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 discrètes

Thème

TRANSFORMATIONS MONOMIALES DES ESPACES DE HAMMING

Présenté par :

- ROUKAILA KHOULOUD

- BELAROUI SABAH

Soutenu publiquement le : 07 / 06 / 2026

Mohamed Ourabah Benmeddour	M.C.B	Univ. M'sila	Président
Lahcene Ladjelat	M.C.B	Univ. M'sila	Encadreur
Mehenni Abdelkrim	M.C.B	Univ. M'sila	Examinateur

Année universitaire 2025/2026

TRANSFORMATIONS MONOMIALES DES ESPACES DE HAMMING

ROUKAILA KHOULOUD. BELAROUI SABAH

2025/2026

Dédicace

Au nom d'Allah, le Tout Miséricordieux, le Très Miséricordieux.

Je rends grâce à Dieu Tout-Puissant de m'avoir permis d'achever ce travail et de mener à bien ce parcours académique.

Je dédie ce mémoire :

À mes chers parents, en témoignage de ma profonde reconnaissance pour leurs sacrifices, leur soutien indéfectible et leurs prières constantes, qui ont constitué une source essentielle de motivation et de persévérance tout au long de mes études.

À l'ensemble de ma famille, pour leur encouragement continu et leur présence bienveillante.

À mes enseignants, pour la qualité de leur encadrement, leur rigueur scientifique et la richesse de leurs enseignements durant mon parcours universitaire.

À toute personne ayant contribué, de près ou de loin, à la réalisation de ce travail.

Enfin, je dédie ce modeste travail à tous ceux qui ont marqué positivement mon parcours académique et scientifique.

Sabah et Kholoud

Remerciements

Nous remercions Allah le Tout-Puissant pour Sa grâce, Son aide et Son soutien tout au long de notre parcours.

« Et lorsque votre Seigneur proclama : Si vous êtes reconnaissants, J'augmenterai certainement Mes bienfaits pour vous. »

Sourate Ibrahim, verset 7.

Les mots ne suffisent pas pour exprimer notre profonde gratitude et notre reconnaissance envers toutes les personnes qui ont contribué à la réalisation de ce travail.

Nous adressons nos sincères remerciements à notre encadrante **Dr. Ladjlet Lahcen**, pour son aide précieuse, ses conseils, son orientation et son soutien tout au long de ce travail.

Nous remercions également tous les enseignants qui nous ont accompagnés durant notre parcours universitaire et qui nous ont transmis leur savoir avec dévouement.

Nos remerciements les plus respectueux vont aussi aux membres du jury pour l'honneur qu'ils nous font en acceptant d'évaluer ce mémoire.

Enfin, nous exprimons notre gratitude à toutes les personnes, proches ou lointaines, qui ont contribué de près ou de loin à l'aboutissement de ce mémoire.

Sabah et Kholoud

Table des matières

Introduction **1**

1 Notions préliminaires **3**

1.1 Groupe 3

1.2 Sous-groupe 4

1.3 Sous-groupe normal 5

1.4 Produit direct de deux groupes 6

1.5 Groupe symétrique 7

1.6 Corps finis 8

1.7 Codes correcteurs d erreurs 9

1.7.1 Codes de longueur fixe 9

1.7.2 Distance de Hamming 10

1.7.3 Poids de Hamming 10

1.7.4 Distance minimale et paramètres d'un code 11

2 Transformations monomiales **14**

2.1 Isométries de $(\mathbb{F}_q^n, d_H)$ 14

2.2 Isométries lineaires 15

2.3 Transformations monomiales de $\mathbb{F}_q^n$ 17

2.4 Matrice monomiale 19

3 Exemples et applications **30**

3.1 Equivalence des codes 30

3.1.1 Equivalence des codes lineaires 30

Conclusion **35**

Bibliographie **36**

Introduction

Dans le domaine des communications numériques et du stockage de données, la transmission d'informations est exposée à des perturbations dues au bruit des canaux. La théorie des **codes correcteurs d'erreurs**, née des travaux pionniers de Claude Shannon et Richard Hamming, offre des solutions mathématiques pour garantir l'intégrité de ces informations. L'étude de ces codes repose fondamentalement sur des structures algébriques modernes, notamment la théorie des groupes et des corps finis.

L'objectif de ce mémoire est d'exposer les fondements algébriques des codes et de l'espace de Hamming et d'analyser les transformations monomiales (les isométries lineares) qui préservent les propriétés essentielles de l'espace et ses codes, relativement a la distance de Hamming.

Le **premier chapitre** est dédié aux notions préliminaires. Nous y rappelons les concepts fondamentaux de la théorie des groupes (groupes symétriques, produits directs) et des corps finis, avant d'introduire les paramètres fondamentaux d'un code tels que la distancé et le poids de Hamming.

Le **deuxième chapitre** constitue le but théorique de notre étude. Il traite des isométries et en particulier les transformations monomiales (isométries linéaires) de l'espace de Hamming $(\mathbb{F}_q^n, d_H)$. Nous y analysons comment ces transformations, représentées par des matrices monomiales, agissent sur les vecteurs tout en préservant la métrique de l'espace, ce qui est important pour l'étude de la structure des codes.

Enfin, le **troisième chapitre** est consacré aux exemples et aux applications. Nous abordons la notion d'**équivalence des codes**, particulièrement pour les codes linéaires, en montrant comment les outils développés précédemment permettent de classifier les codes et de simplifier leur analyse structurelle à travers des exemples concrets.

Chapitre 01

Notions préliminaires

Chapitre 1

Notions préliminaires

Ce premier chapitre est consacré à l'établissement des fondements mathématiques indispensables à la compréhension des développements ultérieurs de ce travail. Dans un premier temps, nous introduisons les structures algébriques de base, notamment la notion de **groupe**, de sous-groupe et de produit direct et semi-direct, qui constituent un outil puissant de l'algèbre abstraite. L'étude se poursuit sur les **corps finis**, outils fondamentaux dans la conception des systèmes de communication numériques.

Par la suite, nous effectuons une transition vers la théorie de l'information en présentant les concepts élémentaires des **codes correcteurs d'erreurs**. Cette partie traite spécifiquement des codes de longueur fixe et définit la métrique essentielle telles que la **distance de Hamming** et le poids de Hamming. Enfin, nous terminons par l'analyse des paramètres fondamentaux d'un code, en mettant l'accent sur la distance minimale, élément déterminant pour évaluer la capacité d'un système à détecter et à corriger les altérations de données lors de leur transmission.

1.1 Groupe

Soit G un ensemble non vide et $*$ une application définie par :

$$* : G \times G \longrightarrow G$$

$$(a, b) \longmapsto a * b$$

Définition 1. *Le couple $(G, *)$ est un groupe si :*

a) La loi $*$ est associative, c'est-à-dire :

$$\forall a, b, c \in G, \quad a * (b * c) = (a * b) * c.$$

b) L'ensemble G possède un élément neutre e pour $*$, c'est-à-dire :

$$\exists e \in G, \ \forall a \in G, \quad a * e = e * a = a.$$

c) Tout élément $a \in G$ admet un symétrique (ou inverse), c'est-à-dire :

$$\forall a \in G, \ \exists b \in G, \quad a * b = b * a = e.$$

On dira de plus que le groupe $(G, *)$ est *commutatif* (ou *abélien*) si la loi de composition $*$ est commutative, c'est-à-dire :

$$\forall x, y \in G, \quad x * y = y * x.$$

Exemple 2. *1.* $\{(\mathbb{R}, +), (\mathbb{C}, +)\}$ *sont des groupes commutatifs pour l'addition.*

2. $(\mathcal{M}_n(\mathbb{R}), +)$ *: l'ensemble des matrices carrées muni de l'addition des matrices est un groupe commutatif.*

3. $(\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ *: sont des groupes commutatifs pour le multiplicatif.*

4. $(GL_n(\mathbb{R}), \cdot)$ *: l'ensemble des matrices carrées inversibles d'ordre $n \times n$.*

5. D_n *: le groupe des symétries d'un polygone régulier à n arêtes.*

$$D_n = \left\{ \langle r, s \rangle \mid r^n = e, \ s^2 = e \right\}$$

1.2 Sous-groupe

Définition 3. *Un sous-ensemble non vide H d'un groupe $(G, *)$ est un sous-groupe de G si et seulement si :*

1. $\forall x, y \in H$, $x * y \in H$;
2. $\forall x \in H$, $x^{-1} \in H$.

Exemple 4. *1. G et $\{e\}$ sont des sous-groupes de G, appelés sous-groupes triviaux de G (e est l'élément neutre de G).*

2. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

3. $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$ est un sous-groupe de $(GL_n(\mathbb{R}), \cdot)$.

Définition 5. *Soit H un sous-groupe de G. Si H est différent de G et de $\{e\}$, on dit que H est un sous-groupe propre de G.*

Notation 6. *Si H est un sous-groupe de G, on note $H \leq G$.*

Exemple 7. *1. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.*

2. $(\mathbb{Q}^*, \times) \leq (\mathbb{R}^*, \times) \leq (\mathbb{C}^*, \times)$.

3. A_n l'ensemble des permutations paires de S_n.

1.3 Sous-groupe normal

Définition 8. *Soit G un groupe et $H \subseteq G$ un sous-groupe. On dit que H est un* ***sous-groupe normal*** *de G si :*

$$\forall g \in G, \quad gHg^{-1} = H.$$

Ceci est équivalent à :

$$\forall g \in G, \ \forall h \in H, \quad ghg^{-1} \in H,$$

ou encore :

$$\forall g \in G, \quad gH = Hg.$$

On note :

$$H \trianglelefteq G.$$

Exemple 9. *1. Considérons le groupe $G = \mathbb{Z}$ (les entiers avec l'addition) et $H = 2\mathbb{Z}$ (les entiers pairs).*

Alors H est un sous-groupe de G, et même un sous-groupe normal, car $\mathbb{Z}$ est abélien. En effet :

$$\forall g, h \in \mathbb{Z}, \quad g + h - g = h \in H.$$

Donc :

$$2\mathbb{Z} \trianglelefteq \mathbb{Z}.$$

2. Exemple non abélien

Dans le groupe S_3, le sous-groupe alterné A_3 est un sous-groupe normal :

$$A_3 \trianglelefteq S_3.$$

1.4 Produit direct de deux groupes

Si G_1 et G_2 sont deux groupes, alors on peut munir le produit cartésien (ensembliste) $G_1 \times G_2$ de structure de groupe, appelé *groupe produit (direct)* de G_1 et G_2 en posant pour loi interne

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2),$$

$x_1, y_1 \in G_1$ et $x_2, y_2 \in G_2$.

Si G_1 et G_2 sont deux groupes finis, alors l'ordre du groupe produit direct $G_1 \times G_2$ est $|G_1|\,|G_2|$, le produit de leurs ordres.

On peut étendre cette notion pour définir le produit direct de s groupes

$$\prod_{i=1}^{s} G_i = G_1 \times G_2 \times \cdots \times G_s.$$

Produit semi-direct de deux sous-groupes

Supposons que H et K soient deux groupes. Si $\rho : K \longrightarrow \mathrm{Aut}(H)$ est un homomorphisme de K dans le groupe des automorphismes de H, alors sur le produit

cartésien $H \times K$, on peut définir un autre groupe $H \rtimes_\rho K$ appelé *produit semi-direct* de H et K déterminé par ρ.

La loi de composition interne est par définition

$$(h_1, k_1)(h_2, k_2) = \Big(h_1\rho(k_1)(h_2),\ k_1k_2\Big).$$
$$(h, k)(h', k') = \Big(h\,\rho(k)(h'),\ kk'\Big).$$

L'ordre de $H \rtimes_\rho K$ lorsque H et K sont finis est $|H|\,|K|$.

Le théorème suivant sert d'utile.

Théorème 10. *Soient H et K deux sous-groupes d'un groupe G, si*

(i) $H \trianglelefteq G$

(ii) $G = HK$

(iii) $H \cap K = \{e\}$

alors $G \cong H \rtimes_\rho K$, avec $\rho(k)(h) = khk^{-1}$ pour tout $k \in K$ et $h \in H$.

Ici l'action de K sur H est par conjugaison.

1.5 Groupe symétrique

Définition 11. *Soit E un ensemble non vide, l'ensemble $S(E)$ des bijections de E sur E, muni de la loi de composition des applications, est dit groupe symétrique de E.*

Si E est fini, de cardinal $n \geq 1$, on note S_n le groupe symétrique de E, les éléments de S_n sont appelés des permutations de E.

Notation : Une permutation σ de S_n est représentée par un systéme (tableau) à deux lignes et n colonnes :

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$$

Composition des permutations : si

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} \quad \text{et} \quad \tau = \begin{pmatrix} 1 & \cdots & n \\ \tau(1) & \cdots & \tau(n) \end{pmatrix}$$

alors

$$\sigma \circ \tau(i) = \sigma(\tau(i))$$

On compose les permutations de droite à gauche.

Exemple 12. *Le groupe symétrique* $S_3 = \{id, (12), (13), (23), (123), (132)\}$

1.6 Corps finis

Dans cette section, nous citons quelques définitions et propriétés élémentaires liées aux corps finis. Elles seront utiles pour les codes correcteurs d'erreurs et les structures algébriques et métriques étudiées ultérieurement (espace vectoriel de dimension finie sur un corps fini, distances, isométrie, ...).

Définition 13. *Un corps fini d'ordre* $q \in \mathbb{N}^*$ *est un corps de cardinal fini égal à* q. *Un tel corps a pour caractéristique un entier premier* p, *c'est-à-dire,*

$$p = \min\{m \in \mathbb{N}^* \mid m \cdot 1 = 0\}.$$

0 et 1 sont, respectivement, les éléments neutres de l'addition et de la multiplication dans le corps. Le corps premier d'un corps fini est donc $\mathbb{Z}/p\mathbb{Z}$.

Le théorème suivant montre qu'un corps fini existe et est unique à isomorphisme près.

Théorème 14. *(a) L'ordre d'un corps fini* K *est* $q = p^m$, *avec* p *la caractéristique et* m *le degré de* K *sur* $\mathbb{Z}/p\mathbb{Z}$.

(b) Pour tout entier premier p *et tout* $m \in \mathbb{N}^*$, *il existe un corps fini d'ordre* $q = p^m$. *Deux corps finis de même ordre* $q = p^m$ *sont isomorphes.*

Exemple 15. *(i) Pour* p *entier premier,* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ *est un corps fini d'ordre* p.

(ii) $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1) = \{0, 1, \omega, 1+\omega\}$ *est le corps fini d'ordre 4. Ici* $\omega = \overline{X}$ *est la classe de* X *modulo* (X^2+X+1)*, l'idéal engendré par le polynôme* $X^2+X+1 \in \mathbb{F}_2[X]$.

1.7 Codes correcteurs d erreurs

1.7.1 Codes de longueur fixe

Soit Q un ensemble non vide de q éléments. En tradition Q est appelé un *alphabet* de q *lettres*. Dans la suite de ce travail Q, sera le corps fini $\mathbb{F}_q$ d'ordre q. Soit n un entier naturel non nul.

Définition 16. *Un code de longueur* n *sur l'alphabet* Q *est une partie non vide* C *de*

$$Q^n = Q \times Q \times \cdots \times Q \quad (n \textit{ fois}).$$

Les éléments du code C *sont appelés les mots de code. Le nombre* $M = |C|$ *des mots de code de* C *est le cardinal ou la taille de* C*. Un* (n, M) *code* C *sur* Q *est un code de longueur* n *et de taille* M *sur l'alphabet* Q*.*

Exemple 17.
- $C = \{011, 100, 000\}$ *est un* $(3, 3)$ *code sur* $\mathbb{F}_2$*.*
- $D = \{abcd, dddb, adda, dcba, cdab\}$ *est un* $(4, 5)$ *code sur* $Q = \{a, b, c, d\}$*.*
- $L = \{001\omega1, 1\omega110, 000\omega1, 1010\omega, 10011, 00100\}$ *est un* $(5, 6)$ *code sur le corps fini* $\mathbb{F}_4$ *défini dans l'exemple 1.2.1 (ii).*

Dans le cas où l'alphabet est un corps fini $\mathbb{F}_q$ d'ordre q et l'ensemble $\mathbb{F}_q^n$ est muni de sa structure naturelle d'espace vectoriel, une classe importante des codes apparaît : les *codes linéaires*.

Un code *linéaire* de longueur n sur $\mathbb{F}_q$ est un sous-espace vectoriel C de $\mathbb{F}_q^n$. Si $\{G_1, G_2, ..., G_k\}$ est une base de C, alors la matrice G d'ordre $k \times n$, dont les lignes sont les vecteurs $G_1, G_2, ..., G_k$, est appelée *matrice génératrice* de C.

Dans ce cas :

$$C = \{mG \mid m \in \mathbb{F}_q^k\}.$$

1.7.2 Distance de Hamming

Une simple notion de distance est définie sur Q^n. Elle est introduite dans le but de compter le nombre des erreurs et de mesurer la différence entre deux mots $x = x_1x_2 \dots x_n$ et $y = y_1y_2 \dots y_n$ de Q^n.

Définition 18. *Pour deux mots $x = x_1x_2 \dots x_n$ et $y = y_1y_2 \dots y_n$ de Q^n, la distance de Hamming de x à y est le nombre $d_H(x, y)$ des positions $i = 1, 2, \dots, n$ telles que $x_i \neq y_i$.*

La distance de Hamming est une *métrique* sur Q^n :

— $d_H(x, y) \geq 0$ et $d_H(x, y) = 0 \iff x = y$,

— $d_H(x, y) = d_H(y, x)$,

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

pour tous x, y, z mots de Q^n.

L'espace métrique (Q^n, d_H) est appelé *espace de Hamming.*

Exemple 19. — $d_H(011, 100) = 3$ *sur* $\mathbb{F}_3$.

— $d_H(dddb, adda) = 2$ *sur* $Q_4 = \{a, b, c, d\}$.

— $d_H(01\omega10, 1\omega110) = 3$ *sur* $\mathbb{F}_5$.

1.7.3 Poids de Hamming

Dans le cas où $Q = \mathbb{F}_q$ le corps fini d'ordre q, on peut définir le *poids de Hamming* d'un mot de l'espace vectoriel $\mathbb{F}_q^n$.

Définition 20. *Le poids de Hamming d'un mot $x = x_1x_2 \dots x_n$ de $\mathbb{F}_q^n$ est l'entier naturel :*

$$w_H(x) = |\{i = 1, 2, \dots, n \mid x_i \neq 0\}|.$$

Autrement dit,

$$w_H(x) = d_H(x, 0),$$

où 0 désigne le vecteur nul $00 \dots 0 \in \mathbb{F}_q^n$.

1.7.4 Distance minimale et paramètres d'un code

L'efficacité d'un code se mesure par le nombre d'erreurs que le code peut détecter et corriger. Ce nombre est obtenu par la *distance minimale* du code : le minimum des distances entre deux mots de code distincts.

Définition 21 (Distance minimale)**.** *Soit C un code de longueur n sur Q. La distance minimale de C est le nombre naturel*

$$d_H(C) = \min\{d_H(x, y) \mid x, y \in C,\ x \neq y\}.$$

Un (n, M, d)-code sur Q est un code de longueur n, de cardinal M, et de distance minimale $d_H(C) = d$ sur l'alphabet Q. Les nombres n, M et d sont les paramètres du code.

Dans le cas où le code est linéaire de dimension k sur le corps fini $\mathbb{F}_q$, on dit que c'est un $[n, k, d]$-code linéaire sur $\mathbb{F}_q$, et n, k, et d sont ses paramètres.

Exemple 22. *L'ensemble $\{000, 110, 011, 101\}$ est un $(3, 4, 2)$-code sur $\mathbb{F}_2$.*

Polynôme énumérateur des poids

Pour étudier le problème d'équivalence de deux codes, Nicolas Sendrier dans a défini la notion de *signature*. Le polynôme énumérateur des poids d'un code C sert à définir une signature associée au code C. Il permet aussi d'étudier les propriétés concernant les poids des mots de code.

Définition 23 (Distribution des poids)**.** *Soit C un (n, M, d)-code sur Q. La* distribution des poids *de C est la suite des entiers naturels*

$$\{A_0, A_1, \ldots, A_n\}$$

où A_i est le nombre de mots de code de poids i.

On voit clairement que

$$0 \leq A_i \quad et \quad d = \min\{i = 1, 2, \ldots, n \mid A_i \neq 0\}.$$

Définition 24 (Polynôme énumérateur des poids)**.** *Soit C un (n, M, d)-code sur Q. Le polynôme énumérateur des poids du code C est le polynôme $W_C(X) \in \mathbb{Z}[X]$ défini par :*

$$W_C(X) = \sum_{i=0}^{n} A_i X^i.$$

Exemple 25. *Soit $C = \{000, 110, 011, 101\}$ le code de paramètres $(3, 4, 2)$ sur $\mathbb{F}_2$. La suite de distribution des poids de C est*

$$\{1, 0, 3, 0\},$$

d'où le polynôme énumérateur des poids du code C est

$$W_C(X) = 1 + 3X^2.$$

Chapitre 02

Transformations monomiales

Chapitre 2

Transformations monomiales

Ce deuxième chapitre s'articule autour de l'étude approfondie des **transformations monomiales** et de leur rôle central dans l'analyse de la structure des codes. L'objectif principal est d'explorer les transformations qui préservent les propriétés métriques du code, en particulier la distance de Hamming. Nous commençons par définir les **isométries** de l'espace vectoriel $(\mathbb{F}_q^n, d_H)$, en mettant en évidence les applications qui conservent les distances entre les mots du code.

Par la suite, nous distinguons les isométries linéaires et introduisons formellement les transformations monomiales de $\mathbb{F}_q^n$ comme étant une extension naturelle des permutations. Le chapitre traite également de la représentation matricielle de ces transformations à travers l'étude de la **matrice monomiale**, qui combine à la fois une matrice de permutation et une matrice diagonale inversible. Cette caractérisation algébrique est cruciale pour comprendre l'équivalence entre les codes et pour identifier les symétries internes qui facilitent les processus de décodage et d'analyse structurelle.

2.1 Isométries de $(\mathbb{F}_q^n, d_H)$

Les isométries de l'espace $(\mathbb{F}_q^n, d_H)$ permettent de définir une classication des codes correcteurs d'erreurs, comme elles appliquent un code linéaire d'erreurs sur

un autre et conservent la longueur, la dimension, la distance minimale et autres paramètres. Par suite il est naturel d appeler codes équivalents deux codes isométriques (l'un est l'image de l'autre par une isométrie)

Définition 26. *Une isométrie (ou symétrie) de l'espace métrique* $(\mathbb{F}_q^n, d_H)$ *est une application bijective* $\varphi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ *qui conserve les distances,*

c'est-à-dire,

$$d_H(\varphi(u), \varphi(v)) = d_H(u, v)$$

pour tout $u, v \in \mathbb{F}_q^n$.

2.2 Isométries lineaires

Compte tenu de la structure vectorielle de $\mathbb{F}_q^n$, on peut ajouter la condition de linéarité des isométries afin de s'adapter avec la structure.

Définition 27. *Une transformation monomiales(ou isométrie qui est linéaire) de l'espace* $(\mathbb{F}_q^n, d_H)$ *est isométrie qui est linéaire pour la structure d'espace vectoriel de* $\mathbb{F}_q^n$.

Dans le cas de transformation monomiale, on peut alléger la définition.

Proposition 28. *Une transformation monomiale de l'espace* $(\mathbb{F}_q^n, d_H)$ *est une application linéaire injective* φ *qui conserve le* H*-poids de Hamming.*

$$w_H(\varphi(u)) = w_H(u), \text{ pour tout } u \in \mathbb{F}_q^n.$$

Démonstration. φ est linéaire injective entre deux espaces vectoriels de même dimension, donc surjective, par suite φ est bijective. L'image du vecteur nul $\mathbf{0}$, de poids $w_H(\mathbf{0}) = 0$, par φ est lui-même. Pour $u, v \in \mathbb{F}_q^n$ on a

$$\begin{aligned} d_H(\varphi(u),\varphi(v)) &= d_H(\varphi(u)-\varphi(v),\mathbf{0}) && (3.2.1)\\ &= w_H(\varphi(u)-\varphi(v)) && (3.2.1)\\ &= w_H(\varphi(u-v)) && (\varphi \text{ linéaire})\\ &= w_H(u-v) && (\varphi \text{ isométrie})\\ &= d_H(u-v,\mathbf{0}) && (3.2.1)\\ &= d_H(u,v) && (3.2.1) \end{aligned}$$

□

Définition 29. *Deux $[n,k]_q$-codes monomiales $\mathcal{C}$ et $\mathcal{D}$ sur $\mathbb{F}_q$ sont équivalents s'il existe une isométrie φ de $(\mathbb{F}_q^n, d_H)$ telle que $\varphi(\mathcal{C}) = \mathcal{D}$.*

Définition 30. *Deux $[n,k]_q$-codes monomiale $\mathcal{C}$ et $\mathcal{D}$ sur $\mathbb{F}_q$ sont linéairement équivalents s'il existe une isométrie monomiale φ de $(\mathbb{F}_q^n, d_H)$ telle que $\varphi(\mathcal{C}) = \mathcal{D}$.*

Remarque 31. *Si $\mathcal{C}$ et $\mathcal{D}$ sont équivalents, on dit aussi qu'ils sont isométriques ou symétriques et on écrit*

$$\mathcal{C} \sim \mathcal{D}.$$

Notation 32. *Notons par $Aut(\mathbb{F}_q^n, d_H)$ l'ensemble de toutes les transformations monomiales de l'espace $(\mathbb{F}_q^n, d_H)$.*

L'ensemble $Aut(\mathbb{F}_q^n, d_H)$ possède une structure algébrique remarquable :

Proposition 33. *L'ensemble $Aut(\mathbb{F}_q^n, d_H)$ est un groupe pour la loi de composition des applications $\circ$.*

Démonstration.

— L'application identité de $\mathbb{F}_q^n$ est une transformation monomiales, donc $Aut(\mathbb{F}_q^n, d_H) \neq \varnothing$,

— La composée de deux transformations est une transformation monomiales : Si φ et $\psi \in Aut(\mathbb{F}_q^n, d_H)$, alors pour $u, v \in \mathbb{F}_q^n$

$$\begin{aligned} d_H(\varphi \circ \psi(u), \varphi \circ \psi(v)) &= d_H(\varphi(\psi(u)), \varphi(\psi(v))) \\ &= d_H(\psi(u), \psi(v)) \\ &= d_H(u, v) \end{aligned}$$

□

Et comme la composée de deux bijections est une bijection, il résulte que $\varphi \circ \psi$ est dans $Aut(\mathbb{F}_q^n, d_H)$,

— La composition des applications est associative.

— Si $\varphi \in Aut(\mathbb{F}_q^n, d_H)$, comme $\varphi(u) = s \Leftrightarrow u = \varphi^{-1}(s)$ et $\varphi(v) = t \Leftrightarrow v = \varphi^{-1}(t)$, on trouve

$$\begin{aligned} d_H(\varphi^{-1}(s), \varphi^{-1}(t)) &= d_H(u, v) && \text{définition de } \varphi^{-1} \\ &= d_H(\varphi(u), \varphi(v)) && \varphi \text{ monomiale} \\ &= d_H(s, t) && \text{définition de } \varphi^{-1} \end{aligned}$$

φ^{-1} est évidemment bijective, donc $\varphi^{-1} \in Aut(\mathbb{F}_q^n, d_H)$.

En résumé, $(Aut(\mathbb{F}_q^n, d_H), \circ)$ est un groupe. ■

2.3 Transformations monomiales de $\mathbb{F}_q^n$

Rappelons que d_H désigne la **distance de Hamming** définie sur $\mathbb{F}_q^n$: Pour $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ de $\mathbb{F}_q^n$;

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

Soit $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ une isométrie. Le but de cette section est l'étude des propriétés algébriques de ces isométries.

Proposition 34. *Toute isométrie de $\mathbb{F}_q^n$ est une bijection de $\mathbb{F}_q^n$ sur $\mathbb{F}_q^n$.*

Démonstration. Comme $\mathbb{F}_q^n$ est un ensemble fini, pour montrer que φ est bijective il suffit de montrer que φ est injective.

Soient x, y deux éléments de $\mathbb{F}_q^n$ tels que $\varphi(x) = \varphi(y)$.

d_H est une distance :

$$\varphi(x) = \varphi(y) \implies d_H(\varphi(x), \varphi(y)) = 0$$

φ est une isométrie :

$$d_H(\varphi(x), \varphi(y)) = d_H(x, y)$$

Donc :

$$d_H(x, y) = 0$$

Enfin :

$$x = y$$

□

Rappelons

Notons $Iso(\mathbb{F}_q^n)$ l'ensemble de toutes les isométries de $\mathbb{F}_q^n$ pour la distance de Hamming.

Proposition 35. *L'ensemble $Iso(\mathbb{F}_q^n)$ est un groupe pour la composition des applications.*

Démonstration. 1. $Iso(\mathbb{F}_q^n)$ est stable par la composition : la composition de deux isométries est une isométrie.

Une transformation monomiale est une isométrie linéaire de $\mathbb{F}_q^n$.

Désignons par $Aut(\mathbb{F}_q^n)$ l'ensemble de toutes les transformations monomiale de $\mathbb{F}_q^n$:

$$Aut(\mathbb{F}_q^n) = \{\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n \mid \varphi \text{ transformation monomiale}\}$$

□

Proposition 36. *$(Aut(\mathbb{F}_q^n), \circ)$ est un sous-groupe de $(Iso(\mathbb{F}_q^n), \circ)$.*

L'ensemble des transformations monomiales est un sous-groupe de $Iso(\mathbb{F}_q^n)$.

Démonstration. En utilisant la propriété caractéristique de sous-groupe : si φ et ψ sont deux éléments de $Aut(\mathbb{F}_q^n)$, alors $\varphi \circ \psi^{-1}$ est une isométrie linéaire comme composée de deux isométries linéaires.

$$\text{Donc } \varphi \circ \psi^{-1} \in Aut(\mathbb{F}_q^n)$$

D'où $Aut(\mathbb{F}_q^n)$ est un sous-groupe de $Iso(\mathbb{F}_q^n)$. □

2.4 Matrice monomiale

Soit $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ une transformation monomiale.

$\mathbb{F}_q^n$ étant muni d'une base, la transformation monomiale φ est associée à une matrice $M(\varphi)$ de n lignes et n colonnes sur $\mathbb{F}_q$.

Définition 37. *La matrice associée $M(\varphi)$ de φ est appelée une matrice monomiale sur $\mathbb{F}_q$.*

Cela veut dire que chaque transformation monomiale est représentée par une matrice monomiale $M(f)$ de type $n \times n$ sur $\mathbb{F}_q$.

Cas particulier (matrice de permutation)

Soit $\sigma \in S_n$ une permutation du groupe symétrique de degré n, c'est-à-dire une bijection :

$$\sigma : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$$

$$i \longmapsto \sigma(i)$$

On peut définir σ comme une isométrie linéaire de $\mathbb{F}_q^n$ par :

$$\sigma : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$$

$$(x_1, \ldots, x_n) \longmapsto (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

C'est-à-dire $\sigma \in Aut(\mathbb{F}_q^n)$.

Pour une permutation $\sigma \in S_n$ et un mot $x = (x_1, x_2, \ldots, x_n)$ de $\mathbb{F}_q^n$, on définit le mot $\sigma(x)$ de $\mathbb{F}_q^n$ par :

$$\sigma(x) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

C'est le mot obtenu en permutant les coordonnées du mot x suivant la permutation σ.

Comme première remarque ces deux mots ont le même poids de Hamming :

$$w_H(x) = w_H(\sigma(x)).$$

Définition 38. *La matrice monomiale associée à $\tilde{\sigma}$ est appelée* ***matrice de permutation*** *(associée à σ).*

Remarque 39. *Une matrice monomiale (ou matrice de permutation généralisée) est une matrice carrée qui possède exactement un seul coefficient non nul par ligne et par colonne. Elle généralise les matrices de permutation : les « 1 » sont remplacés par des valeurs non nulles arbitraires. Tout matrice de permutation est une matrice monomiales.*

Caractéristiques principales :

1. ***Structure :*** *Une seule entrée non nulle par ligne et par colonne.*
2. ***Inversibilité :*** *Une matrice monomiale est inversible si et seulement si tous ses éléments non nuls le sont.*
3. ***Produit :*** *Le produit de deux matrices monomiales est également une matrice monomiale.*

Caractéristiques principales

Posons

— D_n : l'ensemble des matrices diagonales inversibles.

— P_n : l'ensemble des matrices de permutations.

Proposition 40. *Les ensembles D_n et P_n sont des sous groupes de $Aut(\mathbb{F}_q^n)$.*

Démonstration. Toute matrice de D_n (respectivement de P_n) est une matrice monomiale associée à une transformation monomiale, elles conservent le poids. Ce qui donne de fait que D_n et P_n sont des sous-groupes de $Aut(\mathbb{F}_q^n)$. Ce qui donne le fait que D_n et P_n sont des sous groupes de $Aut(\mathbb{F}_q^n)$.

Soit $(G, \star)$ un groupe et soirnt H et K deux sous-groupes de G.

On définit la partie $H \star K$ par :

$$Hk = \{\, h \star k \mid h \in H \text{ et } k \in k \,\}.$$

□

Exemple 41.

1)

Soit $G = (\mathbb{Z}, +)$, $H = 2\mathbb{Z}$ et $K = 3\mathbb{Z}$.

Alors

$$H + K = \{\, h + k \mid h \in 2\mathbb{Z},\ k \in 3\mathbb{Z} \,\}$$

$$= \{\, 2x + 3y \mid x, y \in \mathbb{Z} \,\}.$$

2)

Soit $G = S_4$.

On considère les permutations suivantes :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12),$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = (234).$$

On définit alors les sous-groupes :

$$H_2 = \langle \sigma \rangle = \{\mathrm{id}, \sigma\},$$

$$K_2 = \langle \tau \rangle = \{\mathrm{id}, \tau, \tau^2\}.$$

$$H \circ K = \{\alpha \circ \beta \mid \alpha \in H,\ \beta \in K\}$$

$$= \{\mathrm{id}, \tau, \tau^2, \sigma, \sigma\tau, \sigma\tau^2\}.$$

On a :

$$\sigma = (12), \qquad \tau = (234).$$

$$\tau^2 = (234) \circ (234) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (243).$$

$$\sigma\tau = (12)(234) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234).$$

$$\sigma\tau^2 = (12)(243) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1243).$$

Ainsi,

$$H \circ K = \{\mathrm{id},\ (12),\ (234),\ (243),\ (1234),\ (1243)\}.$$

Définition 42. *Soient H et K deux sous-groupes d'un groupe $(G, \star)$.*

On dit que G est le produit de H et K (ou que H et K engendrent G) si

$$G = HK.$$

Exemple 43.

1)

Soit $G = (\mathbb{Z}, +)$, $H = 2\mathbb{Z}$ et $K = 3\mathbb{Z}$.

$$H + K = 2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}.$$

Donc $\mathbb{Z}$ est la somme de H et K.

2)

Soit $G = S_4$, $H = \langle\sigma\rangle$ et $K = \langle\tau\rangle$ avec

$$\sigma = (12), \qquad \tau = (234).$$

On sait que

$$|G| = 4! = 24, \qquad |H \circ K| = 6.$$

Donc

$$G \neq H \circ K.$$

Ainsi, G n'est pas le produit de H et K (ils n'engendrent pas G par le produit).

Définition 44. *Soient H et K deux sous-groupes d'un groupe $(G, *)$.*

On dit que G est le produit de H et K (ou que H et K engendrent G) si :

$$G = H * K.$$

Exemple 45.

1. $G = (\mathbb{Z}, +), \quad H = 2\mathbb{Z}, \quad K = 3\mathbb{Z}.$

   On a :

   $$H + K = 2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}.$$

   Donc $\mathbb{Z}$ est la somme de H et K.

2. $G = (S_4, \cdot)$, $\quad H = \langle \sigma \rangle$, $\quad K = \langle \tau \rangle$,

   avec :

   $$\sigma = (12), \qquad \tau = (234).$$

   On a :

   $$|G| = 4! = 24, \qquad |H \circ K| = 6.$$

   Donc :

   $$G \neq H \circ K.$$

   Ainsi, G n'est pas le produit de H et K (ils n'engendrent pas G).

Remarque 46. *Si $G = HK$, alors tout élément $g \in G$ s'écrit sous la forme*

$$g = hk, \qquad h \in H,\ k \in K,$$

(l'écriture n'est pas unique).

Proposition 47. *Le groupe* $\mathrm{Aut}(\mathbb{F}_q^n)$ *est engendré par D_n et O_n, c'est-à-dire :*

$$\mathrm{Aut}(\mathbb{F}_q^n) = D_n\, O_n.$$

Démonstration. Pour tout $\varphi \in \mathrm{Aut}(\mathbb{F}_q^n)$, on a

$$\varphi(0) = 0,$$

où 0 est le vecteur nul de $\mathbb{F}_q^n$.

Soit $\{e_1, e_2, \ldots, e_n\}$ la base canonique de $\mathbb{F}_q^n$, c'est-à-dire :

$$e_1 = (1, 0, \ldots, 0), \quad e_2 = (0, 1, \ldots, 0), \quad \ldots \quad e_n = (0, 0, \ldots, 1).$$

On a, pour tout $i = 1, \ldots, n$:

$$w_H(e_i) = 1.$$

Comme φ est une isométrie linéaire, alors

$$w_H(e_i) = w_H\Big(\varphi(e_i)\Big).$$

Donc

$$w_H\Big(\varphi(e_i)\Big) = 1, \qquad i = 1, \ldots, n.$$

D'autre part, pour $i \neq j$ dans $\{1, \ldots, n\}$, on a

$$d_H(e_i, e_j) = 2.$$

Puisque φ est une isométrie linéaire,

$$d_H(e_i, e_j) = d_H\Big(\varphi(e_i), \varphi(e_j)\Big).$$

Donc

$$d_H\Big(\varphi(e_i), \varphi(e_j)\Big) = 2.$$

Comme $w_H\Big(\varphi(e_i)\Big) = 1$, alors $\varphi(e_i)$ possède une seule coordonnée non nulle. Il existe donc une position $j = \sigma(i)$ telle que

$$\varphi(e_i) = (0, \ldots, 0, \lambda_i, 0, \ldots, 0),$$

avec $\lambda_i \in \mathbb{F}_q^*$.

Ainsi,

$$\varphi(e_i) = \lambda_i \, e_{\sigma(i)}, \qquad \sigma \in S_n.$$

Donc, pour tout $i = 1, 2, \ldots, n$:

$$\varphi(e_i) = \lambda_i \, e_{\sigma(i)}$$

avec $\lambda_i \in \mathbb{K}^*$ et $\sigma \in S_n$.

Les $\{\sigma(i)\}_{i \in \{1,2,\ldots,n\}}$ sont distincts, car σ est une permutation.

Donc la matrice monomiale M de φ dans la base canonique $\{e_1, e_2, \ldots, e_n\}$ est :

$$M = (\varphi(e_1) \ \varphi(e_2) \ \cdots \ \varphi(e_n))$$

$$M = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}$$

Toute matrice monomiale M est le produit d'une matrice diagonale inversible D et d'une matrice de permutation σ.

$$M = D \cdot \sigma$$

où

$$D = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

et σ est une matrice de permutation.

Par suite :

$$\mathrm{Aut}(\mathbb{F}_q^n) = D_n \cdot P_n$$

□

Proposition 48. *On a :*

— $D_n \cap P_n = \{I_n\}$

— $D_n \trianglelefteq \mathrm{Aut}(\mathbb{F}_q^n)$ *(sous-groupe normal)*

Démonstration. Soit $M \in D_n \cap P_n$.

Comme $M \in D_n$, alors

$$M = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

et comme $M \in P_n$, ses coefficients sont 0 ou 1 avec exactement un 1 par ligne et par colonne.

Donc nécessairement :

$$M = I_n$$

Soit $\lambda_i \in \mathbb{F}_q^\times$.

Comme $M \in D_n$, on a :

$$\lambda_1 = \lambda_2 = \cdots = \lambda_n = 1$$

Donc :

$$M = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = I_n$$

Ainsi :

$$D_n \cap P_n = \{I_n\}$$

2) D_n est un sous-groupe normal de $\mathrm{Aut}(\mathbb{F}_q^n)$ si :

$$\forall \varphi \in \mathrm{Aut}(\mathbb{F}_q^n), \quad \varphi D_n \varphi^{-1} \subset D_n$$

c'est-à-dire :

$$\forall \varphi \in \mathrm{Aut}(\mathbb{F}_q^n),\ \forall d \in D_n, \quad \varphi d \varphi^{-1} \in D_n$$

On prend φ une matrice monomiale. □

Exemple 49. *pour* $n = 2$

$$\begin{pmatrix} 0 & \lambda_2 \\ \lambda_1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \begin{pmatrix} 0 & \lambda_1^{-1} \\ \lambda_2^{-1} & 0 \end{pmatrix} = \begin{pmatrix} \lambda_2 \alpha_2 \lambda_2^{-1} & 0 \\ 0 & \lambda_1 \alpha_1 \lambda_1^{-1} \end{pmatrix}$$

Par récurrence sur n*, la relation :*

$$\varphi d \varphi^{-1} \in D_n$$

est vraie pour tout $\varphi \in \mathrm{Aut}(\mathbb{F}_q^n)$ *et tout* $d \in D_n$.

En résumé, nous avons le théorème suivant :

Théorème 50. *Le groupe* $\mathrm{Aut}(\mathbb{F}_q^n)$ *des transformations monomiales de* $\mathbb{F}_q^n$ *est le produit semi-direct de* D_n *et* P_n.

C'est-à-dire :

$$\mathrm{Aut}(\mathbb{F}_q^n) = D_n \rtimes P_n$$

Chapitre 03

Exempeles et applications

Chapitre 3

Exemples et applications

3.1 Equivalence des codes

3.1.1 Equivalence des codes lineaires

L'information, représentée sous forme de vecteur de F_q^n, est transmise à travers un canal susceptible d'être bruité, c'est-à-dire que l'information reçue peut différer de celle envoyée. La théorie des codes correcteurs d'erreurs a été développée afin de détecter et corriger ces erreurs.

Ces dernières peuvent être mesurées en introduisant la notion de distance sur l'espace F_q^n, ce qui conduit naturellement à s'interroger sur la ressemblance entre certaines parties (codes) de cet espace, possédant les mêmes propriétés métriques. Cette ressemblance correspond à la notion d'isométrie de F_q^n.

L'ensemble des isométries de F_q^n possède une structure algébrique remarquable, permettant de définir de manière mathématique rigoureuse l'équivalence des codes de longueur n sur le corps fini F_q par transformation monomiale.

L'équivalence des codes constitue l'un des problèmes importants de la théorie des codes correcteurs d'erreurs : étant donnés deux codes ayant les mêmes paramètres, comment déterminer s'ils sont équivalents ou non, et comment identifier la relation (transformation monomiale, isométrie, ...) qui définit cette équivalence.

Définition 51. *Soient C et D deux codes de longueur n sur $\mathbb{F}_q$. On dit que D est* ***équivalent à*** *C s'il existe une transformation monomiales $\varphi \in Iso(\mathbb{F}_q^n)$ telle que*

$$D = \varphi(C).$$

Cette relation définit une relation d'équivalence sur l'ensemble des codes de longueur n sur $\mathbb{F}_q$, d'où la terminologie codes équivalents *.*
D'une autre meniere

$$\mathcal{C} \sim \mathcal{D} \Leftrightarrow \exists \varphi \in Iso(\mathbb{F}_q^n) : \mathcal{D} = \varphi(\mathcal{C})$$

1. *La relation $\sim$ est reflexive :*
   $\mathcal{C} \sim \mathcal{C} \Leftrightarrow \varphi = id_{\mathbb{F}_q^n} \in Iso(\mathbb{F}_q^n)$.
2. *La relation $\sim$ est symetrique :*
   $\mathcal{C} \sim \mathcal{D} \Leftrightarrow \varphi(\mathcal{C}) = \mathcal{D}$
   $\mathcal{C} = \varphi^{-1}(\mathcal{D}), \varphi^{-1} \in Iso(\mathbb{F}_q^n) \Leftrightarrow \mathcal{D} \sim \mathcal{C}$.
3. *La relation $\sim$ est transitive :*
   $\mathcal{C} \sim \mathcal{D} \Leftrightarrow \varphi(\mathcal{C}) = \mathcal{D}$
   $\mathcal{D} \sim \mathcal{M} \Leftrightarrow \psi(\mathcal{D}) = \mathcal{M}$
   $\mathcal{M} = \psi(\varphi(\mathcal{C})) = \psi \circ \varphi(\mathcal{C})$
   $\varphi \circ \psi \in Iso(\mathbb{F}_q^n)$. *Donc* $\mathcal{C} \sim \mathcal{M}$

Il peut arriver que, pour un code C et une transformation monomiales $\varphi \in Iso(\mathbb{F}_q^n)$, on ait

$$\varphi(C) = C.$$

Cela signifie que le code C est globalement invariant sous l'action de φ.

L'ensemble des transformation monomiales laissant C invariant possède une structure algébrique importante. On le note

$$\mathrm{Aut}(C) = \{\, \varphi \in Iso(\mathbb{F}_q^n) \mid \varphi(C) = C \,\}.$$

Proposition 52. *Soient C et D deux codes de longueur n sur le corps fini $\mathbb{F}_q$. Si C et D sont équivalents et si C est un code linéaire de dimension k, alors D est aussi un code linéaire de dimension k.*

Démonstration. Supposons que C soit un code linéaire de dimension k et que D lui soit équivalent $\varphi \in Iso(\mathbb{F}_q^n)$, telle que

$$D = \varphi(C).$$

Soient $\varphi(x), \varphi(y) \in D$ avec $x, y \in C$ et $\lambda \in \mathbb{F}_q$.

On a

$$\varphi(x) - \varphi(y) = (x_{\varphi(1)}, x_{\varphi(2)}, \ldots, x_{\varphi(n)}) - (y_{\varphi(1)}, y_{\varphi(2)}, \ldots, y_{\varphi(n)}),$$

$$= (x_{\varphi(1)} - y_{\varphi(1)}, x_{\varphi(2)} - y_{\varphi(2)}, \ldots, x_{\varphi(n)} - y_{\varphi(n)}),$$

$$= \Big((x-y)_{\varphi(1)}, (x-y)_{\varphi(2)}, \ldots, (x-y)_{\varphi(n)}\Big) = \varphi(x-y).$$

Comme C est linéaire, on a $x - y \in C$, donc

$$\varphi(x) - \varphi(y) \in \varphi(C) = D.$$

D'autre part,

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

$\varphi(x) = (\lambda_1 x_{\varphi(1)}, \lambda_2 x_{\varphi(2)}, ...\lambda_n x_{\varphi(n)})$

$$\varphi(\lambda x) = \varphi(\lambda x_1, \lambda x_2, ...\lambda x_n) = \Big(\lambda_1(\lambda x)_1, \lambda_2(\lambda x)_2, ...\lambda_n(\lambda x)_n\Big),$$

$$= \Big(\lambda x_{\varphi(1)}, \lambda x_{\varphi(2)}, \ldots, \lambda x_{\varphi(n)}\Big) = \lambda\, \varphi(x),$$

ce qui montre que $\lambda\varphi(x) \in D$.

Ainsi, D est un sous-espace vectoriel de $\mathbb{F}_q^n$. De plus, si $\{v_1, v_2, \ldots, v_k\}$ est une base de C, alors

$$\{\varphi(v_1), \varphi(v_2), \ldots, \varphi(v_k)\}$$

forme une base de D.

Autrement dit, une matrice génératrice de D s'obtient en transformation monomiales, selon φ, les colonnes d'une matrice génératrice de C. □

Ce résultat montre que deux codes équivalents possèdent les mêmes propriétés en termes de détection et de correction des erreurs. Ils ont notamment la même

longueur n, le même cardinal M (ou la même dimension k dans le cas linéaire) ainsi que la même distance minimale d. La distribution des poids et le des poids restent également inchangés.

Proposition 53. *Si deux codes de longueur n sont équivalents pa, alors ils ont les mêmes transformation monomiales, la même distribution des poids ainsi que le même polynôme énumérateur des poids.*

Remarque 54. ***1.*** *Les deux résultats précédents peuvent être utilisés sous leur forme contraposée : si deux codes diffèrent par au moins un de leurs paramètres, ou par leur distribution des poids, ou encore par leur polynôme énumérateur des poids, alors ils ne sont pas équivalents par permutation. Par exemple, les codes binaires*

$$C = \{000, 100, 010, 110\}, \quad D = \{101, 011, 110\}$$

ne sont pas équivalents par permutation. En effet, C est linéaire alors que D ne l'est pas, et la distance minimale de C est 1, tandis que celle de D est 2.

2. *En revanche, la réciproque est fausse en général. Deux codes peuvent avoir les mêmes paramètres, ainsi que la même distribution des poids (et donc le même polynôme énumérateur), sans être équivalents par permutation. Considérons les deux codes ternaires*

$$A = \{00, 10, 11\}, \quad B = \{00, 02, 22\} \subset \mathbb{F}_3^2.$$

Ils possèdent les mêmes paramètres ($n = 2, M = 3, d = 1$), ainsi que le même polynôme énumérateur des poids

$$1 + X + X^2,$$

mais ils ne sont pas équivalents par permutation.

Matrice monomiales

Soient G_1 une matrice génératrices du codes de C.

Soient G_2 une matrice génératrices du codes de D.

$$\mathcal{C} \sim \mathcal{D} \Leftrightarrow \exists \varphi \in Iso(\mathbb{F}_q^n) : \mathcal{D} = \varphi(\mathcal{C})$$

$$\mathcal{C} \sim \mathcal{D} \Leftrightarrow \exists \mathcal{M} monomiale : G_1\mathcal{M} = G_2$$

.

Exemple 55. *Considérons les deux matrices génératrices G_1 et G_2 sur $\mathbb{F}_2$:*

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

En permutant les lignes de G_2 (ce qui revient à mettre G_2 sous forme systématique), on obtient G_1. Ainsi, les deux matrices engendrent le même code.

Exemple 56. *On donne les deux matrices génératrices G_1 et G_2 sur le corps $\mathbb{F}_3$*

$$G_1 = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{pmatrix},$$

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Il existe donc une matrice monomiale M telle que :

$$G_1 M = G_2,$$

Ce qui implique,

$$C_2 = C_1 M.$$

Conclusion

Le sujet de ce travail s'inscrit dans le domaine de la théorie des groupes et de ses applications à l'étude des codes, en particulier dans l'espace de Hamming et la notion d'isométrie.

Dans le but d'étudier l'équivalence des codes, nous avons commencé par présenter les définitions fondamentales ainsi que les propriétés qui en découlent. Nous avons ensuite appliqué des outils issus de la théorie des groupes afin de mieux comprendre l'équivalence isométrique et d'exploiter ses propriétés.

Par la suite, nous nous sommes concentrés sur les transformations monomiales, qui représentent des isométries linéaires de l'espace de Hamming. Nous avons montré que ces transformations forment un groupe pouvant s'exprimer comme un produit semi-direct de deux groupes.

En conclusion, la théorie des groupes constitue un outil mathématique très puissant, permettant de résoudre de nombreux problèmes et de mieux comprendre les structures algébriques, notamment dans le domaine des codes et de l'espace de Hamming.

Bibliographie

[1] A. Jeanneret et D. Lines, *Théorie des groupes, des anneaux, des corps et des modules*, Cépaduès-Éditions, Toulouse, France.

[2] L. Ladjelat, *Méthodes de la théorie des groupes pour les codes algébriques*, Thèse de doctorat en sciences, Université Mohamed Boudiaf de M'sila, 2025.

[3] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, A. Wassermann, *Error-Correcting Linear Codes : Classi cation by Isometry and Applications*, Springer-Verlag Berlin Heidelberg, 2006.

[4] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[5] G. Lachaud et S. Vladut, *Les codes correcteurs d erreurs*, La recherche 278, volume 26, juillet-août 1995.

[6] L. Ladjelat, *Étude de L équivalence de deux codes sur un corps*, mémoire de magister, université Mohamed Boudiaf de M sila, 2004.

[7] L. Ladjelat, *On the Action of the Symmetric Group on Error-Correcting Codes*, Applied Sciences, vol. 18, pp. 60-65, 2016.

[8] F. J. Macwilliams et N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland Mathematical Library, North-Holland, Amsterdam, 1977.

[9] P. S. Modenov et A. S. Parkhomenko, *Geometric Transformations, Volume 1, Euclidean and Affine Transformations*, Academic Press Inc., 1965.

[10] N. Sendrier, *Cryptosystèmes à clé publique basés sur les codes correcteurs d erreurs*, INRIA Rocquencourt, Mémoire d habilitation à diriger des recherches, mars 2002.

ملخص

في هذا العمل، نناقش مفهوم التحويلات المونومية (أحادية الحد) لفضاء هامينج $(\mathbb{F}_q^n, d_H)$، بالإضافة إلى خصائصها وبنية مجموعة هذه التحويلات باعتبارها زمرة تحت قانون تركيب التطبيقات. نبين أن هذه الزمرة هي عبارة عن جداء نصف مباشر لزمرتين. وأخيراً، نعرض بعض التطبيقات في مجال رموز تصحيح الأخطاء.

كلمات مفتاحية

الجداء النصف مباشر، الرموز المتكافئة، المتساوي القياس، رموز تصحيح الأخطاء.

Abstract

In this work, we study the concept of monomial transformations of the Hamming space $(\mathbb{F}_q^n, d_H)$, as well as their properties and the structure of the set of these transformations, considered as a group under function composition. We demonstrate that this group is a semi-direct product of two groups. Finally, we present some applications to error-correcting codes.

Key words

semi-direct product, equivalent codes, isometry, error-correcting codes.

Résumé

Dans ce travail, nous étudions le concept des transformations monomiales de l'espace de Hamming $(\mathbb{F}_q^n, d_H)$, ainsi que leurs propriétés et la structure de l'ensemble de ces transformations considéré comme un groupe pour la composition des applications. Nous montrons que ce groupe est le produit semi-direct de deux groupes. Enfin, nous présentons quelques applications aux codes correcteurs.

Mot-clés

produit semi-direct, codes équivalents, isométrie, codes correcteurs.