{P}$ et par suite $B_1(e)\subseteq\mathcal{P}$.
  Mais $card(B_1(e))=p^m-1$ et comme $B_1(e)$ est une famille libre, on en déduit que $dim(\mathcal{P})\geq p^m-1$. Or $\mathcal{P}\neq F[G]$ donc $dim(\mathcal{P})\leq p^m-1$.Ceci montre que $dim(\mathcal{P})=p^m-1$ ainsi $B_1(e)$ est une base de $\mathcal{P}$
- Pour $1\leq j\leq m(p-1)$, supposons que $B_j(e)$ est une base de $\mathcal{P}^j$.Puisque $B_{j+1}(e)$ est une famille libre,il reste à montrer qu'elle engendre $\mathcal{P}^{j+1}$.Montrons que les produits $x=\prod_{k=1}^{j+1}x_k$ sont combinaisons linéaires d'éléments de $B_{j+1}(e)$.On a :
  $x=\prod_{k=1}^{j+1}x_k=(\prod_{k=1}^{j}x_k)x_{j+1}=yx_{j+1}$,
  avec $y=(\prod_{k=1}^{j}x_k)\in\mathcal{P}^j$ et $x_{j+1}\in\mathcal{P}$.Par hypothèse y et x_{j+1} sont combinaisons linéaires d'élément de $B(e)$ vérifiant $\sum_{k=1}^{m}g_k\geq j$ et $\sum_{k=1}^{m}g_k\geq 1$. Donc x est combinaison linéaire d'éléments de $B(e)$ vérifiant $\sum_{k=1}^{m}g_k\geq j+1$. Donc $B_{j+1}(e)$ est une base de $\mathcal{P}^j$ ■

On a montré que $(\mathcal{P}^j)_{j\in\mathbb{N}*}$ est une suite strictement décroissante et donc stationnaire il existe un entier non nul j_0 tel que $\mathcal{P}^{j_0}=0$

Proposition 2.1.8 *Avec $M = m(p-1)$, on a $\mathcal{P}^M \neq 0$ et $\mathcal{P}^{M+1} = 0$*

Preuve:

Les $B_j(e)$ forment une suite décroissante en partant de la plus grande $B(e)$ à la plus petite $B_{m(p-1)}(e)$. Donc $\mathcal{P}^{m(p-1)}$ ne peut contenir aucun idéal propre de $F[G]$ que lui même, alors $\mathcal{P}^M \neq 0$ et $\mathcal{P}^{M+1} = 0$ ■

CODES DE REED-MULLER

3.1 codes de REED-MULLER classiques

3.1.1 Généralités

Pour tous $w \in F_2^m$,v^w est la fonction définie de $F_2^{F_2^m}$ vers F_2 par :

$$v^w(x) = \begin{cases} 1 \quad si \quad x = w \\ 0 \qquad sinon \end{cases}$$

$F_2^{F_2^m}$ muni de l'addition et de la multiplication des applications est une algèbre sur F_2

Proposition 3.1.1 *L'ensemble* $\{v^w, w \in F_2^m\}$ *est une base de* $F_2^{F_2^m}$ *sur* F_2.

Preuve:

Soient $f \in F_2^{F_2^m}$ et $x \in F_2^m$ .Alors $(\sum_{a \in F_2^m} f(a)v^a)(x) = f(x)$.

D'où $f = \sum_{a \in F_2^m} f(a)v^a$.

Soit $n \in \mathbb{N}$. Soient $\{w_i, i \in [|1,n|]\} \subseteq F_2^m$ et $\lambda_i \in F_2, i \in [|1,n|]$ tels que $\sum_{i=1}^{n} \lambda_i v_i^w = 0$.

Alors,$\forall j \in [|1,n|]$, $(\sum_{i=1}^{n} \lambda_i v_i^w)(w_j) = 0$, cet à dire ,$\forall j \in [|1,n|]$, $\lambda_j = 0$.

Ainsi $\{v^w, w \in F_2^m\}$ est un système libre et générateur de $F_2^{F_2^m}$; c'est donc une base de $F_2^{F_2^m}$ sur F_2. ■

Corollaire 3.1.1 *L'algèbre* $F_2^{F_2^m}$ *a pour dimension* 2^m *sur* F_2.

Preuve:

D'après la proposition précédente, $\{v^w, w \in F_2^m\}$ est une base de $F_2^{F_2^m}$.

Donc $dim(F_2^{F_2^m}) = card\{v^w, w \in F_2^m\} = 2^m$.

$\forall i \in [|1,n|], x_i$ est la fonction est la fonction définie de F_2^m vers F_2 par :

$x_i(a) = a_i \quad \forall a = (a_1, a_2, ..., a_{m-1}, a_m) \in F_2^m$. ■

Notation1 Soit $I \subseteq [|1,m|]$. On note : $x^I = \begin{cases} \prod_{k=1}^{m}(x_k + 1 + w_k) & si \quad I \neq \varnothing \\ 1 & sinon \end{cases}$

et $\mathbb{M}_2 = \{x^I, I \subseteq [|1,m|]\}$

Lemme 3.1 *Pour tous* $w \in F_2^m$, $v^w = \prod_{k=1}^{m}(x_k + 1 + w_k) = \sum_{I_w \subseteq J \subseteq [|1,m|]} x^J$.

Preuve:

Soit $w = (w_1, ..., w_m) \in F_2^m$.

$\forall a = (a_1 ...., a_m) \in F_2^m$, on a :

$$\begin{aligned} v^w(a) = 1 &\iff \forall i \in [|1,n|], a_i = w_i \\ &\iff \forall i \in [1,n], a_i + w_i + 1 = 1 \\ &\iff \prod_{k=1}^{m}(x_k + 1 + w_k) = 1 \end{aligned}$$

Ainsi,$\forall a = (a_1, ..., a_m) \in F_2^m, v^w(a) = \prod_{k=1}^{m}(x_k + 1 + w_k)(a)$, cet à dire,

$$v^w = \prod_{k=1}^{m}(x_k + 1 + w_k)$$

. En développant le terme $v^w = \prod_{k=1}^{m}(x_k + 1 + w_k)$,on obtient une combinaison linéaire de $x^J, J \subseteq [|1,m|]$ à cœfficients dans F_2, cet à dire $\sum_{J \subseteq [|1,m|]} x^J$.

Proposition 3.1.2 $\mathbb{M}_2$ *est une base de* $F_2^{F_2^m}$ *sur* F_2

Preuve:

Soit $w \in F_2^m$. Alors ,d'après le **lemme2.1** $v^w = \sum_{I \subseteq [1,m]} x^I$. D'où $\mathbb{M}_2$ est un système générateur de $F_2^{F_2^m}$.

Soit $I \subseteq [1,m]$.Alors le nombre x^I tel que $cardI = i$ est égal à C_m^i.

Ainsi $card(\mathbb{M}_2) = \sum_{i=0}^{m} card(\{x^I, cardI = i\}) = \sum_{i=0}^{m} C_m^i = 2^m$. Comme $card(\mathbb{M}_2) = 2^m$ et $\mathbb{M}_2$ est un système générateur de $F_2^{F_2^m}$ alors, $\mathbb{M}_2$ est une base de $F_2^{F_2^m}$ ■

3.1.2 Définition d'un code de Reed-Muller,exemples et propriétés

3.1.2.1 Définition et exemples

Soit $m \in \mathbb{N}$ et soit $r \in [|1,m|]$

Définition 3.1.1 *On appelle* ***code de Reed-Muller*** *d'ordre r de longueur 2^m le sous-espace sectoriel de $F_2^{F_2^m}$ engendré par $\{x^I, I \subseteq [1,m]$ et $card(I) \leq r\}$.*
On utilisera la notation ***R(r,m)*** *pour désigner un code de Reed-Muller d'ordre r de $F_2^{F_2^m}$.*

Nous généralisons la notion de code de Reed-Muller pour $r \in \mathbb{Z}$ en posant :
$R(r,m) = \begin{cases} 0 \quad si \qquad r < 0 \\ F_2^{F_2^m} \quad si \quad r > m \end{cases}$.

Exemple 3.1.1

1. $m = 1$, $\mathbb{M}_2 = \{1, x_1\}$.
   - *Si* $r = 0, R(0,1) =< 1 >= \{0,1\}$
   - *si* $r = 1, R(1,1) =< \{1, x_1\} >= \{0, 1, x_1, 1 + x_1\}$
2. $m = 2$, $\mathbb{M}_2 = \{1, x_1, x_2, x_1x_2\}$.
   - *Si* $r = 0, R(0,2) =< \{1\} >= \{0,1\}$
   - *Si* $r = 1, R(1,2) =< \{1, x_1, x_2\} >= \{0, 1, x_1, x_2, 1 + x_1, 1 + x_2, x_1 + x_2, 1 + x_1 + x_2\}$

Remarque 3.1.1
$R(0,m) = \{0,1\}$ *et* $R(m,m) = F_2^{F_2^m}$.

3.1.2.2 Quelques propriétés

Proposition 3.1.3 *Soit $r, s \in ([|1,m|])^2$ tel que $r \preceq s$. Alors $R(r,m) \subseteq R(s,m)$.*

Preuve:

Comme $\{x^I, I \subseteq [|1,m|]$ et $card(I) \leq r\} \subset \{x^I, I \subseteq [|1,m|]$ et $card(I) \leq s\}$,et par conséquent $\{x^I, I \subseteq [|1,m|]$ et $card(I) \leq r\} \subseteq R(s,m)$.Puisque $\{x^I, I \subseteq [1,m]$ et $card(I) \leq r\}$ engendre le sous espace vectoriel $R(r,m)$ et que $R(s,m)$ est est un sous espace vectoriel de $F_2^{F_2^m}$ alors, $R(r,m) \subseteq R(s,m)$. ■

Théorème 3.1.1 $\forall r \in [|1,m|]$, $dim R(r,m) = \sum_{i=0}^{r} C_i^m$.

Preuve:

Soit $r \in [|1,m|]$. D'après la définition ci-dessus, $R(1,m)$ est engendré par l'ensemble $\{x^I, I \subseteq [|1,m|]$ et $card(I) \leq r\}$ qui est un système libre de $R(r,m)$ car c'est une partie non vide de $\mathbb{M}_2$.Ainsi $\dim R(r,m) = \sum_{i=0}^{r} |\{x^I, card(I) = i\}| = \sum_{i=0}^{r} C_i^m$. ■

Théorème 3.1.2 (MACWILLIAM F.J ET SLOANE N.J.A) *[5] :*

$\forall r \in [|0, m|]$, *la distance minimale de* $R(r,m)$ *est* $d = 2^{m-r}$

Proposition 3.1.4 *L'application :*

$$\begin{array}{rccc} \alpha : & F_2^{F_2^m} & \longrightarrow & F_2^{2^m} \\ & \sum_{w \in F_2^m} a_w v^w & \longmapsto & (a_w)_{w \in F_2^m} \end{array}$$

est un isomorphisme de F_2*-espace vectoriels.*

Preuve:

Soient $\sum_{w \in F_2^m} a_w v^w \in F_2^{F_2^m}$, $\sum_{w \in F_2^m} b_w v^w \in F_2^{F_2^m}$ et $\lambda \in F_2$. Alors :

$$\begin{aligned} \alpha(\sum_{w \in F_2^m} a_w v^w + \lambda \sum_{w \in F_2^m} b_w v^w) &= \alpha(\sum_{w \in F_2^m} (a_w + \lambda b_w) v^w) \\ &= (a_w + \lambda b_w)_{w \in F_2^m} \\ &= (a_w)_{w \in F_2^m} + \lambda (b_w)_{w \in F_2^m} \\ &= \alpha(\sum_{w \in F_2^m} a_w v^w) + \lambda \alpha(\sum_{w \in F_2^m} b_w v^w) \end{aligned}$$

Ainsi α est une application linéaire.

Bijectivité : $\sum_{w \in F_2^m} a_w v^w \in Ker(\alpha)$ équivaut à $(a)_{w \in F_2^m} = 0$; se qui signifie que $\forall w \in F_2^m, a_w = 0$; d'où α est bijective.

Or $\dim F_2^{F_2^m} = 2^m = \dim F_2^{2^m}$; d'où α est bijective. En conclusion, α est un isomorphisme de F_2-espaces vectoriel.

Exemple 3.1.2

Ecriture dans $F_2^{2^m}$ *pour les cas* $m = 1, 2$.

a) $m = 1$

Dans ce cas,tout code de Reed-Muller a la longueur $2.\{v^0, v^1\}$ *est une base de* $F_2^{F_2}$*.Dans* F_2^2 *on a :*

$x_1 = 0v^0 + v^1 = (0,1)$, *et* $v^0 + v^1 = (1,1)$.

Si $r = 0, R(0,1) = \{(0,0),(1,1)\}$ *et si* $r = 1, R(1,1) = \{(0,0),(1,1),(0,1),(1,0)\}$.

b) $m = 2$.

Dans ce cas tous code de Reed-Muller est de longueur 4*.Posons :* $e_1 = (0,0), e_2 = (0,1)$, $e_3 = (1,0), e_4 = (1,1)$. $v^{e_i}, i \in [1,4]$ *est une base de* $F_2^{F_2^2}$.

Dans F_2^4, *on a :* $1 = (1,1,1,1), x_1 = (0,0,1,1), x_2 = (0,1,0,1)$ *et* $x_1 x_2 = (0,0,0,1)$.

- $r = 0, R(0,2) = \{(0,0,0,0),(1,1,1,1)\}$.
- $r = 1, R(1,2) = \{(1,1,1,1),(0,0,1,1),(1,1,0,0),(1,0,1,0),(0,1,1,0),(1,0,0,1),(0,0,0,0)\}$.
- $r = 2, R(2,2) = F_2^4$

.

3.1.2.3 Matrice génératrice d'un code de Reed-Muller

Soit $r \in [|0,m|]$.D'après la définition ci-dessus,$R(r,m)$ est un code linéaire de longueur 2^m et sa dimension est $k = \sum_{i=0}^{r} C_m^i$ d'après le théorème1.

Définition 3.1.2 *Une matrice génératrice de $R(r,m)$ est toute matrice de type $k \times 2^m$ donc les lignes sont constitués des vecteurs $x^I, I \subseteq [1,m]$ et $card(I) \leq r$ écrit dans une base de $F_2^{F_2^m}$.*

Exemple 3.1.3

Ici,les vecteurs $x^I, I \subseteq [1,m]$ et $card(I) \leq r$ sont écrits dans la base $\{v^w, w \in F_2^m\}$.

-Une matrice génératrice de $R(1,1)$ est $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

-Le sous espace vectoriel $R(1,2)$ est engendré par les vecteurs $1 = (1,1,1,1), x_1 = (0,0,1,1)$, $x_2 = (0,1,0,1)$. *Une matrice génératrice de $R(1,2)$ est* $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$.

-$R(1,3)$ est engendré par :

$1 = (1,1,1,1,1,1,1,1); x_1 = (0,0,0,0,1,1,1,1); x_2 = (0,0,1,1,0,1,0,1); x_3 = (0,1,0,1,0,0,1,1)$ *;*

d'où la matrice génératrice de $R(1,3)$ est :

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

.

3.1.2.4 Orthogonal d'un code de Reed-Muller

Proposition 3.1.5 *L'application :*

$$\begin{array}{rccc} <;>: & F_2^{F_2^m} \times F_2^{F_2^m} & \longrightarrow & F_2 \\ & (f,g) & \longmapsto & \sum_{a \in F_2^m} f(a)g(a) \end{array}$$

est une forme bilinéaire symétrique non dégénérée.

Proposition 3.1.6 $R(m-1,m) = \{f \in F_2^{F_2^m}, \sum_{a\in F_2^m} f(a) = 0\}$

.

Preuve:

Posons $H = \{f \in F_2^{F_2^m}, \sum_{a\in F_2^m} f(a) = 0\}$.$H$ est un sous-espace vectoriel de $F_2^{F_2^m}$,car H est le noyau de l'application linéaire

$$\begin{array}{rccc} \varphi: & F_2^{F_2^m} & \longrightarrow & F_2 \\ & f & \longmapsto & \sum_{a\in F_2^m} f(a) \end{array}$$

Montrons que : $R(m-1,m) \subset H$.

Pour le faire,il suffit de montrer que $\forall I \subset [|1,m|], card(I) \leq m-1, x^I \in H$.

Soit $I \subset [1,m], card(I) \leq m-1$.

- f est constante de valeur c,alors $\sum_{a\in F_2^m} f(a) = c2^m = 0$;
- f n'est pas une constante,soit $j \in [|1,m|]$. Alors :

$$\begin{aligned} \sum_{a\in F_2^m} f(a) &= \sum_{a\in F_2^m} x^I(a) \\ &= \sum_{(a_1,\ldots,a_n)\in F_2^m} \prod_{i\in I} a_i \\ &= \sum_{a_j\in F_2} \Big(\sum_{a_i\neq a_j} \prod_{i\in I} a_i \Big) \\ &= 2\Big(\sum_{a_i\neq a_j} \prod_{i\in I} a_i \Big) \\ &= 0 \end{aligned}$$

■

.

Réciproquement,si $J \subset [|1,m|], card(J) \leq m$, alors $f = x_1x_2...x_n$.

$\sum_{a\in F_2^m} f(a) = \sum_{(a_1,a_2,\ldots,a_m)\in F_2^m} a_1a_2...a_m \neq 0 \neq$.

Donc,$x^I \notin R(m-1,m)$ entraine $x^J \notin H$. D'où $H \subset R(m-1,m)$

Proposition 3.1.7 $\forall r \in [|0,m|], R(r,m)^\perp = R(m-r-1,m)$,*où* $R(r,m)^\perp$ *désigne l'orthogonal de* $R(r,m)$

Preuve:

Soit $r \in [|0,m|].R(r,m)^\perp$ est un sous espace vectoriel de $F_2^{F_2^m}$.

Soient $f = x^I$ et $g = x^J$ tel que $cardI \leq r$ et $cardJ \leq m-r-1$.

$card(I \cup J) \leq m-1$ implique $fg = x^{I \cup J}$, $(\text{car} \forall i \in [1,m], x_i^2 = x_i)$ et $fg \in R(m-1,m)$. et d'après la **proposition 3.1.6**,on a $\sum_{a \in F_2^m} f(a)g(a) = 0$. Donc $R(m-r-1,m) \subseteq R(r,m)^{\perp}$.
De plus :

$$\begin{aligned} dim(F_2^{F_2^m}) - dim(R(r,m)) &= 2^m - \sum_{i=0}^{r} C_m^i \\ &= \sum_{i=0}^{m} C_m^i - \sum_{i=0}^{r} C_m^i \\ &= \sum_{i=r+1}^{m} C_m^i \\ &= \sum_{i=0}^{m-r-1} C_m^i \\ &= dim(R(m-r-1,m)) \end{aligned}$$ ■

En conclusion, $R(r,m)^{\perp} = R(m-r-1,m)$

3.1.2.5 Poids minimum d'un code de Reed-Muller

Dans cette partie,nous nous servions essentiellement de la distance d,définie de la manière suivante :

$$\begin{array}{rccc} d: & \mathcal{P}(F_2^m) \times \mathcal{P}(F_2^m) & \longrightarrow & \mathbb{N} \\ & (A,B) & \longmapsto & \mathbb{N} \end{array}.$$

Définition 3.1.3 – *Soit $s \in \mathcal{P}(F_2^m)$. Le poids de s est $d(s,\varnothing)$ et est noté $|s|$*

- *On appelle distance minimal de $R(m-r,m)$ le réel positif*
  $min(\{d(A,B), A \neq B, A, B \in R(m-r,m)\})$
- *On appelle poids minimum de $R(m-r,m)$ le réel positif*
  $min(\{d(A,\varnothing), A \in R(m-r,m)\})$

Remarque 3.1.2
Soit $r \in [|0,m|]$. Alors le poids minimum de $R(m-r,m)$ est 2^r

3.2 Codes de Reed-Muller vu sur une algèbre de groupe

Dans cette partie, nous allons montrer que sur les algèbres de groupes, les codes de Reed-Muller sont exactement les puissances du radical. Ce résultat a été montré par Berman dans [1].

Rappel :

On appelle **code de Reed-Muller** d'ordre r de longueur 2^m le sous-espace-vectoriel de $F_2^{F_2^m}$ engendré par $\{x^I, I \subseteq [1,m] \text{ et } card(I) \leq r\}$.

Soit $j \in \mathbb{N}^*$.Montrons que $\mathcal{P}^j$ est engendrée de la même façon

Lemme 3.2 *Soit S un sous ensemble non vide $F_2^{F_2^m}$.Alors*

$$\prod_{g \in <S>} (X^g - 1) = \begin{cases} \sum_{g \in <S>} X^g & \textit{si S est une famille libre} \\ 0 & \textit{sinon} \end{cases}$$

Où $< S >$ est le sous espace-vectoriel de $F_2^{F_2^m}$ engendré par S

Preuve:

Soient $r \in \mathbb{N}$ et $S = g_1, g_2, ..., g_r$ un sous ensemble de F_{2^m}

i) Supposons que S soient un système libre.Alors

$$\begin{aligned} \prod_{g \in <S>} (X^g - 1) &= \prod_{i=1}^{r} (X_i^g - 1) \\ &= \sum_{L_r \subseteq [|1,r|]} (-1)^{r-|L_r|} X^{\sum_{i \in L_r} gi} \end{aligned}$$

Or pour tout $L_r \subseteq [|1,r|], (-1)^{r-|L_r|} = 1$ dans F_2 ;donc

$$\begin{aligned} \prod_{g \in <S>} (X^g - 1) &= \sum_{L_r \subseteq [|1,r|]} (-1)^{r-|L_r|} X^{\sum_{i \in L_r} gi} \\ &= \sum_{h \in <S>} X^h \end{aligned}$$

ii) Si S est un système lié, soit $S' \subseteq S$ tel que S' soit un système libre. Soit $g_0 \in S \backslash S'$

$$\begin{aligned} \prod_{g \in S' \cup g_0} (X^g - 1) &= [\prod_{g \in S'} (X^g - 1)](X^{g_0} - 1) \\ &= \sum_{h \in <S'>} X^h (X^{g_0} - 1) \\ &= \sum_{h \in <S'>} X^{h+g_0} - \sum_{h \in <S'>} X^h \\ &= \sum_{h \in <S'>} X^h + \sum_{h \in <S'>} X^h \\ &= 2 \sum_{h \in <S'>} X^h \\ &= 0 \end{aligned}$$

■

Puisque $\mathcal{P}$ est linéairement engendré par les produits de la forme $(X^{g_1} - 1)(X^{g_2} - 1)...(X^{g_j} - 1)$ où les g_i sont les éléments de $F_2^{F_2^m}$.Les seuls j-sous ensemble $g_1, g_2, ..., g_j$ qui sont linéairement indépendant sont nécessaire pour engendré $\mathcal{P}$

Corollaire 3.2.1 *$\mathcal{P}^j$ est engendré par les fonctions caractéristiques du F_2-algèbre*

Théorème 3.2.1 (P.Charpin) *[3] :*
Le code de Reed-Muller R(m-j,m) est égal à $\mathcal{P}^j$

3.3 Intérêt pédagogique

Ce travail nous a permis de :

- pouvoir saisir, rédiger et présenter des documents mathématiques et scientifiques de qualité avec le logiciel LaTeX ;
- maitriser certains logiciels mathématiques ;
- découvrir un champ d'application des mathématiques dont nous présenterons aux élèves afin de les motiver

Chapitre Quatre

Conclusion et perspectives

Les codes de Reed-Muller ont un lien très fort avec les algèbres de groupes. L'étude des codes de Reed-Muller sur cette structure nous a permis de déterminer les propriétés de ces codes.

Nous avons montré que les codes de Reed-Muller ont des propriétés algébriques intéressantes en ce sens qu'ils permettent une exploration utilisant les outils mis en place lors de l'étude des idéaux de $F[G]$. Ces propriétés algébriques vont nous permettre d'étudier l'encodage de ces codes et lorsqu'on y ajoute les propriétés combinatoire on peut étudier l'encodage et le décodage de ces codes.

Bibliographie

[1] BERMANN S.D.,*On the theory of groups codes*, Kibernetika, 1, 1967, P. 31-39

[2] CHARPIN P.,*Codes idéaux de certaines algèbres modulaires*, Thèse de 3^e cycle, Université de Paris-VII, 1982

[3] CHARPIN P.,*Puissance du radical d'une algèbre modulaire et codes cycliques*,Revue du CETHEDEC, 18^e année, 4^e trimestre 1981, MS 81-2, p. 35-43

[4] KASAMI T., LIN S., W.W.,*New généralisation of the Reed-Muller codes*, IEEE Trans, Info. Theory, II-14 p. 189-199

[5] MacWilliams F.J. et Sloane N.J.A.,*The theory of error correcting codes*, North Holland, 1977

[6] N.BOURBAKI,*livre II ,algèbre*,Herman,Paris,1953.

[7] NJOCK Edward Georges,*Théorie de Galois et applications*,Presse Universitaire de Yaoundé,1999

[8] Poli A.,*Codes dans certaines algèbres modulaires*, Thèse de Doctorat d'Etat, Université p. Sabatier, Toulouse