REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Mohamed Boudiaf de M'sila

Faculté des Mathématiques et de l'Informatique

Département des Mathématiques

Mémoire de Master

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

Thème

Le polynôme énumérateur des poids et quelques applications

Présentée par :

KHODJA Soumia & HABOUCHE Afaf

Devant le jury composé de :

Mr D. MIHOUBI	Prof,	Université de M'sila	**Président**.
Mr L. LADJELAT	M.A.A,	Université de M'sila	**Encadreur**.
Mr L. HEBOUB	M.A.A,	Université deM'sila	**Examinateur**.

Année universitaire :2020/2021

Remerciements

Avant toute chose, nous remercions **ALLAH** qui nous donné la patience, le courage et la santé pour accomplir ce mémoire.

Nous tenons à exprimer nous profonds remerciements au notre directeur de recherche **LADJELAT Lahcene.** Nous le remercions énormément pour ses précieuses conseils, ses remarques pertinentes et son soutien permanent.

Nous remercions également les membres de jury pour leur acceptation d'évaluer ce mémoire et de l'enrichir pzr leurs propositions.

Remerciements particuliers aux honorables messieurs Mr. **MIHOUBI Douadi** et le Mr. **HEBOUB Lakhdar**.

Nous remercions tous les professeurs de la faculté de Mathématiques et tous ceux qui nous ont aides de pris ou de loin.

Notations

$\mathbb{F}_q$	Le corps fini à q éléments
$[\mathbb{K} : \mathbb{L}]$	Dimension de $\mathbb{K}$ sur $\mathbb{L}$
$car(\mathbb{K})$	Caractéristique de $\mathbb{K}$
$\binom{n}{k}$	Nombre de combinaisons de k élèments parmi n
$[n, k, d]$	La longueur n, la dimension k et la distance minimale d d'un code linéaire
$d_H(x, y)$	Distance de Hamming entre x et y
$w_H(x)$	Poids de Hamming du vecteur x
$\|T\|$	Cardinal de l'ensemble T
G	Matrice génératrice de C
$C^\perp$	Code dual de C
H	Matrice de contrôle de C
A_i	Nombre des mots du code de poids
$W_C(x, y)$	Polynôme énumérateur des poids du code linéaire C

Table des matières

Introduction

Dans ce mémoire, on s'intérèsse à l'étude de polynôme énumérateur des poids d'un code de longeur fixe sur un corps fini.

D'abord on rappelle les notions de base nécéssaires (corps fini, code correcteurs d'erreurs, distance de Hamming), ensuite on étudie les polynôme énumérateur des poids en citant quelques exemple. Enfin, on cite un resultat important (le théorème de MacWilliams) et une application (probabilité des erreurs).

Dans le premier chapitre, on rappelle les notions préliminaires fondamentales liées à ce travail (anneau, corps finis, code correcteurs d'erreur, distance de Hamming), ces notions sont nécéssaires pour comprendre les chapitres suivant de ce travail. On y mentionne quelques exemples pour expliquer mieux les notions.

Le deuxième chapitre vise à présenter le concept du polynôme énumérateur des poids.

Pour cette raison on parle de la distrubution des poids (pour Hamming), et les polynômes homogènes. On donne quelques exemples.

Enfin, le dernier chapitre est consacré d'un part au théorème de MacWilliams qui permet de relier le polynôme énumérateur d'un code au polynôme énumérateur de son dual, d'autre part on voit comment le polynôme énumérateur est utilisé pour le calcul de probabilité d'erreur.

Chapitre 1

Introduction et Notions préliminaires

Dans ce chapitre nous parlons des définition, des concepts de base et de certaines propriétés des corps finis, ainsi que des codes.

1.1 Corps Finis

Dans cette section on rappelle les notions préliminaires fondamentales liées à ce travail (anneaux, corps finis).

1.1.1 Anneau

Définition 1.1.1. Soit A un ensemble non vide muni de deux opératios internes " $+$ " et ".". Le tripet $(A, +, .)$ est dit anneau si:
1) $(A, +)$ est un groupe commutatif.
2) La loi "." est associative: $\forall x, y, z \in A : (x.y).z = x.(y.z)$.
3) La loi "." est distributive par rapport à la loi " $+$ " :

$$\forall x, y, z \in A : \begin{cases} x.(y+z) = x.y + x.z \\ (x+y).z = x.z + y.z \end{cases}.$$

Remarque 1.1.1.
1) Si la loi "." possède un élément neutre 1_A:

$$\forall x \in A : x.1_A = 1_A.x = x$$

on dit que l'anneau est unitaire.
2) Si la loi "." est commutatif:

$$\forall x, y \in A : x.y = y.x$$

on dit que l'anneau A est commutatif.

Notation 1.1.1.
1) L'élément neutre de $(A, +)$ est noté 0 et appelé le zéro de A. La symétrique d'un élément $x \in A$ est noté $-x$.

2) Si "." posède un élément neutre, il est souvent noté 1, l'inverse de $x \in A$ pour ".", s'il existe, est noté x^{-1}.

Exemples 1.1.1.

1) Si $\mathbb{Z}$ est l'ensemle des entiens relatifs, alors $(\mathbb{Z}, +, .)$ est un anneau commutatif unitaire infini.

2) Soit $n \in \mathbb{N}^*$et $M_n(\mathbb{R})$ L'ensemble des matrices carrèes $n \times n$ sur $\mathbb{R}$, alors $(M_n(\mathbb{R}), +, .)$ est un anneau avec

$$0 = \begin{pmatrix} 0 & 0 & . & . & . & 0 \\ 0 & 0 & . & . & . & 0 \\ . & & . & & & . \\ . & & & . & & . \\ . & & & & . & . \\ 0 & 0 & . & . & . & 0 \end{pmatrix} \quad \text{et} \quad 1 = \begin{pmatrix} 1 & 0 & . & . & . & 0 \\ 0 & 1 & . & . & . & 0 \\ . & & . & & & . \\ . & & & . & & . \\ . & & & & . & . \\ 0 & 0 & . & . & . & 1 \end{pmatrix}$$

3) $(\mathbb{Z}/n\mathbb{Z}, +, .)$ est un anneau commutatif unitaire pour l'addition "+" et la multiplication "." modulo n.

Idéal d'un anneau

Soit $(A, +, .)$ un anneau commutatif unitaire

Définition 1.1.2. Soit I un sous ensemble non vide de A, on dit que I est un idéal de A si il vérifie:

1) $\forall x, y \in I$, $x - y \in I$.

2) $\forall a \in A$, $\forall x \in I$, $ax \in I$.

Exemple 1.1.2.

Soit $A = \mathbb{Z}/6\mathbb{Z}$ et $I = \{\overline{0}, \overline{2}, \overline{4}\}$

on a

$-$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{4}$
$\overline{4}$	$\overline{4}$	$\overline{2}$	$\overline{0}$

$.$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{4}$	$\overline{2}$

donc I est un idéal de $\mathbb{Z}/6\mathbb{Z}$

Idéal principal

Définition 1.1.3. Un idéal I est un idéal principal s'il est engendré par un élément a, c'est-à-dire s'il existe $a \in A$ tel que:

$$I = (a) = \{ax : \ x \in A\}.$$

Exemple 1.1.3.
Dans $\mathbb{Z}$ tout les idéaux sont principaux.

Corps

Définition 1.1.4. Un corps est un anneau unitaire $(A, +, .)$ tel que tout élément non nul est inversible.
C'est-à-dire :

$$U(A) = A - \{0\}$$

où $U(A)$ est le groupe des unités de A.

Exemples 1.1.4.
1) $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ et $(\mathbb{C}, +, .)$ sont des corps.
2) Pour $p \in \mathbb{N}^*$premier , on a

$$\begin{aligned} A &= \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{p-1}\} \\ U(\mathbb{Z}/p\mathbb{Z}) &= \{x \in \mathbb{Z}/p\mathbb{Z} : (x, p) = 1\} \\ &= \{\overline{1}, \overline{2}, ..., \overline{P-1}\} = \mathbb{Z}/p\mathbb{Z} - \{0\}. \end{aligned}$$

alors si p est premier, $(\mathbb{Z}/p\mathbb{Z}, +, .)$ est un corps.

Anneau intègre

Soit $(A, +, .)$ un anneau, d'élément zéro 0.

Définition 1.1.5. Un élément $a \in A$ est dit diviseur de zéro s'il $\exists$ $b \in A, b \neq 0$ tel que

$$a.b = 0 \text{ ou } b.a = 0.$$

Exemple 1.1.5.
dans l'anneau $\mathbb{Z}/6\mathbb{Z}$ des entiers modulo 6 on a $\overline{2}.\overline{3} = \overline{0}$
alors $\overline{2}, \overline{3}$ sont des diviseurs de zéro dans $\mathbb{Z}/6\mathbb{Z}$.

Définition 1.1.6. Un anneau intègre est un anneau qui ne possède pas de diviseur de zéro autre que zéro.

Autrement dit : A est intègre $\Leftrightarrow$ si $a, b \in A : a.b = 0 \Rightarrow a = 0$ ou $b = 0$.

Exemples 1.1.6.
1) $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre.
2) $(\mathbb{Z}, +, .)$ est un anneau intègre.

Anneau principale

Définition 1.1.7. Un anneau principal est un anneau intègre tel que tout ideal de cet anneau est un idèal principal.

Exemples 1.1.7.
1) $\mathbb{Z}$ est un anneau principal.
2) $\Bbbk$ corps commutatif, l'anneau $\Bbbk[x]$ est un anneau principal.

Anneaux des polynômes

Définition 1.1.8. Soit $(A, +, .)$ un anneau. On appele polynôme à une indéterminée x à coefficients dans A une somme de la forme $a_0 + a_1x^1 + ... + a_nx^n$ tels que $n \in \mathbb{N}$ et $a_0, a_1, ..., a_n$ sont dans A.

Soient: $f(x) = a_0 + a_1x + ... + a_nx^n$ et $g(x) = b_0 + b_1x + ... + b_sx^s$ deux polynômes dans $A[x]$

on définit l'addition et la multiplication des polynômes f et g comme suit:

$(f, g) \longmapsto f+g(x) = (a_0+b_0)+(a_1+b_1)x+...+(a_i+b_i)x^i$
$(f, g) \longmapsto f \cdot g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + ... + (a_0b_n + a_1b_{n-1} + ... + a_nb_0)x^n + ... + a_nb_sx^{n+s}$

proposition 1.1.1.
$(A[x], +, .)$ est un anneau appelé l'anneau des polynôme en x sur A.

1.1.2 Corps finis

Définition 1.1.9. Un corps fini est un corps dont le nombre de ses éléments est fini.

Un corps fini à q élément est noté $\mathbb{F}_q$ ou $GF(q)$ (pour Galois field of q elements).

Exemple 1.1.8.
Si $p \in \mathbb{N}^*$ est premier, l'anneau $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est un corps fini à p éléments.

prenons comme cas particulier $p = 5$
On a
$\overline{2} \times \overline{3} = \overline{1}$
$\overline{4} \times \overline{4} = \overline{1}$
$\overline{1} \times \overline{1} = \overline{1}$
Alors
l'inverse de $\overline{2}$ est $\overline{3}$
l'inverse de $\overline{3}$ est $\overline{2}$
l'inverse de $\overline{4}$ est $\overline{4}$
l'inverse de $\overline{1}$ est $\overline{1}$
$\overline{0}$ n'admit pas un inverse

Caractéristique d'un corps
$\mathbb{K}$ corps commutatif, $0_{\mathbb{K}}$ et $1_{\mathbb{K}}$ sont respectivement les neutres de $\mathbb{K}$ pour l'addition "+" et la multiplication "."
pour $n \in \mathbb{N}$, on définit:

$$n.1_{\mathbb{K}} = \underbrace{1_{\mathbb{K}} + 1_{\mathbb{K}} + ... + 1_{\mathbb{K}}}_{n \text{ fois}}$$

Deux cas peuvent se présenter:

1) $n.1_{\mathbb{K}} = 0_{\mathbb{K}} \Leftrightarrow n = 0$
on dit que le corps $\mathbb{K}$ est de caractéristique nulle et on écrit $car(\mathbb{K}) = 0$.

2) $\exists\ n \in \mathbb{N}$, $n \neq 0$ tel que $n.1_{\mathbb{K}} = 0_{\mathbb{K}}$
on dit que le corps est de caractéristique non nulle.

Soit $p \in \mathbb{N}^*$ le plus petit entier naturel non nul vérifiant : $p.1_{\mathbb{K}} = 0_{\mathbb{K}}$,
p est appelé la caractéristique de $\mathbb{K}$.

Proposition 1.1.2. *Soit $\mathbb{K}$ un corps commutatif.*
1) *Si $car(\mathbb{K}) = p \succ 0$, alors p est premier.*
2) *Si $\mathbb{K}$ est un corps fini , alors $car(\mathbb{K})$ est premier.*
3) *Si $car(\mathbb{K}) = p \succ 0$ et $m \in \mathbb{N}$ verifie $m.1_{\mathbb{K}} = 0_{\mathbb{K}}$, alors $p \mid m$.*
4) *Tout corps fini à caractéristique p contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Exemples 1.1.9.
1) Le corps $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ est de caractéristique égale à 2.
2) Le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$ est de caractéristique égale à 3.
3) Le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.
4) le corps $\mathbb{Q}$ des nombres rationnels est de caractéristique nulle.

Théorème 1.1.1.
Soit $\mathbb{K}$ un corps commutatif de caractéristique p premier, $a, b \in \mathbb{K}$ et $n \in \mathbb{N}$ on a:
1) $(a+b)^p = a^p + b^p$.
2) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

Exemple 1.1.10. pour $\mathbb{K} = \mathbb{Z}/3\mathbb{Z}$ on a

$$(a+b)^3 = a^3 + b^3.$$

Théorème 1.1.2. *Soit $\mathbb{K}$ un corps fini d'ordre q, alors*:
1) $\forall x \in \mathbb{K}$, $x^q - x = 0$.
2*)* $q = p^n$, *avec* $n = [\mathbb{K} : \mathbb{Z}/p\mathbb{Z}]$.

Exemple 1.1.11.
Soit $\mathbb{F}_8$ un corps fini d'ordre 8 on a $8 = 2^3$ avec $q = 8$, $p = 2$, $n = 3$.

Élément irréductible

Soit A un anneau commutatif unitaire

Définition 1.1.10. Un élément $a \in A$ est dit irréductible dans A si:
1) $a \neq 0$ et $a \notin U(A)$.
2) Si $a = x.y$ dans A avec $x, y \in A$, alors $x \in U(A)$ ou $y \in U(A)$.

Exemples 1.1.12.
1) $A = \mathbb{R}[x]$, $f(x) = x^2 + 1$, $f(x)$ est irréductible dans $\mathbb{R}[x]$.
2) $A = \mathbb{C}[x]$, $f(x) = x^2 + 1$, $f(x)$ n'est pas irréductible dans $\mathbb{C}[x]$.

Construction d'un corps fini

Théorème 1.1.3. *Soit $f(x)$ un pôlynome irréductible de degré n sur le corps $\mathbb{F}_P = \mathbb{Z}/p\mathbb{Z}$, p premier, alors l'anneau quotient $\mathbb{F}_P[x]/(f(x))$ est un corps fini d'ordre $q = p^n$.*

Exemple 1.1.13.

Soit le corps $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$. On considère le polynôme $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$.

Comme le polynome $f(x)$ est irréductible sur $\mathbb{F}_2$, l'anneau quotient $\mathbb{F}_2[x]/ < x^3 + x + 1 >$ est un corps fini d'ordre $q = 2^3 = 8$.

On a

$$\mathbb{F}_2[x]/ < x^3 + x + 1 >= \{a_0 + a_1x + a_2x^2 + < x^3 + x + 1 >: a_0, a_1, a_2 \in \mathbb{F}_2\}$$

Si on pose $\alpha = \overline{x} = x + < x^3 + x + 1 >$, ce dernier s'écrit

$$\mathbb{F}_2[x]/ < x^3 + x + 1 >= \{a_0 1 + a_1\alpha + a_2\alpha^2 : a_0, a_1, a_2 \in \mathbb{F}_2\}$$

avec: $f(\alpha) = \overline{0} \Leftrightarrow \alpha^3 + \alpha + 1 = \overline{0}$ dans $\mathbb{F}_2[x]/ < x^3 + x + 1 >$

Donc

$$\mathbb{F}_2[x]/ < x^3 + x + 1 >= \{\overline{0}, \overline{1}, \alpha, 1 + \alpha, \alpha^2, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\}.$$

1.2 Codes correcteurs d'erreurs

dans cette section on rappelle que

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

1.2.1 Distance de Hamming

Définition 1.2.1. La distance de Hamming sur $\mathbb{F}_q^n$ est l'application:

$$d_H = \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{R}_+$$

définie par:

$$d_H(x, y) = |\{i = 1 \leq i \leq n : x_i \neq y_i\}|$$

pour $x = x_1 x_2 ... x_n$; $y = y_1 y_2 ... y_n \in \mathbb{F}_q^n$.

Exemples 1.2.1.
1) Sur $\mathbb{F}_2^3$ on a $d_H(111, 110) = 1$.
2) Sur $\mathbb{F}_3^4$ on a $d_H(1221, 0211) = 2$.

Propositions 1.2.1. *$d_H : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{R}_+$ est une distance sur $\mathbb{F}_q^n$ c'est-à-dire*
1) $\forall\ x, y \in \mathbb{F}^n$; $d_H(x, y) = 0$,*si et seulement si* $x = y$.
2) $\forall\ x, y \in \mathbb{F}^n$; $d_H(x, y) = d_H(y, x)$.
3) $\forall\ x, y, z \in \mathbb{F}^n$; $d_H(x, z) \leq d_H(x, y) + d_H(y, z)$.

Preuve
Soient x, y et $z \in \mathbb{F}^n$;
1)

$$\begin{aligned} d_H(x, y) = 0 &\iff |\{i = 1, ..., n : x_i \neq y_i\}| = 0 \\ &\iff \{i = 1, ..., n : x_i \neq y_i\} = \phi \\ &\iff \forall i = 1, ..., n; x_i = y_i \\ &\iff x = y \end{aligned}$$

2)
$$\begin{aligned} d_H(x,y) &= |\{i=1,...,n : x_i \neq y_i\}| \\ &= |\{i=1,...,n : y_i \neq x_i\}| \\ &= d_H(y,x) \end{aligned}$$

3) Pour l'inégalité triangulaire $d_H(x,z) \leq d_H(x,y) + d_H(y,z)$, on a

$$\{i : x_i = y_i\} \cap \{i : y_i = x_i\} \subset \{i : x_i = z_i\}$$

Par passage au complémentaire

$$\{i : x_i = z_i\}^C \subset (\{i : x_i = y_i\} \cap \{i : y_i = z_i\})^C$$

$$\{i : x_i \neq z_i\} \subset \{i : x_i \neq y_i\} \cup \{i : y_i \neq z_i\}$$

Donc

$$|\{i : x_i \neq z_i\}| \leq |\{i : x_i \neq y_i\} \cup \{i : y_i \neq z_i\}|.....(*)$$

et comme

$$\begin{aligned} |\{i : x_i \neq y_i\} \cup \{i : y_i \neq z_i\}| &\leq |\{i : x_i \neq y_i\}| + |\{i : y_i \neq z_i\}| \\ &\leq d_H(x,y) + d_H(y,z).....(**) \end{aligned}$$

De $(*)$ et $(**)$ on obtient

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

Donc $\left(\mathbb{F}_q^n, d_H\right)$ est un espace métrique appelé espace de Hamming.

1.2.2 Le poids de Hamming

Définition 1.2.2. Soit $x = x_1x_2...x_n \in \mathbb{F}_q^n$. Le poids de Hamming de x est le nombre naturel $w_H(x)$ définie par:

$$w_H(x) = d_H(x, 0) = \text{card}\{i : 1 \leq i \leq n \ / x_i \neq 0\}.$$

Exemples 1.2.2.
1) Sur $\mathbb{F}_2$ pour $n = 4$ on a: $w_H(1101) = 3$.
2) Sur $\mathbb{F}_3$ pour $n = 6$ $w_H(000120) = 2$.
3) $w_H(0) = w_H(00...0) = 0$.

1.2.3 Code sur un corps fini

$\mathbb{F}_q$ est le corps fini d'ordre q et $n \in \mathbb{N}^*$.

Définition 1.2.3. Un code de longueur n sur $\mathbb{F}_q$ est un sous-ensemble non vide C de $\mathbb{F}_q^n$.

Le code est appelé code binaire si $q = 2$;
Le code est appelé code ternaire si $q = 3$;

Pour un tel code, on appelle

n : la longueur du code C.
M : la taille de $C = |C|$ =card$(C) = \#C$.

Les éléments de $\mathbb{F}_q^n$ sont appelés les mots de longueur n sur $\mathbb{F}_q$.

Les éléments de C sont appelés les mots de code C.
$R = R(C) = \frac{Log|c|}{n}$: est appelé le taux de transmission de C(le taux d'information), avec $Log(q)$ est le logarithme de base q.

Notation 1.2.1. n, M, d sont appelés les paramètres du code C.
On dit que C est un code de paramètres $[n, M, d]$ sur $\mathbb{F}_q$.

Exemple 1.2.3.

$C = \{0000, 0011, 1100, 1111\} \subset \mathbb{F}_2^4$ est un code sur $\mathbb{F}_2$ de paramétres $[4, 2]$.

L'application "codage"

Définition 1.2.4. Soit C un code de paramétres $[n, k]$ sur le corps fini $\mathbb{F}_q$.

L'application codage est une application *injective* définie par:

$$\begin{array}{rcl} & \phi : \quad \mathbb{F}_q^k & \longrightarrow \mathbb{F}_q^n \\ m = \underbrace{a_1 a_2 ... a_k}_{\text{message}} & \longmapsto & x = \underbrace{x_1 x_2 ... x_k x_{k+1} ... x_n}_{\text{mot de code}} \end{array}$$

telle que
$C = \operatorname{Im} \phi = \phi(\mathbb{F}_q^k) \subset \mathbb{F}_q^n$
$m \in \mathbb{F}_q^k \longmapsto \phi(m) = x \in \mathbb{F}_q^n$.

Exemple 1.2.4.
Soit $\mathbb{F}_2 = \{0, 1\}$, $k = 3$ et $n = 6$;
C est un code de paramétres $(6, 8, 2)$ sur $\mathbb{F}_2$
On a

$$\begin{array}{c} \phi : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2^6 \\ a_1 a_2 a_3 \longrightarrow a_1 a_1 a_2 a_2 a_3 a_3 \end{array}$$

$C = \{a_1 a_1 a_2 a_2 a_3 a_3 : a_1, a_2, a_3 \in \mathbb{F}_2\}$
coder 101 en utilisant le code de répétition $C(n = 2)$
$101 \longrightarrow 110011 \in C$.

La distance minimale d'un code

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

Définition 1.2.5. La distance minimale de C est le nombre naturel $d(C)$ définie par:

$$d(C) = Min\{d_H(x,y) : x, y \in C, x \neq y\}$$

On a

$$\forall x, y \in C, x \neq y \text{ on a} : d \leq d_H(x,y).$$

Exemples 1.2.5.
1) Soit $C = \{001, 111, 101\} \subset \mathbb{F}_2^3$, alors

$$d(C) = 1$$

2) Soit $D = \{01, 10\} \subset \mathbb{F}_2^2$, alors

$$d(D) = 2$$

Lemme 1.2.1. *Soit C un code de paramètres (n, M, d) sur $\mathbb{F}_q$. pour $x, y \in C$ et $x \neq y$ on a:*

$$B(x, \left[\frac{d-1}{2}\right]) \cap B(y, \left[\frac{d-1}{2}\right]) = \phi.$$

Preuve. Supposons qu'il existe $z \in B(x, \left[\frac{d-1}{2}\right]) \cap B(y, \left[\frac{d-1}{2}\right])$ on a:

$$d \leq d_H(x,y) \leq d_H(x,z) + d_H(z,y) \leq \left[\frac{d-1}{2}\right] + \left[\frac{d-1}{2}\right]$$

Alors

$$d \leq 2.\left[\frac{d-1}{2}\right] \leq 2.\frac{d-1}{2} = d-1 \text{ (contradiction)}$$

$$\text{car: } [a] \leq a < [a]+1 \quad a \in \mathbb{R}.$$

Théorème 1.2.1. *(Borne de Hamming)*
Si C un code de type (n, M, d) sur $\mathbb{F}_q$ alors,

$$M \sum_{i=0}^{\left[\frac{d-1}{2}\right]} C_n^i (q-1)^i \leq q^n.$$

Preuve. Soit C un (n, M, d) code sur $\mathbb{F}_q$
On a

$$\bigcup_{x \in C} B(x, \left[\frac{d-1}{2}\right]) \subset \mathbb{F}_q^n$$

$$\Longrightarrow$$

$$\left| \bigcup_{x \in C} B(x, \left[\frac{d-1}{2}\right]) \right| \leq \left|\mathbb{F}_q^n\right|$$

donc

$$\sum_{x \in C} \left| B(x, \left[\frac{d-1}{2}\right]) \right| \leq q^n$$

d'où

$$M \sum_{i=0}^{\left[\frac{d-1}{2}\right]} C_n^i (q-1)^i \leq q^n.$$

Proposition 1.2.2. *Soit C un (n, M, d) code sur $\mathbb{F}_q$;*
Alors:
1) *C détècte au plus $d-1$ erreurs.*
2) *C corrige au plus $\left[\frac{d-1}{2}\right]$ erreurs.*

1.2.4 Codes Linéaires

Soit $\mathbb{F}_q$ un corps fini à q élément et $n \in \mathbb{N}^*$,on appele éspace vectoriel de dimension n sur $\mathbb{F}_q^n$.

pour l'opérations internes " + " et "." on a
$(x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n) = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$.
$\lambda(x_1, x_2, ..., x_n) = (\lambda x_1, \lambda x_2, ..., \lambda x_n)$.

Définition 1.2.6. Un code linéaire de longueur n sur $\mathbb{F}_q$ est un sous éspace vectoriel de $\mathbb{F}_q^n$.

Si C est un code linéaire de dimension k, on a: $M = |C| = q^k$.

C code linéaire de longueur n , de dimension k(ou $M = q^k$) et de distance minimale d, Alors on dit que:

C est un code linéaire de paramètres (n, q^k, d) sur $\mathbb{F}_q^n$, ou

C est un code linéaire de type (de paramètres) $[n, k, d]$ sur $\mathbb{F}_q$.

Remarques 1.2.1.

1) Le vecteur null $0 = (0, 0, ..., 0) = 000...0$ est un mot de code de tout code linéaire.

2) $\dim(C) = k \iff M = |C| = q^k$.

Matrice génératrice d'un code linéaire

Soit C un code linéaire, de longueur n et de dimension k.

Définition 1.2.7. Une matrice génératrice de C est une matrice d'ordre $k \times n$ sur $\mathbb{F}_q$ dont les lignes sont des vecteurs de base de C.

Soit $\{g_1 = g_{11}g_{12}...g_{1n}, g_2 = g_{21}g_{22}...g_{2n}, ..., g_k = g_{k1}g_{k2}...g_{kn}\}$ une base du code C, la matrice:

$$G = \begin{pmatrix} g_{11} & g_{12} & . & . & . & g_{1n} \\ g_{21} & g_{22} & . & . & . & g_{2n} \\ . & & . & & & . \\ . & & & . & & . \\ . & & & & . & . \\ g_{k1} & g_{k2} & . & . & . & g_{kn} \end{pmatrix}$$

est une matrice génératrice de C.

Exemple 1.2.6. Soit $\{100, 010\}$ est une base du code linéaire C,la matrice

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

est une matrice génératrice de C.

Propriété 1.2.1. *Si* $G = \begin{pmatrix} g_1 \\ g_2 \\ . \\ . \\ . \\ g_k \end{pmatrix}$

est une matrice génératrice d'un code linéaire C*, alors*
$C = \{\lambda_1 g_1 + \lambda_2 g_2 + ... + \lambda_k g_k$ *tel que* $\lambda_i \in \mathbb{F}_q, 1 \leq i \leq k\}$
$= \{(\lambda_1, \lambda_2, ..., \lambda_k)G$ *tel que* $\lambda_i \in \mathbb{F}_q; 1 \leq i \leq k\}$.

Soit $x = x_1 x_2 ... x_n \in \mathbb{F}_q^n$, $x \in C \iff \exists\, m \in \mathbb{F}_q^n : x = mG$
C *code linéaire* $[n, k, d]$ *sur* $\mathbb{F}_q^n$, G *matrice génératrice de* C .
l'application ϕ :

$$\begin{array}{c} \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n \\ m \longrightarrow x = \phi(m) = mG \end{array}$$

est appelée application codage

$C = \phi(\mathbb{F}_q^n) = \operatorname{Im}\phi \subset \mathbb{F}_q^n$.

Exemple 1.2.7.
Soit $C = \{000, 100, 010, 110\}$ un code sur $\mathbb{F}_2$;

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

est une matrice génératrice de C;

l'applicatoin codage:

$$\begin{array}{c} \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^3 \\ m = \lambda_1\lambda_2 \longmapsto x = x_1x_2x_3 = mG \end{array}$$

$$mG = (\lambda_1, \lambda_2)\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = (\lambda_1, \lambda_2, 0) = \lambda_1\lambda_2 0$$

$$\begin{aligned} C &= \left\{mG : m \in \mathbb{F}_2^2\right\} \\ &= \left\{\lambda_1\lambda_2 0 : \lambda_1, \lambda_2 \in \mathbb{F}_2^2\right\} \end{aligned}$$

Par exemple
· Coder 01 par C done $01G = 010 \in C$.
· Décoder 110 par C on a $110 = mG \implies m = 11 \in \mathbb{F}_2^2$.

Le produit scalaire

Définition 1.2.8. Soit $x = x_1x_2...x_n$ et $y = y_1y_2...y_n$ deux vecteurs de l'espace vectoriel $\mathbb{F}_q^n$. On définit le produit scalaire de x et y par la formule suivant :

$$\langle x, y\rangle = x \cdot y = x_1y_1 + x_2y_2...x_ny_n = \sum_{i=1}^{n} x_iy_i$$

Si $\langle x, c\rangle = 0$, on dit que x et c sont ortogonaux, dans se cas on écrit $x \perp c$.

Exemles 1.2.8.
1) Sur $\mathbb{F}_2$ et pour $n = 4$
$\langle 1010, 0111\rangle = 1$
$\langle 1010, 1010\rangle = 0$.
2) Sur $\mathbb{F}_3$ et pour $n = 3$, $\langle 120, 111\rangle = 1 + 2 + 0 = 3 = 0$.

Le dual d'un code

Définition 1.2.9. Soit C un code linéaire de type $[n, k, d]$ sur $\mathbb{F}_q$, le code dual de C est l'ensemble $C^\perp$ défini par:

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

Exemple 1.2.9.
Sur $\mathbb{F}_2$ si $C = \{000, 011, 110, 101\}$, alors le code dual de C est $C^\perp = \{000, 111\}$.

Proposition 1.2.3.
$C^\perp$ est une code linéaire de type $[n, n - k]$.

Preuve. Soit $C \subset \mathbb{F}_q^n$ un code linéaire de paramètres $[n, k, d]$ sur $\mathbb{F}_q$.

Soient $x, y \in C^\perp$ et $\lambda \in \mathbb{F}_q$, pour $c \in C$
On a: $\langle x - y, c\rangle = \langle x, c\rangle - \langle y, c\rangle = 0 - 0 = 0$
$\langle \lambda x, c\rangle = \lambda \langle x, c\rangle = 0$
$\Longrightarrow$ $x - y \in C^\perp$ et $\lambda x \in C^\perp$
Donc $C^\perp$ est un code linéaire sur $\mathbb{F}_q$;
et on a

$$\dim(\mathbb{F}_q^n) = \dim(C) + \dim(C^\perp)$$

$$n = k + \dim(C^\perp)$$

$$\dim(C^\perp) = n - k.$$

Définition 1.2.10. Si $C = C^\perp$ on dit que C est un code *auto-dual.*

Exemple 1.2.10.

On a $C = \{0000, 0011, 1100, 1111\}$ est un code auto-dual sur $\mathbb{F}_2^4$
car $\dim(C^\perp) = n - k = 4 - 2 = 2 = \dim(C) \Longleftrightarrow C = C^\perp$

et $\forall\ x, y \in C$ On a $\langle x, y\rangle = 0 \Longleftrightarrow C \subset C^\perp$

Matrice de contrôle

C est un code linéaire de paramètres $[n, k, d]$ sur $\mathbb{F}_q$, $C^\perp$ est le code dual de type$[n, n - k, d]$.

Définition 1.2.11. Une matrice de contrôle H du code C est une matrice génératrice de code dual $C^\perp$.

Remarque 1.2.2. H d'ordre $(n - k) \times n$.

Exemple 1.2.11.
Soit C un code linéaire de type $[4, 2]$ sur $\mathbb{F}_3$, de matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

G est dans la forme standard $(I_2|A)$, alors $H = (-A^\top|I_2) = \begin{pmatrix} -2 & -2 & 1 & 0 \\ -2 & -1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$.

Chapitre 2

Le polynôme énumérateur des poids

Dans ce chapitre, nous donnons la définition et les propriétés du polynôme énumérateur des poids.

polynôme homogène

Soit $f(x_1, ..., x_n)$ un polynôme en $x_1, ..., x_n$ sur $\mathbb{K}$
c'est-à-dire $f \in \mathbb{K}[x_1, ..., x_n]$.

Définition 2.1 On dit que f est un polynôme homogène de dégré d si:

$$f(tx_1, ..., tx_n) = t^d f(x_1, ..., x_n)$$

pour tout $t \in \mathbb{K}$

c'est-à-dire tous les termes de f sont de dégré d.

Exemple 2.1
Soit

$$f(x_1, x_2) = x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3$$

alors on a :

$$\begin{aligned} f(tx_1, tx_2) &= t^3 x_1^3 + t^2 x_1^2 t x_2 + t x_1 t^2 x_2^2 + t^3 x_2^3 \\ &= t^3 f(x_1, x_2) \end{aligned}$$

donc f est homogène de dégré 3.

2.1 Le polynôme énumérateur des poids

Définition 2.1.1. ([2],[11]) Soit C un code linéaire de paramètres $[n, M, d]$ sur $\mathbb{F}_q$. Le polynôme énumérateur homogène des poids du code C est le polynôme $W_C(x, y)$ défini par:

$$W_C(x,y) = \sum_{c \in C} x^{n-w_H(c)} y^{w_H(c)}$$

Soit A_i le nombre de mots de poids i dans C

$$A_i = \{c \in C \mid w_H(c) = i\}$$

l'ensemble $\{A_0, A_1, ..., A_n\}$ est appelé la distribution des poids. Le polynôme énumérateur de C est:

$$\begin{aligned} W_C(x,y) &= \sum_{c \in C} x^{n-w_H(c)} y^{w_H(c)} \\ &= \sum_{i=0}^{n} A_i x^{n-i} y^i \\ &= A_0 x^n + A_1 x^{n-1} y + ... + A_n y^n. \end{aligned}$$

Ici x et y sont indéterminés, et $W_C(x,y)$ est un polynôme homogène de dégré n en x et y. Il est souvent utile que $W_C(x,y)$ soit un polynôme homogène. Mais nous pouvons toujours nous débarrasser de x en posant $x = 1$. Et on définit

$$W_C(1,y) = W_C(y) = \sum_{i=0}^{n} A_i y^i.$$

Exemples 2.1.1.

1) Le code $C = \{110, 000, 011, 111, 010, 001\}$ dans $\mathbb{F}_2^3$, on a $A_0 = 1$; $A_1 = 2$; $A_2 = 2$; $A_3 = 1$, et

$$W_C(x,y) = x^3 + 2x^2y + 2xy^2 + y^3.$$

2) Le code $\{000, 011, 101, 110\}$ dans $\mathbb{F}_2^3$, noté C, le dual $C^\perp$ est $\{000, 111\}$, et les énumérateurs de poids sont respectivement:

$$\begin{aligned} W_C(x,y) &= x^3 + 3xy^2. \\ W_{C^\perp}(x,y) &= x^3 + y^3. \end{aligned}$$

3) Le code $\{0000, 0011, 1100, 1111\}$ dans $\mathbb{F}_2^4$, noté C, est auto-dual: $C^\perp = C$, et

$$W_C(x,y) = x^4 + 2x^2y^2 + y4.$$

Remarque 2.1.1.
On a les relations suivants entre $W_C(y)$ et $W_C(x,y)$

$$W_C(y) = W_C(1,y)$$

et

$$W_C(x,y) = x^n W_C(x^{-1}y)$$

Et donné l'énumérateur de poids $W_C(y)$ ou l'énumérateur de poids homogène $W_C(x,y)$, la distribution des poids $\{A_i\}_{i=0}^n$ est determinée par les coefficients.

Il est clair que l'énumérateur de poids et l'énumérateur de poids homogène peuvent être écrits en une autre forme, c'est-à-dire

$$W_C(y) = \sum_{c \in C} y^{w_H(c)}$$

et

$$W_C(x,y) = \sum_{c \in C} x^{n - w_H(c)} y^{w_H(c)}.$$

Remarque 2.1.2.
Soit C un code linéaire. Alors A et la distance minimale $d(c)$, qui est égal au poids minimun, est déterminée par l'énumérateur de poids comme suit:

$$d(C) = \min\{i \ / \ A_i \neq 0, i \succ 0\}.$$

Il détermine également la dimension k de C (et par suite $M = q^k$), puisque:

$$W_C(1,1) = \sum_{i=0}^{n} A_i = q^k = M.$$

Théorème d'Euler. ([12])

Théorème 2.1.1. *Soit $\varphi(x_1, x_2, ..., x_n)$ une fonction définie sur $\mathbb{R}^n$ avec valeur dans R, que l'on suppose différentiable en tout point si la fonction φ est homogène de degré m, alors on a*

$$\begin{aligned} m\varphi(x_1, x_2, ..., x_n) &= \sum_{i=1}^{n} x_i \frac{\partial \varphi}{\partial x_i}(x_1, x_2, ..., x_n) \\ \textit{telque pour tout} \quad (x_1, x_2, ..., x_n) &\in \mathbb{R}^n. \end{aligned}$$

Preuve. φ est une fonction homogène d'ordre m, si

$$\varphi(\lambda x_1, \lambda x_2, ..., \lambda x_n) = \lambda^m \varphi(x_1, x_2, ..., x_n)$$

pour $\lambda \succ 0$, on dérive $\varphi(\lambda x_1, \lambda x_2, ..., \lambda x_n)$ par rapport $\lambda = 1$

$$\frac{d\varphi(\lambda x_1, \lambda x_2, ..., \lambda x_n)}{d\lambda} = \sum_{i=1}^{n} \frac{\partial \varphi(\lambda x_1, \lambda x_2, ..., \lambda x_n)}{\partial(\lambda x_i)} \times \frac{\partial(\lambda x_i)}{\partial \lambda}$$

alors

$$= \sum_{i=1}^{n} \frac{\partial \varphi(\lambda x_1, \lambda x_2, ..., \lambda x_n)}{\partial(\lambda x_i)} \times x_i$$

donc

$$= \sum_{i=1}^{n} \frac{\partial \varphi(x_1, x_2, ..., x_n)}{\partial x_i} \times x_i.$$

Et on dérive $\lambda^m \varphi(x_1, x_2, ..., x_n)$ par rapport $\lambda = 1$

$$\begin{aligned}\frac{d(\lambda^m\varphi(x_1,x_2,...,x_n))}{d\lambda} &= m\lambda^{m-1}\varphi(x_1,x_2,...,x_n)\\ &= m\varphi(\lambda x_1,\lambda x_2,...,\lambda x_n).\end{aligned}$$

Remarque 2.1.3 Pour $m=1$ on a

$$\varphi(x_1,x_2,...,x_n)=\sum_{i=1}^{n}x_i\frac{\partial\varphi}{\partial x_i}(x_1,x_2,...,x_n).$$

Chapitre 3

Quelques Applications

3.1 Théorème de MacWilliams

Dans cette section, nous designons par $\mathbb{F}_q$ un corps fini d'ordre $q = p^m$ énumérateurs de poids des codes linéaires, òu p est un nombre premier. Les éléments de $\mathbb{F}_q$ sont désignés par $w_0 = 0, w_1, ..., w_{q-1}$ dans un ordre fixe.

Ce théorème est l'un des résultats les plus remarquables de la théorie du codage. Il dit que l'énumérateur de poids du code dual C est complétement déterminé par l'enumérateur de poids de C.

Lemme 3.1.1. ([2]) *Soient A un espace vectoreil sur le corps complexe $\mathbb{C}$ et $f : \mathbb{F}^n \longrightarrow A$ une application.*

On definit la transformation de Fourir par:

$$\widehat{f}(u) = \sum_{v \in \mathbb{F}^n} f(v)(-1)^{u.v}$$

alors pour tout code linéaire $C \subset \mathbb{F}^n$ on a

$$\sum_{v \in C^\perp} f(v) = \frac{1}{|C|} \sum_{u \in C} \widehat{f}(u).$$

Preuve. On a

$$\sum_{u \in C} \widehat{f}(u) = \sum_{u \in C} \sum_{v \in \mathbb{F}^n} f(v)(-1)^{u.v} = \sum_{v \in \mathbb{F}^n} f(v) \sum_{u \in C} (-1)^{u.v}$$

Si $v \in C^\perp$, la somme intérieure est égale à $|C|$ mais si $v \notin C^\perp$, $u.v = 0$, et 1 également souvent et la somme intérieure est égale à zéro.

Théorème de MacWilliams (*cas binaire*) ([11])

Théorème 3.1.1. *Soit $\mathbb{F}^n$ l'ensemble de tous les vecteurs binaires de longueur n. Il s'agit d'un espace vectoriel de dimension n sur le corps $\mathbb{F}_2$. Si C est un code linéaire binaire $[n,k]$ avec code dual $C^\perp$, alors*

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y) \qquad (1)$$

De manière équivalente

$$\sum_{k=0}^{n} A_k^1 x^{n-k} y^k = \frac{1}{|C|} \sum_{i=0}^{n} A_i (x,y)^{n-i} (x-y)^i \qquad (2)$$

ou

$$\sum_{u \in C^\perp} x^{n-w_H(u)} y^{w_H(u)} = \frac{1}{|C|} \sum (x+y)^{n-w_H(u)} (x-y)^{w_H(u)} \qquad (3)$$

les équations (1),(2) et (3) sont parfois appleés identités de MacWilliams.

preuve. Nous applications le lemme avec

$$f(u) = x^{n-w_H(u)} y^{w_H(u)}$$

ensuite nous avons

$$\widehat{f}(u) = \sum_{r \in \mathbb{F}^n} (-1)^{u.v} x^{n-w_H(u)} y^{w_H(v)}$$

Soit $u = (u_1 ... u_n)$; $v = (v_1 ... v_n)$. Alors

$$\begin{aligned} \widehat{f}(u) &= \sum_{v \in \mathbb{F}^n} (-1)^{u_1 v_1 + ... + u_n v_n} \prod_{i=1}^{n} x^{1-v_i} y^{v_i} \\ &= \sum_{v_1=0}^{1} \sum_{v_2=0}^{1} ... \sum_{v_n=0}^{1} \prod_{i=1}^{n} (-1)^{u_1 v_n} x^{1-v_i} y^{v_i} \qquad (4) \end{aligned}$$

tout comme

$$a_0b_0c_0+a_0b_0c_1+a_0b_1c_0+a_0b_1c_1+a_1b_0c_0+a_1b_0c_1+a_1b_1c_0+a_1b_1c_1 = (a_0+a_1)(b_0+b_1)(c_0+c_1)$$

donc (5) est égale à

$$\prod_{i=1}^{n}\sum_{\omega=0}^{n}(-1)^{u_i w_H} x^{1-w_H} y^{w_H}$$

si $u_i = 0$ la somme intérieure est $x + y$.Si $u_i = 1$, C'est $x - y$.Ainci $\widehat{f}(u) = (x + y)^{n-w_H(u)}(x - y)^{w_H(u)}$

Ensuit, l'équation (4) lit

$$\sum_{u\in C^{\perp}} x^{n-w_H(u)} y^{w_H(u)} = \frac{1}{|C|}(x + y)^{n-w_H(u)}(x - y)^{w_H(u)}$$

Lemme 3.1.2. ([11]) *Si C est un code linéaire binaire de paramètres $[n, k]$, alors*

$$\sum_{u\in C^{\perp}} f(u) = \frac{1}{|C|}\sum_{u\in C}\widehat{f}(u)$$

Preuve. On a

$$\sum_{u\in C}\widehat{f}(u) = \sum_{u\in C}\sum_{u\in\mathbb{F}^n}(-1)^{u.v} f(v)$$

donc

$$= \sum_{v\in\mathbb{F}^n} f(v)\sum_{u\in C}(-1)^{u.r}$$

alors

$$= |C|\sum_{r\in C} f(v)$$

Exemples 3.1.1. Nous appliquons le théorème de MacWilliams aux exemples du page (24)

1) On a $W_C(x,y) = x^3 + 2x^2y + 2xy^2 + y^3$

$$\frac{1}{6}W_C(x+y,x-y) = \frac{1}{6}[(x+y)^3 + 2(x+y)^2(x-y) + 2(x+y)(x-y)^2 + (x-y)^3$$
$$= x^3 + \frac{1}{3}xy^2$$

2) On a $W_C(x,y) = x^3 + 3xy^2$

$$\frac{1}{4}W_C(x+y,x-y) = \frac{1}{4}\left[(x+y)^3 + (x+y)(x-y)^2\right]$$
$$= x^3 + y^3$$

ce a qui est en effet $W_{C^\perp}(x,y)$, encore une fois,

$$\frac{1}{2}W_{C^\perp}(x+y,x-y) = \frac{1}{2}\left[(x+y)^3 + (x-y)^3\right]$$
$$= x^3 + 3xy^2 = W_C(x,y)$$

illustrant que le théoréme est symétrique par rapport aux rôles de C et $C^\perp$.

3) On a $W_C(x,y) = x^4 + 2x^2y^2 + y^4$, donc

$$\frac{1}{4}W_C(x+y,x-y) = \frac{1}{2}\left[(x+y)^4 + 2(x+y)^2(x-y)^2 + (x-y)^4\right]$$
$$= x^4 + 2x^2y^2 + y^4 = W_C(x,y)$$

ce qui est correct puisque C est auto-dual.

Théorème de MacWilliams sur un corps fini quelconque. ([11])

Théorème 3.1.2. *Soit $C^\perp$ un code de type $[n,k]$ sur $\mathbb{F}_q$, alors*

$$W_{C^\perp}(x,y) = \frac{1}{q^k}W_C(x+(q-1)y, x-y).$$

Exemples 3.1.2.

1) Le code zéro $C = \{0\}$ a un énumérateur de poids homogène x^n est sont dual $\mathbb{F}_q^n$ a un énumérateur de poids homogène $((x+(q-1)y)n$.

2) Le code de répétition n fois homogène $x^n + (q-1)y^n$ et l'énumérateur de poids homogène de son code dual dans le cas binaire est $\frac{1}{2}(x+y)^n + (x-y)$ pour arbitraire, nous avous

$$\begin{aligned} W_{C^\perp}(x,y) &= \frac{1}{q} W_C(x+(q-1)y, x-y) \\ &= \frac{1}{q} W_C((x+(q-1)y)^n, (q-1)(x-y)^n) \\ &= \sum_{w=0}^{n} \binom{n}{w_H} \frac{(q-1)^{w_H} + (q-1)(-1)^{w_H}}{q} x^{n-w_H} y^{w_H}. \end{aligned}$$

Théorème de MacWilliams pour les codes non linéaire. ([11])

Théorème 3.1.3. *On appelle le* $(n+1)$*-tuple* $\{A_0, ..., A_n\}$*, òu*

$$A_i = \sum_{w_H(v)=i} C$$

La distribution de poids de C*. C'est la généralisation naturelle de la distribution de poids d'un code. Bien sûr* $\sum A_i = M$*.*

$$\begin{aligned} W_C(x,y) &= \sum_{v \in \mathbb{F}^n} C_i x^{n-w_H(v)} y^{w_H(v)} \\ &= \sum_{i=0}^{n} A_i x^{n-i} y^i. \end{aligned}$$

Théorème 3.1.4.

$$W_{C^\perp}(x,y) = \frac{1}{M} W_{C^\perp}(x+y, x-y)$$

Ce théorème peut être considérer comme des théorèmes de MacWilliams pour les codes non linéaire.

3.2 Probabilité

Dans cette section, nous verrons si les messages reçus peuvent être déchiffrés correctement ou toutes les erreurs détectées.

Théorème 3.2.1. ([8]) *Soit $C \subset \mathbb{F}_q^n$ un code linéaire. Notons A_i le nombre des mots de C de poids i. La probabilité qu'un message reçu contienne une erreur non détectée est donné par*

$$\sum_{i=1}^{n} A_i p^i (1-p)^{n-i} (q-1)^{-i}$$

En particulier, si C est un code binaire, c'est-à-dire si $q = 2$, cette probabilité est

$$\sum_{i=1}^{n} A_i p^i (1-p)^{n-i} = W_C(1-p, p) - (1-p)^n,$$

où $W_C(x, y)$ est l'énumérateur de poids de C.

preuve. Soit c un mot de code, et supposons que e est l'erreur commise dans la transmission de c , c'est-à-dire $e = x - c$ où x est le message reçu. Puisque C est linéaire, x sera un mot de code si et seulement si e l'est. Ainsi l'erreur possible est non détecté si e est un mot de code différent de 0.

Supposons que $i = w_H(e)$. La probabilité de i erreurs dans i positions spécifiés est $p^i(1-p)^{n-i}$, et le nombre de choix pour ces i positions parmi n positions est $\binom{n}{i}$. Ainsi $\binom{n}{i} p^i (1-p)^{n-i}$ est la probabilité que l'erreur e ait un poids i.

D'autre part il y a $\binom{n}{i}(q-1)^i$ mots de poids i puisqu'il y a $\binom{n}{i}$ choix pour les positions non nulles, et $q-1$ choix possibles pour chacune de ces positions. Ainsi, la probabilité que le mot d'erreur e de poids i soit un mot de code est $\frac{A_i}{\binom{n}{i}(q-1)^i}$.

Par suite, la probabilité que e soit un mot de code de poids i est la probabilité que e ait un poids i multipié par la probabilité qu'un mot de poids i soit un mot de code, à savoir

$$\begin{aligned} prob[w_H(e) &= i, e \in C] = \frac{A_i}{\binom{n}{i}(q-1)^i} \cdot \binom{n}{i} p^i (1-p)^{n-i} \\ &= A_i p_i (1-p)^{n-i}. \end{aligned}$$

Ainsi, la probabilité que e soit un mot de code non nul est la somme de ces expressions de $i = 1$ à $i = n$, et cela prouve l'affirmation.

Exemple 3.2.1.
Le code $C = \{0000, 1000, 0100, 1100\}$ dans $\mathbb{F}_2^4$, on a $A_0 = 1$; $A_1 = 2$; $A_2 = 1$; $A_3 = 0$; $A_4 = 0$, et le polynôme énumérateur de poids est:

$$W_C(x, y) = x^4 + 2x^3y + x^2y^2,$$

comme C est une code binaire, alors la probabilité est:

$$\begin{aligned} \sum_{i=1}^{n} A_i p^i (1-p)^{n-i} &= W_C(1-p, p) - (1-p)^n \\ &= (1-p)^4 + 2(1-p)^3 p + (1-p)^2 p^2 + (1-p)^4 \\ &= 2p(1-p)^3 + p^2(1-p)^2. \end{aligned}$$

Conclusion

Dans ce travial, on a essayé de faire une étude sur le polynôme énumérateur des poids (d'aprés Hamming) en expliquant les notions fondamentales nécéssaires pour cette étude. Le polynôme joue un rôle important pour déterminer la distribution des poids d'un code et à calculer la probabilité liée à l'erreur de transmission.

Bibliographie

[1] Bachoc, C. Master CSI 2 Année 2004-2005 Cours de codes (UE Codes/Signal).

[2] Hall Jr, M., & van Lint, J. H. (1974). Combinatorics: proceedings of the Advanced Study Institute on combinatorics held at Nijenrode Castle, 1974, Breukelen, The Netherlands, July 8-20, 1974.

[3] Jurrius, R., & Pellikaan, R. (2009). Codes, arrangemens and weight enumerators. Soria Summer School on Computational Mathematics (S3CM): Applied Computational Algebraic Geomertric Modelling.

[4] Kac, M. (1943). Paul R. Halmos, Finite dimensional vector spaces. Bulletin of the American Mathematical Society, 49(5), 349-350.

[5] Ladjelat, L. 2019/2020. Corps finis. Cours 1érè Mestre . Algèbre Mathémathique Discrèt. Université de M'sila.

[6] Ladjelat, L. 2019/2020. Aneaux et extensions algèbrique. Cours 1^{ere} Mestre. Algèbre Mathémathique Discrèt. Université de M'sila.

[7] Ladjelat, L. 2020/2021. Codage Algèbrique. Cours $2^{\text{éme}}$ Mestre . Algèbre Mathémathique Discrèt. Université de M'sila.

[8] Lemmermeyer, F. (2005). Error-correcting Codes. Training Report.

[9] Lang, S. (2002). Graduate Texts in Mathematics: Algebra. Springer.

[10] Ling, S., & Xing, C. (2004). Coding theory: a first course. Cambridge University Press.

[11] MacWilliams, F. J., & Sloane, N. J. A. (1977). The theory of error correcting codes (Vol. 16). Elsevier.

[12] Marceau, E. 13 avril 2015. Fonctions homogène, théorème d'Euler et applications en actuariat.

[13] WILDON, M. ERROR CORRECTING CODES MT361/MT461/MT5461.

ملخص

في هذه المذكرة قمنا بتقديم دراسة عن كثير حدود العادّ للثقل حسب مفهوم هامينغ.

في الأول قدمنا تذكيرا بالخصائص الأساسية التي تحتاج إليها في هذا العمل (الحقل المنته,الشفرة المصححة للأخطاء).

بعد ذلك ذكرنا كثير الحدود العادّ وبعض خواصه المتعلقة بالتجانس.

وأخيرا ذكرنا نظرية ماكويليامس الخاصة بكثير الحدود العادّ للثقل وكذلك تطبيق هذا الأخير في حساب بعض الإحتمالات المتعلقة بالشفرات المصححة للأخطاء.

Résume

Dans ce mémoire, nous présentons une étude sur le polynôme énumérateur d'un code correcteur d'erreurs selon Hamming .

Nous commençons par rappelle des notions fondamentales (corps fini, code correcteur d'erreurs), ensuite nous parlons du polynôme énumérateur et quelques propriétés (homogénieté).

Enfin, nous étions le théorème de MacWilliams et une application dans le calcul de la probabilité liée aux codes correcteurs d'erreurs.

Abstract

In This memory, we present a study of the weight enumerator polynomial of an error-correcting code with respect to Hamming. We start by recalling some definition of fundamental notions(Finite Field, error-correcting code).

After that we talk about the weight enumerator polynomial and some of its properties (homogeniety).

Finally, we state the theorem of MacWilliams and an application to error-correcting codes.