RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
Université Mohamed Boudiaf de M'sila
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

N^o d'ordre :.....

Thèse

Présentée pour l'obtention du diplôme de Doctorat Sciences

Filière : Mathématiques

Option : Algèbre

Par :

LADJELAT Lahcene

Thème

Méthodes de la Théorie des Groupes pour les Codes Algébriques

Soutenue le 13/11/2025 devant le jury composé de :

AMROUNE Abdelaziz	Professeur	Université de M'sila	Président
MIHOUBI Douadi	Professeur	Université de M'sila	Rapporteur
BENSALEM Naceurdine	Professeur	Université de Sétif	Examinateur
TRABELSI Nadir	Professeur	Université de Sétif	Examinateur

Année universitaire : 2025/2026

Remerciements

Louange à *Dieu*, Seigneur des Mondes,
et que la bénédiction et la paix
soient sur le dernier des envoyés de *Dieu*, notre prophète *Mohammed* et sa famille.

Je tiens à remercier tout d'abord mon directeur de thèse, Monsieur *Mihoubi Douadi*, professeur à l'université de *M'sila*, qui a accepté de diriger ce travail tout au long des années. La confiance qu'il m'a accordée et ses qualités humaines et scientifiques ont été toujours présentes dans l'élaboration de cette thèse. Sa disponibilité permanente et son inquiétude à l'avance de mes travaux me valent beaucoup. Qu'il soit aussi remercié pour sa gentillesse et pour ses nombreux encouragements qu'il m'a adressés. Je tiens à exprimer ma profonde reconnaissance pour l'attention qu'il a portée à ce travail. Pour tout cela et d'autres, merci.

Je remercie également Monsieur *AMROUNE Abdelaziz*, professeur à l'université de *M'sila,* qui a accepté de présider le jury de soutenance et a pris le temps de lire, corriger, et donner des précieux conseils afin que ce travail s'approche de la soutenabilité. Merci pour son calme et sa patience.

J'adresse tous mes remerciements à Monsieur *BENSALEM Naceurdine*, professeur à l'université de *Sétif*, et à Monsieur *TRABELSI Nadir*, professeur à l'université de *Sétif*, de l'honneur qu'ils m'ont fait en acceptant d'être membres honorables du jury de soutenance. Leurs nombreuses lectures et corrections de cette thèse ont été très appréciables. Tous mes remerciements pour l'honneur qu'ils m'ont fait en acceptant d'être examinateurs.

Je tiens à remercier *tous les membres du Département de Mathématiques* de l'université de *M'sila*, mes amis qui m'ont fait partager des moments agréables en discutant ou en enseignant les mathématiques. Ce sont des moments oasis.

Je voudrais remercier particulièrement et profondément *mes parents*, *ma sœur* qui vivent toujours dans mon cœur. Cette thèse et moi vous devons beaucoup.

Un grand merci est adressé chaleureusement à *toute la famille* pour me soutenir, me supporter, m'encourager... pendant toute la durée de ma thèse et particulièrement durant les derniers mois de rédaction.

Enfin, je voudrais exprimer ma reconnaissance et ma gratitude à *tous ceux* qui ont contribué de près ou de loin à la réalisation de ce travail.

Dédicaces

$\mathcal{A}$ la mémoire de mes parents,

ma sœur,

Que *Allah* veille sur eux et leur accorde son salut et sa miséricorde,

$\mathcal{A}$ toute la famille ;

qui n'a pas cessé de m'encourager,

de m'aider par ses mots,

ses actes,

ses sourires,...

Table des matières

Notations

Symbole	:	**Signification**	◁
$\|E\|$	:	le cardinal d'un ensemble fini E	3
S_n	:	le groupe symétrique de degré n	3
$G_1 \times G_2$	:	le produit direct des groupes G_1 et G_2	4
$H \rtimes_\rho K$	:	le produit semi-direct des groupes H et K	4
$[G : H]$	:	l'indice du sous-groupe H dans le groupe G	5
Gx_0 ou $\mathcal{O}(x_0)$	:	l'orbite contenant l'élément x_0	8
G_x	:	le stabilisateur d'un élément x	10
$\mathbb{F}_q$	:	le corps fini d'ordre q	13
$\mathbb{F}_q^n$	:	l'espace vectoriel de dimension n sur $\mathbb{F}_q$	14
d_H	:	la distance de Hamming sur Q^n	16
w_H	:	le poids de Hamming dans $\mathbb{F}_q^n$	17
$d_H(C)$	:	la distance minimale d'un code C	17
$W_C(X)$	:	le polynôme énumérateur des poids d'un code $\mathcal{C}$	18
$(\mathbb{F}_q^n, d_H)$	:	l'espace métrique de Hamming	20
$Symm(\mathbb{F}_q^n, d_H)$	:	le groupe des isométries de l'espace de Hamming $(\mathbb{F}_q^n, d_H)$	21
$\sigma(\mathcal{C})$	:	le code équivalent à $\mathcal{C}$ par σ	23
$Perm(\mathcal{C})$	:	le groupe des permutations d'un code $\mathcal{C}$	23
$\langle x, y \rangle$	:	le produit scalaire standard de deux mots x et y	26
$\mathcal{C}_i$	:	le code $\mathcal{C}$ poinçonné en i	36
$\mathcal{C}^\sigma$	:	le code équivalent à $\mathcal{C}$ par σ^{-1}	40
$S(\mathcal{C}, i)$	:	l'image de $(\mathcal{C}, i)$ par une signature S	41
$\pi = (k_1, k_2, ..., k_m)$	:	la partition π d'un entier en m parts	55
d_π	:	la π-métrique associée à une partition π	58
$Symm(\mathbb{F}_q^n, d_\pi)$	:	l'ensemble des isométries de l'espace $(\mathbb{F}_q^n, d_\pi)$	58
S_π	:	le sous-groupe des permutations admissibles	63

Introduction

La théorie des groupes est l'une des disciplines basiques en mathématiques, c'est le langage algébrique des symétries. Elle trouve ses applications dans plusieurs domaines : en mathématiques, en physique, en chimie, en cryptographie et dans d'autres domaines de sciences de la vie. La référence [20] de R. Lidl et G. Pilz donne un survol de ses applications.

La théorie des codes correcteurs d'erreurs (ou la théorie algébrique du codage) est née au vingtième siècle pour résoudre un problème d'ingénierie concernant la transmission efficace de l'information. Un émetteur envoie un message à travers un canal de transmission qui n'est pas parfait en général. Un récepteur à l'autre côté du canal reçoit le message supposé envoyé. Occasionnellement, le message reçu diffère de celui envoyé : une erreur (ou plus) s'est produite. La théorie des codes correcteurs vise à détecter et corriger cette (ou ces) erreur(s). Elle est d'une importance capitale pour de nombreuses applications dans le domaine de l'informatique ou de l'ingénierie. Le travail de Claude Shannon (en 1948) "The mathematical theory of communication" constitue le point de repère de la théorie (voir [3]).

Plusieurs domaines de mathématiques sont en connexion avec la théorie des codes correcteurs : l'algèbre, la combinatoire, la géométrie, la cryptographie et la théorie des nombres pour en citer quelques-unes. Un nombre important de raisons et de motifs poussent les mathématiciens à faire appel à la théorie des groupes pour mieux comprendre les codes. Les techniques issues des groupes ont permis d'analyser le problème du codage et du décodage (par exemple la construction du tableau standard dans le cas des codes linéaires [23], de construire des classes importantes de codes (codes cycliques, partie des codes algèbre d'un groupe (group algebra codes) [3]), et aussi ont permis de mieux définir les concepts indispensables aux codes (équivalence des codes, chapitres deuxième et troisième de cette thèse).

Lors d'une transmission à travers un canal, pour mesurer la différence entre un mot (message) envoyé et un autre reçu, le concept de distance joue un rôle fondamental. C'est une application qui attribue un nombre réel positif à une paire de mots dans un espace et qui vérifie certains axiomes. Le résultat est un espace métrique. Après avoir défini cette structure sur l'ensemble des mots, il est naturel d'étudier les transformations (applications bijectives) qui préservent cette structure. Cela conduit à la théorie des groupes. Et c'est de cette manière qu'apparaissent le groupe d'isométries de l'espace métrique et le groupe des permutations d'un code correcteur d'erreurs.

Ce travail, intitulé "*Méthodes de la théorie des groupes pour les Codes Algébriques*" a été préparé au sein du Laboratoire des Mathématiques Pures et Appliquées (LMPA) du Département de Mathématiques de la Faculté des Mathématiques et Informatique, Université Mohamed Boudiaf, M'sila.

Dans cette thèse, nous considérons l'étude du problème de l'équivalence de deux codes correcteurs par permutation relativement à la distance de Hamming (le deuxième chapitre) et l'étude des propriétés du sous-groupe des permutations admissibles relativement à une distance associée à une partition de la longueur des codes (le troisième chapitre) :

- **Problème des codes équivalents par permutation** : Soit n un entier naturel non nul. $\mathbb{F}_q$ désigne le corps fini d'ordre q et $(\mathbb{F}_q^n, d_H)$ l'espace vectoriel de dimension n sur $\mathbb{F}_q$ muni de la distance de Hamming d_H. Le groupe symétrique de degré n est noté S_n.

  Deux codes $\mathcal{C}$ et $\mathcal{D}$ de longueur n sur $\mathbb{F}_q$ sont *équivalents par permutation* s'il existe une permutation σ de S_n telle que $\mathcal{D} = \sigma(\mathcal{C})$, où

  $$\sigma(\mathcal{C}) = \left\{ (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) \mid (x_1, x_2, ..., x_n) \in \mathcal{C} \right\}.$$

  L'équivalence des codes est un problème important de la théorie des codes car elle permet de classifier les codes, de faire transférer les propriétés et les paramètres des codes (linéarité, distance minimale, polynôme énumérateur des poids...). Parfois l'équivalence permet d'identifier le code et de simplifier son étude (code systématique

ayant une matrice génératrice standard). Enfin, citons ses applications en cryptographie ([8] et [22]).

Ce problème fut étudié par Petrank et Roth [30]. Comme résultat, ils ont montré que décider que deux codes sont équivalents ou non est un problème au moins aussi difficile que le problème de l'isomorphisme des graphes. Pour la question de trouver la permutation qui envoie un code correcteur à un autre code sachant que ces codes sont équivalents, une tentative de répondre à cette question est donnée par le travail de Nicolas Sendrier dans [34] et [35] en utilisant la notion de *signature* : propriété relative à une position d'un code.

La collection de toutes les permutations laissant globalement invariant un code $\mathcal{C}$, c'est-à-dire l'ensemble :

$$Perm(\mathcal{C}) = \{\sigma \in S_n \mid \sigma(\mathcal{C}) = \mathcal{C}\},$$

possède une structure algébrique remarquable, c'est le groupe des permutations de $\mathcal{C}$. Son étude est un problème qui aide à tirer de considérables résultats concernant l'équivalence des codes.

- **Problème des permutations admissibles :** pour étudier la capacité des codes à détecter et corriger les erreurs, la distance de Hamming est la plus classique et la plus utilisée pour sa connexion avec les machines traitant l'information. En 2006, Feng, Xu et Hickernell dans [11] ont introduit une distance d_π sur $\mathbb{F}_q^n$ associée à une partition π de l'entier positif n, la longueur des mots de $\mathbb{F}_q^n$. Soient n et m deux entiers positifs tels que $m \leq n$. Une partition de l'entier positif n en m parts ([1]) est une suite décroissante $\pi = (k_1, k_2, ..., k_m)$ de m entiers positifs $k_1, k_2, ..., k_m$ qui vérifient

$$n = k_1 + k_2 + ... + k_m \ .$$

La partition π induit une décomposition de l'espace $\mathbb{F}_q^n$ en produit direct de m sous-espaces vectoriels.

$$\mathbb{F}_q^n = \mathbb{F}_q^{k_1} \times \mathbb{F}_q^{k_2} \times ... \times \mathbb{F}_q^{k_m}$$

de sorte qu'un vecteur v de $\mathbb{F}_q^n$ s'écrive sous la forme

$$v = (v_1, v_2, ..., v_m)$$

avec $v_i \in \mathbb{F}_q^{k_i}$ pour $i = 1, 2, ..., m$.

La π-distance entre deux vecteurs $u = (u_1, u_2, ..., u_m)$ et $v = (v_1, v_2, ..., v_m)$ de $\mathbb{F}_q^n$ est le nombre $d_\pi(u, v)$ de leurs blocs différents :

$$d_\pi(u, v) = |\{i = 1, 2, ..., m \mid u_i \neq v_i\}|.$$

Autour de ce concept, plusieurs travaux sont élaborés. M. M. S. Alves, L. Panek et M. Firer donnèrent dans l'article "*Error-Block Codes and Poset Metric*" [Advances in Mathematics of Communications, Volume 2, No 1, 2008] une description complète du groupe des isométries linéaires de l'espace métrique $(\mathbb{F}_q^n, d_\pi)$. Alves et Panek dans [28] s'intéressèrent à l'étude des *isométries* de $\mathbb{F}_q^n$ muni de cette distance. Ces isométries forment un groupe pour la composition des applications, il est le *produit semi-direct.*

$$Symm(F_q^n, d_\pi) \cong S_\pi \ltimes \prod_{i=1}^{i=m} S_{q^{k_i}}$$

de deux de ses sous-groupes. L'un des deux est le sous-groupe S_π des *permutations admissibles,* concepts qui sont traités dans le troisième chapitre.

Notre contribution à l'étude de ces problèmes apparaît dans l'utilisation des techniques liées à la théorie des groupes finis, qui nous a permis de dériver des résultats remarquables attachés à la notion d'équivalence des codes correcteurs (définition de l'équivalence des codes, nombre des codes équivalents, nombre des permutations définissant le même code équivalent et conjugaison des groupes des permutations des codes équivalents...). Pour le problème de détermination de la permutation, entre deux codes équivalents, basé sur la notion de signature due à Nicolas Sendrier, nous nous sommes concentrés sur un cas particulier, où la signature associée vérifie une certaine condition pour laquelle nous avons pu calculer cette permutation. Des exemples illustrant les résultats sont exhibés.

Encore, nous avons tiré des résultats importants en appliquant la notion de l'action d'un groupe. Pas mal de profits sont tirés de l'application de cette notion : des définitions apparaissent si claires, si rigoureuses et bien structurées (définition de l'équivalence des compositions, permutations admissibles...), des résultats bien fondés se démontrent (nombres des compositions équivalentes, l'ordre du sous-groupe des permutations admissibles...).

Ce travail a fait l'objet d'une publication [19] dont les résultats sont présentés dans le deuxième chapitre.

Cette thèse se déroule comme suit, elle est paliée sur trois chapitres constituant le travail tout entier :

- Le premier chapitre est une introduction pour les concepts de base, les terminologies nécessaires et les principales notations qui constituent les outils de base pour explorer les chapitres qui suivent. On commence par présenter des notions et des résultats de la théorie des groupes (en particulier finis) tels que les classes latérales suivant un sous-groupe, le théorème de Lagrange et surtout le concept de l'action d'un groupe. Ensuite, on présente le terme de corps finis et l'espace vectoriel associé : espace des mots de longueur fixée. Enfin, on termine par les codes correcteurs, quelques notions et résultats qui y sont liés dans la littérature du codage (distance et poids de Hamming, polynôme énumérateur des poids...).

- Le deuxième chapitre a pour but l'étude de l'équivalence des codes : On commence par la donnée des définitions et les propriétés qui s'en déduisent. On applique des outils issus de la théorie des groupes pour mieux comprendre l'équivalence et pour tirer d'autres propriétés. Ces propriétés sont citées et démontrées (transfert des paramètres, préservation de linéarité, conservation des polynômes énumérateurs des poids, nombre des codes équivalents, nombre des permutations définissant le même code équivalent et conjugaison des groupes de permutations des codes équivalents, etc.). Enfin, on se concentre sur le problème de détermination de la permutation entre deux codes équivalents basé sur la notion de signature due à Nicolas Sendrier dans [34] et [35]. Notre intention porte sur un cas particulier, où la signature associée vérifie une certaine condition. Sous cette condition on peut déterminer cette permutation. Des exemples illustrant les résultats sont exhibés.

▲ Le troisième chapitre rassemble les notions fondamentales de partition d'un entier positif, la distance associée et les permutations admissibles. Nous démontrons quelques résultats relatifs à ces notions en nous appuyant sur le concept du groupe agissant sur un ensemble (compositions d'un entier positif et leurs équivalences, permutations admissibles et les résultats qui s'en déduisent, nombre des compositions équivalentes, l'ordre du sous-groupe des permutations admissibles, etc.). Les travaux [11] et [28] constituent les références et les raisons de cette étude.

Chapitre 1

Préliminaires et concepts de base

Ce chapitre est un chapitre de préliminaires. Il s'agit ici de présenter les concepts de base et les principales notations, qui constituent les outils de base pour explorer les chapitres qui suivent : définitions et énoncés de la théorie des groupes, codes correcteurs d'erreurs, etc.

D'autres éléments viendront les compléter au cours des chapitres suivants.

1.1 Un peu de la théorie des groupes

Dans cette section, la terminologie nécessaire et les notations usuelles de la théorie des groupes sont rassemblées. On y reviendra aux chapitres qui suivent pour l'étude de l'équivalence des codes (deuxième chapitre) et pour montrer des résultats liés aux permutations admissibles associées à une partition de l'entier naturel n (troisième chapitre). Pour une description si détaillée, les références suivantes comptent : [2, 6, 10, 12, 13, 20, 25, 31, 32] et [36].

1.1.1 Définitions de base

Définition 1.1.1 *Un groupe est un ensemble non vide G muni d'une loi de composition binaire interne $(x, y) \longmapsto xy : G \times G \to G$ satisfaisant aux axiomes suivants :*

`(G1)` *la loi est associative :* $\forall a, b, c \in G \quad (ab)c = a(bc)$,

`(G2)` *la loi admet un élément neutre e tel que* $\forall a \in G \quad ae = ea = a$,

(G3) *Tout élément $a \in G$ possède un symétrique $a^{-1} \in G$ tel que* $aa^{-1} = a^{-1}a = e$.

Exemple 1.1.1 *Soit E un ensemble non vide. L'ensemble $S(E)$ des bijections de E sur lui-même est un groupe pour la loi de composition des applications. Ce groupe est appelé* groupe symétrique de E. *Si de plus l'ensemble $E = \{1, 2, ..., i, ..., n\}$ (où E est fini de cardinal $|E| = n$), le groupe $S(E)$ est noté S_n et appelé* groupe symétrique de degré n. *Ses éléments sont les* permutations. *Le groupe S_n est fini d'ordre $n!$.*

La notation

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

veut dire que pour la permutation $\sigma \in S_n$, l'image de tout $i \in E = \{1, 2, ..., i, ..., n\}$ est l'élément $\sigma(i)$ de E. On utilise aussi la notation classique d'un *cycle* $\sigma = (a_1 a_2 ... a_k) \in S_n$ défini par

$$\begin{cases} \sigma(a) = a \text{ pour } \ a \neq a_i \\ \sigma(a_i) = a_{i+1} \text{ modulo } k \end{cases}$$

L'entier naturel k est appelé l'ordre du cycle σ.

Définition 1.1.2 *Soit H une partie non vide d'un groupe G. On dit que H est un sous-groupe de G si H est un groupe pour la loi de composition de G.*

La définition précédente est équivalente à la condition suivante

$$\forall x, y \in H, \quad x\, y^{-1} \in H.$$

Un sous-groupe de S_n est appelé un groupe de permutations de degré n.

Remarque 1.1.1 *Soit G un groupe et x un élément de G. Si H est un sous-groupe de G, alors il en est de même pour xHx^{-1}. Le sous-groupe xHx^{-1} est le conjugué de H (on dit que H et xHx^{-1} sont conjugués).*

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

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

Produit semi-direct de deux sous-groupes

Supposons que H et K soient deux groupes. Si $\rho : K \longrightarrow Aut(H)$ 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

$$(h, k)(h', k') = (h\rho(k)(h'), kk')$$

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

Le théorème suivant sert d'utile

Théorème 1.1.1 *([2], Theorem 23.3) 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.

1.1.2 Classes latérales

Soient H un sous-groupe de G et x un élément de G.

Définition 1.1.3 *La classe à gauche de x modulo H est la partie xH de G définie par*

$$xH = \{xh \mid h \in H\}.$$

L'ensemble de toutes les classes à gauche modulo H forme une partition de G. On le note souvent G/H.

Si de plus G est fini, le cardinal de G/H est appelé *l'indice de H dans G*. Ce dernier est noté $[G : H]$.

Le théorème suivant, dû à *Lagrange,* établit une relation entre l'ordre d'un groupe fini G, l'ordre et l'indice d'un sous-groupe de G.

Théorème 1.1.2 (Lagrange) *Si G est un groupe fini, alors*

$$|G| = [G : H]\,|H|$$

En particulier, l'ordre et l'indice de H sont des diviseurs de l'ordre de G.

L'étude des codes équivalents de longueur n dans le deuxième chapitre est basée sur le groupe des permutations d'un code, ce dernier est un sous-groupe du groupe symétrique S_n. Les permutations admissibles vues au troisième chapitre forment un sous-groupe d'un groupe symétrique de degré égal au nombre des blocs d'une partition de n. Le théorème suivant montre qu'on peut réaliser tout groupe comme un groupe de permutations. Cela justifie notre restriction aux groupes symétriques finis.

Théorème 1.1.3 (Cayley) *Tout groupe G est isomorphe à un sous-groupe du groupe symétrique $S(G)$.*

Cet isomorphisme est conséquence du monomorphisme canonique

$$\varphi : G \longrightarrow S(G)$$
$$a \longmapsto \varphi_a$$

défini par $\varphi_a(x) = ax$, pour tout x de G.

Si le groupe G est fini, alors le corollaire suivant a lieu :

Corollaire 1.1.1 *Un groupe fini d'ordre n peut être identifié à un sous-groupe de S_n.*

Preuve. Un ensemble fini G de cardinal n est équipotent à $\{1, 2, ..., n\}$, par conséquent $S(G)$ et S_n sont isomorphes. ■

1.1.3 Action d'un groupe sur un ensemble

Dans toute cette section, G est un groupe d'élément neutre e et X un ensemble non vide.

Définition 1.1.4 *Une action à gauche de G sur X est une application*

$$\gamma : G \times X \longrightarrow X$$
$$(g, x) \longmapsto gx$$

qui vérifie :

`(A1)` *$ex = x$, pour tout x de X,*

`(A2)` *$g_1(g_2x) = (g_1g_2)x$, pour tout g_1, g_2 de G et tout x de X.*

On dit aussi que le groupe G *opère* à gauche sur X. L'ensemble X sur lequel est définie l'action à gauche de G est appelé un G-ensemble.

Les axiomes de la définition précédente impliquent que, pour tout $g \in G$, la *translation à gauche*

$$\gamma_g : X \longrightarrow X$$
$$x \longmapsto gx$$

est une bijection. c'est-à-dire $\gamma_g \in S(X)$.

L'axiome (A2) veut dire que l'application

$$\begin{aligned} G &\longrightarrow S(X) \\ g &\longmapsto \gamma_g \end{aligned}$$

est un homomorphisme de groupes. Par conséquent toute action à gauche d'un groupe G sur un ensemble X définit un homomorphisme $G \longrightarrow S(X)$, et réciproquement, tout tel homomorphisme définit une action de G sur X. D'où la proposition suivante qui donne une définition équivalente :

Proposition 1.1.1 *Une action à gauche d'un groupe G sur un ensemble X est équivalente à la donnée d'un homomorphisme de groupes $G \longrightarrow S(X)$.*

D'une manière similaire, on définit une action *à droite* d'un groupe G sur un ensemble X. Dans tout ce qui suit, et dans le but de simplification, une action d'un groupe sur un ensemble est réservée pour une action à gauche.

Exemple 1.1.2 *Sur l'ensemble $\{1, 2, ..., n\}$, on définit une action dite* naturelle *du groupe symétrique S_n par $(\sigma, i) \longmapsto \sigma(i)$.*

Tout sous-groupe H de S_n définit une action sur $\{1, 2, ..., n\}$.

Exemple 1.1.3 *Pour tout groupe G, la conjugaison*

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto gxg^{-1} \end{aligned}$$

est une action de G sur lui-même.

Cette action induit une action de G sur l'ensemble de tous les sous-groupes de G :

$$(g, H) \longmapsto gHg^{-1}$$

pour tout $g \in G$ et tout sous-groupe H de G.

Exemple 1.1.4 *Le groupe des automorphismes $Aut(G)$ d'un groupe G définit une action sur G.*

Remarque 1.1.2 *Le théorème 1.1.3 de Cayley affirme que tout groupe G est isomorphe à un sous-groupe de $S(G)$. Ce qui est équivalent à dire que G opère sur lui-même (par translation à gauche, par exemple).*

Orbites d'une action

Soit $(g, x) \longmapsto gx$ une action d'un groupe G sur un ensemble X.

Définition 1.1.5 *Une partie S de X est* stable *sous l'action de G si*

$$\forall g \in G \quad \forall x \in S, \quad gx \in S$$

Dans ce cas, l'action de G sur X induit une action de G sur S.

Sur l'ensemble X, on définit la relation binaire :

$$\text{Pour } x, y \in X \qquad x \sim y \Longleftrightarrow \exists g \in G \text{ tel que } y = gx$$

La relation $\sim$ est une relation d'équivalence sur X. Les classes d'équivalence sont appelées les G-orbites ou, simplement, orbites si aucune confusion n'est à craindre. Les orbites forment une partition de X.

par définition, une orbite contenant x_0 est

$$Gx_0 = \mathcal{O}(x_0) = \{gx_0 \mid g \in G\}$$

C'est la plus petite partie *stable* de X contenant x_0.

Exemple 1.1.5 (a) *L'orbite d'un élément $i \in \{1, 2, ..., n\}$ sous l'action naturelle de S_n est l'ensemble $\{1, 2, ..., n\}$ tout entier.*

(b) *Pour un groupe G qui agit sur lui-même par conjugaison, les orbites sont les classes de conjugaison de G.*

(c) *L'orbite d'un sous-groupe H de G sous l'action*

$$(g, H) \longmapsto gHg^{-1}$$

est

$$\left\{gHg^{-1} \mid g \in H\right\}$$

C'est l'ensemble de tous les sous-groupes conjugués de H.

Remarque 1.1.3 *La notion d'action de groupe G sur un ensemble X permet de définir le concept d'objets mathématiques orbites. D'une part ces orbites confèrent à X une partition, ce qui permet d'établir une classification des éléments de X. D'autre part, les orbites caractérisent les parties stables de X. En effet une partie de X est stable, si et seulement si, elle est réunion d'orbites. Par exemple, un sous-groupe H de G est normal si et seulement si il est réunion des classes de conjugaison.*

Une action d'un groupe G sur un ensemble X est dite *transitive* si

$$\forall x, y \in G,\ \exists g \in G \text{ tel que } \ y = gx$$

C'est-à-dire qu'une seule orbite existe, qui est X tout entier. Par exemple l'action naturelle de S_n sur $\{1, 2, ..., n\}$ est transitive.

1.1.4 Stabilisateur (groupe d'isotropie)

Le deuxième objet mathématique défini par une action d'un groupe G sur l'ensemble X est *le stabilisateur (ou groupe d'isotropie)* d'un élément $x \in X$. C'est un sous-groupe de G des éléments laissant x fixe. Ce sous-groupe de G présente ce qui est en face de l'orbite partie de X.

Définition 1.1.6 *Le stabilisateur (ou groupe d'isotropie) d'un élément $x \in X$ est*

$$G_x = \{g \in G \mid gx = x\}$$

La proposition suivante montre que le stabilisateur possède une structure algébrique, c'est un *sous-groupe* du groupe opérant sur l'ensemble. Cela justifie l'appellation *sous-groupe d'isotropie*. Le deuxième énoncé de la proposition montre que les stabilisateurs de deux éléments équivalents par action sont conjugués, donc isomorphes. Par conséquent ils peuvent être identifiés.

Proposition 1.1.2 *Soit G un groupe opérant sur un ensemble X.*

(i) *Le stabilisateur G_x de $x \in X$ est un sous-groupe de G,*

(ii) *Si $y = gx$, avec $g \in G$ et x, $y \in X$, alors $G_y = g\ G_x\ g^{-1}$.*

Preuve.

(i) Soient g_1, g_2 deux éléments de G_x, alors les axiomes `(A1)` et `(A2)` de la définition 1.1.4 permettent d'écrire

$$g_1 g_2^{-1} x = g_1 g_2^{-1}(g_2 x) = g_1 x = x$$

ce qui prouve que $g_1 g_2^{-1} \in G_x$, et par suite G_x est un sous-groupe de G.

(ii) Certainement, si $h\ x = x$, alors

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

et par suite

$$g\ G_x\ g^{-1} \subset G_y$$

Réciproquement, si $h\ y = y$, alors

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

et donc $g^{-1}\ h\ g \in G_x$. c'est-à-dire $h \in g\ G_x\ g^{-1}$ et $G_y \subset g\ G_x\ g^{-1}$. ■

L'homomorphisme $G \longrightarrow S(X)$ qui définit l'action de G sur X d'une manière équivalente, selon la proposition 1.1.1, a pour noyau le sous-groupe normal de G

$$Ker(G \longrightarrow S(X)) = \bigcap_{x \in X} G_x$$

Exemple 1.1.6 *Considérons un groupe G opérant sur lui-même par conjugaison. Pour $x \in G$ nous avons,*

$$G_x = \{g \in G \mid gx = xg\}$$

C'est le centralisateur *de x dans G. L'intersection $\bigcap_{x \in X} G_x$ est* le centre $Z(G)$ *: l'ensemble des éléments de G qui commutent avec tout élément de G.*

Exemple 1.1.7 *Soit H un sous-groupe d'un groupe G. Considérons l'action*

$$\begin{array}{c} G \times G/H \longrightarrow G/H \\ (g, xH) \longmapsto gxH \end{array} .$$

Alors $G_H = H$ et $G_{xH} = xHx^{-1}$.

D'une manière générale, si S est une partie non vide de X, on définit le stabilisateur G_S de S par

$$G_S = \{g \in G \mid gS = S\}$$

avec

$$gS = \{gs \mid s \in S\}.$$

Comme dans la preuve de la proposition 1.1.2, on peut voir que

$$G_{gS} = g\ G_S\ g^{-1}.$$

1.1.5 Relation entre orbite et stabilisateur

Le groupe G opère transitivement sur X s'il existe une seule orbite. Pour une action quelconque, même si elle n'est pas transitive, l'action de G sur une orbite Gx_0 d'un élément $x_0 \in X$ est toujours transitive. Ce qui permet d'énoncer le théorème suivant reliant l'orbite Gx_0 de x_0 avec son stabilisateur G_{x_0}. Ce théorème constitue un outil puissant pour compter le cardinal d'une orbite, partie de X, en fonction de l'indice du stabilisateur correspondant, sous-groupe de G.

Théorème 1.1.4 (Orbite-stabilisateur) *Soit G un groupe qui opère sur un ensemble X, et soit Gx_0 l'orbite contenant x_0. L'application*

$$gG_{x_0} \longrightarrow gx_0 : (G/G_{x_0}) \longrightarrow Gx_0$$

est bijective.

Preuve. L'application est bien définie et injective puisque

$$g_1G_{x_0} = g_2G_{x_0} \Longleftrightarrow g_2^{-1}g_1 \in G_{x_0} \Longleftrightarrow g_1x_0 = g_2x_0$$

.

L'application est surjective car G opère transitivement sur l'orbite Gx_0. ■

Dans le cas où G et X sont finis, le corollaire suivant a lieu :

Corollaire 1.1.2 *Si G est un groupe fini opérant sur un ensemble fini X, alors pour tout x_0 de X,*

$$|G| = |Gx_0| \ \ |G_{x_0}| .$$

Preuve. D'après le théorème précédent, et comme G et X sont finis, nous avons

$$|Gx_0| = [G : G_{x_0}] = \frac{|G|}{|G_{x_0}|}.$$

La dernière relation est fréquemment utilisée pour calculer $|Gx_0|$. ■

1.2 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 1.2.1 *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,

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

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. Pour une démonstration, on peut consulter [14] et [33].

Théorème 1.2.1 **(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.*

Désormais, $\mathbb{F}_q$ désigne *le corps fini* d'ordre q. Pour plus de détails sur les corps finis, nous renvoyons à [3, 4, 5, 7, 9, 10, 12, 14, 15, 18, 20] et [23]. Les références [21] et [26] sont entièrement consacrées à l'étude des corps finis et de leurs propriétés.

Exemple 1.2.1 `(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 $X^2+X+1 \in \mathbb{F}_2[X]$.*

1.2.1 Espace vectoriel $\mathbb{F}_q^n$

L'espace ambiant pour construire des codes correcteurs est $\mathbb{F}_q^n$. C'est l'ensemble produit cartésien de n copies de $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(x_1, x_2, ..., x_n) \mid x_i \in \mathbb{F}_q\}$$

$\mathbb{F}_q^n$ est un espace vectoriel de dimension n sur $\mathbb{F}_q$ pour les opérations :

$$(x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n) = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$$
$$\lambda.(x_1, x_2, ..., x_n) = (\lambda x_1, \lambda x_2, ..., \lambda x_n), \ \ \lambda \in \mathbb{F}_q$$

Un élément $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_q^n$ est appelé un mot de longueur n sur $\mathbb{F}_q$. La notation $x = x_1 x_2 ... x_n$ est populaire chez les théoriciens des codes correcteurs d'erreurs. Les scalaires $x_1, x_2, ..., x_n$ sont les coordonnées (ou les positions) de x sur $\mathbb{F}_q$.

1.3 Codes correcteurs d'erreurs

La théorie du codage trouve son origine dans le problème de la transmission de l'information à travers un canal de transmission bruité. L'information circule sous forme d'un message composé de k lettres appartenant à un ensemble fini Q appelé *alphabet* convenablement choisi selon les circonstances relatives à la communication et le canal. Malheureusement, pour des causes différentes, des erreurs finissent par se produire : le message reçu est différent du message envoyé. Une tentative de recommencer la transmission, pour corriger l'erreur, n'est pas toujours possible (perte de message original, résultat non enregistré, manque de temps, risque de produire d'autres erreurs, etc.). L'alternative est de corriger l'erreur à partir du message reçu. *La théorie des codes correcteurs d'erreurs* (encore appelée *théorie algébrique des codes*) a pour but l'étude systématique des moyens permettant de détecter et corriger les erreurs produites lors de transmission de messages à travers un canal bruité. La solution revient à remplacer le message (composé de k lettres), qu'on veut envoyer, par un autre message plus long appelé *mot de code* (composé de $n \geq k$ lettres de Q) en ajoutant

des redondances de manière à ce que les erreurs puissent être détectées et corrigées. C'est le mot de code ainsi construit qui sera transmis.

Dans cette section, certains aspects mathématiques et notions de base de la théorie des codes correcteurs sont cités : code correcteur, distance de Hamming, polynôme énumérateur des poids, etc. Pour plus sur les aspects et les origines de la théorie du codage et la théorie de l'information, on peut voir les références [4, 5, 9, 17, 20] et [29] qui figurent à la fin de ce travail. L'ouvrage de Macwilliams et Sloane [23] est une référence compréhensive volumineuse , qui contient une bibliographie assez extensive pour la théorie des codes correcteurs (selon Lidl et Pliz [20]), traditionnellement il est nommé *La Bible de la théorie des codes*. Citons encore le livre de Van Lint [37] qui présente une référence standard dans la théorie.

1.3.1 Code 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 1.3.1 *Un code de longueur n sur l'alphabet Q est une partie non vide C de $Q^n = Q \times Q \times ... \times Q$ (n 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 1.3.1 *$C = \{011, 100, 000\}$ est un $(3, 3)$ code sur $\mathbb{F}_2$.*

Exemple 1.3.2 *$D = \{abcd, dddb, adda, dcba, cdab\}$ est un $(4, 5)$ code sur $Q = \{a, b, c, d\}$.*

Exemple 1.3.3 *$L = \{01\omega\omega1, 1\omega110, 000\omega1, 1010\omega, 10011, 00100\}$ 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

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

1.3.2 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 $x = x_1x_2...x_n$ et $y = y_1y_2...y_n$ de Q^n.

Définition 1.3.2 (Distance de Hamming) *Pour deux mots $x = x_1x_2...x_n$ et $y = y_1y_2...y_n$ de Q^n, la distance de Hamming de x à y est le nombre $d_H(x, y)$ des positions $i = 1, 2, ..., n$ telles que $x_i \neq y_i$.*

c'est-à-dire

$$d_H(x, y) = |\{i = 1, 2, ..., n \mid x_i \neq y_i\}|.$$

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

$$\begin{aligned} &d_H(x, y) \geq 0 \text{ et } d_H(x, y) = 0 \Leftrightarrow x = y, \\ &d_H(x, y) = d_H(y, x) \\ &d_H(x, z) \leq d_H(x, y) + d_H(y, z) \end{aligned}$$

pour x, y et z mots de Q^n. L'espace métrique (Q^n, d_H) est appelé *l'espace de Hamming.*

Exemple 1.3.4 $d_H(011, 100) = 3$ *sur* $\mathbb{F}_2^3$.

Exemple 1.3.5 $d_H(dddb, adda) = 2$ *sur* $Q^4 = \{a, b, c, d\}^4$.

Exemple 1.3.6 $d_H(01\omega\omega1, 1\omega110) = 5$ *sur* $\mathbb{F}_4^5$.

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 1.3.3 (Le poids de Hamming) *Le poids de Hamming d'un mot* $x = x_1x_2...x_n$ *de* $\mathbb{F}_q^n$ *est l'entier naturel*

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

Autrement dit,

$$w_H(x) = d_H(x, \mathbf{0}).$$

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

L'efficacité d'un code se mesure par le nombre des 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 1.3.4 *Soit* C *un code de longueur* n *sur* Q. *La distance minimale de* C *est le nombre naturel*

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

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 les paramètres.

Exemple 1.3.7 *l'ensemble* $\{000, 110, 011, 101\}$ *est un* $(3, 4, 2)$*-code sur* $\mathbb{F}_2$.

1.3.3 Polynôme énumérateur des poids

Pour étudier le problème d'équivalence de deux codes, Nicolas Sendrier dans [34] et [35] 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 1.3.5 *Soit C un (n, M, d)-code sur Q. La distribution des poids de C est la suite des entiers naturels $\{A_0, A_1, ..., A_n\}$ avec A_i qui est le nombre des mots de code de poids i.*

On voit clairement que

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

Définition 1.3.6 *Soit C un (n, M, d)-code sur Q. Le polynôme énumérateur des poids du code C est le polynôme $W_C(X)$ de $\mathbb{Z}[X]$ défini par*

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

Exemple 1.3.8 *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*

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

1.4 Conclusion

Dans ce chapitre, il s'agit de rassembler les concepts et les terminologies nécessaires qui présentent le fil conducteur des chapitres qui suivent. Tout d'abord on a commencé par présenter des notions et des résultats de la théorie des groupes (en particulier finis) tels que

les classes latérales suivant un sous-groupe, le théorème de Lagrange et surtout le concept de l'action d'un groupe qui constitue l'axe principal autour duquel tournent les preuves présentées dans ce travail à travers les chapitres postérieurs. Ensuite on a présenté le concept du corps fini (alphabet constituant les mots de code) et l'espace vectoriel associé : espace des mots de longueur fixée. Enfin, on a terminé par les codes correcteurs, quelques notions et résultats qui y sont liés dans la littérature du codage (distance et poids de Hamming, polynôme énumérateur des poids, etc.).

Chapitre 2

Codes équivalents par permutation

L'information (représentée sous forme de vecteur de $\mathbb{F}_q^n$) est transmise à travers un canal qualifié 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 inventée dans le but de détecter et corriger ces erreurs. Cette dernière peut être mesurée en introduisant la notion de distance sur l'espace $\mathbb{F}_q^n$, qui par suite impose la question importante de ressemblance des parties (codes) de $\mathbb{F}_q^n$ relativement à ladite distance : parties ayant mêmes propriétés métriques. Cette ressemblance n'est autre que l'*isométrie de* $\mathbb{F}_q^n$.

L'ensemble des isométries de $\mathbb{F}_q^n$, relativement à une distance, possède une structure algébrique remarquable ayant des propriétés intéressantes. Il permet de définir de façon mathématique rigoureuse *l'équivalence des codes de longueur* n *sur* le corps fini $\mathbb{F}_q$.

L'équivalence des codes présente un des problèmes importants dans la théorie des codes correcteurs d'erreurs : Étant donné deux codes de mêmes paramètres, comment confirmer qu'ils sont ou non équivalents, et comment trouver la relation (permutation, isométrie...) qui définit cette équivalence.

La liste qui suit cite quelques réponses sur la question de nécessité et le but de définir une équivalence des codes :

1. L'équivalence permet de *classifier* les codes, c'est-à-dire de partitionner l'ensemble des codes en classes disjointes. Chaque classe contient des codes qui partagent les mêmes propriétés (algébriques, métriques, géométriques, etc.).

2. Deux codes équivalents ont la *même structure* (linéarité, cyclicité, etc.) et possèdent les *mêmes paramètres* du codage (longueur, dimension, taille, distance minimale, polynôme énumérateur de poids, etc.). Tout ça implique que les codes équivalents possèdent les mêmes capacités *de détection et correction des erreurs.*

3. Parfois l'équivalence permet *d'identifier* le mieux un code correcteur donné : le code linéaire binaire de matrice génératrice (les lignes forment une base du code)

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

est un code équivalent par permutation à celui de matrice génératrice

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

qui a la forme standard d'un code *cyclique* de $\mathbb{F}_2^7$.

4. En cryptographie, un cryptosystème (système de cryptage) fondé sur la théorie des codes correcteurs d'erreurs utilise comme clé secrète un code linéaire et comme clé publique un code équivalent (voir pour détails les références [8] et [22]).

Ce chapitre a pour but l'étude de l'équivalence des codes : On commence par donner des définitions et les propriétés qui s'en déduisent. On applique des outils issus de la théorie des groupes pour mieux comprendre l'équivalence et pour tirer d'autres propriétés. Enfin, on aborde, pour un cas particulier, le problème de détermination de permutation définissant l'équivalence.

Dans tout ce chapitre, soient n un entier naturel non nul et q une puissance d'un nombre premier. $\mathbb{F}_q$ désigne le corps fini d'ordre q et $(\mathbb{F}_q^n, d_H)$ l'espace vectoriel de dimension n sur $\mathbb{F}_q$ muni de la distance de Hamming d_H. Le groupe symétrique de degré n est noté S_n.

Définition 2.0.1 *[3] Une isométrie (ou symétrie) de l'espace de Hamming $(\mathbb{F}_q^n, d_H)$ est une application bijective $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ qui conserve les distances, c'est-à-dire*

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

pour tout x, $y \in \mathbb{F}_q^n$.

Si de plus f est linéaire, c'est une isométrie linéaire.

L'ensemble $Symm(\mathbb{F}_q^n, d_H)$ des isométries de l'espace de Hamming $(\mathbb{F}_q^n, d_H)$ est un groupe pour la composition des applications [pour plus, voir la sous-section 1 de la section 3.3].

2.1 Codes équivalents par permutation

Les références [3] et [15] constituent des sources pour plus de détails sur le contenu de cette section et les sections qui suivent. Les travaux [34] et [35] de N. Sendrier sont des lectures principales conseillées. Ils présentent le point de départ et d'appui de ce travail. Une partie de ces sections a fait l'objet d'une publication (article) [19].

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

$$\sigma(x) = (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) \tag{2.1.1}$$

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

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

Ceci permet de préserver les suites de distribution des poids et les polynômes énumérateurs des codes équivalents (voir 3.3 du Chapitre 1).

Faire associer à tout mot $x \in \mathbb{F}_q^n$ un autre mot $\sigma(x) \in \mathbb{F}_q^n$ défini de façon unique revient à considérer la permutation $\sigma \in S_n$ comme étant l'application $\widetilde{\sigma}$:

$$\begin{array}{c} \widetilde{\sigma} : \ \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n \\ (x_1, x_2, ..., x_m) \longmapsto (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(m)}) \end{array} . \tag{2.1.2}$$

Cette application conserve les distances de Hamming entre les mots de $\mathbb{F}_q^n$:

Si $x = (x_1, x_2, ..., x_n)$ et $y = (y_1, y_2, ..., y_n)$ sont deux mots, alors

$$d_H(x, y) = d_H(\widetilde{\sigma}(x), \widetilde{\sigma}(y)) = d_H(\sigma(x), \sigma(y)).$$

C'est-à-dire une *isométrie* de $\mathbb{F}_q^n$. En réalité c'est une isométrie linéaire.

La correspondance

$$\begin{array}{c} \Psi : \ S_n \longrightarrow Symm(\mathbb{F}_q^n, d_H) \\ \sigma \longmapsto \widetilde{\sigma} \end{array} .$$

est un homomorphisme injectif de groupes, ce qui permet d'identifier le groupe des permutations S_n à un sous-groupe de $Symm(\mathbb{F}_q^n, d_H)$. De plus, Ψ étant un homomorphisme de groupes, si σ et τ sont de S_n, alors

$$\widetilde{\sigma\tau} = \widetilde{\sigma} \circ \widetilde{\tau}$$

et si id (resp. $id_{\mathbb{F}_q^n}$) désigne l'identité de S_n (resp. $Symm(\mathbb{F}_q^n, d_H)$), alors on a

$$\widetilde{id} = id_{\mathbb{F}_q^n}.$$

Ce qui aboutit à la remarque suivante :

Remarque 2.1.1 *Si σ et τ sont des permutations de S_n, alors pour tout mot x de $\mathbb{F}_q^n$ on a les deux égalités*

$$(\sigma\tau)(x) = \sigma(\tau(x)) \quad et \quad id(x) = x.$$

Pour définir la relation d'équivalence de deux codes, on fait étendre la définition et la notation 2.1.1 au cas des codes de $\mathbb{F}_q^n$.

Pour un code $\mathcal{C}$ de longueur n sur $\mathbb{F}_q$ et pour une permutation σ de S_n, on note par $\sigma(\mathcal{C})$ la partie de $\mathbb{F}_q^n$ définie par :

$$\sigma(\mathcal{C}) = \left\{\sigma(x) \in \mathbb{F}_q^n \mid x \in \mathcal{C}\right\} = \left\{(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) \mid (x_1, x_2, ..., x_n) \in \mathcal{C}\right\}.$$

C'est simplement l'image directe du code $\mathcal{C} \subset \mathbb{F}_q^n$ par l'application $\widetilde{\sigma}$ définie par 2.1.2.

On peut aussi avoir la remarque suivante :

Remarque 2.1.2 *Si σ et τ sont des permutations de S_n, alors pour tout code $\mathcal{C}$ de longueur n sur $\mathbb{F}_q$ on a les deux égalités*

$$(\sigma\tau)(\mathcal{C}) = \sigma(\tau(\mathcal{C})) \quad et \quad id(\mathcal{C}) = \mathcal{C}.$$

Maintenant, nous sommes dans la position de définir l'équivalence des codes correcteurs d'erreurs.

Définition 2.1.1 *[20] Soient $\mathcal{C}$ et $\mathcal{D}$ deux codes de longueur n sur $\mathbb{F}_q$. On dit que $\mathcal{D}$ est équivalent par permutation à $\mathcal{C}$ s'il existe une permutation σ de S_n telle que $\mathcal{D} = \sigma(\mathcal{C})$.*

Cette relation est clairement une relation d'*équivalence* dans l'ensemble de tous les codes de longueur n sur $\mathbb{F}_q$. Ce qui justifie la terminologie codes équivalents par permutation.

Il arrive parfois que pour un code $\mathcal{C}$ de longueur n sur $\mathbb{F}_q$ et une permutation σ de S_n, on trouve que

$$\sigma(\mathcal{C}) = \mathcal{C}.$$

C'est-à-dire que $\mathcal{C}$ est *globalement invariant* par l'application $\widetilde{\sigma}$ définie par 2.1.2. La collection de toutes les permutations laissant globalement invariant $\mathcal{C}$ possède une structure algébrique remarquable. Notons cet ensemble par $Perm(\mathcal{C})$:

$$Perm(\mathcal{C}) = \{\sigma \in S_n \mid \sigma(\mathcal{C}) = \mathcal{C}\}$$

Proposition 2.1.1 *Soient $\mathcal{C}$ un code de longueur n sur $\mathbb{F}_q$ et S_n le groupe symétrique de degré n. L'ensemble $Perm(\mathcal{C})$ est un sous-groupe de S_n, appelé le groupe de permutations du code $\mathcal{C}$.*

Démonstration. Il suffit d'appliquer la définition 1.1.2 d'un sous-groupe en prenant en considération la remarque 2.1.2. Si σ et τ sont permutations de $Perm(\mathcal{C})$, alors on a

$$\begin{aligned} \sigma\tau(\mathcal{C}) &= \sigma(\tau(\mathcal{C})), && \text{Remarque 2.1.2} \\ &= \sigma(\mathcal{C}), && \tau \in Perm(\mathcal{C}) \\ &= \mathcal{C}, && \sigma \in Perm(\mathcal{C}) \end{aligned}$$

ce qui donne $\sigma\tau \in Perm(\mathcal{C})$. De plus

$$\begin{aligned} \sigma(\mathcal{C}) = \mathcal{C} &\iff \sigma^{-1}(\sigma(\mathcal{C})) = \sigma^{-1}(\mathcal{C}), && \text{car } \widetilde{\sigma^{-1}} \text{ application} \\ &\iff (\sigma^{-1}\sigma)(\mathcal{C})) = \sigma^{-1}(\mathcal{C}), && \text{Remarque 2.1.2} \\ &\iff id(\mathcal{C}) = \sigma^{-1}(\mathcal{C}), \\ &\iff \mathcal{C} = \sigma^{-1}(\mathcal{C}), && \text{Remarque 2.1.2} \end{aligned}$$

ce qui prouve que $\sigma^{-1} \in Perm(\mathcal{C})$. ■

Voici quelques exemples de groupes de permutations et de codes équivalents :

Exemple 2.1.1 *Soit $\mathcal{C}$ le code de longueur n sur $\mathbb{F}_q$ défini par $\mathcal{C} = \{aa...a \mid a \in \mathbb{F}_q\}$. C'est un code de paramètres (n, q, n) appelé* code de répétition. *On voit aisément que $Perm(\mathcal{C}) = S_n$. Le seul code équivalent à $\mathcal{C}$ est $\mathcal{C}$ lui-même.*

Exemple 2.1.2 *Soit $\mathcal{D}$ le code linéaire binaire $[3, 2, 1]$ défini par sa matrice génératrice*

$$G(\mathcal{D}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Un calcul simple est résumé dans le tableau suivant. Ce tableau parle de lui-même :

$\underline{\mathcal{D}}$	$\underline{x_1x_2x_3 \mapsto x_{\sigma(1)}x_{\sigma(2)}x_{\sigma(3)}}$	**000**	**100**	**001**	**101**
$id(\mathcal{D})$	$x_1x_2x_3 \mapsto x_1x_2x_3$	**000**	**100**	**001**	**101**
$(12)(\mathcal{D})$	$x_1x_2x_3 \mapsto x_2x_1x_3$	000	010	001	011
$(13)(\mathcal{D})$	$x_1x_2x_3 \mapsto x_3x_2x_1$	**000**	**001**	**100**	**101**
$(23)(\mathcal{D})$	$x_1x_2x_3 \mapsto x_1x_3x_2$	000	100	010	110
$(123)(\mathcal{D})$	$x_1x_2x_3 \mapsto x_2x_3x_1$	000	001	010	011
$(132)(\mathcal{D})$	$x_1x_2x_3 \mapsto x_3x_1x_2$	000	010	100	110

On a $Perm(\mathcal{D}) = \{id, (13)\}$*, sous-groupe d'ordre* 2*. Les codes équivalents à* $\mathcal{D}$ *sont au nombre de 3, à savoir* $\mathcal{D}$*, le code* $(12)(\mathcal{D}) = (123)(\mathcal{D})$ *(troisième et sixième lignes) et le code* $(23)(\mathcal{D}) = (132)(\mathcal{D})$ *(cinquième et septième lignes).*

Exemple 2.1.3 *On considère sur le corps* $\mathbb{F}_4$ *d'ordre 4 le code* $\mathcal{F} = \{00, 1\omega, \omega 1, \omega^2 1\}$ *de paramètres* $(2, 4, 2)$ *avec* ω *la classe de* $X \in \mathbb{F}_2[X]$ *modulo* $X^2 + X + 1$*.*

On a $Perm(\mathcal{F}) = \{id\}$, sous-groupe trivial de S_2 et $(12)\mathcal{F} = \{00, 1\omega, \omega 1, 1\omega^2\}$, un code équivalent à $\mathcal{F}$.

2.2 Propriétés diverses

Dans cette section, nous allons présenter quelques propriétés communes que partagent deux codes correcteurs *équivalents*. Ces propriétés montrent bien que la notion d'équivalence, pour elle-même, est très importante. Nous présenterons aussi quelques remarques concernant les groupes de permutations. La notion du dual d'un code ainsi que des propriétés relatives à l'équivalence sont citées.

2.2.1 Dual d'un code correcteur d'erreurs

On considère l'espace vectoriel $\mathbb{F}_q^n$ de dimension n sur le corps fini $\mathbb{F}_q$. Soit aussi $\mathcal{C}$ un code de paramètres (n, M) sur $\mathbb{F}_q$.

Pour deux mots (vecteurs) $x = (x_1, x_2, ..., x_n)$ et $y = (y_1, y_2, ..., y_n)$ de $\mathbb{F}_q^n$, on définit leur produit scalaire standard par :

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

C'est un scalaire, c'est-à-dire un élément du corps fini $\mathbb{F}_q$.

Il est aisé de voir que l'application produit scalaire

$$\begin{aligned} \langle ., . \rangle : \quad & \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q \\ & (x, y) \longmapsto \langle x, y \rangle \end{aligned} .$$

est une application bilinéaire symétrique, par contre elle perd la propriété d'être définie positive. Considérons par exemple dans $\mathbb{F}_2^4$ le produit scalaire $\langle 1111, 1111 \rangle = 0$ ou dans $\mathbb{F}_3^5$ le produit scalaire $\langle 11112, 11112 \rangle = 0$.

Pour le code $\mathcal{C}$ on associe la partie $\mathcal{C}^\perp$ de $\mathbb{F}_q^n$ définie par

$$\mathcal{C}^\perp = \left\{ y \in \mathbb{F}_q^n \mid \forall x \in \mathcal{C}, \quad \langle x, y \rangle = 0 \right\}$$

Cette partie a la propriété suivante :

Proposition 2.2.1 *Si $\mathcal{C}$ est un code correcteur de longueur n sur le corps fini $\mathbb{F}_q$, alors $\mathcal{C}^\perp$ est un code correcteur linéaire de longueur n sur $\mathbb{F}_q$. Le code $\mathcal{C}^\perp$ est appelé le code dual (ou orthogonal) de $\mathcal{C}$.*

Preuve. On voit que le vecteur nul $\mathbf{0} = 00...0$ appartient à $\mathcal{C}^\perp$, ce qui montre que $\mathcal{C}^\perp$ n'est pas vide. Pour un mot de code $x \in \mathcal{C}$, soit l'application

$$\begin{aligned} \langle x, . \rangle : \mathbb{F}_q^n & \longrightarrow \mathbb{F}_q \\ y & \longmapsto \langle x, y \rangle \end{aligned}$$

Cette application est linéaire de noyau $\ker \langle x, . \rangle = x^\perp$, sous-espace vectoriel de $\mathbb{F}_q^n$. Comme $\mathcal{C}^\perp = \bigcap_{x \in \mathcal{C}} x^\perp$ intersection de sous-espaces, la proposition en résulte. ■

Remarque 2.2.1 *1. Le code dual $\mathcal{C}^\perp$ est toujours linéaire même si $\mathcal{C}$ n'est pas linéaire,*

2. Si $\mathcal{C}$ est un code linéaire de dimension k (donc de cardinal $M = q^k$), alors le dual $\mathcal{C}^\perp$ est de dimension $n-k$ (donc de cardinal $M = q^{n-k}$).

3. En général, la propriété $\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}$ n'est pas vraie pour les codes linéaires de $\mathbb{F}_q^n$. Prenons par exemple $\mathcal{C} = \{0000, 1100, 0011, 1111\}$ sur $\mathbb{F}_2$, on voit que $\mathcal{C} = \mathcal{C}^\perp$.

Relativement à la relation d'équivalence et à la notion de groupe de permutations, un code et son dual possèdent les propriétés suivantes :

Proposition 2.2.2 *1. Soit $\mathcal{C}$ un code correcteur de longueur n sur $\mathbb{F}_q$ et soit $\mathcal{C}^\perp$ son code dual, alors on a $Perm(\mathcal{C}) = Perm(\mathcal{C}^\perp)$,*

2. Si $\mathcal{D}$ est un code équivalent à $\mathcal{C}$ tel que $\mathcal{D} = \sigma(\mathcal{C})$ pour $\sigma \in S_n$, alors $\mathcal{D}^\perp$ est équivalent à $\mathcal{C}^\perp$ avec $\mathcal{D}^\perp = \sigma(\mathcal{C}^\perp)$. c'est-à-dire que l'image du dual est le dual de l'image.

Démonstration. Soient $x = (x_1, x_2, ..., x_n)$ et $y = (y_1, y_2, ..., y_n)$ de $\mathbb{F}_q^n$. Rappelons que pour $\sigma \in S_n$ le vecteur $\sigma(x)$ est le vecteur $\sigma(x) = (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$. Par suite

$$\langle \sigma(x), \sigma(y) \rangle = x_{\sigma(1)} y_{\sigma(1)} + x_{\sigma(2)} y_{\sigma(2)} + ..., x_{\sigma(n)} y_{\sigma(n)},$$

σ étant une permutation qui envoie l'ensemble $\{1, 2, ..., n\}$ sur lui-même, on obtient que

$$\langle \sigma(x), \sigma(y) \rangle = \langle x, y \rangle$$

La permutation σ conserve le produit scalaire.

Soient maintenant $\sigma \in Perm(\mathcal{C})$ et $x \in \mathcal{C}^\perp$. Montrons que $\sigma(x) \in \mathcal{C}^\perp$. Pour tout mot de code $y \in \mathcal{C}$ on a

$$\begin{aligned} \langle \sigma(x), y \rangle &= \left\langle \sigma^{-1}(\sigma(x)), \sigma^{-1}(y) \right\rangle \\ &= \left\langle x, \sigma^{-1}(y) \right\rangle \end{aligned}$$

Comme $\sigma \in Perm(\mathcal{C})$ sous-groupe de S_n, alors $\sigma^{-1} \in Perm(\mathcal{C})$ et $\sigma^{-1}(y) \in \mathcal{C}$. Par suite

$$\langle \sigma(x), y \rangle = \left\langle x, \sigma^{-1}(y) \right\rangle = 0$$

Cela montre que $\sigma(\mathcal{C}^{\perp}) \subset \mathcal{C}^{\perp}$.

En appliquant ce dernier résultat pour $\sigma^{-1} \in Perm(\mathcal{C})$, on obtient $\sigma^{-1}(\mathcal{C}^{\perp}) \subset \mathcal{C}^{\perp}$. Ce qui donne après composition par σ la relation $\mathcal{C}^{\perp} \subset \sigma(\mathcal{C}^{\perp})$. D'où l'égalité voulue $\sigma(\mathcal{C}^{\perp}) = \mathcal{C}^{\perp}$.

La deuxième assertion de la proposition veut dire qu'on demande de démontrer l'égalité

$$\sigma(\mathcal{C}^{\perp}) = (\sigma(\mathcal{C}))^{\perp}.$$

Soient alors $x \in \sigma(\mathcal{C}^{\perp})$ et $y \in \sigma(\mathcal{C})$. Nous avons donc $x = \sigma(a)$ et $y = \sigma(b)$ avec $a \in \mathcal{C}^{\perp}$ et $b \in \mathcal{C}$; ensuite nous avons

$$\langle x, y \rangle = \langle \sigma(a), \sigma(b) \rangle = \langle a, b \rangle = 0,$$

ce qui entraîne que $\sigma(\mathcal{C}^{\perp}) \subset (\sigma(\mathcal{C}))^{\perp}$. L'inclusion inverse se démontre de la même manière. Ce qui achève la preuve de la proposition. ■

La relation d'équivalence des codes correcteurs conserve la linéarité : Un code correcteur équivalent par permutation à un code linéaire est linéaire.

Proposition 2.2.3 *Soient $\mathcal{C}$ et $\mathcal{D}$ deux codes de longueur n sur un corps fini $\mathbb{F}_q$. Si $\mathcal{C}$ et $\mathcal{D}$ sont équivalents par permutation et $\mathcal{C}$ est linéaire de dimension k, alors le code $\mathcal{D}$ est aussi linéaire de dimension k.*

Démonstration. Supposons que $\mathcal{C}$ soit un code linéaire de dimension k, équivalent par permutation au code $\mathcal{D}$ et que $\sigma(\mathcal{C}) = \mathcal{D}$ avec $\sigma \in S_n$.

Soient $\sigma(x), \sigma(y) \in \mathcal{D}$, où $x, y \in \mathcal{C}$ et $\lambda \in \mathbb{F}_q$. On a

$$\begin{aligned}\sigma(x)-\sigma(y) &= (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) - (y_{\sigma(1)}, y_{\sigma(2)}, ..., y_{\sigma(n)}) \\ &= (x_{\sigma(1)} - y_{\sigma(1)}, x_{\sigma(2)} - y_{\sigma(2)}, ..., x_{\sigma(n)} - y_{\sigma(n)}) \\ &= ((x-y)_{\sigma(1)}, (x-y)_{\sigma(2)}, ..., (x-y)_{\sigma(n)}) \\ &= \sigma(x-y),\end{aligned}$$

$x - y$ étant dans $\mathcal{C}$ car $\mathcal{C}$ est linéaire, cela montre que $\sigma(x) - \sigma(y)$ est dans $\sigma(\mathcal{C}) = \mathcal{D}$.

D'autre part,

$$\begin{aligned}\sigma(\lambda x) &= ((\lambda x)_{\sigma(1)}, (\lambda x)_{\sigma(2)}, ..., (\lambda x)_{\sigma(n)}) \\ &= (\lambda(x)_{\sigma(1)}, \lambda(x)_{\sigma(2)}, ..., \lambda(x)_{\sigma(n)}) \\ &= \lambda(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) \\ &= \lambda\sigma(x),\end{aligned}$$

qui prouve que $\lambda\sigma(x) \in \mathcal{D}$. Le code $\mathcal{D}$ est alors linéaire de base $\{\sigma(v_1), \sigma(v_2), ..., \sigma(v_k)\}$ si le code linéaire $\mathcal{C}$ est de base $\{v_1, v_2, ..., v_k\}$. c'est-à-dire qu'une matrice génératrice de $\mathcal{D} = \sigma(\mathcal{C})$ est obtenue en permutant, suivant la permutation σ, *les colonnes* d'une matrice génératrice donnée de $\mathcal{C}$. ■

Ce qui montre que deux codes équivalents par permutation possèdent les mêmes propriétés relatives à la détection et correction des erreurs, c'est ce qu'affirme la proposition suivante. Rappelons dans ce but que pour un code correcteur de longueur n sur un corps fini $\mathbb{F}_q$, les paramètres sont : la longueur n, le cardinal (la taille) M (ou la dimension k si le code est linéaire) et la distance minimale d. La distribution des poids et le polynôme énumérateur des poids sont comme dans la sous-section 1.3.3 du premier chapitre.

Proposition 2.2.4 *Deux codes de longueur n qui sont équivalents par permutation possèdent les mêmes paramètres, la même distribution des poids et le même polynôme énumérateur des poids.*

Preuve. Soient $\mathcal{C}$ et $\mathcal{D}$ deux codes de longueur n sur un corps fini $\mathbb{F}_q$. Supposons que $\mathcal{D} = \sigma(\mathcal{C})$ pour une permutation $\sigma \in S_n$. Le code $\mathcal{D}$ est l'image directe du code $\mathcal{C} \subset \mathbb{F}_q^n$ par l'application $\widetilde{\sigma}$ définie par 2.1.2. Cette application transforme *bijectivement* $\mathcal{C}$ vers $\mathcal{D}$, ils ont donc la même longueur et le même cardinal. Si les codes sont linéaires, la proposition 2.2.3 montre qu'ils ont la même dimension sur $\mathbb{F}_q$.

L'égalité

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

traduisant la conservation des poids, assure par conséquent la conservation de la distribution des poids, ce qui préserve le polynôme énumérateur des poids. ■

Remarque 2.2.2 *1. Les deux dernières propositions peuvent être utilisées dans leurs sens contraposés : Deux codes qui se diffèrent en l'un des paramètres, ou leurs distributions des poids ou leurs polynômes énumérateurs des poids sont des codes non équivalents par permutation. Ainsi les codes binaires* $\mathcal{C} = \{000, 100, 010, 110\}$ *et* $\mathcal{D} = \{101, 011, 110\}$ *ne sont pas équivalents par permutation. Le premier est linéaire tandis que le deuxième ne l'est pas,* $\mathcal{C}$ *a pour distance minimale* 1 *alors que celle de* $\mathcal{D}$ *est* 2.

2. En général, la réciproque des deux dernières propositions n'est pas vraie. Deux codes peuvent avoir les mêmes paramètres, même distribution des poids (et par suite même polynôme énumérateur des poids) sans être équivalents par permutation. Considérons les deux codes ternaires $\mathcal{A} = \{00, 10, 11\}$ *et* $\mathcal{B} = \{00, 02, 22\}$ *de* $\mathbb{F}_3^2$ *; ils possèdent les mêmes paramètres* ($n = 2$, $M = 3$, $d = 1$)*, même polynôme énumérateur des poids* $1 + X + X^2$ *alors que* $\mathcal{A}$ *et* $\mathcal{B}$ *ne sont pas équivalents par permutation.*

2.3 La théorie des groupes s'applique

La théorie des groupes joue un rôle important en algèbre, géométrie, combinatoire et autres sciences. Elle permet de mieux comprendre les objets et d'en tirer de très remarquables résultats. Pour la théorie des codes correcteurs d'erreurs, la notion de *l'action d'un groupe sur un ensemble* permet de redéfinir les concepts de codes équivalents et de groupe de

permutations en termes qui existent déjà dans le langage des groupes, et elle peut être utilisée aussi pour montrer d'autres propriétés telles que le nombre des codes équivalents à un code donné et l'ordre du groupe de permutations d'un code.

Dans toute cette section, notons par $\mathbb{C}(n,q)$ l'ensemble de tous les codes de longueur n sur un corps fini $\mathbb{F}_q$. C'est un ensemble fini d'ordre $2^{q^n}-1$.

Vu la remarque 2.1.1, le groupe symétrique S_n opère sur $\mathbb{F}_q^n$ de manière naturelle en permutant les composantes d'un mot via l'application suivante :

$$\begin{array}{rcl} \Phi : S_n \times \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (\sigma, x) & \longmapsto & \sigma(x) \end{array} ;$$

avec x et $\sigma(x)$ sont définis comme dans 2.1.1.

On peut étendre l'application Φ en une application $\overline{\Phi}$ définie sur $S_n \times \mathbb{C}(n,q)$ en posant

$$\begin{array}{rcl} \overline{\Phi} : S_n \times \mathbb{C}(n,q) & \longrightarrow & \mathbb{C}(n,q) \\ (\sigma, \mathcal{C}) & \longmapsto & \sigma.\mathcal{C} \end{array} ;$$

où $\sigma.\mathcal{C}$ est la partie

$$\sigma.\mathcal{C} = \sigma(\mathcal{C}) = \left\{\sigma(x) \in \mathbb{F}_q^n \mid x \in \mathcal{C}\right\} = \left\{(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) \mid (x_1, x_2, ..., x_n) \in \mathcal{C}\right\}.$$

Nous avons donc le résultat suivant :

Lemme 2.3.1 *Soit l'application $\overline{\Phi} : S_n \times \mathbb{C}(n,q) \longrightarrow \mathbb{C}(n,q)$ définie par $(\sigma, \mathcal{C}) \longmapsto \sigma.\mathcal{C}$, alors $\overline{\Phi}$ est une action du groupe symétrique S_n sur $\mathbb{C}(n,q)$, l'ensemble des codes de $\mathbb{F}_q^n$.*

Preuve. C'est exactement ce que la remarque 2.1.2 affirme. ■

Étant définie l'action $\overline{\Phi}$, on peut profiter de toute la terminologie de la sous-section 1.1.3 du chapitre premier. Ainsi la relation d'équivalence associée à cette action est

$$\mathcal{C} \sim \mathcal{D} \Longleftrightarrow \exists\ \sigma \in S_n : \sigma.\mathcal{C} = \mathcal{D} \quad \text{pour } \mathcal{C}, \mathcal{D} \in \mathbb{C}(n,q)$$

qui est exactement la notion de l'équivalence par permutation de deux codes.

L'orbite d'un code $\mathcal{C} \in \mathbb{C}(n,q)$ est l'ensemble $\mathcal{O}(\mathcal{C}) = (S_n)\mathcal{C}$ de tous les codes équivalents par permutation à $\mathcal{C}$:

$$\mathcal{O}(\mathcal{C}) = (S_n)\mathcal{C} = \{\sigma(\mathcal{C}) \mid \sigma \in S_n\},$$

alors que pour $Perm(\mathcal{C})$ le groupe des permutations du code $\mathcal{C}$, on peut énoncer la proposition suivante :

Proposition 2.3.1 *Le groupe $Perm(\mathcal{C})$ des permutations d'un code $\mathcal{C} \in \mathbb{C}(n,q)$ est le stabilisateur $(S_n)_{\mathcal{C}}$ de $\mathcal{C}$ par l'action $\overline{\Phi}$.*

On retrouve une autre fois le fait que $Perm(\mathcal{C})$ est un sous-groupe de S_n (proposition 1.1.2.(i)).

Il est naturel de chercher à calculer le nombre des codes équivalents par permutation à $\mathcal{C}$, c'est-à-dire le cardinal de l'orbite $\mathcal{O}(\mathcal{C})$. Le théorème 1.1.4 et le corollaire 1.1.2 nous apportent la réponse :

$$|(S_n)\mathcal{C}| = |\mathcal{O}(\mathcal{C})| = [S_n : (S_n)_{\mathcal{C}}] = \frac{n!}{|(S_n)_{\mathcal{C}}|} = \frac{n!}{|Perm(\mathcal{C})|}.$$

D'où le théorème suivant :

Théorème 2.3.1 *Soit $\mathcal{C}$ un code de longueur n sur un corps fini $\mathbb{F}_q$. Le nombre des codes équivalents par permutation à $\mathcal{C}$ est l'entier*

$$\frac{n!}{|Perm(\mathcal{C})|}.$$

Exemple 2.3.1 *En se référant à l'exemple 2.1.2, on trouve $|\mathcal{O}(\mathcal{D})| = \frac{3!}{|Perm(\mathcal{C})|} = \frac{6}{2} = 3$ codes équivalents à $\mathcal{D}$.*

Supposons que $\mathcal{C}$ et $\mathcal{D}$ soient deux codes équivalents vérifiant $\sigma.\mathcal{C} = \mathcal{D}$ avec $\sigma \in S_n$. Leurs groupes des permutations sont respectivement $Perm(\mathcal{C})$ et $Perm(\mathcal{D})$. Une relation importante relie ces deux groupes : *ils sont conjugués.*

Proposition 2.3.2 *Soient $\mathcal{C}$ et $\mathcal{D}$ deux codes équivalents tels que $\sigma.\mathcal{C} = \mathcal{D}$, $\sigma \in S_n$. Alors les groupes des permutations $Perm(\mathcal{C})$ et $Perm(\mathcal{D})$ sont conjugués. Plus précisément, on a $Perm(\mathcal{D}) = \sigma Perm(\mathcal{C})\sigma^{-1}$.*

Preuve. C'est une simple application de l'énoncé (ii) de la proposition 1.1.2. ■

Gardons encore cette situation : Les codes $\mathcal{C}$ et $\mathcal{D}$ sont équivalents par permutation tels que $\sigma.\mathcal{C} = \mathcal{D}$, $\sigma \in S_n$. La permutation σ est connue de nous d'une manière ou d'une autre. Une question naturelle vient de se poser par suite en ce qui concerne les permutations $\tau \in S_n$ vérifiant $\tau.\mathcal{C} = \mathcal{D}$, ce sont les permutations qui assurent l'équivalence de $\mathcal{C}$ et $\mathcal{D}$ ou, en d'autres termes, les permutations qui envoient $\mathcal{C}$ vers $\mathcal{D}$. *Peut-on calculer leur nombre ? Qu'elle relation relie ces permutations à la permutation initiale σ ? Qu'elle action exercent-t-elles sur le groupe symétrique S_n ?*

Encore la théorie des groupes est prête pour nous donner des réponses. Dans le but de répondre à cette question (multiple), considérons sur S_n la relation $\mathcal{T}$ définie par :

$$\text{pour } \sigma \text{ et } \tau \text{ dans } S_n : \qquad \sigma \mathcal{T} \tau \Longleftrightarrow \sigma.\mathcal{C} = \tau.\mathcal{C}$$

ce qui est équivalent à dire que les deux permutations σ et τ définissent le même code équivalent à $\mathcal{C}$, qui est $\mathcal{D}$. La relation $\mathcal{T}$ ainsi définie est une relation d'équivalence dans S_n. Notons par $[\sigma]$ la classe d'équivalence de $\sigma \in S_n$

$$[\sigma] = \{\tau \in S_n \mid \tau \mathcal{T} \sigma\},$$

et par $S_n/\mathcal{T}$ l'ensemble quotient de S_n par la relation $\mathcal{T}$.

Nous avons

$$\begin{aligned} \sigma \mathcal{T} \tau &\Longleftrightarrow \sigma.\mathcal{C} = \tau.\mathcal{C} \\ &\Longleftrightarrow (\sigma^{-1}\tau).\mathcal{C} = \mathcal{C} \\ &\Longleftrightarrow (\sigma^{-1}\tau) \in Perm(\mathcal{C}) \\ &\Longleftrightarrow \sigma Perm(\mathcal{C}) = \tau Perm(\mathcal{C}) \end{aligned}$$

Cette équivalence permet de définir une application de l'ensemble $S_n/\mathcal{T}$ dans l'ensemble $S_n/Perm(\mathcal{C})$ des classes latérales à gauche modulo $Perm(\mathcal{C})$ comme suit :

$$\begin{aligned} T : S_n/\mathcal{T} &\longrightarrow S_n/Perm(\mathcal{C}) \\ [\sigma] &\longmapsto \sigma Perm(\mathcal{C}) \end{aligned}$$

Cette application est bien une bijection, ce qui permet de conclure que $|S_n/\mathcal{T}| = |S_n/Perm(\mathcal{C})|$,

$$\begin{aligned} |S_n/\mathcal{T}| &= |S_n/Perm(\mathcal{C})| \\ &= [S_n : Perm(\mathcal{C})] \\ &= \tfrac{n!}{|Perm(\mathcal{C})|} \qquad \text{(Théorème de Lagrange 1.1.2)} \end{aligned}$$

Le cardinal de $S_n/\mathcal{T}$ est le même que celui des codes équivalents à $\mathcal{C}$. Cela veut dire que **la partition de S_n relativement à la relation $\mathcal{T}$ est essentiellement (à bijection près) la même que celle de S_n relativement au sous-groupe $Perm(\mathcal{C})$.**

Maintenant passons à calculer le cardinal de la classe $[\sigma]$ contenant toutes les permutations qui définissent le même code équivalent $\sigma.\mathcal{C} = \mathcal{D}$ à $\mathcal{C}$ que la permutation σ. La relation

$$\sigma.\mathcal{C} = \tau.\mathcal{C} \Leftrightarrow \tau^{-1}\sigma \in Perm(\mathcal{C})$$

conduit à définir l'application

$$\begin{aligned} f : [\sigma] &\longrightarrow Perm(\mathcal{C}) \\ \tau &\longmapsto \tau^{-1}\sigma \end{aligned}$$

L'application f est bijective :

- $f(\tau) = f(\rho) \Leftrightarrow \tau^{-1}\sigma = \rho^{-1}\sigma \Leftrightarrow \tau = \rho$, ainsi f est injective ;
- pour $\omega \in Perm(\mathcal{C})$, la permutation $\sigma\omega^{-1}$ appartient à $[\sigma]$ et vérifie $f(\ \sigma\omega^{-1}) = (\sigma\omega^{-1})^{-1}\sigma = \omega\sigma^{-1}\sigma = \omega$ et f est surjective.

Enfin les ensembles $[\sigma]$ et $Perm(\mathcal{C})$ ont le même cardinal : $|[\sigma]| = |Perm(\mathcal{C})|$.

Ce qui vient d'être prouvé confirme le théorème suivant :

Théorème 2.3.2 *Soient $\mathcal{C}$ un code de longueur n sur un corps fini $\mathbb{F}_q$ et $\mathcal{T}$ la relation d'équivalence sur S_n définie par : $\sigma\mathcal{T}\tau \iff \sigma.\mathcal{C} = \tau.\mathcal{C}$ pour σ, τ de S_n.*

1. *Si $[\sigma]$ est la classe des permutations définissant le même code $\sigma.\mathcal{C}$ équivalent à $\mathcal{C}$, alors $|[\sigma]| = |Perm(\mathcal{C})|$.*

2. *Le cardinal de l'ensemble quotient $S_n/\mathcal{T}$ est $\frac{n!}{|Perm(\mathcal{C})|}$.*

Exemple 2.3.2 *En se reportant à l'exemple 2.1.2, nous avons $\mathcal{D} = \{000, 100, 001, 101\}$ code de $\mathbb{F}_2^3$ et soit $\sigma = (123) \in S_3$. Alors nous obtenons $[(123)] = \{(123), (12)\}$ de cardinal 2 égal au cardinal de $Perm(\mathcal{D}) = \{id, (13)\}$, de plus $S_n/\mathcal{T} = \{[id], [(123)], [(132)]\}$ de cardinal $3 = \frac{3!}{|Perm(\mathcal{C})|} = \frac{6}{2} = 3$.*

2.4 Détermination de l'équivalence

Le problème de détermination de l'équivalence de deux codes correcteurs de même longueur consiste à répondre aux deux questions suivantes :

Première question : on donne deux codes correcteurs de même longueur sur un corps fini, comment savoir s'ils sont équivalents par permutation ou non ? Cette question fut étudiée par Petrank et Roth [30]. Comme résultat, ils ont montré que répondre à cette question est un problème au moins aussi difficile que le problème de l'isomorphisme des graphes.

Deuxième question : la deuxième question est de trouver la permutation qui envoie un code correcteur à un autre code, sachant que ces deux codes sont équivalents. Une tentative de répondre à cette question est donnée par le travail de Nicolas Sendrier dans [34] et [35] en utilisant la notion de *signature* : propriété relative à une position d'un code.

Dans cette section, nous exposons les définitions et les notations concernant le code poinçonné et la signature. Nous examinons spécifiquement un cas particulier où la signature vérifie une condition (être non discriminante en un nombre suffisant de positions), sous laquelle la permutation définissant l'équivalence peut être calculée.

2.4.1 Code poinçonné

Pour se servir de la notion de signature, Nicolas Sendrier (dans [34] et [35]) donne la définition de code poinçonné suivante : Soient $\mathcal{C}$ un code de longueur n sur un corps fini $\mathbb{F}_q$, et i un entier de l'ensemble $\{1, 2, ..., n\}$ des indices des coordonnées des mots de $\mathbb{F}_q^n$.

Définition 2.4.1 *Le code $\mathcal{C}$ poinçonné en la position i est la partie de $\mathbb{F}_q^n$ constituée de tous les mots de $\mathcal{C}$ en remplaçant toutes les i-ème coordonnées par zéro $0 \in \mathbb{F}_q$.*

C'est-à-dire l'ensemble

$$\left\{(x_1, x_2, ..., x_{i-1}, 0, x_{i+1}, ..., x_n) \in \mathbb{F}_q^n \mid \exists\ (x_1, x_2, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n) \in \mathcal{C}\right\}.$$

Notation 2.4.1 *Le code $\mathcal{C}$ poinçonné en la position i est noté $\mathcal{C}_i$*

$$\mathcal{C}_i = \left\{(x_1, x_2, ..., x_{i-1}, 0, x_{i+1}, ..., x_n) \in \mathbb{F}_q^n \mid \exists\ (x_1, x_2, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n) \in \mathcal{C}\right\}$$

Exemple 2.4.1 *Soit le code $\mathcal{C} = \{110, 011, 111\} \subset \mathbb{F}_2^3$, alors nous avons $\mathcal{C}_1 = \{010, 011\}$, $\mathcal{C}_2 = \{100, 001, 101\}$ et $\mathcal{C}_3 = \{110, 010\}$.*

Remarque 2.4.1 *Dans la définition traditionnelle (voir par exemple [23]) d'un code poinçonné, la position i est supprimée, et le code résultant est de longueur $n - 1$:*

$$\mathcal{C}_i = \left\{(x_1, x_2, ..., x_{i-1}, x_{i+1}, ..., x_n) \in \mathbb{F}_q^n \mid \exists (x_1, x_2, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n) \in \mathcal{C}\right\}.$$

La définition adoptée laisse la longueur invariante, ce qui permet de travailler dans le même espace $\mathbb{F}_q^n$. De plus les mots $(x_1, x_2, ..., x_{i-1}, 0, x_{i+1}, ..., x_n)$ et $(x_1, x_2, ..., x_{i-1}, x_{i+1}, ..., x_n)$ peuvent être identifiés à un isomorphisme près (selon la structure d'espace vectoriel de $\mathbb{F}_q^n$ poinçonné en i et $\mathbb{F}_q^{n-1}$).

Nous allons donner une définition équivalente à celle qui précède, mais plus parlante et qui permet de vérifier facilement certaines propriétés des codes poinçonnés.

Pour i un entier de l'ensemble $\{1, 2, ..., n\}$, soit l'application $\boldsymbol{P}_i$ définie comme suit :

$$\begin{array}{rccc} \boldsymbol{P}_i : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & x & \longmapsto & x - x_i e_i \end{array}$$

avec $x = (x_1, x_2, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n)$ dans la base canonique standard de $\mathbb{F}_q^n$:

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

Nous obtenons donc la définition suivante, qui est équivalente à la définition 2.4.1.

Définition 2.4.2 *Soit $\mathcal{C}$ un code de longueur n sur $\mathbb{F}_q$. Le code $\mathcal{C}$ poinçonné en la position i est l'image directe de $\mathcal{C}$ par l'application $\boldsymbol{P}_i$.*

C'est donc la partie $\mathcal{C}_i = \boldsymbol{P}_i(\mathcal{C})$.

Proposition 2.4.1 *Soient $\mathcal{C}$ et $\mathcal{D}$ deux codes de longueur n sur un corps fini $\mathbb{F}_q$.*

1. *Si $\mathcal{C}$ est un code linéaire, alors le code $\mathcal{C}_i$ est aussi linéaire.*
2. *Pour i,$j \in \{1, 2, ..., n\}$, on a $(\mathcal{C}_i)_j = (\mathcal{C}_j)_i$.*
3. *$(\mathcal{C} + \mathcal{D})_i = \mathcal{C}_i + \mathcal{D}_i$.*

Preuve. La démonstration repose sur les propriétés de l'application

$$\boldsymbol{P}_i : x \in \mathbb{F}_q^n \longmapsto \boldsymbol{P}_i(x) = x - x_i e_i.$$

En effet :

– *Pour 1.* $\mathcal{C}_i = \boldsymbol{P}_i(\mathcal{C})$ est linéaire comme image d'un code linéaire $\mathcal{C}$ par une application linéaire $\boldsymbol{P}_i$;

– *Pour 2.* si i et j sont dans $\{1, 2, ..., n\}$ et $x \in \mathbb{F}_q^n$, nous avons

$$\boldsymbol{P}_i \circ \boldsymbol{P}_j(x) = x - x_j e_j - x_i e_i = x - x_i e_i - x_j e_j = \boldsymbol{P}_j \circ \boldsymbol{P}_i(x)$$

Cela montre que $\boldsymbol{P}_i \circ \boldsymbol{P}_j = \boldsymbol{P}_j \circ \boldsymbol{P}_i$ et les applications $\boldsymbol{P}_i$ et $\boldsymbol{P}_j$ commutent, ainsi

$$(\mathcal{C}_j)_i = \boldsymbol{P}_i \circ \boldsymbol{P}_j(\mathcal{C}) = \boldsymbol{P}_j \circ \boldsymbol{P}_i(\mathcal{C}) = (\mathcal{C}_i)_j$$

– *Pour 3.* Soient $x \in \mathcal{C}$ et $y \in \mathcal{D}$, alors $\boldsymbol{P}_i(x+y) = \boldsymbol{P}_i(x) + \boldsymbol{P}_i(y)$ par linéarité de $\boldsymbol{P}_i$, ce qui entraîne que $(\mathcal{C}+\mathcal{D})_i = \mathcal{C}_i + \mathcal{D}_i$. ■

Notation 2.4.2 *À cause de la deuxième propriété* $(\mathcal{C}_i)_j = (\mathcal{C}_j)_i$*, on écrit simplement* $\mathcal{C}_{\{i,j\}}$*. Cela nous permet de définir le code* $\mathcal{C}_{\{i_1,i_2,...,i_s\}}$*, c'est-à-dire* $\mathcal{C}$ *poinçonné aux positions* $i_1, i_2, ..., i_s \in \{1, 2, ..., n\}$.

Passons maintenant à l'étude de la relation entre équivalence par permutation des codes et poinçonnage en une position.

Si σ est une permutation du groupe symétrique S_n et $i \in \{1, 2, ..., n\}$, alors pour tout $x \in \mathbb{F}_q^n$ nous avons

$$\sigma \circ \boldsymbol{P}_i(x) = \sigma(x - x_i e_i) = \sigma(x_1, x_2, ..., x_{i-1}, 0, x_{i+1}, ..., x_n) = \sigma(x_1, x_2, ..., x_{i-1}, a_i, x_{i+1}, ..., x_n)$$

avec $a_i = 0$. Par suite

$$\sigma \circ \boldsymbol{P}_i(x) = (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(i-1)}, a_{\sigma(i)}, x_{\sigma(i+1)}, ..., x_{\sigma(n)})$$

La permutation σ change les positions sans avoir changé leurs valeurs, par conséquent il existe une position $j \in \{1, 2, ..., n\}$ telle que $\sigma(j) = i$ et telle que la valeur $a_i = 0$ de la position i soit transférée à la position $j = \sigma^{-1}(i)$. Ce qui revient à calculer tout d'abord

$$\sigma(x_1, x_2, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(i-1)}, x_{\sigma(i)}, x_{\sigma(i+1)}, ..., x_{\sigma(n)})$$

puis le poinçonner en la position $j = \sigma^{-1}(i)$, c'est-à-dire calculer $\boldsymbol{P}_{\sigma^{-1}(i)} \circ \sigma(x)$. Donc on peut affirmer que

$$\sigma \circ \boldsymbol{P}_i(x) = \boldsymbol{P}_{\sigma^{-1}(i)} \circ \sigma(x)$$

Si de plus $\mathcal{C}$ est un code de longueur n, on peut énoncer la proposition suivante :

Proposition 2.4.2 *Soient $\mathcal{C}$ un code de longueur n sur un corps fini $\mathbb{F}_q$ et σ une permutation de S_n. Pour tout $i \in \{1, 2, ..., n\}$, on a*

$$\sigma(\mathcal{C}_i) = \sigma(\mathcal{C})_{\sigma^{-1}(i)}.$$

c'est-à-dire que si $\mathcal{C}$ et $\mathcal{D}$ sont deux codes équivalents par σ, alors les deux codes $\mathcal{C}_i$ et $(\mathcal{D})_{\sigma^{-1}(i)}$ sont aussi équivalents par σ.

2.4.2 Signature

La notion de signature est une propriété locale d'un code et une position, qui ne change pas lorsqu'on fait agir une permutation sur le code et la position. Elle a été introduite par Nicolas Sendrier dans [34] et [35] dans le but de déterminer l'équivalence de deux codes correcteurs. Dans cette section, nous allons donner les définitions et les propriétés élémentaires de signature, expliquer et prouver des relations relatives à l'équivalence par permutations et le groupe de permutations des codes. Nous finirons cette section en étudiant un cas particulier de signature associée à un code où la signature vérifie une certaine condition sous laquelle la permutation de l'équivalence peut être calculée.

Avant de commencer, nous allons spécifier quelques remarques et notations que nous allons prendre en considération seulement pour cette section. Rappelons que pour $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_q^n$ et pour $\sigma \in S_n$, nous avons posé

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

et si $\mathcal{C}$ est un code de longueur n, le code équivalent par σ est le code

$$\sigma(\mathcal{C}) = \left\{\sigma(x) \in \mathbb{F}_q^n \mid x \in \mathcal{C}\right\} = \left\{(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) \mid (x_1, x_2, ..., x_n) \in \mathcal{C}\right\}.$$

Nous avons adopté cette définition car elle nous a permis d'utiliser des outils issus de la théorie des groupes (théorème de Lagrange, action d'un groupe sur un ensemble, etc.) dans le but de montrer des propriétés intéressantes des codes équivalents et du groupe des permutations d'un code (section 2.3), alors que la définition traditionnelle (utilisée par Sendrier

dans [34] et [35]et MacWilliams dans [23]) de $\sigma(x)$ et $\sigma(\mathcal{C})$ est

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

avec

$$\sigma(\mathcal{C}) = \left\{\sigma(x) \in \mathbb{F}_q^n \mid x \in \mathcal{C}\right\} = \left\{(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, ..., x_{\sigma^{-1}(n)}) \mid (x_1, x_2, ..., x_n) \in \mathcal{C}\right\}.$$

Cette dernière ne permet pas de définir une action à gauche du groupe symétrique S_n sur les ensembles $\mathbb{F}_q^n$ et $\mathbb{C}(n,q)$, l'ensemble des codes de $\mathbb{F}_q^n$, car $(\sigma\tau)(x) \neq \sigma(\tau(x))$ et $(\sigma\tau)(\mathcal{C}) \neq \sigma(\tau(\mathcal{C}))$. D'autre part la définition adoptée donne la relation

$$\sigma(\mathcal{C}_i) = \sigma(\mathcal{C})_{\sigma^{-1}(i)}.$$

qui ne peut être compatible avec la définition de signature à cause de l'indice $\sigma^{-1}(i)$ dans $\sigma(\mathcal{C})_{\sigma^{-1}(i)}$ (voir la définition de signature 2.4.3), alors que la définition traditionnelle l'est.

Remarquons aussi que ces deux définitions sont équivalentes dans le sens

$$\sigma(x) = (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) = y \Longleftrightarrow x = \sigma^{-1}(y) = (y_{\sigma^{-1}(1)}, y_{\sigma^{-1}(2)}, ..., y_{\sigma^{-1}(n)})$$

et

$$\sigma(\mathcal{C}) = \mathcal{D} \Longleftrightarrow \mathcal{C} = \sigma^{-1}(\mathcal{D}),$$

qui veut dire qu'agir σ sur x (resp. $\mathcal{C}$) selon la définition traditionnelle est le même qu'agir σ^{-1} selon la définition adoptée. Pour cette fin, nous convenons de noter

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

et

$$\mathcal{C}^\sigma = \left\{x^\sigma \in \mathbb{F}_q^n \mid x \in \mathcal{C}\right\} = \left\{(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, ..., x_{\sigma^{-1}(n)}) \mid (x_1, x_2, ..., x_n) \in \mathcal{C}\right\}.$$

pour $\sigma \in S_n$, $x \in \mathbb{F}_q^n$ et $\mathcal{C} \in \mathbb{C}(n,q)$. Cette convention permet de conclure :

Proposition 2.4.3 *Soient $\mathcal{C}$ un code de longueur n sur un corps fini $\mathbb{F}_q$ et σ une permutation de S_n. Pour tout $i \in \{1, 2, ..., n\}$, on a*

$$(\mathcal{C}_i)^\sigma = (\mathcal{C}^\sigma)_{\sigma(i)}.$$

La démonstration de la proposition est la même que celle de la proposition 2.4.2.

Soit E un ensemble non vide. $\mathbb{C}(n, q)$ est l'ensemble des codes de $\mathbb{F}_q^n$.

Définition 2.4.3 *[34] Une signature $\mathcal{S}$ sur E est une application qui à tout code $\mathcal{C} \in \mathbb{C}(n, q)$ et tout élément $i \in \{1, 2, ..., n\}$ associe un élément $\mathcal{S}(\mathcal{C}, i)$ de E telle que*

$$\forall \sigma \in S_n \quad \mathcal{S}(\mathcal{C}^\sigma, \sigma(i)) = \mathcal{S}(\mathcal{C}, i).$$

De manière plus formelle,

$$\begin{array}{rccc} \mathcal{S}: & \mathbb{C}(n,q) \times \{1,2,...,n\} & \longrightarrow & E \\ & (\mathcal{C}, i) & \longmapsto & \mathcal{S}(\mathcal{C}, i) \end{array}$$

telle que

$$\forall \sigma \in S_n \quad \mathcal{S}(\mathcal{C}^\sigma, \sigma(i)) = \mathcal{S}(\mathcal{C}, i).$$

Exemple 2.4.2 *Rappelons que pour un code $\mathcal{C} \in \mathbb{C}(n, q)$, la notation $W_{\mathcal{C}}(X)$ désigne le polynôme énumérateur des poids du code $\mathcal{C}$ et $\mathcal{C}_i$ le code $\mathcal{C}$ poinçonné en i. Un exemple de signature est donné par l'application*

$$\begin{array}{rccc} \mathcal{S}: & \mathbb{C}(n,q) \times \{1,2,...,n\} & \longrightarrow & E \\ & (\mathcal{C}, i) & \longmapsto & \mathcal{S}(\mathcal{C}, i) = W_{\mathcal{C}_i}(X) \end{array}$$

nous avons pour $\sigma \in S_n$,

$$\mathcal{S}(\mathcal{C}^\sigma, \sigma(i)) = W_{(\mathcal{C}^\sigma)_{\sigma(i)}}(X) = W_{(\mathcal{C}_i)^\sigma}(X) = W_{\mathcal{C}_i}(X) = \mathcal{S}(\mathcal{C}, i),$$

La deuxième égalité résulte de la proposition 2.4.3 et la troisième de la proposition 2.2.4.

Définition 2.4.4 *Une signature* $\mathcal{S} : \mathbb{C}(n,q) \times \{1,2,...,n\} \longrightarrow E$ *est dite totalement discriminante relativement à* $\mathcal{C} \in \mathbb{C}(n,q)$ *si*

$$\mathcal{S}(\mathcal{C},i) \neq \mathcal{S}(\mathcal{C},j) \quad \textit{pour tout } i \neq j \textit{ dans } \{1,2,...,n\}\,.$$

Ce qui revient au même que de dire que l'application partielle

$$\begin{array}{rccl} \mathcal{S}_{\mathcal{C}} : & \{1,2,...,n\} & \longrightarrow & E \\ & i & \longmapsto & \mathcal{S}_{\mathcal{C}}(i) = \mathcal{S}(\mathcal{C},i) \end{array}$$

est injective.

La définition d'une signature totalement discriminante relativement à un code $\mathcal{C} \in \mathbb{C}(n,q)$ fait appel à de nombreuses questions qui se posent naturellement, à titre d'exemples : cette signature est-elle *aussi* totalement discriminante relativement à un code $\mathcal{D} = \mathcal{C}^\sigma$ équivalent par permutation à $\mathcal{C}$? Quel est le groupe de permutations $Perm(\mathcal{C})$ (et par suite $Perm(\mathcal{D})$) de $\mathcal{C}$ (de $\mathcal{D}$) ? Et enfin peut-on déterminer la permutation σ assurant l'équivalence de $\mathcal{C}$ et $\mathcal{D} = \mathcal{C}^\sigma$. La réponse à ces questions est apportée par le théorème suivant :

Théorème 2.4.1 *Soient* $\mathcal{C}$ *et* $\mathcal{D}$ *deux codes équivalents de longueur* n *sur un corps fini* $\mathbb{F}_q$. *Si* $\mathcal{S}$ *est une signature totalement discriminante relativement à* $\mathcal{C}$, *alors*

1. *Le groupe de permutations* $Perm(\mathcal{C})$ *de* $\mathcal{C}$ *est trivial, i.e. réduit à l'élément neutre,*
2. $\mathcal{S}$ *est aussi une signature totalement discriminante relativement à* $\mathcal{D}$,
3. *Si* $\mathcal{D} = \mathcal{C}^\sigma$ *pour* $\sigma \in S_n$, *alors* σ *peut être déterminée et elle est unique.*

Preuve. Par hypothèse, $\mathcal{S}$ est une signature totalement discriminante relativement à $\mathcal{C}$, alors

1. Si $\sigma \in Perm(\mathcal{C})$, on a d'une part

$$\forall i \in \{1,2,...,n\} \quad \mathcal{S}(\mathcal{C}^\sigma, \sigma(i)) = \mathcal{S}(\mathcal{C},i)$$

et d'autre part puisque $\sigma \in Perm(\mathcal{C})$

$$\mathcal{S}(\mathcal{C}^\sigma, \sigma(i)) = \mathcal{S}(\mathcal{C}, \sigma(i))$$

cela entraîne

$$\forall i \in \{1, 2, ..., n\} \quad \sigma(i) = i$$

et σ est l'identité de S_n

2. Soient $i, j \in \{1, 2, ..., n\}$ tels que $\mathcal{S}(\mathcal{D}, i) = \mathcal{S}(\mathcal{D}, j)$. Comme σ est une permutation, il existe a, $b \in \{1, 2, ..., n\}$ qui vérifient $\sigma(a) = i$ et $\sigma(b) = j$. Compte tenu du fait que $\mathcal{D} = \mathcal{C}^\sigma$, nous avons alors

$$\begin{array}{lll} \mathcal{S}(\mathcal{D}, i) = \mathcal{S}(\mathcal{D}, j) & \Longleftrightarrow & \mathcal{S}(\mathcal{C}^\sigma, \sigma(a)) = \mathcal{S}(\mathcal{C}^\sigma, \sigma(b)) \\ & \Longleftrightarrow & \mathcal{S}(\mathcal{C}, a) = \mathcal{S}(\mathcal{C}, b) \qquad \mathcal{S} \text{ est signature} \\ & \Longleftrightarrow & a = b \qquad \mathcal{S} \text{ totalement discriminante pour } \mathcal{C} \\ & \Longleftrightarrow & \sigma(a) = \sigma(b) \qquad \sigma \text{ est permutation} \\ & \Longleftrightarrow & i = j \end{array}$$

Cela prouve que $\mathcal{S}$ est aussi totalement discriminante pour $\mathcal{D} = \mathcal{C}^\sigma$,

3. Soient respectivement les ensembles A et B des valeurs $\mathcal{S}(\mathcal{C}, i)$ et $\mathcal{S}(\mathcal{D}, j)$. Pour tout $i, j \in \{1, 2, ..., n\}$:

$$A = \{\mathcal{S}(\mathcal{C}, i) \mid i \in \{1, 2, ..., n\}\}$$
$$B = \{\mathcal{S}(\mathcal{D}, j) \mid j \in \{1, 2, ..., n\}\}$$

$\mathcal{S}$ est une signature totalement discriminante relativement à $\mathcal{C}$ et $\mathcal{D}$, il en résulte que chaque ensemble A et B est de cardinal n. Comme les codes $\mathcal{C}$ et $\mathcal{D}$ sont équivalents et $\mathcal{D} = \mathcal{C}^\sigma$, nous pouvons écrire

$$\forall i \in \{1, 2, ..., n\} \quad \mathcal{S}(\mathcal{C}, i) = \mathcal{S}(\mathcal{C}^\sigma, \sigma(i)) = \mathcal{S}(\mathcal{D}, \sigma(i)) \qquad (\star)$$

De plus, l'équivalence de $\mathcal{C}$ et $\mathcal{D}$ implique que $A = B$, ce qui montre

$$\exists j \in \{1, 2, ..., n\} \text{ unique tel que } \mathcal{S}(\mathcal{C}, i) = \mathcal{S}(\mathcal{D}, j) \qquad (\star\star)$$

La conjonction de $(\star)$ et $(\star\star)$, en remarquant que $\mathcal{S}$ est totalement discriminante pour $\mathcal{D}$, nous montre que

$$\sigma(i) = j$$

La permutation σ est ainsi déterminée pour tout $i \in \{1, 2, ..., n\}$.

L'unicité de σ provient du fait que $Perm(\mathcal{C})$ est trivial et du théorème 2.3.2. ■

Exemple 2.4.3 *Considérons les deux codes binaires de longueur* 3 *suivants :*

$$\mathcal{C} = \{100, 101, 011\}$$

et

$$\mathcal{D} = \{001, 011, 110\}\,.$$

Comme signature nous prenons $\mathcal{S}(\mathcal{U}, i) = W_{\mathcal{U}_i}(X)$*, le polynôme énumérateur des poids du code* $\mathcal{U}_i$*, le code* $\mathcal{U}$ *poinçonné en* i*. Nous avons alors*

$$\begin{array}{lcl} \mathcal{C}_1 = \{000, 001, 011\} & \longrightarrow & \mathcal{S}(\mathcal{C}, 1) = 1 + X + X^2 \\ \mathcal{C}_2 = \{100, 101, 001\} & \longrightarrow & \mathcal{S}(\mathcal{C}, 2) = 2X + X^2 \\ \mathcal{C}_3 = \{100, 010\} & \longrightarrow & \mathcal{S}(\mathcal{C}, 3) = 2X \end{array}$$

La signature $\mathcal{S}$ *est une signature totalement discriminante relativement à* $\mathcal{C}$*,*

Pour $\mathcal{D}$*, nous avons*

$$\begin{array}{lcl} \mathcal{D}_1 = \{001, 011, 010\} & \longrightarrow & \mathcal{S}(\mathcal{D}, 1) = 2X + X^2 \\ \mathcal{D}_2 = \{001, 100\} & \longrightarrow & \mathcal{S}(\mathcal{D}, 2) = 2X \\ \mathcal{D}_3 = \{000, 010, 110\} & \longrightarrow & \mathcal{S}(\mathcal{D}, 3) = 1 + X + X^2 \end{array}$$

La signature $\mathcal{S}$ *est aussi totalement discriminante relativement à* $\mathcal{D}$*.*

En comparant les valeurs des signatures pour $\mathcal{C}$ *et* $\mathcal{D}$*, on trouve que*

$$\begin{array}{rcl} \mathcal{S}(\mathcal{C}, 2) & = & \mathcal{S}(\mathcal{D}, 1) \\ \mathcal{S}(\mathcal{C}, 3) & = & \mathcal{S}(\mathcal{D}, 2) \\ \mathcal{S}(\mathcal{C}, 1) & = & \mathcal{S}(\mathcal{D}, 3) \end{array}$$

et par suite la permutation σ est le cycle (132). *Une vérification immédiate montre que*

$$\begin{aligned}\mathcal{C}^\sigma &= \left\{(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)}) \mid (x_1, x_2, x_3) \in \mathcal{C}\right\} \\ &= \{(x_2, x_3, x_1) \mid (x_1, x_2, x_3) \in \mathcal{C}\} \\ &= \mathcal{D}.\end{aligned}$$

Remarquons aussi que $Perm(\mathcal{C}) = Perm(\mathcal{D})$ sont triviaux.

CAS PARTICULIER

Le théorème 2.4.1 permet de calculer la permutation entre deux codes équivalents dans le cas où la signature considérée est totalement discriminante. Notons que dans le cas où le groupe de permutations du code est *non trivial*, une telle signature *n'existe pas*. Toutes ces remarques nous ont incités à examiner un cas particulier où la signature n'est pas totalement discriminante.

Soient comme précédemment deux codes correcteurs équivalents $\mathcal{C}$ et $\mathcal{D} = \mathcal{C}^\sigma$ de $\mathbb{C}(n, q)$, $\sigma \in S_n$. Supposons qu'on ait une signature

$$\begin{array}{rccl}\mathcal{S}: & \mathbb{C}(n,q) \times \{1, 2, ..., n\} & \longrightarrow & E \\ & (\mathcal{C}, i) & \longmapsto & \mathcal{S}(\mathcal{C}, i)\end{array}$$

où E est un ensemble non vide. Supposons en outre que la signature $\mathcal{S}$ vérifie la condition suivante :

$$\left\{\begin{array}{l} \exists\ i_1, i_2, ..., i_s \in \{1, 2, ..., n\} \text{ distincts}, \quad 2 \leq s \leq n-2, \text{ tels que} \\ \qquad\qquad \mathcal{S}(\mathcal{C}, i_1) = \mathcal{S}(\mathcal{C}, i_2) = ... = \mathcal{S}(\mathcal{C}, i_s) \\ \text{et si } \ i, j \in \{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_s\} \text{ distincts}, \qquad \mathcal{S}(\mathcal{C}, i) \neq \mathcal{S}(\mathcal{C}, j) \end{array}\right. \qquad (\divideontimes)$$

Cela veut dire que la signature $\mathcal{S}$ ne discrimine pas les positions $i_1, i_2, ...,$ et i_s de $\{1, 2, ..., n\}$ et que l'application partielle

$$\begin{array}{rccl}\mathcal{S}_\mathcal{C}: & \{1, 2, ..., n\} & \longrightarrow & E \\ & i & \longmapsto & \mathcal{S}_\mathcal{C}(i) = \mathcal{S}(\mathcal{C}, i)\end{array}$$

est injective sur la partie $\{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_s\}$.

Sur $\{1, 2, ..., n\}$, on peut définir une relation $\mathcal{R}_\mathcal{C}$ par :

$$\text{Pour } i, j \in \{1, 2, ..., n\}, \quad i \ \mathcal{R}_\mathcal{C} \ j \Leftrightarrow \mathcal{S}(\mathcal{C}, i) = \mathcal{S}(\mathcal{C}, j)$$

La relation $\mathcal{R}_\mathcal{C}$ est une relation d'équivalence car elle est la relation associée à l'application partielle $\mathcal{S}_\mathcal{C}$. Sous la condition $(\divideontimes)$, l'ensemble quotient $\{1, 2, ..., n\} / \mathcal{R}_\mathcal{C}$ est

$$\left\{ \{i_1, i_2, ..., i_s\}, \{i\}_{i \in \{1,2,...,n\} \setminus \{i_1, i_2, ..., i_s\}} \right\}.$$

Comme les codes $\mathcal{C}$ et $\mathcal{D} = \mathcal{C}^\sigma$ sont équivalents, la signature $\mathcal{S}$ agit avec le code $\mathcal{D}$ de la même manière qu'avec $\mathcal{C}$, elle ne discrimine pas s positions, ce sont les images $\{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\}$ de $\{i_1, i_2, ..., i_s\}$ par σ. De plus, si on fait agir $Perm(\mathcal{C})$ (et de même $Perm(\mathcal{D})$) sur $\{i_1, i_2, ..., i_s\}$ (respectivement $\{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\}$) de façon naturelle, cette partie restera stable, c'est-à-dire,

$$\forall \tau \in Perm(\mathcal{C}), \tau(\{i_1, i_2, ..., i_s\}) \subset \{i_1, i_2, ..., i_s\}.$$

En résumé, le théorème suivant a lieu :

Théorème 2.4.2 *Soient $\mathcal{C}$ et $\mathcal{D}$ deux codes correcteurs de $\mathbb{C}(n, q)$ et $\mathcal{S}$ une signature qui vérifie la condition $(\divideontimes)$. Alors,*

1. *La partie $\{i_1, i_2, ..., i_s\}$ est stable sous l'action naturelle du groupe $Perm(\mathcal{C})$,*
2. *Si $\mathcal{D} = \mathcal{C}^\sigma$ pour une permutation $\sigma \in S_n$, alors la signature $\mathcal{S}$ vérifie la même condition $(\divideontimes)$ avec $\mathcal{D}$ et la partie $\{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\}$.*

Preuve. Les hypothèses du théorème étant supposées vraies, nous avons donc :

1. Si $\tau \in Perm(\mathcal{C})$, alors
$$\mathcal{S}(\mathcal{C}, i) = \mathcal{S}(\mathcal{C}, \tau(i)) \qquad (i)$$
c'est-à-dire que
$$\forall \ i \in \{1, 2, ..., n\}, \quad i \ \mathcal{R}_\mathcal{C} \ \tau(i)$$

De plus

$$\mathcal{S}(\mathcal{C}, i_1) = \mathcal{S}(\mathcal{C}, i_2) = ... = \mathcal{S}(\mathcal{C}, i_s) \qquad (ii)$$

Appliquer (i) à (ii) nous donne

$$\begin{aligned}\mathcal{S}(\mathcal{C}, i_1) = \mathcal{S}(\mathcal{C}, i_2) = ... = \mathcal{S}(\mathcal{C}, i_s) \\ = \mathcal{S}(\mathcal{C}, \tau(i_1)) = \mathcal{S}(\mathcal{C}, \tau(i_2)) = ... = \mathcal{S}(\mathcal{C}, \tau(i_s))\end{aligned}$$

Ce qui montre que si $\tau \in Perm(\mathcal{C})$, alors $\tau(\{i_1, i_2, ..., i_s\}) \subset \{i_1, i_2, ..., i_s\}$.

2. $\mathcal{S}$ est une signature et comme $\mathcal{D} = \mathcal{C}^\sigma$ pour une permutation $\sigma \in S_n$, nous pouvons écrire

$$\mathcal{S}(\mathcal{C}, i_a) = \mathcal{S}(\mathcal{C}^\sigma, \sigma(i_a)) = \mathcal{S}(\mathcal{D}, \sigma(i_a)) \text{ pour } i_a \in \{i_1, i_2, ..., i_s\}.$$

Soient maintenant $i, j \in \{1, 2, ..., n\} \setminus \{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\}$ distincts. Il existe t, r distincts de $\{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_s\}$ tels que $i = \sigma(t)$ et $j = \sigma(r)$.

Par suite nous avons,

$$\mathcal{S}(\mathcal{D}, i) = \mathcal{S}(\mathcal{C}^\sigma, \sigma(t)) = \mathcal{S}(\mathcal{C}, t)$$

et

$$\mathcal{S}(\mathcal{D}, j) = \mathcal{S}(\mathcal{C}^\sigma, \sigma(r)) = \mathcal{S}(\mathcal{C}, r).$$

Comme $\mathcal{S}(\mathcal{C}, t) \neq \mathcal{S}(\mathcal{C}, r)$, nous obtenons $\mathcal{S}(\mathcal{D}, i) \neq \mathcal{S}(\mathcal{D}, j)$. ■

Sous les hypothèses du théorème précédent (la condition $(\divideontimes)$ a lieu), il existe au moins une position $i \in \{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_s\}$ qui est discriminée par la signature $\mathcal{S}$ relativement à $\mathcal{C}$, c'est-à-dire si j est une autre position de $\{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_s\}$ distincte de i, alors

$$\mathcal{S}(\mathcal{C}, j) \neq \mathcal{S}(\mathcal{C}, i).$$

La position i étant fixée, soit alors l'application $\Phi_\mathcal{C}$ définie par

$$\begin{aligned}\Phi_\mathcal{C} : \quad \{i_1, i_2, ..., i_s\} &\longrightarrow E \\ a &\longmapsto \mathcal{S}(\mathcal{C}_i, a)\end{aligned}$$

Supposons que les codes $\mathcal{C}$ et $\mathcal{D}$ soient équivalents par permutation et que nous voulons déterminer la permutation $\sigma \in S_n$ qui vérifie $\mathcal{D} = \mathcal{C}^\sigma$. Cela, nous faisons face au problème de détermination de σ.

Si l'application $\Phi_\mathcal{C}$, définie ci-dessus, est injective, alors on peut calculer les images $\sigma(j)$ pour tout $j \in \{1, 2, ..., n\}$. La permutation σ est ainsi déterminée et la proposition suivante a lieu :

Proposition 2.4.4 *Sous les hypothèses du théorème 2.4.2 et si l'application $\Phi_\mathcal{C}$ est injective, alors la permutation σ est bien déterminée.*

Preuve. $\Phi_\mathcal{C}$ est injective, alors

$$\forall a, b \in \{i_1, i_2, ..., i_s\}, \ \ a \neq b \Leftrightarrow \Phi_\mathcal{C}(a) \neq \Phi_\mathcal{C}(b)$$

Le code $\mathcal{D}$ vérifie $\mathcal{D} = \mathcal{C}^\sigma$ pour une permutation $\sigma \in S_n$. De l'égalité

$$\mathcal{S}(\mathcal{C}, i) = \mathcal{S}(\mathcal{C}^\sigma, \sigma(i)) = \mathcal{S}(\mathcal{D}, \sigma(i)) = \mathcal{S}(\mathcal{D}, k)$$

où, selon le théorème 2.4.2, l'entier $k \in \{1, 2, ..., n\} \setminus \{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\}$ est une position discriminée par la signature $\mathcal{S}$ relativement à $\mathcal{D}$, on conclut que

$$k = \sigma(i)$$

l'image de i. On peut montrer que l'application $\Phi_\mathcal{D}$

$$\begin{array}{rccc} \Phi_\mathcal{D} : & \{j_1, j_2, ..., j_s\} & \longrightarrow & E \\ & c & \longmapsto & \mathcal{S}(\mathcal{D}_k, c) \end{array}$$

définie de l'ensemble $\{j_1, j_2, ..., j_s\} = \{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\}$ dans E (de la même manière que l'application $\Phi_\mathcal{C}$) est aussi injective.

Calculons successivement les images

$$\Phi_\mathcal{C}\{i_1, i_2, ..., i_s\} = \{\Phi_\mathcal{C}(i_1), \Phi_\mathcal{C}(i_2), ..., \Phi_\mathcal{C}(i_s)\}$$

et

$$\Phi_{\mathcal{D}}\{j_1, j_2, ..., j_s\} = \{\Phi_{\mathcal{D}}(j_1), \Phi_{\mathcal{D}}(j_2), ..., \Phi_{\mathcal{D}}(j_s)\},$$

puisque $\mathcal{D} = \mathcal{C}^{\sigma}$, nous avons pour $a = i_h$, $1 \leq h \leq s$,

$$\Phi_{\mathcal{C}}(a) = \mathcal{S}(\mathcal{C}_i, a) = \mathcal{S}((\mathcal{C}_i)^{\sigma}, \sigma(a)) = \mathcal{S}(\mathcal{D}_{\sigma(i)}, \sigma(a)) = \mathcal{S}(\mathcal{D}_k, \sigma(a)) = \Phi_{\mathcal{D}}(\sigma(a)),$$

avec $c = \sigma(a) \in \{j_1, j_2, ..., j_s\}$. Cela montre que les deux ensembles $\Phi_{\mathcal{C}}\{i_1, i_2, ..., i_s\}$ et $\Phi_{\mathcal{D}}\{j_1, j_2, ..., j_s\}$ sont égaux. Par suite, en comparant ses éléments, on trouve que $\Phi_{\mathcal{C}}(a)$ égale un élément $\Phi_{\mathcal{D}}(j_r)$:

$$\Phi_{\mathcal{C}}(a) = \Phi_{\mathcal{D}}(j_r).$$

En comparant, on trouve que

$$\Phi_{\mathcal{D}}(\sigma(a)) = \Phi_{\mathcal{D}}(j_r).$$

Compte tenu de l'injectivité de $\Phi_{\mathcal{D}}$ (qui résulte de celle de $\Phi_{\mathcal{C}}$), on conclut que $\sigma(a) = \sigma(i_h) = j_r$, avec $1 \leq h \leq s$. Et ainsi l'image $\sigma(a)$ de $a \in \{i_1, i_2, ..., i_s\}$ par σ est déterminée. Pour $a \in \{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_s\}$, on procède de la même manière que celle suivie pour déterminer l'image de la position discriminée i. Et en conséquence la permutation σ est déterminée. ■

Exemple 2.4.4 *Considérons les deux codes binaires $\mathcal{C}$ et $\mathcal{D}$ de longueur 4 définis par :*

$$\mathcal{C} = \{0110, 0101, 0111, 1010, 1111\}$$

et

$$\mathcal{D} = \{0011, 1010, 1011, 0101, 1111\}.$$

Prenons comme signature :

$$\mathcal{S}(\mathcal{U}, i) = W_{\mathcal{U}_i}(X)$$

le polynôme énumérateur des poids du code $\mathcal{U}_i$*, le code* $\mathcal{U} \in \mathbb{C}(4,2)$ *poinçonné en* i*, pour* $i = 1, 2, 3, 4$*. Un calcul simple nous donne alors,*

$$\begin{array}{lcl}
\mathcal{C}_1 = \{0110, 0101, 0111, 0010\} & \longrightarrow & \mathcal{S}(\mathcal{C}, 1) = X + 2X^2 + X^3 \\
\mathcal{C}_2 = \{0010, 0001, 0011, 1010, 1011\} & \longrightarrow & \mathcal{S}(\mathcal{C}, 2) = 2X + 2X^2 + X^3 \\
\mathcal{C}_3 = \{0100, 0101, 1000, 1101\} & \longrightarrow & \mathcal{S}(\mathcal{C}, 3) = 2X + X^2 + X^3 \\
\mathcal{C}_4 = \{0110, 0100, 1010, 1110\} & \longrightarrow & \mathcal{S}(\mathcal{C}, 4) = X + 2X^2 + X^3
\end{array}$$

Ainsi les positions 1 *et* 4 *ne peuvent être discriminées. Un calcul analogue donne pour le code* $\mathcal{D}$ *et ses codes poinçonnés,*

$$\begin{array}{lcl}
\mathcal{D}_1 = \{0011, 0010, 0101, 0111\} & \longrightarrow & \mathcal{S}(\mathcal{D}, 1) = X + 2X^2 + X^3 \\
\mathcal{D}_2 = \{0011, 1010, 1011, 0001\} & \longrightarrow & \mathcal{S}(\mathcal{D}, 2) = X + 2X^2 + X^3 \\
\mathcal{D}_3 = \{0001, 1000, 1001, 0101, 1101\} & \longrightarrow & \mathcal{S}(\mathcal{D}, 3) = 2X + 2X^2 + X^3 \\
\mathcal{D}_4 = \{0010, 1010, 0100, 1110\} & \longrightarrow & \mathcal{S}(\mathcal{D}, 4) = 2X + X^2 + X^3
\end{array} .$$

On remarque aussi que les positions 1 *et* 2 *ne peuvent être discriminées. On voit aisément que*

$$\begin{array}{l}
\mathcal{S}(\mathcal{C}, 2) = \mathcal{S}(\mathcal{D}, 3) = 2X + 2X^2 + X^3 \\
\mathcal{S}(\mathcal{C}, 3) = \mathcal{S}(\mathcal{D}, 4) = 2X + X^2 + X^3
\end{array} ,$$

ce qui donne

$$\begin{array}{l}
\sigma(2) = 3 \\
\sigma(3) = 4
\end{array} .$$

Choisissons la position discriminée $i = 2$*, pour ce choix* $k = \sigma(i) = 3$*. Introduisons maintenant les applications* $\Phi_{\mathcal{C}}$ *et* $\Phi_{\mathcal{D}}$ *associées à* $\mathcal{C}$ *et* $\mathcal{D}$*:*

$$\begin{array}{rccl}
\Phi_{\mathcal{C}} : & \{1, 4\} & \longrightarrow & \mathbb{Z}[X] \\
 & a & \longmapsto & \mathcal{S}(\mathcal{C}_2, a)
\end{array}$$

et

$$\begin{array}{rccl}
\Phi_{\mathcal{D}} : & \{1, 2\} & \longrightarrow & \mathbb{Z}[X] \\
 & c & \longmapsto & \mathcal{S}(\mathcal{D}_3, c)
\end{array}$$

nous voyons que

$$\Phi_{\mathcal{C}}(1) = \mathcal{S}(\mathcal{C}_2, 1) = 2X + X^2$$
$$\Phi_{\mathcal{C}}(4) = \mathcal{S}(\mathcal{C}_2, 4) = 1 + X + X^2$$

et que

$$\Phi_{\mathcal{D}}(2) = \mathcal{S}(\mathcal{D}_3, 2) = 2X + X^2$$
$$\Phi_{\mathcal{D}}(1) = \mathcal{S}(\mathcal{D}_3, 1) = 1 + X + X^2 \quad .$$

L'application $\Phi_{\mathcal{C}}$ (et par suite $\Phi_{\mathcal{D}}$) est injective. En comparant les images de $\Phi_{\mathcal{C}}$ et $\Phi_{\mathcal{D}}$ nous obtenons

$$\mathcal{S}(\mathcal{C}_2, 1) = \mathcal{S}(\mathcal{D}_3, 2)$$
$$\mathcal{S}(\mathcal{C}_2, 4) = \mathcal{S}(\mathcal{D}_3, 1) \quad ,$$

ce qui implique que

$$\sigma(1) = 2$$
$$\sigma(4) = 1 \quad ,$$

et la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234) \in S_4$$

vérifie

$$\mathcal{D} = \mathcal{C}^{\sigma} = \mathcal{C}^{(1234)}$$

équation montrant l'équivalence des deux codes binaires $\mathcal{C}$ et $\mathcal{D}$.

2.5 Conclusion

Ce chapitre contient une étude peu large sur la notion d'équivalence des codes correcteurs, axe autour duquel tout le chapitre tourne. Les notions de base indispensables sont rappelées, les propriétés qui s'en suivent sont citées et démontrées (transfert des paramètres, préservation de linéarité, conservation des polynômes énumérateurs des poids, identité des groupes des permutations à un isomorphisme près...). L'utilisation des notions et des résultats liés à la théorie des groupes finis (tels le théorème de Lagrange, les classes latérales suivant un sous-groupe, l'action d'un groupe, etc.) permet de dériver des résultats remarquables attachés à la notion d'équivalence des codes correcteurs (définition de l'équivalence des codes,

nombre des codes équivalents, nombre des permutations définissant le même code équivalent et conjugaison des groupes de permutations des codes équivalents...). La dernière section du chapitre se concentre sur le problème de détermination de la permutation entre deux codes équivalents basée sur la notion de signature due à Nicolas Sendrier. Notre intention porte sur un cas particulier, où la signature associée vérifie une certaine condition. Sous cette condition, nous avons pu présenter une étude capable de calculer cette permutation. Des exemples illustrant les résultats sont exhibés. À titre de conclusion, la théorie des groupes est un outil très puissant qui peut contribuer à une meilleure compréhension des codes correcteurs d'erreurs.

Chapitre 3

Permutations admissibles associées à une partition d'un entier

Les codes de longueur n sur un alphabet Q sont des parties non vides de Q^n. Pour étudier leur capacité à détecter et corriger les erreurs, la notion de *distance* est introduite. Plusieurs distances sont ainsi exploitées : distance de Hamming [23] (Q un corps fini), distance de Lee [15] et [37] ($Q = \mathbb{Z}_4$ l'anneau des entiers modulo 4), distance modulaire [37] ($Q = \mathbb{Z}$), distance arithmétique [37] ($Q = \mathbb{Z}$), etc. Dans le cas où Q est un corps fini $\mathbb{F}_q$, la distance de Hamming est la plus classique et la plus utilisée pour sa connexion avec les machines traitant l'information. Les autres distances sont préférables pour d'autres situations. En 2006, Feng, Xu et Hickernell dans [11] ont introduit une distance d_π sur $\mathbb{F}_q^n$ associée à une partition π de l'entier positif n représentant la longueur des mots de $\mathbb{F}_q^n$. Autour de ce concept, plusieurs travaux sont élaborés.

Alves et Panek dans [28] s'intérèssent à l'étude des isométries de $\mathbb{F}_q^n$ muni de cette distance. Ces isométries forment un groupe pour la composition des applications, il est le *produit semi-direct* de deux de ses sous-groupes. L'un des deux est le sous-groupe des *permutations admissibles* dont notre travail y est consacré.

Dans ce chapitre, nous présentons des notions fondamentales de la partition d'un entier positif, la distance associée et les permutations admissibles. Puis, nous démontrons quelques

résultats révélant quelques propriétés relatives à ces notions en nous appuyant sur l'outil puissant d'un groupe agissant sur un ensemble. Les travaux [11] et [28] sont les références et les motivations pour cette étude.

3.1 Partition d'un entier positif

Un entier positif est un entier naturel non nul, c'est-à-dire un élément de $\mathbb{N}^\star$.

Soient n et m deux entiers positifs tels que $m \leq n$. L'écriture de n en somme de m entiers positifs est une expression de la forme

$$n = k_1 + k_2 + ... + k_m \tag{3.1.1}$$

avec k_1, k_2, ..., k_m des entiers positifs.

Cela revient à la donnée d'une suite finie $(k_1, k_2, \ldots, k_m)$ d'entiers positifs $k_1, k_2, \ldots, k_m$ vérifiant l'égalité 3.1.1.

L'entier positif m représente la longueur de la suite et les entiers $k_1, k_2, \ldots, k_m$ sont les termes (ou les parts). Cette suite est appelée *une composition de n en m termes (ou parts).* Les termes de cette suite ne sont pas forcément distincts et la suite n'est pas nécessairement ordonnée d'une manière monotone.

Exemple 3.1.1 *Les suites* $(2, 2, 3)$, $(3, 2, 2)$ *et* $(2, 3, 2)$ *sont des compositions de* 7 *en* 3 *termes.*

Exemple 3.1.2 *La suite* $(1, 1, 1, 1, 1)$ *est une composition de* 5 *en* 5 *termes.*

Exemple 3.1.3 *Les suites* $(3, 3, 3, 3)$ *et* $(1, 2, 3, 6)$ *sont des compositions de* 12 *en* 4 *termes.*

Le fait que l'addition des termes dans l'équation 3.1.1 est commutative, et que les termes des suites de l'exemple premier 3.1.1 ne diffèrent que dans l'ordre dont les termes sont écrits, fait qu'on peut considérer que ces suites sont *essentiellement les mêmes* : c'est-à-dire *équivalentes* dans un sens qu'on va définir. Ce qui nous permet de considérer que les suites $(k_1, k_2, \ldots, k_m)$ vérifiant l'équation 3.1.1 et qui sont *décroissantes* :

c'est-à-dire

$$k_1 \geq k_2 \geq ... \geq k_m \ .$$

Ces suites de composition de n en m termes et qui sont décroissantes sont les *partitions de n en m parts*. Elles sont *les représentantes* des compositions de n en m termes dans le sens qui suit.

Pour tout entier positif $m \leq n$, on considère l'ensemble $(\mathbb{N}^\star)^m$ produit cartésien de m copies de $\mathbb{N}^\star$: c'est l'ensemble

$$(\mathbb{N}^\star)^m = \{(n_1, n_2, ..., n_m) \mid n_i \in \mathbb{N}^\star \text{ pour tout } i = 1, 2, ..., m \ \},$$

on considère aussi le groupe symétrique S_m de degré m (c'est-à-dire des permutations de $\{1, 2, ..., m\}$).

Soit l'application δ de $S_m \times (\mathbb{N}^\star)^m$ dans $(\mathbb{N}^\star)^m$ définie comme suit :

$$\begin{array}{rcl} \delta : S_m \times (\mathbb{N}^\star)^m & \longrightarrow & (\mathbb{N}^\star)^m \\ (\sigma, (n_1, n_2, ..., n_m)) & \longmapsto & \sigma(n_1, n_2, ..., n_m) \end{array} \tag{3.1.2}$$

telle que $\sigma(n_1, n_2, ..., n_m) = (n_{\sigma(1)}, n_{\sigma(2)}, ..., n_{\sigma(m)})$.

Pour l'application δ, nous avons le lemme suivant :

Lemme 3.1.1 *L'application δ définie par 3.1.2 est une action du groupe S_m sur l'ensemble $(\mathbb{N}^\star)^m$.*

Preuve. L'application δ est bien définie, de plus pour $\sigma, \tau \in S_m$ et $(n_1, n_2, ..., n_m)$ de $(\mathbb{N}^\star)^m$, on voit que

$$\begin{array}{rcl} \sigma\tau(n_1, n_2, ..., n_m) & = & (n_{\sigma\tau(1)}, n_{\sigma\tau(2)}, ..., n_{\sigma\tau(m)}) \\ & = & (n_{\sigma(\tau(1))}, n_{\sigma(\tau(2))}, ..., n_{\sigma(\tau(m))}) \\ & = & \sigma(n_{\tau(1)}, n_{\tau(2)}, ..., n_{\tau(m)}) \\ & = & \sigma(\tau(n_1, n_2, ..., n_m)), \end{array}$$

et si id désigne l'application identité dans S_m, on a alors

$$\begin{aligned} id(n_1, n_2, ..., n_m) &= (n_{id(1)}, n_{id(2)}, ..., n_{id(m)}) \\ &= (n_1, n_2, ..., n_m). \end{aligned}$$

Les axiomes de la définition 1.1.4 ont lieu, ce qui prouve le lemme. ■

Ce qui nous importe est les compositions d'un entier positif n en m termes. À cette fin, considérons le sous-ensemble $X \subset (\mathbb{N}^\star)^m$ défini par

$$X = \{(n_1, n_2, ..., n_m) \in (\mathbb{N}^\star)^m \mid n = n_1 + n_2 + ... + n_m\}$$

L'ensemble X est stable sous l'action δ : En effet, pour $(n_1, n_2, ..., n_m) \in (\mathbb{N}^\star)^m$ et $\sigma \in S_m$, on a

$$\begin{aligned} (n_1, n_2, ..., n_m) \in X &\Leftrightarrow n = n_1 + n_2 + ... + n_m \\ &\Leftrightarrow n = n_{\sigma(1)} + n_{\sigma(2)} + ... + n_{\sigma(m)} \\ &\Leftrightarrow \sigma(n_1, n_2, ..., n_m) \in X \end{aligned}$$

Ce qui induit une action sur X qui sera notée $\delta_{|X}$.

L'action $\delta_{|X}$ définit une relation d'équivalence sur l'ensemble X dont les classes d'équivalence sont les orbites (3.1.3). Deux compositions de l'entier positif n en m termes sont équivalentes si elles appartiennent à la même orbite. Comme $\mathbb{N}^\star$ est totalement ordonné, on peut choisir comme représentant d'une orbite une *composition décroissante*. D'où la définition suivante :

Définition 3.1.1 *[1] Une partition d'un entier positif n en m parts est une suite décroissante $(k_1, k_2, ..., k_m)$ de m entiers positifs $k_1, k_2, ..., k_m$ qui vérifient*

$$n = k_1 + k_2 + ... + k_m \ .$$

–*Pour l'exemple 3.1.1*, la suite $(3, 2, 2)$ est une partition de 7 en 3 parts. Les deux suites $(3, 2, 2)$ et $(2, 3, 2)$ sont équivalentes. L'orbite contenant $(3, 2, 2)$ est

$$\mathcal{O}((3, 2, 2)) = \{(3, 2, 2), (2, 3, 2), (2, 2, 3)\}\,.$$

–*Pour l'exemple 3.1.3*, la suite $(3,3,3,3)$ est une partition de 12 en 4 parts dont l'orbite est $\mathcal{O}((3,3,3,3)) = \{(3,3,3,3)\}$.

Tandis que la composition $(1,2,3,6)$ est d'orbite $\mathcal{O}((1,2,3,6)) = \mathcal{O}((6,3,2,1))$ contenant 24 éléments.

En général, un élément $(n_1, n_2, ..., n_m) \in X$ a pour orbite sous l'action de $\delta_{|X}$ la partie

$$\mathcal{O}((n_1, n_2, ..., n_m)) = \left\{(n_{\sigma(1)}, n_{\sigma(2)}, ..., n_{\sigma(m)}) \mid \sigma \in S_m\right\}. \tag{3.1.3}$$

Remarque 3.1.1 *Comme $|S_m| = m!$, on voit que $|\mathcal{O}((n_1, n_2, ..., n_m)| \leq m!$.*

Dans tout ce qui suit, n et m sont des entiers positifs fixes avec $m \leq n$. On fixe aussi une partition $\pi = (k_1, k_2, ..., k_m)$ de n en m parts.

3.2 Décomposition de $\mathbb{F}_q^n$ en produit direct

Soit $\mathbb{F}_q^n$ l'espace vectoriel de dimension n sur le corps fini $\mathbb{F}_q$. La partition $\pi = (k_1, k_2, ..., k_m)$ de n induit une décomposition de l'espace $\mathbb{F}_q^n$ en produit direct de m sous-espaces vectoriels

$$\mathbb{F}_q^n = \mathbb{F}_q^{k_1} \times \mathbb{F}_q^{k_2} \times ... \times \mathbb{F}_q^{k_m} \tag{3.2.1}$$

de sorte qu'un vecteur v de $\mathbb{F}_q^n$ s'écrive sous la forme

$$v = (v_1, v_2, ..., v_m) \tag{3.2.2}$$

avec $v_i \in \mathbb{F}_q^{k_i}$ pour $i = 1, 2, ..., m$.

Les vecteurs $v_1, v_2, ..., v_m$ sont *les blocs* de v. Classiquement, ils sont des scalaires du corps $\mathbb{F}_q$, relativement à la partition $\pi = (k_1, k_2, ..., k_m)$ ils sont des vecteurs (de longueur $k_1, k_2, ..., k_m$ respectivement) des sous-espaces vectoriels $\mathbb{F}_q^{k_1}$, $\mathbb{F}_q^{k_2}$, ..., $\mathbb{F}_q^{k_m}$. Dans le cas particulier où $n = m$ et $\pi = (1, 1, ..., 1)$, on se trouve dans le cas classique.

Exemple 3.2.1 –Pour l'exemple 3.1.1, *si* $\mathbb{F}_q = \mathbb{F}_2$ *et* $\pi = (3,2,2)$ *est une partition de* 7 *en* 3 *parts, alors*

$$\mathbb{F}_2^7 = \mathbb{F}_2^3 \times \mathbb{F}_2^2 \times \mathbb{F}_2^2.$$

Un vecteur v *de* $\mathbb{F}_2^7$ *est de la forme* $v = (v_{11},.v_{12}, v_{13}, \mid v_{21}, v_{22}, \mid v_{31}, v_{32}) = (v_1, v_2, v_3)$.

–*Pour l'exemple 3.1.3*, si $\mathbb{F}_q = \mathbb{F}_3$ et $\lambda = (3,3,3,3)$ *est une partition de* 12 *en* 4 *parts, alors*

$$\mathbb{F}_3^{12} = \mathbb{F}_3^3 \times \mathbb{F}_3^3 \times \mathbb{F}_3^3 \times \mathbb{F}_3^3.$$

Un vecteur v *de* $\mathbb{F}_3^{12}$ *est de la forme*
$v = (v_{11},.v_{12}, v_{13}, \mid v_{21}, v_{22}, v_{23}, \mid v_{31}, v_{32}, v_{33}, \mid v_{41}, v_{42}, v_{43}) = (v_1, v_2, v_3, v_4)$.

Comme le produit direct $\mathbb{F}_q^{k_1} \times \mathbb{F}_q^{k_2} \times ... \times \mathbb{F}_q^{k_m}$ et la somme directe $\mathbb{F}_q^{k_1} \oplus \mathbb{F}_q^{k_2} \oplus ... \oplus \mathbb{F}_q^{k_m}$ sont linéairement isomorphes, les deux terminologies sont adoptées.

$$\mathbb{F}_q^n = \mathbb{F}_q^{k_1} \times \mathbb{F}_q^{k_2} \times ... \times \mathbb{F}_q^{k_m} = \mathbb{F}_q^{k_1} \oplus \mathbb{F}_q^{k_2} \oplus ... \oplus \mathbb{F}_q^{k_m}.$$

Définition 3.2.1 *La décomposition 3.2.1 est appelée la décomposition de l'espace* $\mathbb{F}_q^n$ *relativement à la partition* $\pi = (k_1, k_2, ..., k_m)$ *de* n.

3.2.1 La π-distance (π-métrique)

Rappelons la notion de distance de Hamming donnée dans la définition 1.3.2.

Pour deux mots $x = x_1x_2...x_n$ et $y = y_1y_2...y_n$ de $\mathbb{F}_q^n$, la distance de Hamming de x à y est le nombre $d_H(x,y)$ des coordonnées $i = 1, 2, ..., n$ telles que $x_i \neq y_i$.

c'est-à-dire

$$d_H(x,y) = |\{i = 1,2,...,n \mid x_i \neq y_i\}|.$$

et le poids de Hamming de $x = x_1x_2...x_n \in \mathbb{F}_q^n$ est l'entier naturel

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

Autrement dit

$$w_H(x) = d_H(x, \mathbf{0}).$$

où $\mathbf{0}$ désigne le vecteur nul $00...0 \in \mathbb{F}$.

Une généralisation de la distance (et par suite du poids) de Hamming est apparue en 2006 dans [11]. Feng, Xu et Hickernell ont introduit une distance d_π sur $\mathbb{F}_q^n$ associée à une partition π de l'entier positif n.

Considérons la décomposition 3.2.1 de l'espace $\mathbb{F}_q^n$, et deux vecteurs $u = (u_1, u_2, ..., u_m)$, $v = (v_1, v_2, ..., v_m)$ sous la forme 3.2.2 relativement à la partition $\pi = (k_1, k_2, ..., k_m)$ de n.

Définition 3.2.2 *La π-distance entre deux vecteurs $u = (u_1, u_2, ..., u_m)$ et $v = (v_1, v_2, ..., v_m)$ de $\mathbb{F}_q^n$ est le nombre $d_\pi(u, v)$ de leurs blocs différents :*

$$d_\pi(u, v) = |\{i = 1, 2, ..., m \mid u_i \neq v_i\}|,$$

et le π-poids du vecteur $u = (u_1, u_2, ..., u_m)$ est le nombre naturel

$$w_\pi(u) = |\{i = 1, 2, ..., m \mid u_i \neq 0\}|.$$

Il est clair que le nombre $d_\pi(.,.)$ vérifie les axiomes d'une distance sur $\mathbb{F}_q^n$:

- $d_\pi(u, v) = 0 \iff u = v$
- $d_\pi(u, v) = d_\pi(v, u)$
- $d_\pi(u, w) \leq d_\pi(u, v) + d_\pi(v, w).$

Pour la troisième inégalité, appelée *inégalité triangulaire*, remarquons qu'on a

$$\{i = 1, 2, ..., m \mid u_i = v_i\} \cap \{i = 1, 2, ..., m \mid v_i = w_i\} \subset \{i = 1, 2, ..., m \mid u_i = w_i\}$$

d'où, par complémentation, on obtient

$$\{i = 1, 2, ..., m \mid u_i \neq v_i\} \cup \{i = 1, 2, ..., m \mid v_i \neq w_i\} \supset \{i = 1, 2, ..., m \mid u_i \neq w_i\}$$

en passant aux cardinaux

$$|\{i = 1, 2, ..., m \mid u_i \neq v_i\}| \quad + \quad |\{i = 1, 2, ..., m \mid v_i \neq w_i\}| \quad \geq \quad |\{i = 1, 2, ..., m \mid u_i \neq w_i\}|$$

qui n'est autre que l'inégalité triangulaire.

Remarque 3.2.1 *La distance (le poids) de Hamming est un cas particulier de la π-distance. Il suffit de considérer la partition $\pi = (1, 1, ..., 1)$ et $m = n$.*

Ainsi le couple $(\mathbb{F}_q^n, d_\pi)$ est un *espace métrique.*

Exemple 3.2.2 *(suite de l'exemple 3.2.1) –Pour $\mathbb{F}_q = \mathbb{F}_2$ et $\pi = (3, 2, 2)$, une partition de 7 en 3 parts. Si $u = (1, 0, 1 \mid 0, 1 \mid 0, 0) = (u_1, u_2, u_3)$ et $v = (1, 0, 0 \mid 0, 0 \mid 1, 0) = (v_1, v_2, v_3)$ sont deux vecteurs de $\mathbb{F}_2^7$, alors $d_\pi(u, v) = 3$ et $w_\pi(u) = 2$.*

–Pour $\mathbb{F}_q = \mathbb{F}_3$ et $\lambda = (3, 3, 3, 3)$, *une partition de 12 en 4 parts.* Si

$$u = (0, 0, 0 \mid 1, 2, 0 \mid 1, 1, 1 \mid 0, 1, 2) = (v_1, v_2, v_3, v_4)$$

et

$$v = (1, 1, 1 \mid 1, 1, 0 \mid 2, 2, 2 \mid 1, 1, 0) = (v_1, v_2, v_3, v_4)$$

sont de $\mathbb{F}_3^{12}$, alors $d_\lambda(u, v) = 4$ et $w_\lambda(u) = 3$.

Comme les codes de longueur n sur le corps fini $\mathbb{F}_q$ sont des parties de l'espace $\mathbb{F}_q^n$ (section 1.3), la notion analogue de *code linéaire en blocs d'erreurs* est introduite. C'est un sous-espace vectoriel de l'espace $(\mathbb{F}_q^n, d_\pi)$. Il s'ensuit qu'on peut définir, d'une manière égale, la distance minimale d'un code linéaire en blocs d'erreurs $\mathcal{L}$:

Définition 3.2.3 *Un sous-espace $\mathcal{L}$ de $(\mathbb{F}_q^n, d_\pi)$ de dimension k est appelé un $[n, k]_q$-code linéaire en blocs d'erreurs de type π sur $\mathbb{F}_q$.*

En abréviation, un code linéaire en blocs d'erreurs est un LEB-code (pour l'anglais Linear Error-Block).

De même, la distance minimale $d_\pi(\mathcal{L})$ *de* $\mathcal{L}$ *est*

$$\begin{aligned} d_\pi(\mathcal{L}) &= \min\{d_\pi(u,v) \mid u,v \in \mathcal{L},\ v \neq v\} \\ &= \min\{w_\pi(u) \mid u \in \mathcal{L},\ u \neq \mathbf{0}\}. \end{aligned}$$

3.3 Permutations admissibles associées à une partition

Définir une distance sur un ensemble fait appel à plusieurs autres notions telles que la topologie, les suites, l'isométrie, etc. La notion importante d'*isométrie* est indispensable pour l'étude des *symétries* dans un espace métrique. Elle permet d'identifier les parties qui sont métriquement les mêmes, c'est-à-dire qui possèdent les mêmes propriétés relatives à la distance définie. Dans cette section, les isométries (aussi appelées les symétries) de l'espace $\mathbb{F}_q^n$, muni de la π-distance associée à la partition $\pi = (k_1, k_2, ..., k_m)$, sont définies. Une classe d'isométries, à savoir les symétries linéaires, représente une restriction compatible avec la structure d'espace vectoriel de $\mathbb{F}_q^n$. Ces symétries linéaires forment un groupe pour la composition des applications. M. M. S. Alves, L. Panek et M. Firer donnent dans l'article *Error-Block Codes and Poset Metric* [Advances in Mathematics of Communications, volume 2, No 1, 2008] une description complète de ce groupe. Le groupe de toutes les isométries (linéaires et non linéaires) est déterminé et décrit dans [28] comme *le produit semi-direct* de deux sous-groupes. L'un est le sous-groupe des *permutations admissibles*. Notre intention porte sur l'étude des propriétés des permutations admissibles (structure de sous-groupe, ordre, et relation avec les compositions d'un entier positif) en exhibant quelques exemples illustrant les résultats obtenus.

3.3.1 Isométries de $(\mathbb{F}_q^n, d_\pi)$

Les isométries de l'espace $(\mathbb{F}_q^n, d_\pi)$ permettent de définir une classification des codes linéaires en blocs d'erreurs, comme elles appliquent un code linéaire en blocs 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 3.3.1 *Une isométrie (ou symétrie) de l'espace métrique $(\mathbb{F}_q^n, d_\pi)$ est une application bijective $\varphi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ qui conserve les distances,*

c'est-à-dire,

$$d_\pi(\varphi(u), \varphi(v)) = d_\pi(u, v)$$

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

Remarque 3.3.1 *Si la partition est $\pi = (1, 1, ..., 1)$ avec $n = m$, on est dans le cas classique des isométries de l'espace de Hamming $(\mathbb{F}_q^n, d_H)$ dont la définition 3.3.1 donne une généralisation.*

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 3.3.2 *Une isométrie linéaire de l'espace $(\mathbb{F}_q^n, d_\pi)$ est une isométrie qui est linéaire pour la structure d'espace vectoriel de $\mathbb{F}_q^n$ (comme elle est définie en 1.2.1).*

Dans le cas d'isométrie linéaire, on peut alléger la définition.

Proposition 3.3.1 *Une isométrie linéaire de l'espace $(\mathbb{F}_q^n, d_\pi)$ est une application linéaire injective φ qui conserve le π-poids,*

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

Preuve. 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 $w_\pi(\mathbf{0}) = 0$, par φ est lui-même. Pour u, $v \in \mathbb{F}_q^n$ on a

$$\begin{aligned}
d_\pi(\varphi(u), \varphi(v)) &= d_\pi(\varphi(u) - \varphi(v), \mathbf{0}) && (3.2.1)\\
&= w_\pi(\varphi(u) - \varphi(v) && (3.2.1)\\
&= w_\pi(\varphi(u - v)) && (\varphi \textit{ linéaire})\\
&= w_\pi(u - v) && (\varphi \textit{ isométrie})\\
&= d_\pi(u - v, \mathbf{0}) && (3.2.1)\\
&= d_\pi(u, v) && (3.2.1)
\end{aligned}$$

Réciproquement, il est clair qu'une isométrie linéaire est linéaire, injective conservant le π-poids. ■

Deux codes linéaires en blocs d'erreurs $\mathcal{C}$ et $\mathcal{D}$, qui possèdent *les mêmes propriétés métriques*, ont les mêmes propriétés *théoriques relatives à la détection et correction des erreurs*. Donc ils sont considérés *équivalents*.

Définition 3.3.3 *Deux $[n,k]_q$-codes linéaires en blocs d'erreurs $\mathcal{C}$ et $\mathcal{D}$ de type π sur $\mathbb{F}_q$ sont équivalents (resp. linéairement équivalents) s'il existe une isométrie (resp. linéaire) φ de $(\mathbb{F}_q^n, d_\pi)$ telle que $\varphi(\mathcal{C})$=$\mathcal{D}$.*

Remarque 3.3.2 *Si $\mathcal{L}$ et $\mathcal{M}$ sont équivalents, on dit aussi qu'ils sont isométriques ou symétriques et on écrit*

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

Notation 3.3.1 *Notons par $Symm(\mathbb{F}_q^n, d_\pi)$ l'ensemble de toutes les isométries de l'espace $(\mathbb{F}_q^n, d_\pi)$.*

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

Proposition 3.3.2 *L'ensemble $Symm(\mathbb{F}_q^n, d_\pi)$ est un groupe pour la loi de composition des applications $\circ$.*

Preuve.

- L'application identité de $\mathbb{F}_q^n$ est une isométrie, donc $Symm(\mathbb{F}_q^n, d_\pi) \neq \varnothing$,
- La composée de deux isométries est une isométrie : Si φ et $\psi \in Symm(\mathbb{F}_q^n, d_\pi)$, alors pour $u, v \in \mathbb{F}_q^n$

$$\begin{aligned} d_\pi(\varphi \circ \psi(u), \varphi \circ \psi(v)) &= d_\pi(\varphi(\psi(u)), \varphi(\psi(v))) \\ &= d_\pi(\psi(u), \psi(v)) && \varphi \text{ isométrie} \\ &= d_\pi(u, v) && \psi \text{ isométrie} \end{aligned}$$

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

- La composition des applications est associative.
- Si $\varphi \in Symm(\mathbb{F}_q^n, d_\pi)$, comme $\varphi(u) = s \Leftrightarrow u = \varphi^{-1}(s)$ et $\varphi(v) = t \Leftrightarrow v = \varphi^{-1}(t)$, on trouve

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

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

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

Soit $\mathcal{M}$ l'ensemble des applications $T : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ telles que

$$T((v_1, v_2, ..., v_m)) = (T_1(v_1), T_2(v_2), ..., T_m(v_m))$$

où chaque application coordonnée T_i est une bijection de $\mathbb{F}_q^{k_i}$ sur lui-même.
Pour $\mathcal{M}$, on a la proposition suivante :

Proposition 3.3.3 *[28] Soit $\mathcal{M}$ comme il est défini ci-dessus. Alors $\mathcal{M}$ est un sous-groupe de $Symm(\mathbb{F}_q^n, d_\pi)$, isomorphe au produit direct $\prod_{i=1}^{i=m} S_{q^{k_i}}$.*

Ici, $S_{q^{k_i}}$ est le groupe symétrique de degré q^{k_i}.

Pour décrire la structure du groupe $Symm(\mathbb{F}_q^n, d_\pi)$, une classe de permutations de S_m est définie dans ce qui suit.

3.3.2 Permutations admissibles

Rappelons que n, m sont des entiers positifs avec $m \leq n$. On fixe une partition $\pi = (k_1, k_2, ..., k_m)$ de n en m parts.

Définition 3.3.4 *[28] Une permutation $\sigma \in S_m$ est admissible si $k_i = k_{\sigma(i)}$ pour tout $i = 1, 2, ..., m$.*

Remarque 3.3.3 *Pour donner une justification de cette définition, soit l'action*

$$\begin{array}{c} \Phi : S_m \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n \\ (\sigma, (v_1, v_2, ..., v_m)) \longmapsto \sigma(v_1, v_2, ..., v_m) = (v_{\sigma(1)}, v_{\sigma(2)}, ..., v_{\sigma(m)}) \end{array}.$$

Ici $(v_1, v_2, ..., v_m) \in \mathbb{F}_q^n = \mathbb{F}_q^{k_1} \times \mathbb{F}_q^{k_2} \times ... \times \mathbb{F}_q^{k_m}$ *comme dans 3.2.1. Dans le but de respecter l'ordre des sous-espaces* $\mathbb{F}_q^{k_1}$, $\mathbb{F}_q^{k_2}$,..., $\mathbb{F}_q^{k_m}$ *dans la décomposition de* $\mathbb{F}_q^n$, *on doit avoir le vecteur image*

$$\sigma(v_1, v_2, ..., v_m) = (v_{\sigma(1)}, v_{\sigma(2)}, ..., v_{\sigma(m)})$$

dans $\mathbb{F}_q^{k_1} \times \mathbb{F}_q^{k_2} \times ... \times \mathbb{F}_q^{k_m}$. *Et comme* $v_{\sigma(i)} \in \mathbb{F}_q^{k_{\sigma(i)}}$ *pour* $i = 1, 2, ..., m$, *on voit par conséquent que* $\mathbb{F}_q^{k_{\sigma(i)}} = \mathbb{F}_q^{k_i}$. *Ce dernier veut dire que* $k_{\sigma(i)} = k_i$.

Désignons par S_π le sous-ensemble de S_m formé de toutes les permutations admissibles. Nous allons citer quelques propriétés de S_π.

Proposition 3.3.4 *L'ensemble* S_π *des permutations admissibles est un sous-groupe de* S_m.

Démonstration. La preuve qu'on propose est basée sur l'action de $\delta_{|X}$ sur l'ensemble

$$X = \{(n_1, n_2, ..., n_m) \in (\mathbb{N}^\star)^m \mid n = n_1 + n_2 + ... + n_m\}$$

défini dans la section 3.1.

Puisque $\pi = (k_1, k_2, ..., k_m) \in X$, on a pour tout $\sigma \in S_m$

$$\sigma(k_1, k_2, ..., k_m) = (k_{\sigma(1)}, k_{\sigma(2)}, ..., k_{\sigma(m)})$$

D'après la proposition 1.1.2, le stabilisateur $(S_m)_\pi$ de $\pi = (k_1, k_2, ..., k_m)$ est un *sous-groupe* de S_m défini par

$$(S_m)_\pi = \{\sigma \in S_m \mid \sigma\pi = \pi\}$$

On a pour une permutation $\sigma \in S_m$

$$\begin{aligned} \sigma \in (S_m)_\pi &\Leftrightarrow \sigma\pi = \pi \\ &\Leftrightarrow (k_{\sigma(1)}, k_{\sigma(2)}, ..., k_{\sigma(m)}) = (k_1, k_2, ..., k_m) \\ &\Leftrightarrow k_{\sigma(i)} = k_i \text{ pour } i = 1, 2, ..., m \\ &\Leftrightarrow \sigma \in S_\pi \end{aligned}$$

c'est-à-dire que le stabilisateur $(S_m)_\pi$ n'est autre que S_π, ce qui prouve la proposition. ■

La notation S_π apparait très *naturelle*, elle n'est qu'une écriture légère de $(S_m)_\pi$ en rappelant que l'entier positif m est fixé.

Si $\tau = (r_1, r_2, ..., r_m)$ est une composition équivalente à $\pi = (k_1, k_2, ..., k_m)$ telle que $\tau = \sigma\pi$, avec $\sigma \in S_m$, la proposition suivante a lieu :

Proposition 3.3.5 *Si $\tau = (r_1, r_2, ..., r_m)$ est une composition équivalente à $\pi = (k_1, k_2, ..., k_m)$, alors S_π et S_τ sont conjugués. Plus précisément, si $\tau = \sigma\pi$, avec $\sigma \in S_m$, on a*

$$S_\tau = \sigma S_\pi \sigma^{-1}.$$

Preuve. C'est une conséquence immédiate de la proposition 1.1.2. ■

Exemple 3.3.1 *Dans les exemples suivants, π est une partition de n en m parts, τ est une composition équivalente à π :*

(a) *$n = 7$, $m = 3$, $\pi = (3, 2, 2)$ et $\tau = (2, 3, 2)$. Ici on a*

$$S_\pi = \{Id,\ (23)\}$$

π et τ vérifient

$$\tau = (12)\pi \text{ et } \tau = (132)\pi.$$

Dans le premier cas

$$S_\tau = \{Id,\ (13)\} = (12)S_\pi(12),$$

dans le deuxième

$$S_\tau = \{Id,\ (13)\} = (132)S_\pi(123).$$

(b) *$n = 5$, $m = 5$, $\pi = (1,1,1,1,1)$ et $\tau = \pi$. Ici on a $S_\pi = S_\tau = S_5$*

(c) 1) *$n = 12$, $m = 4$, $\pi = (3,3,3,3)$ et $\tau = \pi$. Ici on a*

$$S_\pi = S_\tau = S_4$$

2) *$n = 12$, $m = 4$, $\pi = (6,3,2,1)$ et $\tau = (1,2,3,6)$. Ici on a*

$$S_\pi = \{Id\}$$

π et τ vérifient

$$\tau = (14)(23)\pi$$

et

$$S_\tau = \{Id\} = (14)(23)\ S_\pi\ (14)(23)$$

3) *$n = 12$, $m = 5$, $\pi = (3,3,2,2,2)$ et $\tau = (123)\pi = (3,2,3,2,2)$. Ici on a*

$$S_\pi = \{Id, (12), (34), (35), (45), (453), (435), (12)(34), (12)(35), (12)(45), (12)(453), (12)(435)\}$$

et

$$S_\tau = \{Id,\ (13), (24), (45), (25), (243), (234), (13)(24), (13)(45), (13)(25), (13)(243), (13)(234)\}$$

$$= (123)\ S_\pi\ (132).$$

Remarque 3.3.4 *En se renvoyant à l'exemple 3.3.1* (a)*, on voit que la composition τ provient de π par l'application de deux permutations de S_3, à savoir $\sigma_1 = (12)$ et $\sigma_2 = (132)$. Cela nous incite à poser la question naturelle suivante : Si π et τ sont équivalentes, trouver le nombre des permutations $\sigma \in S_m$ qui envoient π vers τ, i.e. $\tau = \sigma\pi$.*

La réponse à cette question apparait dans ce qui suit :

On voit que si σ_1 et σ_2 sont deux permutations de S_m qui vérifient $\tau = \sigma_1\pi$ et $\tau = \sigma_2\pi$, alors on a

$$\begin{cases} \tau = \sigma_1\pi \\ \tau = \sigma_2\pi \end{cases} \Leftrightarrow \sigma_1\pi = \sigma_2\pi$$
$$\Leftrightarrow \sigma_1^{-1}\sigma_2\pi = \pi$$
$$\Leftrightarrow \sigma_1^{-1}\sigma_2 \in S_\pi, \quad \text{d'après la proposition 3.3.4,}$$
$$\Leftrightarrow \sigma_1 S_\pi = \sigma_2 S_\pi \quad \text{d'après 1.1.2.}$$

,

Cela permet de définir une relation binaire $\mathcal{R}$ dans S_m par

$$\sigma_1 \mathcal{R} \sigma_2 \Leftrightarrow \sigma_1\pi = \sigma_2\pi \Leftrightarrow \sigma_1 S_\pi = \sigma_2 S_\pi$$

$\mathcal{R}$ est une relation d'équivalence. Notons par $[\sigma]$ la classe de σ. On remarque que l'équivalence précédente montre qu'on peut introduire une bijection entre l'ensemble quotient $S_m/\mathcal{R}$ et l'ensemble S_m/S_π des classes latérales à gauche modulo le sous-groupe S_π du groupe S_m en posant $[\sigma] \longmapsto \sigma S_\pi$.

Considérons l'application f définie par

$$\begin{array}{rccc} f: & S_\pi & \longrightarrow & [\sigma] \\ & \alpha & \longmapsto & \sigma\ \alpha \end{array} .$$

f est une bijection, ce qui permet d'énoncer la proposition suivante :

Proposition 3.3.6 *Soient π une partition d'un entier positif n en m parts et τ une composition équivalente. Le nombre des permutations de S_m appliquant π à τ est $|S_\pi|$.*

Remarque 3.3.5

- *Dans la proposition, la partition π peut être remplacée par n'importe qu'elle composition de n en m parts.*
- *Puisque le groupe S_m est fini, les ensembles $S_m/\mathcal{R}$ et S_m/S_π sont aussi finis.*
- *L'équipotence des deux ensembles $S_m/\mathcal{R}$ et S_m/S_π permet de calculer leur cardinal $[S_m : S_\pi]$, indice de S_π dans S_m, qui selon le théorème de Lagrange (Théorème 1.1.1) égale*

$$[S_m : S_\pi] = \frac{|S_m|}{|S_\pi|} = \frac{m!}{|S_\pi|}.$$

Exemple 3.3.2 ***(a)*** *$n = 7$, $m = 3$, $\pi = (3,2,2)$ et $\tau = (2,3,2)$. On a*

$$S_\pi = \{Id,\ (23)\}$$

$|S_\pi| = 2$, deux permutations de S_3 appliquent π sur τ : (12) et (132). L'ensemble quotient $S_3/\mathcal{R}$ a pour cardinal $[S_3 : S_\pi] = 3$. Un calcul simple montre que

$$S_3/\mathcal{R} = \{[Id], [(12)], [(13)]\}.$$

(b) *$n = 5$, $m = 5$, $\pi = (1,1,1,1,1)$ et $\tau = \pi$. On a*

$$S_\pi = S_5$$

$|S_\pi| = 5! = 120$ permutations de S_5 envoient π vers τ, ce sont S_5 tout entier. L'ensemble quotient $S_5/\mathcal{R} = \{S_5\}$ a pour cardinal $[S_5 : S_\pi] = 1$.

Nombre des compositions équivalentes

La proposition suivante permet de calculer le nombre des compositions équivalentes à une partition π donnée. Ce nombre est une fonction en m, nombre de parts et le cardinal de S_π.

Proposition 3.3.7 *Soit $\pi = (k_1, k_2, ..., k_m)$ une partition de n en m parts. Les compositions équivalentes à π sont en nombre égal à $\frac{m!}{|S_\pi|}$.*

Preuve. On propose deux méthodes de démonstration : $\pi = (k_1, k_2, ..., k_m)$ est la partition de n en m parts,

Première méthode :

Soit l'action $\delta_{|X}$ sur l'ensemble

$$X = \{(n_1, n_2, ..., n_m) \in (\mathbb{N}^\star)^m \mid n = n_1 + n_2 + ... + n_m\}$$

définie dans la section 3.1. L'orbite de π selon 3.1.3 est

$$\mathcal{O}(\pi) = \left\{(k_{\sigma(1)}, k_{\sigma(2)}, ..., k_{\sigma(m)}) \mid \sigma \in S_m\right\}.$$

C'est l'ensemble de toutes les compositions de n en m parts qui sont équivalentes à π. Leur nombre est, d'après le corollaire 1.1.2, égal à

$$|\mathcal{O}(\pi)| = [S_m : S_\pi] = \frac{|S_m|}{|S_\pi|} = \frac{m!}{|S_\pi|}.$$

Deuxième méthode :

Considérons l'ensemble quotient $S_m/\mathcal{R}$ de S_m par la relation d'équivalence $\mathcal{R}$, et supposons que

$$S_m/\mathcal{R} = \{[\sigma_1], [\sigma_2], ..., [\sigma_r]\}, \quad r = |S_m/\mathcal{R}|,$$

Chaque classe d'équivalence $[\sigma_i]$ définit une composition $\tau_i = \sigma_i\pi$ de n en m parts, équivalente à π. Ces compositions sont distinctes et en bijection avec les $[\sigma_i]$ par

$$[\sigma_i] \longmapsto \sigma_i\pi$$

Leur nombre, sachant que $S_m = [\sigma_1] \cup [\sigma_2] \cup, ..., \cup [\sigma_r]$, est donc

$$r = |S_m/\mathcal{R}| = \frac{m!}{|S_\pi|}$$

Ce qui achève la preuve. ■

Corollaire 3.3.1 *Soit l'espace $\mathbb{F}_q^n$ muni de la distance de Hamming d_H. Il existe une unique composition de n relative à d_H.*

Exemple 3.3.3 *$n = 7$, $m = 3$, $\pi = (3, 2, 2)$. Comme $S_\pi = \{Id,\ (23)\}$, on a $\frac{3!}{|S_\pi|} = \frac{6}{2} = 3$ compositions équivalentes à π sont rangées comme suit*

$$\begin{aligned} [Id] &\longmapsto \pi = (3, 2, 2) \\ [(12)] &\longmapsto \tau = (2, 3, 2) \\ [(13)] &\longmapsto \nu = (2, 2, 3) \end{aligned}$$

Exemple 3.3.4 $n = 5$, $m = 5$, $\pi = (1,1,1,1,1)$. *On a* $S_\pi = S_5$ *et* $\frac{5!}{|S_\pi|} = \frac{5!}{5!} = 1$. *La partition* π *est l'unique composition équivalente à* π.

L'ordre du sous-groupe S_π

Dans tout ce qui précède, l'ordre du sous-groupe S_π des permutations admissibles joue un rôle important : nombre des compositions équivalentes, cardinal de l'ensemble quotient $S_m/\mathcal{R}$ et le cardinal de $[\sigma]$, la classe de σ modulo la relation $\mathcal{R}$. Il est donc nécessaire de le calculer. Pour cette fin, supposons que la partition $\pi = (k_1, k_2, ..., k_m)$ est telle que

$$\begin{aligned} &k_1 = k_2 = ... = k_{m_1} \succ k_{m_1+1} = k_{m_1+2} = ... = k_{m_1+m_2} \succ ... \\ &\succ k_{m_1+m_2+...+m_{s-1}+1} = k_{m_1+m_2+...+m_{s-1}+2} = ... = k_{m_1+m_2+...+m_{s-1}+m_s}, \end{aligned} \tag{3.3.1}$$

avec

$$m_1 + m_2 + ... + m_s = m. \tag{3.3.2}$$

La proposition suivante a lieu :

Proposition 3.3.8 *Soit* π *une partition de* n *en* m *parts, donnée sous la forme* 3.3.1 *et* 3.3.2, *alors l'ordre du sous-groupe* S_π *des permutations admissibles relativement à* π *est* $|S_\pi| = \prod_{i=1}^{i=s} m_i!$.

c'est-à-dire $|S_\pi| = m_1!\ m_2!\ ...\ m_s!$.

Preuve. Pour toute permutation admissible $\sigma \in S_\pi$, les parties d'indices suivantes : $\{1, 2, ..., m_1\}, \{m_1 + 1, ..., m_1 + m_2\}, ..., \{m_1 + m_2 + ... + m_{s-1} + 1, ..., m_1 + m_2 + ... + m_{s-1} + m_s\}$ sont stables sous l'action de σ, ce qui implique que les restrictions de σ à ces parties sont des permutations de ces parties. Cela permet de définir l'application suivante :

$$\begin{array}{rccl} \Theta: & S_\pi & \longrightarrow & \prod_{i=1}^{i=s} S_{m_i} \\ & \sigma & \longmapsto & (\sigma_{|\{1,2,...,m_1\}}, \sigma_{|\{m_1+1,...,m_1+m_2\}}, ..., \sigma_{|\{m_1+m_2+...+m_{s-1}+1,...,m_1+m_2+...+m_{s-1}+m_s\}}) \end{array}$$

où $\prod_{i=1}^{i=s} S_{m_i}$ est le groupe produit direct des groupes S_{m_i}, $i = 1, 2, ..., s$, muni de la loi produit. L'application Θ est un isomorphisme de groupes. Par conséquent, $|S_\pi| = \left|\prod_{i=1}^{i=s} S_{m_i}\right| = \prod_{i=1}^{i=s} m_i!$.
■

Exemple 3.3.5 ***(a)*** $\underline{n = 7,\ m = 3,\ \pi = (3, 2, 2)}$ *: ici on a* $m_1 = 1$, $m_2 = 2$, $k_1 = 3$, $k_2 = k_3 = 2$. *Donc* $|S_\pi| = 1!\ 2! = 2$.

(b) $\underline{n = 5,\ m = 5,\ \pi = (1, 1, 1, 1, 1)}$. *Ici on a* $m_1 = 5$, $k_1 = k_2 = k_3 = k_4 = k_5 = 1$. *Donc* $|S_\pi| = 5! = 120$.

(c) $\underline{n = 12,\ m = 5,\ \pi = (3, 3, 2, 2, 2)}$. *Ici on a* $m_1 = 2$, $m_2 = 3$, $k_1 = k_2 = 3$, $k_3 = k_4 = k_5 = 2$. *Donc* $|S_\pi| = 2!\ 3! = 2 \times 6 = 12$.

On peut résumer les propositions précédentes en un seul théorème :

Théorème 3.3.1 *Soit π une partition d'un entier positif n en m parts. L'ensemble S_π des permutations admissibles est un sous-groupe de S_m d'ordre $\prod_{i=1}^{i=s} m_i!$. Si τ est une composition équivalente à π, alors S_π et S_τ sont conjugués.*

Enfin, signalons le théorème suivant, démontré en [28], qui donne une description complète du groupe des isométries de l'espace métrique $(\mathbb{F}_q^n, d_\pi)$. Rappelons que selon la proposition 3.3.3, l'ensemble $\mathcal{M}$ des applications $T : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ telles que

$$T((v_1, v_2, ..., v_m)) = (T_1(v_1), T_2(v_2), ..., T_m(v_m)),$$

où T_i est une bijection de $\mathbb{F}_q^{k_i}$ sur lui-même, *est un sous-groupe de $Symm(F_q^n, d_\pi)$, isomorphe au produit direct* $\prod_{i=1}^{i=m} S_{q^{k_i}}$.

Théorème 3.3.2 *[28] Soit π une partition d'un entier positif n en m parts.*

(i) $Symm(F_q^n, d_\pi) = S_\pi \ltimes \mathcal{M}$,

(ii) $Symm(F_q^n, d_\pi) \cong S_\pi \ltimes \prod_{i=1}^{i=m} S_{q^{k_i}}$

La structure du produit semi-direct est induite de l'action de S_π sur $\mathcal{M}$ par conjugaison, c'est-à-dire

$$(\alpha, T)(\beta, R) = (\alpha\beta, (\beta^{-1}T\beta)R)$$

avec α, $\beta \in S_\pi$ et T, $R \in \mathcal{M}$, $\mathcal{M} \trianglelefteq Symm(F_q^n, d_\pi)$.

Lorsque $d_\pi = d_H$ la distance de Hamming (dans ce cas $n = m$, $\pi = (1, 1, ..., 1)$), on a le corollaire suivant :

Corollaire 3.3.2 *[28] Si d_H est la distance de Hamming, alors $Symm(F_q^n, d_H) \cong S_n \ltimes (S_q)^n$.*

3.4 Conclusion

Dans ce chapitre, à travers ses sections, nous avons rappelé les définitions et les notions de base liées à la partition d'un entier positif en un nombre fini de parts : compositions d'un entier positif et leur équivalence, décomposition de l'espace des mots associés, permutations admissibles et les résultats qui s'en découlent. Nous avons tiré des résultats importants en utilisant des techniques issues de la théorie des groupes, à savoir la notion de l'action d'un groupe (la plupart des résultats, sauf ceux qui sont rapportés à une référence). Pas mal des profits sont tirés de l'application des outils de cette agréable théorie : des définitions apparaissent si claires, si rigoureuses et bien structurées (définition de l'équivalence des compositions, permutations admissibles, etc.), des résultats bien fondés se démontrent (nombres des compositions équivalentes, l'ordre du sous-groupe des permutations admissibles, etc.). Toutes ces remarques nous poussent à considérer, à titre de conclusion, que la théorie des groupes est un outil très puissant qui aide à définir, classifier et produire des résultats indispensables de la théorie des codes correcteurs d'erreurs comme dans d'autres théories.

Conclusion et Perspectives

Le sujet de ce travail s'inscrit dans le domaine de la théorie des groupes finis et ses applications à l'étude des symétries des codes correcteurs. Symétries observées de deux angles : équivalence par permutations (équivalence par position relativement à la distance de Hamming) et équivalence par blocs (relativement à une distance associée à une partition de la longueur des mots).

Dans le but d'étudier *l'équivalence des codes* : On a commencé par donner des définitions et les propriétés qui s'en déduisent. On a appliqué des outils issus de la théorie des groupes pour mieux comprendre l'équivalence et pour en tirer d'autres propriétés. Enfin on s'est concentré sur le problème de détermination de la permutation entre deux codes équivalents basé sur la notion de signature due à Nicolas Sendrier. Notre intention porte sur un cas particulier, où la signature associée vérifie une certaine condition. Sous cette condition on a pu déterminer la permutation. Cette partie du travail a fait l'objet d'une publication dont les résultats sont présentés dans la thèse.

Pour la fin d'étudier l'équivalence par blocs (relativement à la π-distance associée à une partition π de longueur des mots n), On a rassemblé les notions fondamentales de partition d'un entier positif, la π-distance associée et les permutations admissibles. En s'appuyant sur le concept du groupe agissant sur un ensemble, on a pu démontrer quelques résultats relatifs à ces notions. Ces résultats obtenus concernent les compositions d'un entier positif et la combinatoire du sous-groupe des permutations admissibles. Ce dernier fut un facteur du produit semi-direct définissant le groupe de toutes les isométries de l'espace des mots relativement à la π-distance.

À titre de conclusion, la théorie des groupes finis est un outil très puissant qui aide à définir, classifier et produire des résultats indispensables dans la théorie des codes correcteurs d'erreurs comme dans d'autres disciplines.

Suite aux travaux présentés dans cette thèse, il reste encore beaucoup à faire avec les groupes finis appliqués aux codes correcteurs d'erreurs. Nous présentons ci-dessous quelques questions que nous prévoyons d'étudier dans des travaux à venir :

1. Relation entre les codes et leurs groupes de permutations vérifiant certaines propriétés,

2. Les p-sous-groupes de Sylow du groupe des permutations d'un code correcteur et ses relations avec la détection et la correction du code,

3. Amélioration de l'étude de détermination des permutations entre deux codes équivalents dans le cas d'une signature non totalement discriminante.

Bibliographie

[1] G. E. Andrews, The Theory of Partitions, Addison-Wesley Publishing Company, USA, 1976.

[2] M. A. Armstrong, *Groups and Symmetry*, Springer-Verlag New York Inc., 1988.

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

[4] J. Bierbrauer, *Introduction to Coding Theory*, Second Edition, CRC Press, Taylor & Francis Group, 2017.

[5] R. Bose, *Information Theory, Coding and Cryptography*, Third Edition, McGraw Hill Education (India) Private Limited, 2016.

[6] A. Bouvier, D. Richard, *Groupes : observation, théorie, pratique*, deuxième édition, Hermann, 1979.

[7] F. Butin, *Algebra* : *Polynomials, Galois Theory and Applications*, Dover Publications, New York, 2017.

[8] H. Cohen. *Les nombres premiers*, La recherche 278, volume 26, juillet-août, 1995.

[9] M. Demazure, *Cours d'algèbre*, Cassini, Paris, 2008.

[10] J. R. Durbin, *Modern Algebra: An Introduction*, John Wiley & Sons, 6^{e} édition, 2009.

[11] K. Feng, L. Xu, and F. J. Hickernell, *Linear error-block codes*, Finite Fields and Their Applications, 12, 638-652. 2006.

[12] L. J. Goldstein, *Abstract Algebra : a first course*, Prentice Hall Inc., Englewood Cliffs, New Jersey, 1973.

[13] J. A. Green, *Sets and Groups*, Routledge & Kegan Paul Ltd, London, 1974.

[14] J. M. Howie, *Fields and Galois Theory*, Springer Undergraduate Mathematics Series, Springer, 2006.

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

[16] N. Koblitz, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics, 2e édition, Springer-Verlag, 1994.

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

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

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

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

[21] R. Lidl et H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1994.

[22] P. Loindreau, *Étude et optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs*, Thèse de doctorat en sciences, École polytechnique, 2001.

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

[24] D. Mercier, *Utilisation de l'algèbre dans les systèmes d'informations*, 5e colloque de l'IREM des Antilles-Guyane, May 2000, France. pp. 1-30. HAL-0076744, url: https://hal.univ-antilles.fr/hal-00767442v1/document.

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

[26] G. L. Mullen & D. Panario, *Handbook of Finite Fields*, Chapman and Hall/CRC Press, 2013.

[27] A. Otmani, *Codes cortex et construction de codes autoduaux optimaux*, thèse de doctorat, université de Limoges, 2002.

[28] L. Panek et al., *Symmetries of the π-distance,* https://arxiv.org/pdf/0901.1043v1 [cs.IT], 8 Jan 2009.

[29] O. Papini, J. Wolfmann, *Algèbre discrète et codes correcteurs,* Mathématiques et Applications, Springer Berlin, Heidelberg, 1995.

[30] E. Petrank, R.M. Roth, *Is code equivalence easy to decide ?* IEEE Transactions on Information Theory, 43, 5, 1602-1604. 1997.

[31] D. J. S. Robinson, *A Course in the Theory of Groups,* second edition, Graduate Texts in Mathematics, Springer Science+Business Media New York, 1996.

[32] S. Roman, *Fundamentals of Group Theory : An Advanced Approach*, Springer Science+Business Media, LLC, 2012.

[33] P. Samuel, *Théorie algébrique des nombres*, Hermann, deuxième édition, 1971.

[34] N. Sendrier, *Un algorithme pour trouver la permutation entre deux codes binaires équivalents,* INRIA-Rocquencourt, Rapport de recherche N° 2853, avril 1996.

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

[36] J. P. Serre, *Finite Groups : An introduction*, International Press, Somerville, Massachusetts, U.S.A., 2016.

[37] J. H. van Lint, *Introduction to Coding Theory*, third edition, Graduate Texts in Mathematics, vol. 86, Springer, Berlin, 1999.

[38] J. Velu, *Méthodes mathématiques pour l'informatique*, Dunod, 1995.

[39] J. Wolfmann, *Évariste Galois et la planète Mars : introduction à la théorie algébrique du codage*, Publications de l'Institut de recherche mathématique de Rennes, 1985, fascicule 4, « Séminaires de mathématiques–science, histoire et société », p. 123-147, url : https://www.numdam.org/item/?id=PSMIR_1985___4_123_0.

Résumé

Dans ce travail, nous étudions le concept de l'équivalence par permutation des codes correcteurs et ses propriétés en nous appuyant sur l'action du groupe symétrique S_n de degré n sur l'espace $(\mathbb{F}_q^n, d_H)$. La détermination de l'équivalence est basée sur la notion de signature due à Nicolas Sendrier, on s'intéresse à un cas particulier. Enfin nous présentons une étude combinatoire des permutations admissibles formant un sous-groupe du groupe de toutes les isométries de l'espace $(\mathbb{F}_q^n, d_\pi)$, sous l'action du groupe symétrique S_m de degré m, nombre des parts d'une partition π de n.

mots-clés : action d'un groupe, codes équivalents, groupe de permutations, partition d'un entier positif, permutations admissibles, isométrie.

Abstract

In this work, we study the concept of equivalence by permutation of error-correcting codes and its properties, based on the action of the symmetric group S_n of degree n on the space $(\mathbb{F}_q^n, d_H)$. The determination of equivalence is based on the notion of signature due to Nicolas Sendrier, and we focus on a particular case. Finally, we present a combinatorial study of admissible permutations forming a subgroup of the group of all isometries of the space $(\mathbb{F}_q^n, d_\pi)$, under the action of the symmetric group S_m of degree m, the number of parts of a partition π of n.

Keywords: action of a group, equivalent codes, permutation group, partition of a positive integer, admissible permutations, isometries.

ملخص

هذا العمل يدخل في اطار نظرية الزمر المنتهية وتطبيقاتها في نظرية تشفير المعلومة. على وجه خاص من جانب دراسة تأثير الزمرة المتناظرة S_n من الدرجة n على الفضاء $(\mathbb{F}_q^n, d_H)$ ذي البعد النوني على الحقل المنتهي $\mathbb{F}_q$ مزودا بمسافة هامينغ d_H. اذ قمنا بدراسة مفهوم التكافؤ بالتبديلات للشفرات المصححة للأخطاء و خصائصه استنادا لمفهوم هذا التأثير. شفرتان C و D متكافئتان بالتبديلات اذا امكن ايجاد تبديلة σ بحيث

$$D = \sigma(C) = \{(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) : (x_1, x_2, \dots, x_n) \in C\}$$

يستند تحديد تبديل التكافؤ بين شفرتين متكافئتين على مفهوم التوقيع الذي يرجع الى نيكولا سندريي حيث قمنا بالاهتمام بحالة خاصة حيث يكون التوقيع غير مميز تماما و يحقق شرطا معينا بدقة.

من جانب اخر قمنا بإجراء دراسة توفيقية للتبديلات المقبولة S_π والتي تشكل زمرة جزئية من زمرة جميع التقايسات للفضاء المتري $(\mathbb{F}_q^n, d_\pi)$ المزود بمسافة مرفقة بتجزئة π للعدد n الذي يمثل بعد الفضاء.

هذا العمل مقسم الى ثلاثة فصول على النحو التالي :

الفصل الاول يمثل مقدمة للمفاهيم الاساسية، المصطلحات الضرورية والترميزات المهمة التي تلزم لدراسة الفصلين التاليين : الزمرة، تأثير زمرة على مجموعة، الحقل المنتهي و الشفرات المصححة للأخطاء...الخ.

الفصل الثاني مركز لدراسة مسألة تكافؤ الشفرات المصححة للأخطاء باستعمال مفهوم تأثير الزمرة المتناظرة من الدرجة النونية على فضاء هامينغ. كذلك كرسنا في هذا الفصل جزءا لدراسة حساب التبديلة المعرفة لتكافؤ الشفرتين بمفهوم توقيع نيكولا ساندريي حيث قمنا بالتعرض لحالة خاصة للتوقيع.

الفصل الثالث في هذا الفصل تطرقنا لمفهوم تجزئة عدد طبيعي لعدة أجزاء و للمسافة المرفقة بها. نسبة لهذه المسافة تقايسات الفضاء المتري $(\mathbb{F}_q^n, d_\pi)$ عبارة عن زمرة شبه جداء زمرتين جزئيتين منها، احداهما زمرة التبديلات

المقبولة. في هذا الفصل قمنا بإجراء دراسة توفيقية لزمرة التبديلات المقبولة اعتمادا على مفهوم تأثير زمرة على مجموعة.

الكلمات المفتاحية: تأثير زمرة، شفرات متكافئة، زمرة التبديلات، تجزئة عدد طبيعي، تبديلات مقبولة، تقايس.