UNIVERSITE DE M'SILA

FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du diplôme de **Master**

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Option : Mathématiques Appliquées et Discrètes

Par

DJAIL SARA

Sujet

ETUDE DE L'EQUIVALENCE DE DEUX CODES CORRECTEURS D'ERREURS PAR ISOMETRIE

Dirigé par :

Mr. MIHOUBI DOUADI

Promotion: 2011/2012

Remerciements

Je rends ma profonde gratitude à dieu qui m'a aidé à réaliser ce modeste travail.

Je tiens tout particulièrement à exprimer ma profonde gratitude à mes parents pour leur encouragement, leur soutien et pour les sacrifices qu'ils ont enduré.

Je tiens à remercier vivement mon promoteur Dr : MIHOUBI. D, d'avoir accepté de diriger ce travail et de créer autour de moi un environnement de recherche par ses conseils et son soutien permanent.

Je tiens, tout particulièrement, à exprimer ma profonde gratitude à monsieur L. LADJELAT *Maître de Conférences à l'Université de M'sila, pour ces conseils précieux et pour ces encouragements, ainsi que pour la confiance et l'aide qu'il ma accordé pour mener ce travail à terme.*

En fin, que tous ceux et celles qui m'ont aidé et soutenus durant tout mon parcours trouvent ici l'expression de mes remerciements les plus sincères.

ملخص

في هذه المذكرة، نهتم بدراسة مشكلة تقايس شفرتين مصححتين للأخطاء (تطبيق يحافظ على مسافة هامينج).

تحديد التكافؤ بين شفرتين مصححتين للأخطاء له هدف هام و هو تصنيف الشفرات.

نقول عن شفرتين أنهما متكافئتان بتقايس أو متقايستان إذا كانا ينتميان إلى نفس المدار تحت تأثير زمرة تقايسات فضاء هامينج. كحالة خاصة متكافئتان بتبديلة إذا كانت إحداهما تساوي الأخرى بتبديل الإحداثيات ، نقدم هنا دراسة تسمح بحساب هذه التبديلة.

الكلمات المفاتيح : شفرة، تكافؤ، تقايس، تبديلة.

Résumé

Dans ce travail, on s'intéresse au problème de l'équivalence de deux codes correcteurs d'erreurs par isométrie (application conservant la distance de Hamming).

La détermination de l'équivalence entre deux codes a pour but essentiel la classification des codes.

Deux codes sont équivalents par isométrie s'ils appartiennent à la même orbite sous l'action du groupe des isométries de l'espace de Hamming. En particulier ils sont équivalents par permutation s'ils sont égaux à une permutation prés de leurs coordonnées; nous présentons ici une étude capable de calculer cette permutation.

Mots clés : *codes correcteur d'erreur, équivalence, isométrie, permutation.*

Abstract

In this work, we study the problem of the isometry of two error-correcting codes. (With respect to an application conserving of the Hamming distance).

The determination of equivalence between two codes has an important focus; it is the classification of codes.

Two codes are said to be equivalent by isometry (or isometric) if they belong to the same orbit under the action of the group isometrics of the Hamming space. In the particular case, they are said equivalent by permutation if they are equal up to a permutation of the code words coordinates; we present here a study able to compute this permutation.

Key words : *error-correcting Codes, equivalence, isometry, permutation.*

SOMMAIRE

NOTATIONS

$|G|$: L'ordre d'un groupe fini G ou le cardinal d'un ensemble fini G.

$[G : H]$: L'indice du sous groupe H dans G.

$\mathbb{Z}$: L'ensemble des entiers relatifs.

$\mathbb{N}$: L'ensemble des entiers naturels.

$\mathbb{Z} / n\mathbb{Z}$: L'ensemble des entiers modulo $n \in \mathbb{N}^*$.

S_n : Groupe symétrique de n éléments.

$\bar{x}$: La classe (l'orbite) de x modulo une relation d'équivalence.

$\mathbb{K}^*$: Le groupe multiplicatif d'un corps $\mathbb{K}$ avec $\mathbb{K}^* = \mathbb{K} - \{0\}$.

$\mathbb{F}_q$: Un corps fini de cardinal q.

$\cong$: Isomorphisme de groupes, de corps, d'espaces vectoriels,…

$[x]$: La partie entière d'un réel x.

$\omega(x)$: Le poids de Hamming d'un mot x.

rg H : Le rang d'une matrice H.

$ker\ H$: L'espace nul d'une matrice H.

I_k : Matrice identique de taille $k \times k$.

${}^tA$: La transposée d'une matrice A.

$\langle x, y \rangle$: Le produit scalaire de x et y.

$C^\perp$: Le dual d'un code C.

$W_C(x, y)$ ou $W(x, y)$: Le polynôme énumérateur des poids d'un code C.

I : Un ensemble ordonné de cardinal n.

$\sigma(c)$: L'action de $\sigma \in S_n$ sur le mot c.

$\sigma(C)$: L'action de $\sigma \in S_n$ sur le code C.

$\sigma(i)$: L'image de $i \in I_n$ par σ.

$perm(C)$: Le groupe de permutations d'un code C.

$\gamma(c)$: une permutation monomiale de degré n de C.

$Aut(C)$: Le groupe d'automorphismes d'un code C.

$Isom(\mathbb{F}_q^n, d)$: Le groupe des isométries linéaires de Hamming.

$C \sim C'$: Les codes C et C' sont équivalents par permutation.

$\mathcal{V}\ (C)$: L'image de C par l'invariant $\mathcal{V}$.

$S(C, i)$: L'image du couple (C, i) par la signature S.

C_i : Le code C poinçonné en i.

INTRODUCTION GENERALE

Présentation du problème

Il est possible de définir la notion d'équivalence de deux codes de plusieurs manières :

- Comme équivalence par permutation.
- Comme équivalence par matrices monomiales.
- Comme équivalence par isométrie.

Chaque définition étant plus générale que les précédentes. Dans ce travail on s'intéresse à l'étude de tout les cas précédents. S'il s'agit des permutations, nous parlerons d'équivalence par permutation, sinon d'équivalence par isométrie.

L'étude de l'équivalence de deux codes est un problème important en théorie des codes correcteurs d'erreurs : supposons que nous ayons deux codes. Il s'agit de trouver une permutation (ou une matrice monomiale..) telle que l'image du premier code par cette permutation est le deuxième code. Deux codes équivalents ont la même structure : même distance minimale, même distribution des poids, leurs groupes de permutations sont isomorphes.

Tout cela nous a incités à nous intéresser à la détermination de l'équivalence par permutation et par isométrie des codes.

Déroulement du mémoire

Le premier chapitre est un chapitre d'introduction où nous présentons des notions et des propriétés fondamentales concernant les groupes, les corps finis et les espaces vectoriels. Nous avons étudié un peu plus en détail les groupes de permutations et les corps finis car ses notions représentent l'outil mathématique utilisé pour l'étude de l'équivalence des codes correcteurs d'erreurs.

Le deuxième chapitre regroupe les définitions et les propriétés fondamentales des codes correcteurs d'erreurs ; nous étudions les codes correcteurs et leurs paramètres. Nous nous traitons une classe particulière des codes ; à savoir les codes linéaires et le code dual. Enfin la définition du polynôme énumérateur qui sera utilisé comme invariant dans le chapitre trois.

Enfin, dans le troisième et dernier chapitre est consacré à l'étude, aussi peu détaillée, des groupes de permutations et de l'équivalence des codes : nous étudions les définitions et les propriétés des groupes de permutations des codes et la notion d'équivalence sur deux niveaux, à savoir équivalence par permutations et par isométries

(application conservant la distance Hamming). Et aussi on utilise les formes matricielles en écrivant les matrices génératrices des codes sous forme standard pour déterminer la permutation qui transforme l'une à l'autre. Enfin nous introduisons les notions des codes poinçonnés et leurs propriétés, les notions d'invariants et signatures introduites par NICOLAS SENDRIER.

Chapitre I

Définitions et propriétés élémentaires

1. Introduction

Ce chapitre est un chapitre de préliminaires. Il s'agit ici de présenter la terminologie est les principales notations ; tout en ciblant les objets étudiés.

Les définitions et résultats énoncés constituent la base pour explorer ces objets. D'autres éléments viendront les compléter au cours des différents chapitres.

2. Groupes

Dans cette section nous rappelons les définitions et les notations usuelles de la théorie des groupes.

2.1 Notation et définition

Soit G un ensemble. Une loi de composition interne sur G est une application φ de $G \times G$ dans G, notée généralement de façon infixe : on écrit $x\varphi y$ plutôt que $\varphi(x, y)$ lorsque $(x, y) \in G \times G$.

2.2 Définition

Un groupe est un ensemble non vide G muni d'une loi de composition interne définie par :

$$(x, y) \mapsto xy$$

Possédant les propriétés suivantes :

- cette loi est associative : pour tout $x, y, z \in G$

$$(xy)z = x(yz)$$

- il existe un élément neutre $e \in G$: pour tout $x \in G$

$$xe = ex = x$$

- tout élément à un inverse : pour tout $x \in G$, il existe un élément $x' \in G$ qu'on notera x^{-1}, tel que :

$$xx' = x'x = e$$

2.3 Remarque

1. Si la loi de G est commutative, c'est-à-dire pour tout $x, y \in G$ on a: $xy = yx$, on dit que G est commutatif ou abélien.

2. Si le cardinal de G est fini, G est dit fini et le nombre de ses éléments est appelé l'ordre de G, et est noté $|G|$.

2.4 Exemples

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de la somme sont des groupes abéliens.
- $\mathbb{Q}^*$, $\mathbb{R}^*$ munis du produit sont des groupes abéliens.
- Soit E un ensemble non vide. L'ensemble $S(E)$ des bijections de E muni de la loi de composition des applications est un groupe appelé le groupe symétrique de E. Si $E = \{1, \dots, n\}$ alors $S(E)$ est noté S_n et appelé le groupe de permutation de E.

2.5 Sous-groupes

Soit H une partie non vide d'un groupe G. H est appelé un sous-groupe de G si :

i) $x, y \in H \Rightarrow xy \in H$.

ii) $x \in H \Rightarrow x^{-1} \in H$.

où x^{-1} désigne l'élément symétrique de x dans G.

On écrit alors $H \leq G$.

2.5.1 Exemples

a) Pour la loi $+$, on a la "tour de groupe" (inclusions successives de sous-groupes / groupes) suivante :

$$\{0\} < 5\mathbb{Z} < \mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$$

b) Pour la multiplication usuelle :

$$\{1\} < \{-1, 1\} < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$$

c) Si G est un groupe, $\{e_G\}$ et G en constituent des sous-groupes (dits triviaux).

2.5.2 Définition

Si H est un sous-groupe de G , la relation $\mathcal{R}_d$ définie dans G par :

$$x\mathcal{R}_d y \Leftrightarrow xy^{-1} \in H$$

est une relation d'équivalence. Les classes d'équivalence à droite de x modulo H sont les ensembles de la forme $Hx = \{hx / h \in H\}$, l'ensemble quotient de G par cette relation est noté $(G/H)_d$.

On peut définir une autre relation d'équivalence, par $x\mathcal{R}_g y \Leftrightarrow x^{-1}y \in H$, et les classes sont alors les ensembles de la forme xH, appelées classes à gauche de x modulo H et noté par $(G/H)_g$.

2.5.3 Lemme

Soit H un sous-groupe de G ; il existe une bijection de $(G/H)_d$ sur $(G/H)_g$.

Preuve

Puisque pour $x, y \in G$ on a :

$$Hx = Hy \Leftrightarrow xy^{-1} \in H \Leftrightarrow (x^{-1})^{-1}\, y^{-1} \in H \Leftrightarrow x^{-1}H = y^{-1}H$$

On vérifie facilement que la correspondance $Hx \mapsto x^{-1}H$ est une application bijective de $(G/H)_d$ dans $(G/H)_g$.

Les ensembles $(G/H)_d$ et $(G/H)_g$ sont donc de même cardinal, ce dernier est appelé l'indice de H dans G et noté $[G : H]$.

On peut alors énoncer le premier théorème de la théorie des groupes.

2.6 Théorème de Lagrange

L'ordre et l'indice d'un sous-groupe H d'un groupe fini G sont des diviseurs de l'ordre de ce groupe et on a :

$$[G : H] = \frac{|G|}{|H|}$$

Preuve

Soit H un sous-groupe d'un groupe G et soit $x \in G$. L'application $y \mapsto yx$ est une bijection de H sur Hx, toutes les classes à droite sont équipotentes à H, donc sont équipotentes entre-elles.

Pour tout $x, y \in H$; soit $Hx = Hy$ ou bien soit $Hx \cap Hy = \emptyset$.

Cela permet de conclure que les classes à droite forment une partition de G.

Comme le cardinal de $(G/H)_d$ est $[G : H]$ nous avons :

$$|G| = |H|.[G : H]$$

2.6.1 Remarque

Dans le cas fini, d le cardinal d'un sous-groupe H est donc un diviseur du cardinal n du groupe G. Réciproquement, si $d|n$, il n'existe pas toujours un sous-groupe de G qui a ce cardinal d.

2.7 Groupe cyclique

L'intersection de sous-groupes de G est un sous-groupe de G, ce qui permet de définir le sous-groupe engendré par une partie A de G : c'est le plus petit sous-groupe de G qui contient A, et c'est l'intersection de tous les sous-groupes de G qui contiennent A.

On le notera $\langle A \rangle$.

2.7.1 Lemme

Soit x un élément de G, il existe un plus petit sous-groupe de G contenant x.

Preuve

Soit x un élément du groupe G, soit $(H_i)_{i\in I}$ la famille non vide des sous-groupe de G contenant x, et soit

$$H = \bigcap_{i\in I} H_i$$

un sous groupe de G contenant x. Si L est un sous-groupe de G contenant x, L est l'un des H_i , donc $H \subset L$.

Le plus petit sous-groupe d'un groupe G contenant x est appelé le sous-groupe de G engendré par x, et il est noté $\langle x\rangle$. L'élément x est dit élément générateur de $\langle x\rangle$.

2.7.2 Exemples

1. le sous-groupe de $(\mathbb{Z}, +)$ engendré par $n \in \mathbb{N}$ est l'ensemble des multiples de n dans $\mathbb{Z}$.
2. le sous-groupe $\langle 5\rangle$ de $\mathbb{Z} / 6\mathbb{Z}$ est $\{5, 4, 3, 2, 1, 0\}$.
3. Le sous-groupe $\langle 3\rangle$ de $\mathbb{Z} / 6\mathbb{Z}$ est $\{3, 0\}$.
4. le sous-groupe

   $\langle\tau\rangle$ de S_3 où $\tau(1) = 1, \tau(2) = 3, \tau(3) = 2$, est $\{id, \tau\}$

   avec id est l'application identique de $\{1,2,3\}$.

2.7.3 Définition

Un groupe G est dit cyclique s'il existe un élément x qui sera appelé générateur tel que $G = \langle x\rangle$.

Il est aisé de vérifier qu'un groupe G est cyclique de générateur x si, et seulement si, tout élément y de G s'écrit x^s où $s \in \mathbb{Z}$.

C'est-à-dire que : $\langle x\rangle = \{x^s \ / \ s \in \mathbb{Z}\}$ avec :

$$x^s = \begin{cases} x.x \ldots x & (\text{s}) \text{ fois si } \ s > 0 \\ e & \text{si } \ s = 0 \\ x^{-1}.x^{-1} \ldots x^{-1} & (-\text{s}) \text{ fois si } \ s < 0 \end{cases}$$

2.7.4 Théorème

Soit G un groupe cyclique.

1) Si G est infini ; G est isomorphe à $\mathbb{Z}$.
2) Si G est fini d'ordre $k \geq 1$, G est isomorphe à $\mathbb{Z}/k\mathbb{Z}$.

2.8 Groupes abéliens finis

Lors de la caractérisation du groupe multiplicatif d'un corps fini, nous aurons besoin au théorème principal des groupes abéliens finis qui permet de parcourir tous les modèles des groupes abéliens finis.

2.8.1 Théorème principal des groupes abéliens finis

Tout groupe abélien fini G est isomorphe à un produit direct $\prod_{i=1}^{r} H_i$ de groupes cycliques non triviaux tels que pour $i = 1,2,3\ldots,r$.

$$|\mathrm{H_i}|\text{divise}|\mathrm{H_{i+1}}|$$

2.8.2 Exemple

Il y a exactement quatre types de groupes abéliens finis non isomorphes d'ordre 100, qui sont : $\mathbb{Z}/100\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

2.9 Groupe symétrique S_n

L'étude des codes équivalents à un code est basée sur le groupe de permutations de ce code, ce groupe est un sous-groupe du groupe symétrique d'un ensemble fini utilisé pour indexer les positions des mots du code. Le groupe d'automorphisme d'un code donné montrera ce dernier comme groupe de permutations d'un autre code. Ce résultat particulier est inspiré par le théorème de CAYLEY qui permet de représenter les groupes comme groupes de permutations.

2.9.1 Théorème de CAYLEY

Tout groupe fini G d'ordre n est isomorphe à un sous-groupe de S_n.

Preuve

On fait opérer G sur lui même par translation à gauche :

$$\varphi : G \times G \to G$$
$$(g, x) \mapsto g \cdot x = gx$$

On sait que cette opération est simplement transitive.

Or, pour tout $g \in G$, l'application : $\theta(g) : G \to G$

$$x \mapsto g \cdot x$$

est un endomorphisme de G.

Et l'application : $\theta : G \to S(G)$

$$g \mapsto \theta(g)$$

est injective. (Car : $\theta(g_1) = \theta(g_2) \Rightarrow \forall x \in G, \theta(g_1)(x) = \theta(g_2)(x) \Rightarrow g_1 x = g_2 x$

$$\Rightarrow g_1 = g_2)$$

En conséquence, G est isomorphe à $Im(\theta)$, c'est-à-dire à un sous groupe de $S(G) \cong S_n$.

2.9.2 L'ordre de S_n

Pour tout $n > 1$, le groupe symétrique S_n est d'ordre $n!$

où $n! = n \times (n-1) \times \ldots \times 2 \times 1$.

Pour une permutation σ de S_n, nous écrivons

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

pour une permutation σ de S_n. Par exemple, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$ est la permutation de $\{1,2,3,4,5\}$ telle que $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 3$, $\sigma(5) = 5$.

Le groupe S_n est non commutatif dès que $n \geq 3$.

(Par exemple $(1,2)(2,3) = (1,2,3)$ et $(2,3)(1,2) = (1,3,2)$).

2.9.3 Groupe de permutations

Soit G un sous-groupe de $S(E)$. On l'appelle un groupe de permutations de E.

Le cardinal $|E|$ de E est le degré de G.

Le cardinal $|G|$ de G est l'ordre de G.

Nous noterons gx l'image $g(x)$ de $x \in E$ sous l'action de la permutation $g \in G$.

Si $gx = x$, nous disons que g fixe x (ou x est fixé par g).

Nous noterons id l'élément neutre de $S(E)$ et g^{-1} le symétrique de g.

2.9.4 Propriété

Si $g, h \in S(E)$, alors $(gh)^{-1} = h^{-1}g^{-1}$.

Preuve

Il suffit de vérifier que $h^{-1}g^{-1}$ est le symétrique de gh dans $S(E)$.

2.9.5 Proposition

Si G est un groupe de permutations de E, alors il en est de même pour xGx^{-1}, pour toute permutation x de E avec :

$$xGx^{-1} = \{xgx^{-1} \,/\, g \in G\}$$

Preuve

Il suffit de montrer que xGx^{-1} est un sous groupe de $S(E)$.

Soient $\alpha, \beta \in xGx^{-1}$; alors ils existent $g_1, g_2 \in G$ tels que :

$\alpha = xg_1x^{-1}$ et $\beta = xg_2x^{-1}$.

$$\alpha\beta = (xg_1x^{-1})(xg_2x^{-1}) = x(g_1x^{-1}xg_2)x^{-1} = xg_1g_2x^{-1} \in xGx^{-1}$$

$\alpha^{-1} = (xg_1x^{-1})^{-1} = xg_1{}^{-1}x^{-1}$; (Par la Propriété 2.9.4)

Donc : $\alpha^{-1} \in xGx^{-1}$

D'après la définition 2.5, xGx^{-1} est un sous-groupe de S(E), pour tout $x \in S(E)$.

2.9.6 Définition

Les notions sont celles de proposition 2.9.5 le groupe xGx^{-1} est appelé le groupe conjugué de G.

2.10 Action d'un groupe fini sur un ensemble

Dans toute cette section, G désigne un groupe fini et E un ensemble fini non vide.

2.10.1 Définition

Le groupe G opère sur l'ensemble E s'il existe une application :

$$\varphi : G \times E \to E$$
$$(g, x) \mapsto g \cdot x$$

satisfaisante, pour tous $g, g' \in G, x \in E$ aux conditions :

i. $g \cdot (g' \cdot x) = (gg') \cdot x$

ii. $e_G \cdot x = x$ ou e_G est l'élément neutre de G.

2.10.2 Exemple

S_n opère naturellement sur $E = \{1, \dots, n\}$ par :

$$(\sigma, x) \in S_n \times E \mapsto \sigma \cdot x = \sigma(x) \in E$$

2.10.3 Remarque et définitions

Soit G un groupe opérant sur un ensemble E. la relation $\mathcal{R}$ définie sur E par :

$$x\mathcal{R}y \Leftrightarrow \exists g \in G;\ y = g \cdot x$$

est une relation d'équivalence .

La classe de $x \in E$ pour la relation $\mathcal{R}$ est appelée l'orbite de x qui sera noté par $G.x$ ou $orb(x)$ ou $\bar{x}$

$$G \cdot x = \{g \cdot x / g \in G\} = \{y \in E / \exists g \in G\ ;\ g \cdot x = y\}$$

Ces orbites forment une partition de E.

L'ensemble $G_x = \{g \in G\ /\ g \cdot x = x\}$ est un sous groupe de G appelé le stabilisateur de x.

3. Corps finis

Nous rappelons dans cette section, des définitions et des propriétés liées au corps finis, nous le faisons très brièvement, qui seront utiles dans ce travail.

3.1 Caractéristique et cardinal d'un corps fini [10]

Soit $\mathbb{K}$ un corps. On considère l'homomorphisme d'anneaux $\varphi : \mathbb{Z} \to \mathbb{K}$ défini par : $\varphi(n) = n \cdot 1 = 1 + \cdots + 1$. $ker\,\varphi$ est un idéal de $\mathbb{Z}$ de la forme $p\mathbb{Z}$. D'autre part, les théorèmes d'isomorphisme donnent $\mathbb{Z}/p\mathbb{Z} \sim \varphi(\mathbb{Z})$ qui est inclus dans $\mathbb{K}$, il est donc intègre. Alors deux cas : p = 0 ou p est un nombre premier.

3.2 Définition

Le nombre p est appelé la caractéristique du corps $\mathbb{K}$. Il est noté $car(\mathbb{K})$.

3.3 Remarques

1. Si $car(\mathbb{K}) = 0$ alors $\varphi(\mathbb{Z})\sim\mathbb{Z}$, donc $\mathbb{K}$ est infini. Alors $\mathbb{Q}$ est le sous-corps premier de $\mathbb{K}$.
2. Si $\mathbb{K}$ est fini on a $p = car(\mathbb{K}) > 0$ alors le sous-corps premier de $\mathbb{K}$ est $\mathbb{Z}/p\mathbb{Z}$ que l'on note aussi $\mathbb{F}_p$. Donc $|\mathbb{K}| = p^m$. Le cardinal d'un corps fini est une puissance d'un nombre premier.

3.4 Définition

Un corps de q éléments est dit un corps fini de cardinal q.

3.5 Exemples

a) Pour p premier; $\mathbb{F}_p$ est un corps fini de cardinal p.

b) L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.

c) $car(\mathbb{Q}) = car(\mathbb{R}) = car(\mathbb{C}) = 0$.

3.6 Théorème

Soit $\mathbb{K}$ un corps fini. Posons $q = card(\mathbb{K})$ alors

i) La caractéristique de $\mathbb{K}$ est un nombre premier p.

ii) $\mathbb{K}$ est un espace vectoriel de dimension finie n sur $\mathbb{F}_p$ et on a $q = p^n$.

Preuve

Comme $\mathbb{Z}$ est infini, $\mathbb{K}$ ne peut être de caractéristique nulle. Donc il contient $\mathbb{F}_p$ avec p premier. Ainsi $\mathbb{K}$ est un espace vectoriel sur $\mathbb{F}_p$, sa dimension n est finie, sinon $\mathbb{K}$ serait infini. En tant qu'espace vectoriel $\mathbb{K}$ est isomorphe à $\mathbb{F}_p^n$; donc $\mathbb{K}$ a p^n éléments.

3.7 Théorème [8]

Soit $\mathbb{K}$ un corps fini de cardinal q.

Le groupe multiplicatif $(\mathbb{K}^*,\cdot)$ est cyclique d'ordre $q - 1$.

Preuve

Le groupe $(\mathbb{K}^*,\cdot)$ est commutatif (car tout corps fini est commutatif, c'est le théorème de WEDDERBURN) et fini. D'après le théorème 2.8.1, il existent des groupes cycliques $H_1, \dots, H_r$ tels que :

$$\mathbb{K}^* \cong H_1 \times H_2 \times \ \dots \times H_r$$

et pour tout $i = 1,2,3\dots, r-1$, $|\mathrm{H_i}|$divise$|\mathrm{H_{i+1}}|$.

L'entier $s = |H_r|$ est donc un exposant de chaque élément de $\mathbb{K}^*$ donc pour tout $x \in \mathbb{K}^*$, $x^s = 1$; en d'autre terme tout les éléments de $\mathbb{K}^*$ sont racine du polynôme $x^s - 1 \in \mathbb{K}[x]$ or ce polynôme admet au plus s racines donc :

$$|\mathbb{K}^*| \leq s$$

Mais $|H_r| = s$ divise $|\mathbb{K}^*|$, d'où $|H_r| = |\mathbb{K}^*|$, et comme $\mathbb{K}^*$ est fini cela entraîne que $\mathbb{K}^* = H_r$.

3.8 Théorème

Soit $\mathbb{K}$ un corps fini de cardinal q.

Pour tout $x \in \mathbb{K}^*$ on a $x^{q-1} = 1$, et pour tout $x \in \mathbb{K}$ on a $x^q = x$.

Preuve

D'après le théorème 3.7, l'ordre de $\mathbb{K}^*$ est $q - 1$; donc pour tout $x \in \mathbb{K}^*$ on a $x^{q-1} = 1$ et par conséquent pour tout $x \in \mathbb{K}$ on a $x^q = x$.

Il en résulte du théorème 3.8 Qu'un corps fini $\mathbb{K}$ à q éléments est l'ensemble des racines du polynôme $x^q - x$.

On note souvent $\mathbb{F}_q$ un corps fini à q éléments.

4. Espaces vectoriels

Dans cette section nous rappelons quelques définitions nécessaires de l'algèbre linéaire, nous citons certaines propriétés qui seront utiles pour définir les codes linéaires à travers le chapitre II.

4.1 Notations

Soit V un espace vectoriel sur un corps $\mathbb{K}$.

V^n désigne l'ensemble des n-uplets $(v_1, v_2, \ldots, v_n)$ avec $v_i \in V$, $dim\, V$ désigne la dimension de V sur $\mathbb{K}$.

4.2 Proposition

Soit $\mathbb{K}$ un corps, l'ensemble $\mathbb{K}^n$ muni de l'addition définie par :

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

et la multiplication par scalaire $\lambda \in \mathbb{K}$:

$\lambda(x_1, x_2, \ldots, x_n) = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$ est un espace vectoriel de dimension n sur $\mathbb{F}_q$.

4.3 Sous espace vectoriel

Soit W un sous ensemble d'un espace vectoriel V sur un corps $\mathbb{K}$. W est un sous espace de V si et seulement si pour tout $\mu, v \in W$, $\lambda \in \mathbb{K}$. $\mu v \in W$ et $\lambda\mu \in W$.

4.4 Exemples

- Soit $V = \mathbb{F}_2^2$ alors $W = \{(a, 0) \,/\, a \in \mathbb{F}_2\}$ est un sous espace de V.
- $W = \{v = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n \,/\, x_1 + x_2 + \ldots + x_n = 0\}$ est un sous espace sur $\mathbb{F}_q$.

4.5 Définitions

Soit $f : V \to W$ une application linéaire et soit A la matrice associée à f.

$ker\, f = ker\, A = \{v \in V / f(v) = 0\}$ est le noyau de f ou l'espace nul de la matrice A .

$Im\, f = f(V) = A.V = \{f(v)\ / v \in V\} = \{A.v / v \in V\}$ est l'espace image de f (ou de la matrice A).

On rappelle que $ker\, f$ (resp. $Im\, f$) est un sous-espace de V (resp. de W).

4.6 Théorème

V et W sont des espaces vectoriels sur $\mathbb{K}$ de dimensions finies.

Soit $T : V \to W$ une application linéaire alors :

$$dim\, V = dim(ker\, T)\ + dim\, T(V)$$

Preuve

En effet il est facile de remarquer que $V / ker\, T$ est isomorphe à $T(V)$ en tant qu'espaces vectoriels.

4.7 Théorème

Soit V un espace vectoriel de dimension finie $n = dim\, V$ sur un corps $\mathbb{K}$ alors :

1) V est isomorphe à $\mathbb{K}^n$.
2) Si $\mathbb{K}$ est un corps fini de cardinal q, V est fini de cardinal q^n.

Preuve

Pour 1), il suffit de considérer l'isomorphisme

$$V \quad \to \quad \mathbb{K}^n$$

$$\alpha_1 e_1 + \cdots + \alpha_n e_n \mapsto (\alpha_1, \ldots, \alpha_n)$$

Où $(e_1, e_2, \ldots, e_n)$ est une base de V sur $\mathbb{K}$.

Pour 2), il découle de 1).

Chapitre II

Codes correcteurs d'erreurs

1. Introduction

Coder, ou encoder une information consiste à lui donner temporairement une certaine forme, l'information étant ultérieurement restituée. Encoder une information peut avoir plusieurs buts.

- Le stockage, la compression de données en est un exemple.
- La possibilité de détecter et / ou de corriger les erreurs qui surviennent lors de la transmission de cette information, c'est-à-dire lorsque l'information devient message. C'est l'objet des codes correcteurs d'erreurs, appelés plus simplement codes correcteurs. C'est ce cadre qui nous intéresse ici.

Le principe de base des codes correcteurs est de rajouter à un message à transmettre une information supplémentaire, appelée information redondante ou de contrôle, de manière à pouvoir détecter et éventuellement corriger de possibles erreurs de transmission. Cette opération s'appelle encodage du message et son résultat est un mot de code. A chaque message est donc associé un mot de code de longueur supérieure à celle du message. Le code est l'ensemble des mots de code ainsi obtenus.

2. Les codes

Soit A un ensemble non vide à q éléments, A sera appelé un alphabet. On commence par supposer que tous les messages à transmettre sont des mots de même longueur $k > 0$ écrits à l'aide d'un alphabet A à q éléments. Chaque message noté $x = x_1 x_2 \dots x_k$, est assimilé à un élément $(x_1, x_2, \dots, x_k)$ de l'ensemble A^k, qui devient ainsi l'espace des messages. On a alors q^k messages possibles; c'est-à-dire l'ensemble des messages sera un partie E de A^k.

La technique du codage par bloc consiste à associer à chaque $x = (x_1, x_2, \dots, x_k) \in E$, un mot plus long, c'est-à-dire un mot de A^n, de façon unique. On introduit ainsi une application injective :

$$\varphi : E \to A^n$$
$$x = (x_1, x_2, \dots, x_k) \mapsto c = (c_1, c_2, \dots, c_n)$$

appelée application de codage ou encodeur. Le message $x \in E$ est modifié pour fournir le mot $c = \varphi(x) \in A^n$. C'est le mot C qui sera transmis et lu par un système quelconque pour donner un message reçu $y = (y_1, y_2, \ldots, y_n)$ qui contient éventuellement quelques erreurs. Notons $C = \varphi(E)$ l'image de φ.

2.1 Définition

un code de longueur n sur l'alphabet A est un sous ensemble non vide C de A^n, et les éléments de C s'appellent les mots du code.

2.2 Exemples

1) $C_1 = \{011,101,110,000\}$ est un code de longueur 3 sur $A = \{0,1\} = \mathbb{F}_2$.
2) $C_2 = \{0101,1010,1111,0000\}$ est un code de longueur 4 sur $\mathbb{F}_2$ et de cardinale 4.
3) $C_3 = \{aa, ba, ab\}$ est un code de longueur 2 sur $A = \{a, b\}$ et de cardinale 3.

2.3 Distance de Hamming

2.3.1 Définition

La distance de Hamming entre deux mots $x = (x_1 x_2 \ldots x_n)$ et $y = (y_1 y_2 \ldots y_n)$ de A^n, et l'on note $d(x, y)$, est le nombre d'indices i de $\{1,2, \ldots, n\}$ tels que $x_i \neq y_i$.
C'est-à-dire :

$$d(x, y) = |\{i / x_i \neq y_i\}|$$

2.3.2 Remarque

On remarquer que la distance de Hamming, est une vraie distance au sens métrique du terme. Rappelons brièvement les propriétés d'une distance $d(x, y)$, faciles à vérifier sur d.

i) $d(x, y) = d(y, x) \geq 0$
ii) $d(x, y) = 0$ si et seulement si $x = y$.
iii) $d(x, y) \leq d(x, z) + d(z, y)$.

Dans la suite, on notera $B(x, R) = \{y \in \mathbb{F}_q^n \ / \ d(x, y) \leq R\}$, la boule de centre x et de rayon R pour la distance de Hamming.
On peut remarquer que $y \in B(x, R) \Leftrightarrow y - x \in B(0, R)$.

2.3.3 Exemple

1) nous avons $d(011,101) = 2$ pour l'exemple 2.2.1).
2) $d(1010,1111) = 2$ et $d(1010,0101) = 4$ pour l'exemple 2.2.2).
3) $d(aa, ab) = 1$ pour l'exemple 2.2.3).

2.3.4 Distance minimale d'un code

La distance minimale d'un code C est la distance minimum entre deux mots distincts de ce code. On la note d :

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

Un code C de longueur n, de cardinal M et de distance minimale d est appelé un code $[n, M, d]$. Les nombres n, M, d sont les paramètres du code.

Sa capacité de correction théorique est définie à partir de cette distance minimale :

2.4 Capacité de correction

2.4.1 Proposition [14]

Soit C un code de distance minimum d, et soit x un message reçu affecté de r erreurs avec $r \geq 1$.

1. Si $2r < d$, c'est-à-dire si $r \leq [(d-1)/2]$, le code C corrige les r erreurs.
2. Si $[(d-1)/2] < r = [d/2]$, (ce qui suppose d pair) le code C détecte l'existence de r erreurs mais ne peut pas toujours les corriger.
3. Si $[d/2] < r \leq d-1$, le code C détecte l'existence d'erreurs mais risque d'effectuer une correction erronée.

Preuve

Soit m le mot de code émis, on a par hypothèse $d(m, x) = r$.

1) Le mot de code m est alors le seul mot de code tel que $d(m, x) \leq r$ supposons en effet un mot de code m′ vérifiant $d(m', x) \leq r$, on a nécessairement $m' = m$ puisque

$$d(m', m) \leq d(m', x) + d(m, x) \leq 2r \leq d - 1 < d$$

2) Il n'existe pas de mot de code m' tel que $d(m', x) < d(m, x) = r$, mais le mot de code m n'est plus nécessairement le seul à vérifier

$$d(m, x) = r$$

3) On sait qu'il y a erreur car x n'appartient pas à C, mais il peut exister un mot de code m′ tel que $d(m', x) < d(m, x) = r$.

L'entier $t = [(d-1)/2]$ est appelé capacité de correction du code C, on dit que C est un code t-correcteur.

2.4.2 Exemple

Dans $\mathbb{F}_2^3$, le code $C = \{011,101,110,000\}$ est de distance minimale 2, ce code détecte une erreur sans pouvoir la corriger.

2.5 Le poids de Hamming

Le poids de Hamming d'un mot $x = (x_1, \dots, x_n)$, noté $\omega(x)$, est le nombre d'indices i tels que $x_i \neq 0$.

$$\omega\,(x) = |\{i\ /\ x_i \neq 0\}| = d(x, 0)$$

Par exemple, dans $\mathbb{F}_2^3$, nous avons $\omega(110) = 2$ et $\omega(001) = 1$.

3. Les Codes linéaires

Dans tout ce qui suit, on choisit pour alphabet A le Corps $\mathbb{F}_q$ à q éléments. Choisissons $E = \mathbb{F}_q^k$ comme ensemble de message. L'ensemble E devient maintenant un espace vectoriel de dimension k sur $\mathbb{F}_q$, et il est naturel de ne considérer que les fonctions d'encodage φ linéaires. Le code $C = \varphi(\mathbb{F}_q^k)$ est alors structuré en sous-espace vectoriel de $\mathbb{F}_q^n$.

3.1 Définition

Un code linéaire de longueur n et de dimension k sur $\mathbb{F}_q$ est un sous-espace vectoriel de dimension k de $\mathbb{F}_q^n$. On supposera toujours $k \geq 2$.

Si la distance minimale de C est d, on dit que C est un code q-aire de paramètres $[n, k, d]$ ou $[n, M, d]_q$-code, et si $q = 2$; le code C est dit code binaire.

Pour un code linéaire C, on retrouve la distance de Hamming par la formule $d(x, y) = \omega(x - y)$, et la distance minimale du code C par

$$d = min\{\omega(\,x\,)\ /\ x \in C\ et\ x \neq 0\}$$

Il résulte de ce qui précède qu'un code linéaire de dimension k possède $M = q^k$ mots indépendamment de sa longueur n.

3.2 Proposition (Borne de singleton)

Soit C un code linéaire de paramètres $[n, k, d]$. Alors C vérifie l'inégalité de Singleton :

$$d + k \leq n + 1$$

Preuve

Soit E le sous-espace vectoriel de $\mathbb{F}_q^n$ constitué des mots dont les $k - 1$ dernières composantes sont nulles. Alors :

$$dim(E) = n - (k - 1) = n - k + 1$$

On en déduit : $dim(C) + dim(E) = n + 1 > n$, ce qui implique $C \cap E \neq \{0\}$.

Soit m un mot non nul de $C \cap E$, on a $d \leq \omega(m) \leq n - k + 1$.

3.3 Définition (Maximum Distance Separable)

Soit C un code linéaire $[n, k, d]$. Le code C est dit maximum distance separable (MDS) s'il atteint la borne de Singleton c'est-à-dire si:

$$d + k = n + 1$$

3.4 Matrice génératrice

Soit C un code. L'espace de messages étant identifié à $\mathbb{F}_q^k$, on encode les messages à l'aide d'un application injective $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^n$ tel que $Im(\varphi) = C$.

Ce qui signifie que si $x = x_1 x_2 \dots x_k$ est un message à encoder, l'encodage $x \mapsto \varphi(x)$ sera représenté matriciellement par :

$$\varphi : x = x_1 x_2 \dots x_k \to (x_{1,} x_{2,} \dots, x_k) G = xG$$

Où G est la transposée de la matrice de φ par rapport aux bases canoniques respectives des espaces vectoriels $\mathbb{F}_q^k$ et $\mathbb{F}_q^n$, c'est-à-dire une matrice de taille $k \times n$ à coefficients dans $\mathbb{F}_q$. Si $g_1, g_2, \dots, g_k$ désignent les k ligne de la matrice G, on a :

$$(x_1 x_2 \dots x_k) G = x_1 g_1 + x_2 g_2 + \cdots x_k g_k$$

3.4.1 Définition

Une matrice génératrice du code C est un matrice G de taille $k \times n$ à coefficients dans $\mathbb{F}_q$ dont les lignes forment une base de l'espace vectoriel C telle que :

$$C = \{c \in \mathbb{F}_q^n \ / \exists\ x \in \mathbb{F}_q^k ; c = xG\}$$

3.4.2 Exemple

Soit G la matrice génératrice du [3,2] code binaire C telle que :

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

déterminions C :

$$C = \{ c_1\ (1,1,0) + c_{\ 2}(0,1,1\ ) \ / \ c_1, c_2 \in F_2\}$$

$$C = \{000,011,110,101\}$$

Ainsi le code C est de paramètres [3,2,2] et $|C| = q^k = 2^2 = 4$, et par exemple le message 11 est codé par $c = 11G = 101$.

3.5 Matrices de contrôle

On peut aussi se donner un sous-espace vectoriel par un système d'équations indépendantes. Soit C un code linéaire. Une matrice de contrôle de C est la matrice d'un système d'équations linéaires homogènes indépendantes dont l'espace des solutions est C.

3.5.1 Définition

une matrice de contrôle H d'un $[n,k,d]_q$-code C est une matrice de taille $(n-k)\times n$ et de rang maximum $(n-k)$, à coefficients dans $\mathbb{F}_q$ telle que :

$$C=\{c\in\mathbb{F}_q^n \,/\, H\,{}^t c=0\}$$

Autrement dit : $C=ker(H)$.

3.5.2 Exemple

Supposons $q=2,\ n=6,\ k=3$ (donc $M=2^3=8$).

Soit C le code de paramètres $[6,3]$ donné par la matrice de contrôle

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

Comme $C=ker(H)$

$c=(c_1,c_2,c_3,c_4,c_5,c_6)\in H \Leftrightarrow H\,{}^t c=0$

$$\Leftrightarrow\begin{cases}c_1+c_2+c_4=0\\c_1+c_3+c_5=0\\c_2+c_3+c_6=0\end{cases}\Leftrightarrow\begin{cases}c_4=-c_1-c_2\\c_5=-c_1-c_3\\c_6=-c_2-c_3\end{cases}$$

$c\in C \Leftrightarrow c=(c_1,c_2,c_3,-c_1-c_2,-c_1-c_3,-c_2-c_3)$

$\Leftrightarrow c=c_1(1,0,0,-1,-1,0)+c_2(0,1,0,-1,0,-1)+c_3(0,0,1,0,-1,-1)$

$\Leftrightarrow c=c_1(1,0,0,1,1,0)+c_2(0,1,0,1,0,1)+c_3(0,0,1,0,1,1)$

$\Leftrightarrow c=c_1v_1+c_2v_2+c_3v_3.$

Donc C est le sous espace de $\mathbb{F}_2^6$ sur $\mathbb{F}_2$ engendré par les vecteurs v_1,v_2,v_3 ou c_1,c_2,c_3 décrive $\mathbb{F}_2$.

Si le message $a=011$ est transmis, alors le mot de code correspond est $c=011110$.

Le code C contient 2^3 mots de code :

$$\{000000,001011,010101,011110,100110,101101,110011,111000\}$$

3.5.3 Théorème

Soit G un matrice génératrice du code C.

Une matrice H de taille $(n-k)\times n$ et de rang $(n-k)$, à coefficients dans $\mathbb{F}_q$, est une matrice de contrôle de C si seulement si on a la relation :

$$H\,{}^t G=0$$

Preuve

Dire que $H\,{}^tG = 0$ équivaut à dire que pour vecteur colonne c de la matrice ${}^tG$, on a $H(c) = 0$. Or les vecteurs colonne de ${}^tG$ sont les vecteurs lignes de G et l'on sait qu'ils constituent une base de l'espace vectoriel C. Donc on a l'inclusion $C \subseteq ker(H)$.

La matrice H étant de rang $(n-k)$, il résulte du théoréme du rang que

$$dim(ker(H)) = n - (n-k) = k = dim(C)$$

d'où l'égalité $C = ker(H)$.

4. Codes systématiques

4.1 Définition

Un $[n,k,d]_q$-code est systématique s'il possède une matrice génératrice que l'on peut écrire par blocs sous la forme

$$G = (I_k \backslash B)$$

Où I_k désigne la matrice unité à k lignes et k colonnes, et B est un matrice de taille $k \times (n-k)$.

L'intérêt d'un code systématique tient au fait que si un message $x = x_1 x_2 \dots x_k$ est encodé par une matrice normalisé G, on le trouve sous forme des k premières composantes du code xG associé à x, puisque

$$c = (\underbrace{x_1 x_2 \dots x_k}_{x}\, c_{k+1} \dots c_n) = xG = (x_1 x_2 \dots x_k)(I_k \backslash B)$$

4.2 Corollaire

Soit C un code systématique, et soit $G = (I_k \backslash B)$ une matrice génératrice normalisée de C. La matrice

$$H = (-{}^tB \backslash I_{n-k})$$

est une matrice de contrôle de C.

Preuve

La matrice ${}^tG$ s'écrit par blocs sous la forme ${}^tG = \begin{pmatrix} I_k \\ {}^tB \end{pmatrix}$, on a donc :

$$H\,{}^tG = (-{}^tB \backslash I_{n-k}) \begin{pmatrix} I_k \\ {}^tB \end{pmatrix} = -{}^tB + {}^tB = 0.$$

4.3 Exemples

a) L'encodage $\varphi(x_1, x_2, x_3) = (x_1, x_2, x_3, x_1 + x_3, x_2 + x_3, x_1 + x_2 + x_3, x_3)$ définit un code systématique C de paramètres [7,3] sur $\mathbb{F}_2$.

L'écriture :

$$(c_1, c_2, \ldots, c_7) = (x_1, x_2, x_3)\left(\begin{array}{ccc|cccc} 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

met en évidence une matrice génératrice de C, et l'on déduit la matrice de contrôle

$$\mathrm{H} = \left(\begin{array}{ccc|cccc} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

b) Soit C le code linéaire de paramètres $[7, 4, 3]$ dont la matrice génératrice est donnée par :

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \sim G' = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ \underbrace{0 & 0 & 0 & 1}_{\mathrm{I}_4} & \underbrace{0 & 1 & 1}_{\mathrm{A}} \end{array}\right)$$

D'ou la matrice de contrôle est donnée par:

$$H' = \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ \underbrace{1 & 1 & 0 & 1}_{-{}^{t}A} & \underbrace{0 & 0 & 1}_{I_3} \end{array}\right)$$

5. Dualité

Soit n un entier naturel non nul.

Le produit scalaire euclidien sur $\mathbb{F}_q^n$ est la forme bilinéaire symétrique qui à pour tout $x = (x_1, x_2, \ldots, x_n)$ et $y = (y_1, y_2, \ldots, y_n)$ deux mots de $\mathbb{F}_q^n$ associé l'élément

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$$

de $\mathbb{F}_\mathrm{q}$.

Par exemple, le produit scalaire euclidien sur $\mathbb{F}_2^3$ de $x = 110$ et $y = 111$ est : $\langle x, y \rangle = 1.1 + 1.1 + 0.1 = 0$

5.1 Définitions

1) Deux mots x, y de $\mathbb{F}_q^n$ sont dits orthogonaux si $\langle x, y \rangle = 0$.
2) Soit C un code linéaire de longueur n, le dual ou l'orthogonal de C est l'ensemble :

$$C^{\perp} = \{y \in \mathbb{F}_q^n;\ \forall x \in C\ ;\ \langle x, y \rangle = 0\}$$

Pour un code linéaire C, le dual $\mathrm{C}^{\perp}$ est aussi un code linéaire sur $\mathbb{F}_\mathrm{q}$. Si de plus C est de matrice génératrice G et de matrice de contrôle H, alors $C^{\perp}$ serait de matrice

génératrice H et de matrice de contrôle G, l'orthogonalité permet de déduire que : $G\,{}^tH = H\,{}^tG = 0$.

Enfin remarquons que si C est un code linéaire $[n,k]$ alors $C^\perp$ est un $[n,n-k]$ car : $dim\,C + dim\,C^\perp = n$.

5.2 Propriétés

Soit C_1 et C_2 deux codes.

i) $(C_1^\perp)^\perp = C_1$.

ii) $(C_1 + C_2)^\perp = C_1^\perp \cap C_2^\perp$ avec $C_1 + C_2 = \{c_1 + c_2 / c_1 \in C_1 \text{et } c_2 \in C_2\}$.

Il peut arriver que pour un code C, le dual $C^\perp$ contient C.

Si $C \subset C^\perp$, alors C est appelé un code auto-orthogonale.

Un code linéaire C est dit un code auto-dual si $C = C^\perp$. La longueur n est alors nécessairement paire. Si G est une matrice génératrice de C, alors C est auto-dual si et seulement si, $n = 2\,dim\,C$ et $G\,{}^tG = 0$.

5.3 Exemples

1. Soit le code linéaire binaire de matrice génératrice

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

Alors $G\,{}^tG = 0$. Par suite, C est auto-dual.

2. Soit le code $C = \{000,011,101,110\}$ de longueur 3 sur $\mathbb{F}_2$ le dual $C^\perp$ de C est $C^\perp = \{y \in \mathbb{F}_2^3, y = abc, \forall c \in C, \langle c, y\rangle = 0\}$.

$$\begin{cases} b + c = 0 \\ a + c = 0 \\ a + b = 0 \end{cases} \Rightarrow \begin{cases} a = b = c = 0 \\ \text{ou} \\ a = b = c = 1 \end{cases}$$

Donc $y_1 = 000$, $y_2 = 111$ d'où $C^\perp = \{000,111\}$.

3. Soit le code $C = \{0000,0011,1100,1111\}$ de longueur 4 sur $\mathbb{F}_2$, le dual $C^\perp$ de C est $C^\perp = \{0000,0011,1100,1111\}$ on remarque que $C^\perp = C$.

6. Le polynôme énumérateur

Le polynôme énumérateur des poids d'un code représente un invariant de ce code qui permet d'étudier des propriétés concernant les poids des mots du code.

6.1 Définition

1) La distribution des poids d'un code C linéaire est le n-uplet $(A_0, A_1, \ldots, A_n)$, où A_i est égal au nombre des mots de C de poids i. En particulier, $A_0 = 1$ et

$$\sum_{i=0}^{n} A_i = q^k$$

où k est la dimension de C.

2) Le polynôme enumérateur des poids d'un code C de longueur n sur $\mathbb{F}_q$ est le polynôme homogène en deux variables x et y, de degré n, défini par:

$$W_C(x,y) = \sum_{c \in C} x^{n-\omega(c)} y^{w(c)} = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

On a (formule de MacWilliams) :

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

pour la démonstration voir par exemple [3].

3) Si nous remplaçants x par 1, nous obtiendrons aussi un polynôme énumérateurs $W_C(y)$ avec

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

qui est le plus utilisé.

6.2 Exemples

a) Considérons le code $C = \{000,011,101,110\}$ de longueur 3 sur $\mathbb{F}_2$ le dual $C^\perp$ de C est $C^\perp = \{000,111\}$ et les polynômes énumérateurs sont respectivement :

$$W_C(x,y) = x^3 + 3xy^2$$
$$W_{C^\perp}(x,y) = x^3 + y^3$$

b) Le code $D = \{00,11\}$ de longueur 2 sur $\mathbb{F}_2$, est auto-dual car $D^\perp = D$ et $W_D(x,y) = W_{D^\perp}(x,y) = x^2 + y^2$.

D'après la formule de MacWilliams on a :

Pour l'exemple a) :

$$\begin{aligned} W_{C^\perp}(x,y) &= \frac{1}{4} W_C(x+y, x-y) \\ &= \frac{1}{4}[(x+y)^3 + 3(x+y)(x-y)^2] \\ &= x^3 + y^3 \end{aligned}$$

pour l'exemple b) :

$$\begin{aligned} W_{D^\perp}(x,y) &= \frac{1}{2} W_D(x+y, x-y) \\ &= \frac{1}{2}[(x+y)^2 + (x-y)^2] \\ &= x^2 + y^2 \end{aligned}$$

Chapitre III

Isométrie linéaire des codes linéaires

1. Introduction

La notation d'équivalence entre deux codes est liée à la notion de groupe de permutation. Elle peut être définie en plusieurs niveaux. Supposons que nous ayons deux codes. Il s'agit de trouver une permutation telle que l'image du premier code par cette permutation est le deuxième code. S'il s'agit de permutation nous dirons que les codes sont équivalents par permutation, si non nous dirons simplement équivalents ou isomorphe.

Deux codes équivalents ont la même distance minimale, même distribution des poids, leurs groupes de permutation (ou d'automorphisme) sont isomorphes.

Tout cela nous a incités à nous intéresser à la détermination de l'équivalence de code.

2. Groupe de permutations et d'automorphismes des codes

Dans cette section nous définissons le groupe de permutations et le groupe d'automorphismes d'un code. Ces groupe, ainsi définis, ont la propriété de préserver la distance de Hamming : ce sont des groupes d'isométrie.

2.1 Groupe de permutations d'un code

Soient n un entier positif non nul et q une puissance d'un nombre premier.

Soit $I = \{1,2,\dots,n\}$ un ensemble ordonné de cardinal n utilisé pour indexer les cordonnées des mots de $\mathbb{F}_q^n$.

Une permutation $\sigma \in S_n$ agit sur les mots de $\mathbb{F}_q^n$ comme suit :

Si $C = (c_i)_{i\in I}$ est un mot de $\mathbb{F}_q^n$, alors :

$$\sigma(C) = \left(c_{\sigma(i)}\right)_{i\in I} = \left(c_{\sigma(1)}, c_{\sigma(2)}, \dots, c_{\sigma(n)}\right)$$

La permutation σ de S_n définit une action sur le code C comme suit :

$$(\sigma, C) \mapsto \sigma(C)$$

avec $\sigma(C) = \{\sigma(c)/c \in C\}$.

2.1.1 Notation

Soit C un code de longueur n sur $\mathbb{F}_q$. Notons $perm(C)$ le sous ensemble de tous les éléments σ de S_n; tels que $\sigma(C) = C$. i .e :

$$perm(C) = \{\sigma \in S_n \,/\, \sigma(C) = C\}$$

2.1.2 Proposition

L'ensemble $perm(C)$, muni du produit usuel des permutations, est un sous groupe de S_n.

Preuve

D'après la définition d'un sous-groupe, il suffit de démontrer que $\sigma_1\sigma_2 \in perm(C)$ et $\sigma_1^{-1} \in perm(C)$ si $\sigma_1, \sigma_2 \in perm(C)$.

Comme $\sigma_1, \sigma_2 \in perm(C)$, nous avons :

$$\begin{aligned}\sigma_1\sigma_2(C) &= \sigma_1\big(\sigma_2(C)\big)\\ &= \sigma_1(C) \text{ car } \sigma_2 \in perm(C)\\ &= C \text{ car } \sigma_1 \in perm(C)\end{aligned}$$

Donc : $\sigma_1\sigma_2 \in perm(C)$.

comme $\sigma_1 \in perm(C)$, alors $\sigma_1(C) = C$, ce qui entraîne que :

$$\begin{aligned}\sigma_1^{-1}\big(\sigma_1(C)\big) = \sigma_1^{-1}(C) &\Leftrightarrow \sigma_1^{-1}\sigma_1(C) = \sigma_1^{-1}(C)\\ &\Leftrightarrow id(C) = \sigma_1^{-1}(C)\\ &\Leftrightarrow C = \sigma_1^{-1}(C)\end{aligned}$$

ce qui veut dire que $\sigma_1^{-1} \in perm(C)$.

2.1.3 Définition

le sous groupe $perm(C)$ de S_n est appelé le groupe de permutations du code C.

2.1.4 Exemples

a) Soit C le code $[3,2]$ défini sur $\mathbb{F}_2$ par sa matrice génératrice G avec

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

C'est -à dire que :

$$C = \{x(0,1,1) + y\,(1,1,0) \text{ où } x, y \in \mathbb{F}_2\}$$

$$C = \{000, 011, 110, 101\}$$

S_3 désigne le groupe symétrique de degré 3 il est donc d'ordre $3! = 6$ à savoir $S_3 = \{id\,, (12), (13), (23), (123), (132)\}$.

pour tout permutation $\sigma \in S_3$, déterminons $\sigma(C)$.

$$id(C) = C$$

$$(12)(C) = \{000, 101, 110, 011\} = C$$

$$(13)(C) = \{000, 110, 011, 101\} = C$$

$$(23)(C) = \{000, 011, 101, 110\} = C$$

$$(123)(C) = \{000, 101, 011, 110\} = C$$
$$(132)(C) = C$$

cela permet de conclure que $perm(C) = S_3$.

b) Soit C_1 le code [3,2] sur $\mathbb{F}_2$ de matrice génératrice G' :

$$G' = (101)$$

Alors :

$$C_1 = \{000, 101\}$$

déterminations (C_1), pour tout $\sigma \in S_3$:

$$id(C_1) = C_1$$
$$(12)(C_1) = \{000, 011\} = C_2$$
$$(13)(C_1) = \{000, 101\} = C_1$$
$$(23)(C_1) = \{000, 110\} = C_3$$
$$(123)(C_1) = \{000, 011\} = C_2$$
$$(132)(C_1) = \{000, 110\} = C_3$$

donc $perm(C_1) = \{id, (13)\}$.

c) Le groupe de permutation du code {0000,0011,1100,1111} sur $\mathbb{F}_2$ est composé des 8 permutations suivantes :

$$id, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)$$

où la notation (ij) désigne une transposition, et $(ijkl)$ désigne un cycle d'ordre 4.

2.2 Groupe d'automorphismes d'un code

2.2.1 Permutation monomiales

2.2.1.1 Définition (matrice de permutations)

Une matrice de permutation est une matrice $n \times n$ inversible à coefficients dans $\{0, 1\} \subset \mathbb{F}_q$ ayant un et un seul élément non nul par ligne et par colonne.

2.2.1.2 Exemples

a) La matrice

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

est une matrice de permutation sur $\mathbb{F}_3$.

b) La matrice

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

est une matrice de permutation sur $\mathbb{F}_q$.

Si $c \in \mathbb{F}_q^n$ et P est une matrice de permutation, alors le produit cP donne un mot de $\mathbb{F}_q^n$ qui est égal en fait à c avec des coordonnées permutées, c'est la raison pour laquelle les matrices de cette sorte dit matrices de permutation.

Par exemple : si $c = (1,2,0)$ de $\mathbb{F}_3^3$ et P la matrice de permutation de l'exemple i) nous aurons :

$$c.P = (1,2,0)\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix} = (1,0,2)$$

2.2.1.3 Définition (matrice monomiale)

Une matrice monomiale est une matrice $n \times n$ inversible à coefficients dans $\mathbb{F}_q$ ayant un et un seul élément non nul par ligne et par colonne.

2.2.1.4 Exemples

1) La matrice

$$\begin{pmatrix}2 & 0 & 0 & 0\\ 0 & 3 & 0 & 0\\ 0 & 0 & 6 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$$

est une matrice monomiale sur $\mathbb{F}_7$.

2) Soit σ une permutation telle que :

$$\sigma\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix}$$

$\sigma(1) = 4\,;\sigma(2) = 3\,;\sigma(3) = 2\,;\sigma(4) = 1.$

La matrice de permutation P est :

$$P = P_{ij} = \begin{cases}P_{ij} = 1 \text{ si } \sigma(i) = j\\ P_{ij} = 0 \text{ si } \sigma(i) \neq j\end{cases}$$

$$P = \begin{pmatrix}P_{11} & P_{12} & P_{13} & P_{14}\\ P_{21} & P_{22} & P_{23} & P_{24}\\ P_{31} & P_{32} & P_{33} & P_{34}\\ P_{41} & P_{42} & P_{43} & P_{44}\end{pmatrix} = \begin{pmatrix}0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\end{pmatrix}$$

Si $q = 2$, toutes les matrices monomiales sont des matrices de permutation , c'est plus intéressant dons le cas $q \neq 2$.

2.2.2 Groupe d'automorphisme

Soient σ une permutation de $I = \{1, 2, \dots, n\}$ et

$$\pi_i : \mathbb{F}_q \to \mathbb{F}_q$$
$$x \longmapsto \pi_i(x) = \alpha_i \cdot x \text{ où } \alpha_i \in \mathbb{F}_q^*, \forall i \in I$$

Alors l'application:

$$\gamma : \mathbb{F}_q^n \to \mathbb{F}_q^n$$

$$(c_1, c_2, \dots, c_n) \mapsto \gamma(c_1, c_2, \dots, c_n) = \pi_i(c_{\sigma(1)})\pi_i(c_{\sigma(2)}) \dots \pi_i(c_{\sigma(n)})$$

est appelée une permutation monomiale de degré n.

On associe à chaque code sur $\mathbb{F}_q$ un certain groupe appelé le groupe d'automorphisme du code C ce groupe est utilise dans l'étude du nombre des codes équivalents à un code donné.

2.2.2.1 Définition

Le groupe d'automorphisme $Aut(C)$ d'un code C est l'ensemble de toutes les permutations monomiales γ de degré n telles que : $\forall c \in C, \gamma(c) \in C$.

2.2.2.2 Exemple

Soit le code : $C = \{0000,0011,1100,1111\}$.

$$Aut(C) = \{id, (2134), (1234), (1324), (1432)\}$$

3. Equivalences des codes

Dans cette section nous définissons l'équivalence des codes, nous montrons quelques propriétés concernent les codes équivalents, et en fin nous montrons que l'équivalence peut être vu comme équivalence par permutations.

3.1 Equivalence par permutation

Soient n un entier naturel non nul, et $I = \{1,2,..,n\}$ ensemble pour indexer les coordonnées des mots de $\mathbb{F}_q^n$.

Pour tout $x \in \mathbb{F}_q^n$; notons $x = (x_1, x_2, \dots, x_n)$ ou simplement $x = x_1x_2 \dots x_n$.

Rappelons l'action du groupe symétrique S_n sur $\mathbb{F}_q^n$.

Pour toute permutation $\sigma \in S_n$, et pour $x \in \mathbb{F}_q^n$: σ agit sur x comme suit :

$$\sigma(x) = \left(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}\right)$$

Une permutation $\sigma \in S_n$ sera notée :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Soit $\mathcal{C}_n$ l'ensemble des codes de longueur n sur $\mathbb{F}_q$. Donc $\mathcal{C}_n$ est une partie de $P\left(\mathbb{F}_q^n\right)$ l'ensemble de toutes les parties de $\mathbb{F}_q^n$.

Soient $\sigma \in S_n$ et C un code de $\mathcal{C}_n$, définissons l'application φ de $S_n \times \mathcal{C}_n$ dans $\mathcal{C}_n$ par $\varphi(\sigma, C) = \sigma(C)$ avec :

$$\sigma(C) = \{\sigma(x) \,/\, x \in C\}$$

3.1.1 Proposition

L'application φ définie une opération de S_n sur $\mathcal{C}_n$. (c'est-à-dire S_n opère sur $\mathcal{C}_n$).

Preuve

soient $\sigma, \tau \in S_n$ et C un code de $\mathcal{C}_n$. $\sigma(C)$ est un sous ensemble de $\mathbb{F}_q^n$, donc un élément de $\mathcal{C}_n$.

$$\sigma\tau(C) = \{\sigma\tau(x) \,/\, x \in C\}$$

Puisque

$$\begin{aligned}\sigma\tau(x) &= \left(x_{\sigma\tau(1)}, \dots, x_{\sigma\tau(n)}\right)\\ &= \left(x_{\sigma(\tau(1))}, \dots, x_{\sigma(\tau(n))}\right)\\ &= \sigma\left(x_{\tau(1)}, \dots, x_{\tau(n)}\right)\\ &= \sigma\left(\tau(x)\right)\end{aligned}$$

Donc

$$\sigma\tau(C) = \{\sigma\left(\tau(x)\right) / \, x \in C\} \; = \sigma(\tau(C))$$

Ce qui prouve que $\varphi(\sigma\tau, C) = \varphi(\sigma, \tau(C))$.

Soit id l'identité de S_n.

$$\begin{aligned}\varphi(id, C) &= id(C)\\ &= \{id(x) \,/\, x \in C\}\\ &= \{x \,/\, x \in C\}\\ &= C\end{aligned}$$

En résumant, le groupe S_n opère sur $\mathcal{C}_n$. Par :

$$(\sigma, C) \to \sigma C$$

L'opération φ permet de définir une relation d'équivalence sur $\mathcal{C}_n$.

En effet ; soit $\sim$ la relation sur $\mathcal{C}_n$ définie par :

Pour deux codes C et C' de $\mathcal{C}_n$;

$$C \sim C' ; \exists \sigma \in S_n ; \sigma(C) = C'$$

3.1.2 Proposition

La relation ~ définie sur $\mathcal{C}_n$ est une relation d'équivalence.

Preuve

1) $\sim$ est réflexive car : pour tout code C de $\mathcal{C}_n$;

$$C = id(C)$$

Ce qui entraîne que : $C \sim C$.

2) $\sim$ est symétrique : soient C et $C^{'}$ de $\mathcal{C}_n$ tels que $C \sim C^{'}$ nous avons :

$$C \sim C^{'}; \exists \sigma \in S_n; \sigma(C) = C'$$

Or

$$\sigma \in S_n \Leftrightarrow \sigma^{-1} \in S_n$$

Donc

$$\begin{aligned} C^{'} = \sigma(C) &\Leftrightarrow \sigma^{-1}(C^{'}) = \sigma^{-1}\big(\sigma(C)\big) \\ &\Leftrightarrow \sigma^{-1}(C^{'}) = (\sigma^{-1}\sigma)(C) \\ &\Leftrightarrow \sigma^{-1}(C^{'}) = id(C) \\ &\Leftrightarrow \sigma^{-1}(C^{'}) = C \\ &\Leftrightarrow C^{'} \sim C \end{aligned}$$

3) $\sim$ est transitive : soient C, $C^{'}$ et $C^{''}$ de $\mathcal{C}_n$ tels que : $C \sim C^{'}$ et $C^{'} \sim C^{''}$

$$C \sim C^{'} \text{ et } C^{'} \sim C^{''} \Leftrightarrow \exists \sigma \in S_n, \exists \tau \in S_n : C^{'} = \sigma(C) \text{ et } C^{''} = \tau(C^{'})$$

$$\Rightarrow \exists \sigma, \tau \in S_n : C^{''} = \tau\sigma(C)$$

Or $\tau, \sigma \in S_n$ et S_n est un groupe, alors $\tau\sigma \in S_n$

Donc $C^{''} = \tau\sigma(C)$ ce qui prouve que : $C \sim C^{''}$.

3.1.3 Définition

Deux codes de même longueur n sur $\mathbb{F}_q$, sont équivalents par permutations s'ils sont équivalents au sens de la relation $\sim$ définie ci – dessus .

Cela revient à dire que de code C et $C^{'}$ de même longueur sont équivalents par permutation s'il existe une permutation $\sigma \in S_n$ telle que : $C^{'} = \sigma(C)$.

3.1.4 Exemples

En se référant aux exemples 2.1.4 nous voyons que :

1) Le code C défini dans l'exemple *a)* est équivalent par permutation à lui même et il n'existe pas un autre code de longueur 3 équivalent par permutation à C autre que C.
2) Le code C_1 défini dans l'exemple *b)* possède trois codes équivalents par permutation, à savoir :
   - Le code C_1 lui même déduit par les permutations id et (13).
   - Le code C_2 déduit de C_1 par (12) et (123).
   - Le code C_3 déduit de C_1 par (23) et (132).

3.1.5 Définition

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

La classe de C selon la relation $\sim$ est appelée orbite de C et sera noté $\bar{C}$. L'ensemble $S_C = \{\sigma \in S_n / \sigma(C) = C\}$ est appelé le stabilisateur de C par S_n.

Pour l'exemple a) de 2.1.4, nous avons $\bar{C} = \{C\}$, tandis que pour l'exemple b) nous avons $\overline{C_1} = \{C_1, C_2, C_3\}$.

3.1.6 Proposition

Le nombre des codes équivalents par permutation à un code C de longueur n est :

$$\frac{n!}{perm(C)}$$

Preuve

Soit $\bar{C}$ l'orbite de C selon l'action de S_n sur $\mathcal{C}_n$.

Soit encore $(S_n / perm(C))_g$ l'ensemble des classes à gauche de S_n modulo $perm(C)$.

Définition l'application : $h : \bar{C} \to (S_n \,/\, perm(C))_g$ définie comme suit :

Pour tout $C_1 = \pi(C)$ de $\bar{C}$:

$$h(C_1) = \pi\, perm(C)$$

Montrons que h est une bijection :

Soit C_1, C_2 deux codes de $\bar{C}$ tels que $C_1 = C_2$, alors il existent deux permutations $\pi_1, \pi_2 \in S_n$ telles que : $C_1 = \pi_1(C)$ et $C_2 = \pi_2(C)$,

$$\begin{aligned} C_1 = C_2 &\Leftrightarrow \pi_1(C) = \pi_2(C) \\ &\Leftrightarrow \pi_2^{-1}\pi_1(C) = C \\ &\Leftrightarrow \pi_2^{-1}\pi_1 \in perm(C) \\ &\Leftrightarrow \pi_1\, perm(C) = \pi_2\, perm(C) \end{aligned}$$

Ce qui prouve que h est une application injective, il reste à montrer qu'il est surjective.

Soit $\sigma\, perm(C) \in (S_n \,/\, perm(C))_g$ alors $\sigma(C)$ est un code équivalent par permutation à C et $h\big(\sigma(C)\big) = \sigma\, perm(C)$.

Ce qui entraîne avec la première partie de la démonstration que h est bijective.

Donc les deux ensemble $\bar{C}$ et $(S_n \,/\, perm(C))_g$ ont même cardinal :

$$\begin{aligned} |\bar{C}| = \left|(S_n \,/\, perm(C))_g\right| &= [S_n : perm(C)] \\ &= \frac{|S_n|}{|perm(C)|} \text{ (Théorème de Lagrange)} \\ &= \frac{n!}{|perm(C)|} \end{aligned}$$

3.1.7 Exemples

En se référant à l'exemple 2.1.4

i. Le code C de cet exemple possède un seul code équivalent par permutation qui n'est autre que C.

ii. Le code C_1 de cet exemple possède

$$\frac{n!}{|perm(C)|} = \frac{3!}{2} = 3$$

codes équivalents par permutation à savoir les codes C_1, C_2, C_3.

3.1.8 Proposition [8]

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

Le nombre des permutations de S_n qui produisent un même code équivalent par permutation à C, est $|perm(C)|$.

Preuve

Nous définissons une relation sur S_n notée par $\equiv$; pour toutes permutations $\sigma_1, \sigma_2 \in S_n$;

$$\sigma_1 \equiv \sigma_2 \Leftrightarrow \sigma_1(C) = \sigma_2(C)$$

Il est évident, que la relation $\equiv$ ainsi définie, est une relation d'équivalence sur S_n.

Cette relation qui veut dire que $\sigma_1 \equiv \sigma_2$, si et seulement si σ_1 et σ_2 définissent le même code équivalent par permutation à C.

Analysons de plus cette relation :

$$\begin{aligned} \sigma_1 \equiv \sigma_2 &\Leftrightarrow \sigma_1(C) = \sigma_2(C) \\ &\Leftrightarrow \sigma_2^{-1}\sigma_1(C) = C \\ &\Leftrightarrow \sigma_2^{-1}\sigma_1 \in perm(C) \\ &\Leftrightarrow \sigma_1\, perm(C) = \sigma_2\, perm(C) \end{aligned}$$

Cette dernière égalité veut dire que les classe à gauche modulo $perm(C)$ de σ_1 et σ_2 sont égaux.

Cela permet de définir une application bijective T de $S_n/\equiv$ ensemble des classes modulo $\equiv$ sur $(S_n \,/\, perm(C))_g$ ensemble des classes à gauche modulo $perm(C)$ comme suit :

$$\begin{aligned} T : S_n/\equiv &\to (S_n \,/\, perm(C))_g \\ \bar{\sigma} &\mapsto \sigma\, perm(C) \end{aligned}$$

Puisque T est bijective, alors :

$$|S_n/\equiv| = \left|(S_n \,/\, perm(C))_g\right|$$
$$= [S_n : perm(C)]$$
$$= \frac{n!}{|perm(C)|}$$

C'est à dire que le nombre des permutations prises comme représentant selon la relation ≡ est le même nombre des codes équivalents à C.

Calculons maintenant le cardinal de $\bar{\sigma}$, c'est à dire que le nombre des permutations que lors ses actions sur C produisent le même code équivalent à C.

Pour cela étudions l'application $\varphi : perm(C) \to \bar{\sigma}$ définie par :

pour tout $\pi \in perm(C)$, $\varphi(\pi) = \sigma\pi^{-1}$.

Au premier lieu φ est bien définie et de plus elle est injective car :

Si $\pi_1, \pi_2 \in perm(C)$, alors $\pi_1(C) = C$ et $\pi_2(C) = C$.

Donc nous avons

$$\varphi(\pi_1) = \sigma\pi_1^{-1} \text{ et } \varphi(\pi_2) = \sigma\pi_2^{-1}$$
$$\pi_1 = \pi_2 \Leftrightarrow \sigma\pi_1^{-1} = \sigma\pi_2^{-1} \Leftrightarrow \varphi(\pi_1) = \varphi(\pi_2)$$

Montrons que φ est surjective, soit $\tau \in \bar{\sigma}$, alors la permutation τ vérifie

$$\tau(C) = \sigma(C) \Leftrightarrow \tau^{-1}\sigma(C) = C$$
$$\Leftrightarrow \tau^{-1}\sigma \in perm(C)$$

et de plus

$$\varphi(\tau^{-1}\sigma) = \sigma(\tau^{-1}\sigma)^{-1} = \sigma\sigma^{-1}(\tau^{-1})^{-1} = id.\tau = \tau$$

Ce qui montre que φ est surjective. En résumant φ est bijection de $perm(C)$ dans $\bar{\sigma}$, ce qui permet de conclure que les ensembles $perm(C)$ et $\bar{\sigma}$ ont même cardinal.

La proposition précédente affirme que si C' est équivalent à C par une permutation σ, il suffit de déterminer l'ensemble $\{\sigma\pi^{-1} \,/\, \pi \in perm(C)\}$ pour déterminer toutes les permutations qui produisent C' à partir de C.

3.1.9 Exemple [2]

Soit le code $C = \{000, 110, 111, 001\}$

S_3 désigne le groupe symétrique de degré 3, il est d'ordre 3!.

A savoir : $S_3 = \{id, (12), (13), (23), (123), (132)\}$.

On a $perm(C) = \{id, (12)\}$, le nombre des codes équivalence à C est

$$\frac{n!}{|perm(C)|} = \frac{3!}{2} = 3$$

Donc C possède 3 codes équivalents.

- ✓ Méthode pour déterminer les 3 codes équivalents à C :

1. On choisi une permutation σ telle que $\sigma \in S_3 - \{perm(C)\}$.

   Soit $\sigma = (132)$, alors le premier code équivalent à C est:

   $$\sigma(C) = (132)(C) = \{000, 101, 111, 010\} = C_1$$

   On calcule l'ensemble $E_1 = \{\sigma \circ perm(C)\}$.

   $$E_1 = \{(132)\} \circ \{id, (12)\} = \{(132), (23)\}$$

2. On choisit une permutation σ telle que $\sigma \notin perm(C)$ et $\sigma \notin E_1$.

   Soit $\sigma = (13)$, alors le deuxième code équivalent à C est :

   $$\sigma(C) = (13)(C) = \{000, 011, 111,100\} = C_2$$

   On calcule l'ensemble $E_2 = \{\sigma \circ perm(C)\}$.

   $$E_2 = \{(13)\} \circ \{id, (12)\} = \{(13), (123)\}$$

Donc les trois codes équivalents à C sont C, C_1 et C_2 tel que :

$$C = \{000, 110, 111, 001\}.$$
$$C_1 = \{000, 101, 111, 010\}.$$
$$C_2 = \{000, 011, 111,100\}.$$

On remarque :

- l'ensemble $E_1 = \{(23), (132)\}$ On a :
  $(132)(C) = C_1$.
  $(23)(C) = C_1$.
- l'ensemble $E_2 = \{(13), (123)\}$ On a :
  $(13)(C) = C_2$.
  $(123)(C) = C_2$.
- $perm(C) = \{id, (12)\}$ on a :
  $id(C) =$ C.
  $(12)(C) = C$.

4. Isométries de l'espace de Hamming

Une isométrie d'un espace métrique est une application de cet espace dans lui-même telle que la distance entre les images de deux mots est égale à la distance entre ces mots. L'ensemble des isométries muni de la composition forme un groupe. Dans le cas d'un espace de Hamming, un résultat de Pierre Bonneau caractérise les isométries.

4.1 Définition

Soit (A^n, d) un espace de Hamming. Une isométrie de Hamming, est une application $f : A^n \to A^n$ telle que : $\forall x, y \in A^n$ on a :

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

4.2 Exemples

i. Soit σ une permutation de S_n, on définit l'application $f_\sigma : A^n \to A^n$, par :

$$f_\sigma(x_1, x_2, \ldots, x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

alors f_σ est une isométrie de Hamming.

ii. Soient $f_1, f_2, \ldots, f_n$ un ensemble de n bijections de A, alors l'application $A^n \to A^n$, telle que $(x_1, x_2, \ldots, x_n) \to (f_1(x_1), f_2(x_2), \ldots, f_n(x_n))$, est une isométrie de Hamming.

iii. Soit les codes ternaires

$$C_1 = \{000, 011, 022\}$$
$$C_2 = \{000, 110, 011\}$$

Sont équidistants de distance minimum 2 et sont donc isométriques.

4.3 Définition

Soit $\mathbb{F}_q$ un corps fini, d la distance de Hamming sur $\mathbb{F}_q^n$.

Une isométrie linéaire, est une application linéaire $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ qui est une isométrie pour d. Si f est linéaire, on a f est une isométrie, si et seulement si :

$$\omega\big(f(x)\big) = \omega(x), \forall x \in \mathbb{F}_q^n.$$

4.4 Théorème [15]

Soit $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ une application. Les assertions suivantes sont équivalentes :

1) f est une isométrie linéaire.
2) Il existe une permutation $\sigma \in S_n$ et des scalaires non nuls $\lambda_1, \lambda_2, \ldots, \lambda_n$, tels que pour tout $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$, on a :

$$f(x_1, x_2, \ldots, x_n) = \big(\lambda_1 x_{\sigma(1)}, \lambda_2 x_{\sigma(2)}, \ldots, \lambda_n x_{\sigma(n)}\big) \ldots\ldots\ldots (*)$$

Preuve

1. Les applications du type $(*)$ sont des isométries linéaires car pour tout x, y, $z \in \mathbb{F}_q^n$ on a :

i) $f(x_1, \ldots, x_n) + f(y_1, \ldots, y_n) = f(x_1 + y_1, \ldots, x_n + y_n)$

Si on pose $z_i = x_i + y_i$ alors :

$f(x_1 + y_1, \ldots, x_n + y_n) = f(z_1, \ldots, z_n)$

$$= (\lambda_1 z_{\sigma(1)}, , \ldots, \lambda_n z_{\sigma(n)})$$
$$= \left(\lambda_1 (x_{\sigma(1)} + y_{\sigma(1)}), \ldots, \lambda_n (x_{\sigma(n)} + y_{\sigma(n)})\right)$$
$$= (\lambda_1 x_{\sigma(1)}, \ldots, \lambda_n x_{\sigma(n)}) + (\lambda_1 y_{\sigma(1)}, \ \ldots, \lambda_n y_{\sigma(n)})$$
$$= f(x_1, \ldots, x_n) + f(y_1, \ldots, y_n)$$

ii) Pour tout $x \in \mathbb{F}_q^n$ et $\forall \alpha \in \mathbb{F}_q^*$ on a :

$$f(\alpha(x_1, \ldots, x_n)) = f(\alpha x_1, \ldots, \alpha x_n)$$
$$= (\alpha\lambda_1 x_{\sigma(1)}, \ldots, \alpha\lambda_n x_{\sigma(n)})$$
$$= \alpha f(x_1, \ldots, x_n)$$

2. Soit f une isométrie linéaire et e_i un vecteur de la base canonique de $\mathbb{F}_q^n$. Comme $\omega(f(e_i)) = \omega(e_i) = 1$, on a $f(e_i) = \lambda_{\tau(i)} e_{\tau(i)}$, où $\lambda_{\tau(i)} \in \mathbb{F}_q^*$ et τ est une application $\{1, 2, \ldots, n\} \rightarrow \{1, 2, \ldots, n\}$.

   Soient $i, j \in \{1, 2, \ldots, n\}$, tels que $\tau(i) = \tau(j) = k$. On a $f(e_i) = \alpha e_k$ et $f(e_j) = \beta e_k$. Ce qui entraîne que $f(e_i - e_j) = (\alpha - \beta) e_k$.

   Supposons que $i \neq j$, alors $\omega(f(e_i - e_j)) = \omega(e_i - e_j) = 2$, car f est une isométrie.

   Or $\omega(f(e_i - e_j)) = \omega((\alpha - \beta) e_k) \leq 1$, ce qui est absurde. Donc $i = j$. Il en résulte que τ est une injection. Comme $\{1, 2, \ldots, n\}$ est fini, c'est une permutation de $\{1, 2, \ldots, n\}$.

   Soit $x = \sum_{i=1}^{n} x_i e_i$, on a :

$$f(x) = \sum_{i=1}^{n} x_i f(e_i) = \sum_{i=1}^{n} \lambda_{\tau(i)} x_i e_{\tau(i)}$$

   Posons $\sigma = \tau^{-1}$ et $j = \tau(i)$, alors :

$$f(x) = \sum_{j=1}^{n} \lambda_j x_{\sigma(j)} e_j$$

Une application de la forme $(*)$, est dite monomiale. Si P est la matrice dans la base canonique d'une telle application, alors chaque ligne et chaque colonne de P contient un seul coefficient non nul.

4.5 Proposition

L'ensemble $Isom(\mathbb{F}_q^n, d)$ des isométries linéaires de Hamming, est un groupe pour la composition des applications. Il est fini d'ordre $(q-1)^n n!$.

Preuve

Il suffit de montrer que $Isom(\mathbb{F}_q^n, d)$ est un sous-groupe du groupe des bijections de $\mathbb{F}_q^n$. En effet, l'identité id de $\mathbb{F}_q^n$ est une isométrie. Si f, g sont des isométries de Hamming, alors $\forall x, y \in \mathbb{F}_q^n$, on a :

$$\begin{aligned} d(f \circ g(x), f \circ g(y)) &= d\left(f(g(x)), f(g(y))\right) \\ &= d(g(x), g(y)) \\ &= d(x, y) \end{aligned}$$

d'où $f \circ g \in Isom(\mathbb{F}_q^n, d)$.

Par ailleurs, on a :

$$\begin{aligned} d(x, y) &= d\left(g(g^{-1}(x)), g(g^{-1}(y))\right) \\ &= d(g^{-1}(x), g^{-1}(y)) \end{aligned}$$

donc : $g^{-1} \in Isom(\mathbb{F}_q^n, d)$.

4.6 Equivalence par isométrie [12]

Deux codes sont équivalents par isométrie s'ils appartiennent à la même orbite sous l'action du groupe des isométries de l'espace de Hamming.

4.6.1 Définitions

Deux codes linéaires C et C' de longueur n sur $\mathbb{F}_q$ sont équivalents par isométrie s'il existe une isométrie linéaire f de $\mathbb{F}_q^n$ telle que :

$$f(C) = C'$$

Deux codes linéaires équivalents ont les mêmes propriétés métriques et mêmes propriétés linéaires. Ainsi deux codes équivalents ont la même la distance minimale.

Soient $f \in Isom(\mathbb{F}_q^n, d)$ et C un code de $\mathcal{C}_n$, définissons l'application ψ de $Isom(\mathbb{F}_q^n, d) \times \mathcal{C}_n$ dans $\mathcal{C}_n$ par $\psi(f, C) = f(C)$ avec :

$$f(C) = \{f(x) \,/\, x \in C\}$$

4.6.2 Proposition

L'application ψ définie une opération de $Isom(\mathbb{F}_q^n, d)$ sur $\mathcal{C}_n$. (c'est-à-dire $Isom(\mathbb{F}_q^n, d)$ opère sur $\mathcal{C}_n$).

Preuve

Soient $g, f \in Isom(\mathbb{F}_q^n, d)$ et C un code de $\mathcal{C}_n$. $f(C)$ est un sous ensemble de $\mathbb{F}_q^n$ donc un élément de $\mathcal{C}_n$.

$$f \circ g(C) = \{f \circ g(x) \,/\, x \in C\}$$

Puisque

$$\begin{aligned} f \circ g(x) &= \big(f \circ g(x_1), \dots, f \circ g(x_n)\big) \\ &= \Big(f\big(g(x_1)\big), \dots, f\big(g(x_n)\big)\Big) \\ &= \Big(f\big(\mu_1 x_{\tau(1)}\big), \dots, f\big(\mu_n x_{\tau(n)}\big)\Big) \\ &= \Big(\mu_1 f\big(x_{\tau(1)}\big), \dots, \mu_n f\big(x_{\tau(n)}\big)\Big) \\ &= \Big(\mu_1 \lambda_1 x_{\sigma(\tau(1))}, \dots, \mu_n \lambda_n x_{\sigma(\tau(n))}\Big) \\ &= \Big(\lambda_1 \mu_1 x_{\sigma(\tau(1))}, \dots, \lambda_n \mu_n x_{\sigma(\tau(n))}\Big) \\ &= f\big(\mu_1 x_{\tau(1)}, \dots, \mu_n x_{\tau(n)}\big) \\ &= f\big(g(x)\big) \end{aligned}$$

Donc :

$$f \circ g(C) = \{f\big(g(x)\big) / \, x \in C\} \; = f(g(C))$$

Ce qui prouve que $\psi(f \circ g, C) = \psi(f, g(C))$.

Soit id l'identité de $Isom\big(\mathbb{F}_q^n, d\big)$.

$$\begin{aligned} \psi(id, C) &= id(C) \\ &= \{id(x) \,/\, x \in C\} \\ &= \{x \,/\, x \in C\} \\ &= C \end{aligned}$$

En résumant, le groupe $Isom\big(\mathbb{F}_q^n, d\big)$ opère sur $\mathcal{C}_n$. Par :

$$(f, C) \to f(C)$$

L' opération ψ permet de définir une relation d'équivalence sur $\mathcal{C}_n$.

En effet ; soit $\sim$ la relation sur $\mathcal{C}_n$ définie par :

Pour deux codes C et C' de $\mathcal{C}_n$;

$$C \sim C' \,;\, \exists f \in Isom(\mathbb{F}_q^n, d) \,;\, f(C) = C'.$$

4.6.3 Proposition

La relation $\sim$ définie sur $\mathcal{C}_n$ est une relation d'équivalence.

Preuve

1) $\sim$ est réflexive car : pour tout code C de $\mathcal{C}_n$;

$$C = id(C)$$

Ce qui entraîne que : $C \sim C$.

2) $\sim$ est symétrique : soient C et $C^{'}$ de $\mathcal{C}_n$ tels que $C \sim C^{'}$ nous avons :

$$C \sim C^{'} \; ; \exists f \in Isom(\mathbb{F}_q^n, d) \; ; f(C) \; = \; C'$$

Or

$$f \in Isom(\mathbb{F}_q^n, d) \Leftrightarrow f^{-1} \in Isom(\mathbb{F}_q^n, d)$$

donc :

$$\begin{aligned} C^{'} = f(C) \Leftrightarrow \; & f^{-1}(C^{'}) = f^{-1}\big(f(C)\big) \\ & \Leftrightarrow f^{-1}(C^{'}) = (f^{-1} \circ f)(C) \\ & \Leftrightarrow f^{-1}(C^{'}) = id(C) \\ & \Leftrightarrow f^{-1}(C^{'}) = C \\ & \Leftrightarrow C^{'} \sim C \end{aligned}$$

3) $\sim$ est transitive : soient C, $C^{'}$ et $C^{''}$ de $\mathcal{C}_n$ tels que : $C \sim C^{'}$ et $C^{'} \sim C^{''}$

$$\begin{aligned} C \sim C^{'} \text{ et } C^{'} \sim C^{''} & \Leftrightarrow \exists f, g \in Isom\big(\mathbb{F}_q^n, d\big) : C^{'} = f(C) \text{ et } C^{''} = g(C^{'}) \\ & \Rightarrow \exists f, g \in Isom\big(\mathbb{F}_q^n, d\big) : \; C^{''} = g \circ f(C). \end{aligned}$$

Or $g, f \in Isom\big(\mathbb{F}_q^n, d\big)$ et $\mathrm{Isom}\big(\mathbb{F}_q^n, d\big)$ est un groupe, alors :

$$g \circ f \in Isom\big(\mathbb{F}_q^n, d\big)$$

Donc $C^{''} = g \circ f(C)$ ce qui prouve que : $C \sim C^{''}$.

4.6.4 Définition

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

La classe de C selon la relation $\sim$ est appelée orbite de C et sera noté $\bar{C}$. L'ensemble $S_C = \{f \in Isom\big(\mathbb{F}_q^n, d\big) \,/\, f(C) = C\}$ est appelé le stabilisateur de C par $Isom\big(\mathbb{F}_q^n, d\big)$.

4.7 Définition

L'ensemble des isométries linéaires qui laissent fixe un code C est un groupe fini pour la composition. On l'appelle le groupe de automorphismes de C.

$$Aut(C) = \big\{f \in Isom(\mathbb{F}_q^n, d) : \; f(C) = \; C\big\}.$$

4.8 Equivalences et matrices génératrices

4.8.1 Proposition [15]

Soient C et C' deux codes linéaires de même longueur n et de même dimension k sur $\mathbb{F}_q$. On note G et $G^{'}$ des matrices génératrices de respectives de C et C' alors C et C' sont équivalents, si et seulement s'il existe $A \in GL_k(\mathbb{F}_q)$ et P une matrice monomiale d'ordre n tel que $G^{'} = AGP$.

Preuve

Soient $u_1,\dots,u_k$ les vecteurs lignes de G et $v_1,\dots,v_k$ ceux de G'. Supposons que C et C' sont équivalents. Il existe une matrice monomiale P telle que $(u_1P,\dots,u_k\,P)$ soit une base de C'. Donc il existe $A \in GL_k(\mathbb{F}_q)$ telle que $Au_iP = v_i,\ \forall i = 1,\dots,k$. Par suite $AGP = G'$.

Réciproquement, supposons qu'il existe $A \in GL_k(\mathbb{F}_q)$ et P une matrice monomiale d'ordre n tel que $G' = AGP$. On a $(Au_1,\dots,Au_k)$ est une base de C.

Donc $(Au_1\,P,\dots,Au_k\,P)$ est une base d'un code équivalent à C.

4.8.2 Proposition [15]

Tout code linéaire est équivalent (isométrique) à un code systématique.

En particulier, si G est la matrice génératrice d'un $[n,k]_q$-code linéaire C sur $\mathbb{F}_q$ alors il existe $A \in GL_k(\mathbb{F}_q)$ et P une matrice de permutation d'ordre n tels que AGP soit normalisée.

Preuve

Comme $rg\,G = k$, G contient k ligne linéairement indépendantes. Il existe alors une matrice de permutation P d'ordre n telle que $GP = [B \mid M]$ avec $B \in GL_k(\mathbb{F}_q)$.

Posons $A = B^{-1}$. Alors $AGP = [I_k \mid AM]$ est normalisée.

4.8.3 Exemples

1) Soit le code linéaire sur le corps $\mathbb{F}_5$, dont une matrice génératrice est :

$$G = \begin{pmatrix} 1 & 2 & 1 & 2 & 4 \\ 3 & 1 & 2 & 2 & 2 \\ 4 & 3 & 3 & 3 & 1 \end{pmatrix}$$

On transforme cette matrice de la manière suivante :

$$G = \begin{pmatrix} 1 & 2 & 1 & 2 & 4 \\ 3 & 1 & 2 & 2 & 2 \\ 4 & 3 & 3 & 3 & 1 \end{pmatrix} \widetilde{(1)} \begin{pmatrix} 1 & 2 & 1 & 2 & 4 \\ 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & 4 & 0 & 0 \end{pmatrix}$$

$$\widetilde{(2)} \begin{pmatrix} 1 & 2 & 1 & 2 & 4 \\ 0 & 1 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \end{pmatrix}$$

$$\widetilde{(3)} \begin{pmatrix} 1 & 0 & 3 & 2 & 4 \\ 0 & 1 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\widetilde{(4)} \begin{pmatrix} 1 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Les opérations effectuées sont :

(1) : $L_2 - 3L_1$, $L_3 - 4L_1$.

(2) : Permutation des colonnes 2 et 4.

(3) : $L_1 - 2L_2$, $L_2 - 4L_3$, $L_3 \times 4$.

(4) : $L_1 - 3L_3$, $L_2 - 4L_3$.

2) Soit C_1 le code [6,3] sur $\mathbb{F}_3$, de fini par sa matrice génératrice G_1:

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

Une permutation de colonne $N°4$ par la colonne $N°1$ on obtient G_2:

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

En permutant la colonne $N°4$ par la colonne $N°3$ on obtient G_3:

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 2 & 1 & 1 \end{pmatrix}$$

Donc G_3 est une matrice génératrice du code C.

C équivalent à C_1 .

3) Soit C le code défini par sa matrice génératrice

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

On transforme cette matrice de la manière suivante :

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \xrightarrow{L_2 \to L_1 + L_2} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$$\xrightarrow{L_1 \to L_1 + L_2} \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\xrightarrow{L_1 \to L_1 + L_3} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

5. Codes poinçonnés

5.1 Notations et définitions

I désigne toujours l'ensemble $\{1,2, \dots, n\} \subset N$.

Pour tout $x \in \mathbb{F}_q^n$, $\text{supp}(x) = \{i \in I : x_i \neq 0\}$ désigne le support de x.

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

Si J est une partie non vide de I, nous noterons E_J l'ensemble des mots de $\mathbb{F}_q^n$ du supports inclus dans J c'est à dire :

$$E_J = \{x \in \mathbb{F}_q^n : \text{supp}(x) \subset J\}$$

et si J est le singleton $\{i\}$, nous noterons simplement E_i:

$$E_i = \{x \in \mathbb{F}_q^n : \text{supp}(x) = \{i\}\} = \{(0, 0, \dots, 0, \alpha, 0, .., 0) \in \mathbb{F}_q^n \ / \ \alpha \in \mathbb{F}_q^*\}$$

5.2 Définition

Le code C poinçonné en i est par définition :

$$C_i = (C + E_i) \cap E_{I\setminus\{i\}}$$

5.3 Remarque

1) L'ensemble C_i est bien un code sur $\mathbb{F}_q$, car il est une partie de $\mathbb{F}_q^n$. Les éléments du code C_i sont tous les éléments de C où les coordonnées indexées par i sont remplacées par zéro (zéro de $\mathbb{F}_q$) .
2) Si le code C est linéaire, il en est de même pour le code poinçonné C_i puisque il est intersection de deux sous espaces vectoriels de $\mathbb{F}_q$.
3) Dans la définition usuelle d'un code poinçonné en i, la position indexée par i est supprimée.

5.4 Propriétés des codes poinçonnes

a) La commutativité : Pour tout code C de longueur n et pour $i, j \in I$ nous avons

$$(C_i)_j = (C_j)_i$$

b) Equivalence : Pour tout code C de longueur n, pour tout $i \in I$, et pour toute permutation $\sigma \in S_n$, nous avons : $\sigma(C_i) = \sigma(C)_{\sigma(i)}$.

Preuve

Pour a) Elle découle de la remarque 7.3

Nous noterons alors chacun de $(C_i)_j$, et $(C_j)_i$ tout simplement par $C_{\{i,j\}}$.

Pour b) La permutation σ change les positions des coordonnées d'un mot d'un code sans changer leurs valeurs. Alors si $b_i = 0$ pour $b = (b_1, b_2, \dots, b_n)$ de C, il est évident que $b_{\sigma(i)} = 0$ pour $\sigma(b) \in \sigma(C)$. donc :

$$\begin{aligned}
\sigma(C_i) &= \{\sigma(b) \ / \ b \in C_i\} \\
&= \{\sigma(b) / \ b \in C \text{ en remplaçant } b_i \text{ par } 0\} \\
&= \{(b_{\sigma(1)}, \dots., b_{\sigma(n)}) \in \sigma(C) \text{ en remplaçant } b_{\sigma(i)} \text{ par } 0\} \\
&= \sigma(C)_{\sigma(i)}
\end{aligned}$$

La propriété 5.4.b). affirme que si C et C' sont deux codes équivalents par permutation avec $\sigma(C) = C'$, alors il en est de même pour C_i et $C'_{\sigma(i)}$ et de plus $\sigma(C_i) = C'_{\sigma(i)}$.

6. Invariants

La notion d'invariant que nous utiliserons ici sera liée à celle d'équivalence. Il s'agit de toute propriété d'un code qui ne changera pas lorsque l'on appliquera une permutation ou plus généralement une isométrie linéaire.

6.1 Définition

Notons $\mathcal{C}$ l'ensemble de tous les codes sur $\mathbb{F}_q$. Soit E un ensemble non vide sur lequel la notion d'égalité est définie.

Un invariant sur E est une application $v : \mathcal{C} \to E$ telle que deux codes équivalents prennent la même valeur par v, c'est-à-dire :

$$\forall C \in \mathcal{C}_n, \forall \sigma \in S_n : v\left(\sigma(C)\right) = v(C)$$

6.2 Exemples

a. La longueur d'un code est un invariant sur $\mathbb{N}$.

b. La distance minimale est un invariant sur $\mathbb{N}$.

c. Le polynôme énumérateur

$$W_C(x) = \sum_{c \in C} x^{\omega(c)}$$

dans sa forme simple, est un invariant sur $\mathbb{N}[X]$.

d. Soit C et C' deux codes équivalents, telle que :

$$C = \{1110, 0111, 1010\}$$
$$C' = \{0011, 1011, 1101\}$$

Comme invariant, nous prenons le polynôme énumérateur des poids.

$$W_C(x) = \sum_{c \in C} x^{\omega(c)} = W(C) = 2x^3 + x^2$$

$$W_{C'}(x) = \sum_{c' \in C'} x^{\omega(c')} = W(C') = 2x^3 + x^2$$

Comme invariant, nous prenons la distance minimale.

Le code C : $d(1110, 0111) = 2$

$d(1110, 0101) = 1$ Donc la distance minimale est égale à 1.

$d(0111, 1010) = 3$

Le code C' : $d(0011, 1011) = 1$

$d(0011, 1101) = 3$ Donc la distance minimale est égale à 1.

$$d(1011, 1101) = 2$$

6.3 Hull d'un code linéaire

6.3.1 Définition

Le Hull d'un code linéaire C est l'intersection de C et son dual $C^{\perp}$ que nous le noterons $H(C)$. c'est-à-dire $H(C) = C \cap C^{\perp}$.

6.3.2 Proposition

Soit C un code linéaire de longueur n et $\sigma \in S_n$.

Alors :

1) $H\left(\sigma(C)\right) = \sigma\big(H(C)\big)$.
2) Si v est invariant, l'application $C \to v\big(H(C)\big)$ est aussi un invariant.

Preuve

Pour 1) il suffit de remarquer que :

$$\sigma(C^{\perp}) = \sigma(C)^{\perp} \text{ et } \sigma(A \cap B) = \sigma(A) \cap \sigma(B)$$

Pour 2) il suffit d'appliquer la définition d'un invariant.

L'invariant est une propriété globale d'un code, il peut nous aider à décider si deux codes sont équivalents où non dans certains cas, par exemple, deux codes de valeurs différentes par un invariant ne sont pas équivalents. Mais il peut arriver que deux codes non équivalents ont la même valeur par un invariant, ce qui est le cas par exemple pour le polynôme énumérateur, la longueur … etc. Pour ces raisons nous allons définir une propriété locale d'un code et une de ses positions.

6.3.3 Exemple

Soit le code C défini sur $\mathbb{F}_2$ par $C = \{000,011,101,110\}$, le dual $C^{\perp}$ de C est $C^{\perp} = \{000,111\}$ et le Hull de (C) est $H(C) = C \cap C^{\perp} = \{000\}$.

7. Signatures

7.1 Définition

Une signature S sur un ensemble E, est une application qui à tout code C de longueur n et à tout élément i de I_n, associe un élément $S(C, i)$ de E et telle que pour toute permutation $\sigma \in S_n$ et pour tout i de I_n:

$$S\big(\sigma(C), \sigma(i)\big) = S(C, i)$$

7.2 Exemple

On peut construire une signature à partir de tout invariant. Soit v un invariant, pour tout code C de longueur n, et pour tout $i \in I_n$, l'application définie par :

$$S(C, i) = v(C_i)$$

est une signature.

On peut définir de la même manière une signature générale à partir de l'équivalence par isométrie linéaire.

7.3 Définitions

- ✓ Une signature générale S sur un ensemble E, est une application qui à tout code C de longueur n et à tout élément i de I_n, associe un élément $S(C,i)$ de E et telle que pour toute i de I_n et pour tout isométrie linéaire f:

$$S\big(f(C),\sigma(i)\big) = S(C,i)$$

- ✓ Une signature est discriminante pour un code C donné de longueur n s'il existe i et j dans I_n tels que $S(C,i) \neq S(C,j)$.
- ✓ Une signature est totalement discriminante pour un code C donné de longueur n si $S(C,i) \neq S(C,j)$ pour tout i et tout j distincts dans I_n.

7.4 Construction des signatures [11]

Soient S et T deux signatures sur deux ensembles E et E' respectivement.

1- La signature produit de S et T est la signature, notée $S \times T$, définie par :

$$S \times T : (C\ ,i\ ) \to \big(S(C\ ,i\ ), T\ (C\ ,i)\big)\ .$$

2- Le dual de *S* est la signature sur *E*, notée $S^{\perp}$, définie par :

$$S^{\perp} :\ (C,i) \to S(C^{\perp},i)$$

7.5 Comparison des signatures

1) Soient S et T deux signatures et soit C un code de longueur n. La signature T est plus discriminante que la signature S pour C, et nous noterons $S \leq_C T$ si :

$$\forall i\ ,j \in I_n, T(C\ ,i) = T(C\ ,j) \Rightarrow S(C,i) = S(C\ ,j)$$

2) La signature S est auto-duale si $S\ \equiv S^{\perp}$.

7.6 Exemple

Considérons les deux codes suivants sur $\mathbb{F}_2$:

$$C = \{1110,0111,1010\}$$

$$C' = \{0011,1011,1101\}$$

Comme invariant, nous prenons le polynôme énumérateur des poids, c'est à dire

$$v(C) = W_C(x) = \sum_{c \in C} x^{\omega(c)} = W(C)$$

Et comme signature, nous prenons la signature suivante :

$$S\ (\ C\ ,i\ )\ =\ v\ (C_i)\ =\ W\ (C_i)$$

$$C_1 = \{0110,0111,0010\} \to W(C_1) = x + x^2 + \ x^3$$

$$C_2 = \{1010,0011\} \quad \rightarrow W(C_2) = 2x^2$$
$$C_3 = \{1100, 0101,1000\} \rightarrow W(C_3) = x + 2x^2$$
$$C_4 = \{1110,0110,1010\} \rightarrow W(C_4) = 2x^2 + x^3$$

Nous voyons que la signature S et totalement discriminante pour C. Pour le code C' nous avons :

$$C_1' = \{0011, 0101\} \quad \rightarrow W(C_1') = 2x^2$$
$$C_2' = \{0011, 1011, 1001\} \rightarrow W(C_2') = 2x^2 + x^3$$
$$C_3' = \{0001, 1001, 1101\} \rightarrow W(C_3') = x + x^2 + x^3$$
$$C_4' = \{0010,1010, 1100\} \rightarrow W(C_4') = x + 2x^2 .$$

Remarquons que :

$$W(C_1) = W(C_3')$$
$$W(C_2) = W(C_1')$$
$$W(C_3) = W(C_4')$$
$$W(C_4) = W(C_2')$$

Nous pouvons donc obtenir immédiatement la permutation σ telle que $C' = \sigma(C)$.

$\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 2$. C'est à dire que $\sigma = (1342)$.

CONCLUSION

Ce travail s'inscrit dans le cadre de la théorie algébrique des codes correcteurs d'erreurs. Plus précisément on s'intéresse à l'étude de l'équivalence de deux codes de mêmes paramètres par isométrie (application qui conserve la distance de Hamming).

Notons que deux codes sont équivalents par isométrie s'ils appartiennent à la même orbite sous l'action du groupe des isométries de l'espace de Hamming.

Ce travail consiste à étudier l'équivalence entre deux codes correcteurs d'erreurs par permutation et par isométrie d'une part, et d'autre part de déterminer la permutation qui établit cette équivalence (dans le cas d'équivalence par permutation).

En fin le problème d'équivalence des codes demeure encore ouvert ce qui demande une recherche approfondie.

BIBLIOGRAPHIE

[1] : Alain Yger, Jacques-Arthur Weil, *Mathématique appliquées L3*, Pearson Education, France, août 2009, P390-395.

[2] : Bennoui Abdelhamid, *Etude sur l'équivalence entre deux codes Correcteurs d'erreurs*, Mémoire présente pour l'obtention du diplôme de magistère, Université de M'sila, 2009.

[3] : Christine Bachoc, *Cours des codes (UE code, signal)*, Université Bordeaux Master CSI2-2004-2005, P12-14.

[4] : FJ. Macwilliams and NJA Sloane, *The théory of error-correcting codes*, North. Holland 1977.

[5] : Gintaras Skersys, *Calcule de groupe d'automorphismes des codes, détermination de l'équivalence des code*, Thèse de doctorat, Université de Limoges, 1999, P19-30.

[6] : Guy Auliac- Jean Delcourt- Rémy Goblot, *Mathématique-Algèbre et géométrie*, Dunod, Paris, 2005, P119-132.

[7] : J. Bernstein Daniel, Johannes Buchmann, *Post-Quantum Cryptography*, Springer, Chicago and Darmstadt, December 2008, P116-118.

[8] : Ladjelat Lahcene, *Etude de l'équivalence de deux codes sur un corps finis*. Mémoire présente pour l'obtention du diplôme de magistère, Université de M'sila, 2004.

[9] : Michel Demazure, *Cours d'algèbre*, Cassini 1997.

[10] : Nicolas Bruyère, *Eléments de théorie des corps finis. Application : les codes correcteurs*, Université de Rouen, 2006, P1-2.

[11] : Nicolas Sendrier, Un *algorithme pour trouver la permutation entre deux codes binaires équivalents*, INRIA-Rocquencout, Rapport de recherche N°2853, Avril 1996, P5-7.

[12] : Nicolas Sendrier, *Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs*, INRIA–Rocquencourt, Mémoire d'habilitation à diriger des recherches, mars 2002, P 06-12.

[13] : Petteri Kaski, Patric R. Ostergard, *Classification Algorithms for Codes and Designs* Springer Berlin Heidelberg New York, 2006, P35-36.

[14] : Pierre wassef, *Arithmétique application aux codes correcteurs et à la cryptographie* Vuibert, décembre 2009, P127-140.

[15] : A. Haily, *Les codes correcteurs, Codes linéaires et codes cycliques (Cours et exercices)*, P 8-18. http://www.dlzlogic.com/CaquotHelp.pdf