N°d'ordre : .....

UNIVERSITE DE M'SILA

FACULTE DES SCIENCES ET DES SCIENCES DE L'INGENIORAT

Département de Mathématiques

MEMOIRE

Présenté pour l'obtention du diplôme de Magistère
Spécialité : Mathématiques
Option : Mathématiques Discrètes

Par
BENNOUI Abedelhamid
SUJET

Etude sur l'équivalence entre deux codes Correcteurs d'erreurs

Soutenu publiquement le .....**devant le jury composé de** :

BOUDRAH Brahim	Pr. **Université de M'sila**	**Président**
MIHOUBI Douadi	M.C **Université de M'sila**	**Rapporteur**
BOUDAOUD Abdelmadjid	Pr. **Université de M'sila**	**Examinateur**
AMROUNE Abdelaziz	M.C **Université de M'sila**	**Examinateur**
BEN LAHCEN Moussa	**M.A.C.C Université de Batna**	**Examinateur**

Promotion : 2008 / 2009

SOMMAIRE

Notations
Introduction générale

CHAPITRE I Définitions et propriétés élémentaires

1. Introduction
2. Groupes
3. Corps finis
4. Espace vectoriel
5. Matrices

CHAPITRE II Codes correcteurs d'erreurs

1. Introduction
2. Les codes
3. Code linéaire
4. Codes systématiques
5. Constructions de nouveaux codes
6. Dualité
7. Polynômes énumerateurs des poids

CHAPITRE III détermination de l'équivalence entre deux codes correcteurs d'erreurs

1. Introduction
2. Groupe de permutations et d'automorphismes d'un code
3. Equivalence des codes
4. Invariants
5. Signatures
6. Un Algorithme Pour Trouver la permutation entre deux codes équivalents

CONCLUSIONS
BIBLIOGRAPHIE

NOTATIONS

$\mathbb{F}_q$	:	un corps fini a q élements
$C(n, k, d)$	:	code linéaire C de longueur n,dimension k et de distance minimal d
G	:	Matrice génératrice de code C
$C^{\perp}$	:	Code dual de C
H	:	Matrice de contrôle de C
$rg(H)$	:	Rang de H
${}^tG$	:	Transposée d'une matrice G
Id_k	:	Matrice indentité de rang k
$G = (Id_k, \|A)$	:	Matrice génératrice en forme systematique
$H = (-A, \|Id_{n-k})$	:	Matrice de contrôle en forme systematique
$W(C)$	:	poids de hamming de C
S_n	:	Groupe symétrique de n éléments
$Aut(C)$	:	Groupe d'automorphisme de C
$C_1 \backsim C_2$	:	Equivalence des codes
A_i	:	Nombre des mots du code C de poids i
$\langle x, y \rangle$	:	Le produit scalaire de x et y
$perm(C)$	:	Le groupe de permutation d'un code C
C_i	:	Le code poinçonné en i
$[G : H]$	:	L'indice du sous groupe H dans G
$\|G\|$	:	L'ordre d'un groupe fini G ou le cardinale d'une ensenble fini G
N	:	L'ensemble des entiers naturels
Z	:	L'ensemble des entiers relatifs
$Ker(H)$	:	L'espace nul d'une matrice H
I	:	un ensemble ordonné de cardinal n
$\sigma(c)$	:	L'action de $\sigma \in S_n$ sur le mot c
$\sigma(i)$	:	L'image de $i \in I$ par σ
$\sigma(C)$	:	L'action de $\sigma \in S_n$ sur le code C
$\gamma(C)$	:	L'image de C par l'invariant γ
$S(c, i)$	:	l'image du couple (c, i) par la signature S
$\sigma(a) = b$	:	Si $a_i = b_{\sigma(i)}$ pour tont $1 \leqslant i \leqslant n$
$C^{\intercal}$	:	Code poinçonné du code C par rapport a l'ensemble $\intercal$
$C_{\intercal}$	:	Code raccourci du code C par rapport a l'ensemble $\intercal$
$\hat{C}$	:	Code étendu du code C
$\overline{C}$	:	L'orbite de code C selon l'action S_n sur ζ_n.
ζ_n	:	L'ensemble de tous les codes de longueur n sur $\mathbb{F}_q$.
ζ	:	L'ensemble de tous les codes sur $\mathbb{F}_q$.
ϕ_C	:	Application injective (Codage).

RESUME

Dans ce mémoire, on s'intéresse à l'étude de l'équivalence entre deux codes correcteurs d'erreurs.

Deux codes C et C' sont dits équivalents s'il existe une permutation $\sigma \in S_n$ telle que $\sigma(C) = C'$.

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

Deux code sont équivalents par permutation s'iles sont égaux à une permutation prés a leur coordonnées.

Dans ce travail on présente une étude capable de calculer cette permutation qui transforme l'un des codes à l'autre en utilisant trois méthodes diffirentes

- En utilisant les matrices géneratrices des deux codes sous formes standard.
- En utilisant les permutations sur les positions.
- En utilisant l'Algorithme de NICOLAS SENDRIER si la signature et totalement discriminante.

MOTS CLES: corps finis, groupes de permutations, matrices, code correcteurs d'erreurs.

ABSTRACT : In this memory, we are interested in studying the equivalence between two error correcting codes. Two codes C and C' were equivalent if there exist a permutation $\sigma \in S_n$ as $\sigma(C) = C'$.

The determination of equivalence between two codes for a basic purpose of the classification codes.

Two code permutation are equivalent if they are equal to a permutation meadows to their coordinates.

In this work we presents a study able to calculate this permutation that transforms one of the codes to another using three methods diffirentes

- Using matrices generations of both forms of standard codes.
- Using the permutations on positions.
- Using the algorithm NICOLAS SENDRIER when the signature and totally descriminent.

KEYWORDS: finite field, permutation of groups, matrix, error-correcting code.

INTRODUCTION GENERALE

Presentation du mémoire

Il est possible de définir la notation d'équivalence de deux codes correcteurs d'erreurs de plusieurs manière.

- Comme équivalence par matrices.
- Comme équivalence par permutations des positions du code ou des symboles figurant des positions fixées.
- Comme équivalence par le groupe de permutation et d'automorphisme de code.

Dans ce travail, on s'intéresse à l'étude de tout les cas précédents.

L'étude de l'équivalence de deux code est un probleme important en théorie des codes correcteus d'erreurs, deux codes équivalents ont même structure, même distance minimale et même distribution des poids.

Déroulement du mémoire

Ce mémoire est composé de trois chapitres.

Dans le premier chapitre on présente les notions fondamentales concernant la théorie des groupes, les corps finis, les espaces vectoriels et les matrices.

Nous avons étudié avec plus de détails les groupes de permutatios et les matrices car ses notions représentent l'outil mathématique nécéssaire pour l'étude de l'équivalence des codes correcteurs d'erreurs.

Dans le deuxiéme chapitre nous présentons les notions fondamentales de la théorie des codes correcteurs d'erreurs (code linéaire, description matricielle des code linéaire, distance minimale, construction de nouveaux codes, code dual...).

Dans le troisiéme chapitre on utilise trois méthodes pour détérminer l'équivalence entre deux codes correcteurs d'erreurs.

Dans la première méthode on a utilisé les formes matricielles en écrivant les matrices génératrices des codes sous forme standard pour détérminer la permutation qui transforme l'une à l'autre.

- Dans la seconde méthode, on a utilisé les permutation du code et aussi les permutations des symboles figurant en position fixées et comme cas pariculier on a étudié.
- Le cas ($n = d$, $k = q$) où on a démontré que le code qui vérifie cette propriété est équivalent à un code de répétition.
- Le cas ($q = 2$) et ce code contient seulement deux mots on a pu démontré que le nombre des codes inéquivalents à un tel code vérifie la propriété précédente est égale a (n).
- Dans le dernier cas, on utilise comme cas particulier une signature totalement discriminante, pour la détermination de la permutation de l'équivalence et on a pu donner un exemple qui réalise l'Algorithme présenté par NICOLAS SENDRIER dans [13].

CHAPITRE I

Définition et propriétés élémentaire

1. INTRODUCTION

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

Les définitions et résultats énoncés dans ce chapitre constituent les mots clés concernant cette études. D'autres éléments viendront les compléter au cours des différents chapitres.

2. GROUPE

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

Définition 1:

Soit G un ensemble non vide.

Une loi de composition interne sur G est une application φ de $G \times G$ dans G.

Notations 2:

Limage $\varphi(x, y)$ de $(x, y) \in G \times G$ par φ noté $x \varphi y$ ou xy si aucune confusion n'est à craindre.

Définition .3:

Soit G un ensemble non vide muni d'une loi de composition interne définie par $(x, y) \mapsto xy$

G possède une structure de groupe (ou par abus de langage que G est un groupe) si cette loi est associative, i.e quelque soient les éléments x, y, z de G : $(xy)z = x(yz)$

- G possède un élément neutre e pour cette loi, i.e pour tout $x \in G$: $xe = ex = x$.
- Tout élément $x \in G$ possède un symétrique unique $\grave{x}$ (ou x^{-1}) de G tel que $x\grave{x} = \grave{x}x = e$.

Exemple 1:

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

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

Remarque 4:

1- Si la loi de G est commutative, c'est-à-dire pour tout $x, y \in G$ on a: $xy = yx$, le groupe G est dit 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 noté $|G|$.

Définition 5:

Soit H une partie non vide d'un groupe G, alors H est dit 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.

Soit H un sous groupe de G; pour tout élément $x \in G$, on définit l'ensemble

$Hx = \{hx / h \in H\}$ appelé la classe à gauche de x modulo H.

De même, on définit $xH = \{xh / h \in H\}$ la classe à droite de x modulo H.

Désignons par $\left[(G/H)_g \text{ respectivement } (G/H)_d \right]$ l'ensemble des classe à gauche (respectivement à droite) modulo H.

Lemme 6:

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

preuve:

Puisqe 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 $(G/H)_g$ dans $(G/H)_d$ $\diamond$

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

Théorème (de lagrange) 7:

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:

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

Groupe cyclique 8:

Il est clair en utilisant la définition 1.5. de voir que l'intersection d'une famille quel conque $(H_i)_{i\in I}$ de sous groupes d'un groupe G est un sous groupe de G.

Lemme 9:

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. Soit $H = \bigcap_{i\in I} H_i$ qui est 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 $H \subset L$. $\diamond$

Le plus petit sous groupe de G contenant x est appelé le sous groupe de G engendré par x, et il noté $gp(x)$. L'élément x est dit élément générateur de $gp(x)$.

Exemple 1:

1- Le sous groupe de $(\mathbb{Z}, +)$ engendré par $n \in N$ est l'ensemble des multiples de n dans $\mathbb{Z}$.

2- Le sous groupe $gp(\bar{3})$ de $\mathbb{Z}/4\,\mathbb{Z}$ est $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.

3- Le sous groupe $gp(\bar{2})$ de $\mathbb{Z}/4\,\mathbb{Z}$est $\{\bar{0}, \bar{2}\}$.

Définition 1:

Un groupe G est dit cyclique s'il existe un élément x de G qui sera appelé générateur tel que $G = gp(x)$.

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 ou $s \in \mathbb{Z}$; c'est-à-dire que:

$$gp(x) = \{x^s / s \in \mathbb{Z}\} \text{ avec } x^s = \begin{cases} x.x.x\ldots x \quad (s) \text{ fois si } s > 0 \\ x^{-1}.x^{-1}.x^{-1}\ldots (-s) \text{ fois si } s < 0 \\ e \text{ si } s = o \end{cases}$$

Théorème 10:

Soit G un groupe cyclique

1- Si G est infini a lors G est isomorphe à $\mathbb{Z}$.

2- Si G est fini d'ordre $k \geqslant 1$ a lors G est isomorphe à $\mathbb{Z}/k\,\mathbb{Z}$.

Groupe symétrique S_n 11:

L'étude des codes équivalents à un code donné est basé sur l'étude du 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 groupe de permutations.

Théorème (de CAYLEY) 12:

Tout groupe G est isomorphe à un sous-groupe du groupe $(S(G), \circ)$.

preuve:

Soit $f : G \to S(G)$ définie par: $f(g) = f_g$

ou $f_g(x) = gx$ pour tout $x \in G$.

Pour tout x de G.Pour un $g_0 \in G$, si $g \in G$, l'équation en x, $g_0 x = g$ possède une solution unique x et il en rélulte que f_{g_0} est une bijection de G sur G. on vérifie facilement que f est une injective.

Comme pour tous:

$x, g, \acute{g} \in G, f_{g\acute{g}}(x) = g\acute{g}x = f_g(\acute{g}x) = f_g(f_{\acute{g}}(x)) = f_g \circ f_{\acute{g}}(x)$

On constate que f est un isomorphisme de G sur $f(G)$ où $f(G)$ et sous groupe $(S(G), \circ)$ $\diamond$

L'ordre de S_n 13:

Pour tout $n \geqslant 1$, le groupe symétrique S_n est d'ordre $n!$ où:

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

une permutation σ de S_n et noté par:

$\sigma = \begin{pmatrix} 1 & 2 & k & n \\ i_1 & i_2 & i_k & i_n \end{pmatrix}$, avec $\sigma(k) = i_k$ et $i_k \in \{1, 2, \ldots, n\}$ pour tout $k \in \{1, 2, \ldots\ldots, n\}$

Groupe de permutation 14:

Si G est un sous-groupe de $S(E)$ donc G et dit un groupe de permutation de E.

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

Proposition 15:

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 $S(E)$. $\diamond$

Proposition 16:

Si G est un groupe de permutations de E. Alors il en est de même pour xGx^{-1}: pour toute permutation x de E on a:

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

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 $\beta = xg_2x^{-1}$

$\alpha \cdot \beta = (xg_1x^{-1})(xg_2x^{-1}) = x(g_1x^{-1}xg_2) \cdot x^{-1} = x(g_1g_2)x^{-1} \in xGx^{-1}$

$\alpha^{-1} = (xg_1x^{-1})^{-1} = xg_1^{-1}x^{-1}$

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

par conséquent xGx^{-1} est un sous-groupe de $S(E)$, pour tout $x \in S(E)$. $\diamond$

Action d'un groupe fini sur un ensemble 17:

Définition 1:

Soit G un groupe (de loi notée multiplicativement) et E un ensemble non vide.On dit que G opère sur E si G est isomorphe à un sous-groupe du groupe symétrique $S(E)$ (groupe de bijection), ce qui équivalent de dire.

Définition 2:

Le groupe G opère sur l'ensemble E s'il existe une application $\varnothing: G \times E \longrightarrow E$ où $\varnothing(g, x)$ sera notée gx qui satisfait, pour tous $g_1, g_2 \in G, x \in E$ aux conditions

i- $g_1(g_2x) = g_1g_2x$.

ii- $1x = x$, où 1 est l'élément neutre de G.

Exemple 1:

S_n opère sur $\overline{1, n}$. En éffet:

$S_n \times \overline{1, n} \longrightarrow \overline{1, n}$

$(\sigma, x) \longrightarrow \sigma \cdot x = \sigma(x)$

Preuve:

On a bien

$\forall(\sigma,\acute{\sigma}) \in S_n^2, \forall x \in \overline{1,n}$:
$\sigma \cdot (\acute{\sigma}x) = \sigma \cdot \grave{\sigma}(x) = \sigma\grave{\sigma}(x) = \sigma \circ \grave{\sigma}(x) = (\sigma \circ \grave{\sigma})(x)$
$1 \cdot x = 1(x) = x$

Exemple 2:

Soit $\sigma \in S_n$, notons $\langle\sigma\rangle = \{\sigma^n, n \in \mathbb{Z}\}$ le sous-groupe de S_n engendré par σ.
Alors $\langle\sigma\rangle$ opère sur $\overline{1,n}$ par l'application
$\langle\sigma\rangle \times \overline{1,n} \longrightarrow \overline{1,n}$
$(\sigma^n, x) \longrightarrow \sigma^n \cdot x = \sigma^n(x)$

preuve:

On a bien:
$\forall(m,n)\mathbb{Z}^2, \sigma^m \cdot \sigma^n(x) = (\sigma^m(\sigma^n(x))) = \sigma^m \circ \sigma^n(x) = (\sigma^m \circ \sigma^n)(x)$
$1_d \cdot x = 1_d(x) = x$ $\diamond$

Remarque 3:

En général, $g_1x = g_2x$ n'entraîne pas $g_1 = g_2$.
En effet, dans S_4, considérons $\sigma_1 = (1,2)$ et $\sigma_2(1,3)$.
On a: $\sigma_1(4) = \sigma_2(4) = 4$ pourtant $\sigma_1 \neq \sigma_2$.

Définition 4:

Soit G un groupe opérant sur un ensemble E.
La relation R définie sur E par:
$xRy \Leftrightarrow \exists g \in G : y = gx$; est une relation d'équivalence.
La classe de $x \in E$ modulo cette relation est appelée l'orbite de x et sera notée par: $G \cdot x$ ou $orb(x)$

telle que : $orb(x) = G \cdot x = \{gx/g \in G\} = \{y \in E/\exists y \in G : y = gx\}$.

preuve:

Réflexivité: $x = 1x$ d'où xRx
Symétrie: si xRy i.e $\exists y \in G : y = gx$, alors:
$\exists h \in G : x = hy$
Il suffit de choisir $h = g^{-1}$. En effet, $hy = g^{-1}y = g^{-1}gx = (g^{-1}g)x = 1x = x$. Donc: yRx

Transitivité:

si xRy et yRz alors, on a:
$y = gx$ et $z = hy$ ou $z = hgx = (hg)x$ d'où xRz.
La classee de $x \in E$ modulo cette relation est appelée l'orbite de x et sera notée par $G \cdot x$ ou bien $orb(x)$.
$G \cdot x = \{gx/g \in G\} = \{y \in E/\exists g \in G : gx = y\}$.

Exemple 1:

Soit $G = S_n$. Si S_n opére sur $\{1,\ldots,n\}$ dans ceci il n'ya qu'une seule orbite, en éffet, soit $x \in [1,n]$.
$\forall y \in \overline{1,n}, \exists \sigma \in S_n : y = \sigma(x)$.

3. CORPS FINIS

Les corps finis représentent, l'outil le plus utilisé dans la théorie des codes correcteurs d'erreurs.

Dans cette section, on donne quelques propriétés, fondamentales des corps finis qui seront utilisés par la suite.

Définition 1:

Soit $(E,+,\cdot)$ un corps.
Le corps E sera dit finis si le $|E|$ est fini. Si $|E| = q \in \mathbb{N}$ le corps E et généralement noté $\mathbb{F}_q$.
Où la caractéristique d'un corps (fini ou non) est le plus petit entier, non nul p tel que: $p \cdot 1 = 0$ ou 0 et 1 représentent respectivement l'élément unité du corps et:
$p \cdot 1 = 1 + 1 + 1 + \ldots\ldots\ldots + 1$ (p fois).
s'il n'existe pas un entier non nul vérifiant $p \cdot 1 = 0$, on dit que le corps est de caractéristique nulle.

Exemple1 :

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

Dans ce cas, il sera désigné par $\mathbb{F}_p$.

Propriétés 2:

La caractéristique d'un corps fini $\mathbb{F}_q$ est un nombre premier p et ce corps contient un sous corps fini isomorphe a $\mathbb{F}_p$.

On dit par abus de langage que $\mathbb{F}_p$ est un sous corps de $\mathbb{F}_q$.

Preuve:

En effet, si p n'est pas premier, alors p s'écrit de la forme $p = s \cdot t, 1 < s < p, 1 < t < p$.

On a donc: $p \cdot 1 = st \cdot 1 = 0$

$= (s \cdot 1) \cdot (t \cdot 1)$

Et comme $\mathbb{F}_q$ est un corps, donc intègre et par suit $s \cdot 1 = 0$ ou $t \cdot 1 = 0$.

Ce qui contredit le fait que p est la caractéristique de $\mathbb{F}_q$.

4. ESPACES VECTORIELS

Dans cette section nous rappelons quelques définitions nécessaires de l'algèbre linéaire, qui seront utilisés par la suite pour définir les codes linéaires.

Notations 1:

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

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

Proposition 2:

Soit $\mathbb{F}_q$ un corps; l'ensemble $\mathbb{F}_q^n$ muni de l'addition définie par

$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$ et la multiplication par scalaire $\lambda \in \mathbb{F}_q$.

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

Sous espace vectoriel 3:

Soit W un sous ensemble d'un espace vectoriel V sur un corps $\mathbb{F}_q$; W est un sous espace de V si et seulement si pour tout $\mu, \nu \in W, \lambda \in \mathbb{F}_q$ on a:

i. $\mu + \nu \in W$

ii. $\lambda\mu \in W$

Exemples 1:

Soit $V = \mathbb{F}_2^2$, alors $W_1 = \{(a,0)/a \in \mathbb{F}_2\}$ est un sous espace de V.

De même $W_2 = \{V = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n / x_1 + x_2 + \dots x_n = 0\}$ est un sous espace sur $\mathbb{F}_q$.

5. MATRICES

Dans cette section, nous présentons les notations sur les matrices que nous utiliserons tout au long de ce document .

Pour étudier les espases vectoriels , les applications linéaires, partout ou interviennent des coefficients , on utilises une représentation sous forme de matrice, rectangulaires ou carrés .

Définition 1:

On appelle matrice à éléments dans un corps $\mathbb{F}_q^k$, tout tableau rectangulaire ou carré d'éléments $a_{ij} \in \mathbb{F}_q^k$ (ou $a_{ij} \in A$), on convient de réserve le premier indice i au numéro de la ligne et le deuxième indice j au numéro de la colonne contenant l'élément a_{ij}.

On note les matrices par M ou (a_{ij}) , $1 \leq i \leq p$, $1 \leq j \leq q$

ou $\begin{pmatrix} a_{11} & a_{12} \dots\dots & a_{1q} \\ a_{p1} & \dots\dots & a_{pq} \end{pmatrix}$

On appelle matrice rectangulaire de type $p \times q$ toute matrice formant un tableau rectangulaire de p lignes et q colonnes .

On appelle matrice carrée d'ordre p toute matrice formant un tableau carré de p lignes et p colonnes .

On appelle i-ème ligne d'une matrice $(a_{ij})(i,j)$ la j-ème colonne du tableau (formé par les éléments $a_{1,j}, a_{2,j} \dots\dots\dots a_{p,j}$).

On appelle diagonale principale d'une matrice carrées d'ordre $p(a_{ij})(i,j)$ la diagonale du

tableau carrée (formé par les éléments $a_{1,1}, a_{2,2} \ldots\ldots\ldots a_{p,p}$) .

Matrices particuliéres 2:

certaines matrices qui possèdent une ou plusieur proprietés spécifiques , ont reçu des nom particulier :

1. Une matrices nulle est une matrice carrée ou rectangulaire dont tous les éléments sont nuls .

Exemples 1:

$$M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad M_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad M_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \text{ etc .....}$$

2. La matrice unité d'ordre n est une matrice carrée dont les élément de la diagonale principale sont

$a_{ii} = 1$, $1 \leq i \leq n$ et tous les autres $a_{i,j} = 0$, $i \neq j$.

Exemples 2:

$$I_1 = (1), I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \text{ etc .....}$$

3. Une matrice scalaire est une matrice carrée d'ordre n

(a_{ij}) , $1 \leq i \leq n$, $1 \leq j \leq n$ telle que $a_{ii} = d$, $1 \leq i \leq n$,et $a_{i,j} = 0$, $i \neq j$.

Exemples 3:

$$M_1 = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \quad M_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix} \quad M_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 4 \end{pmatrix} \text{ , etc .....}$$

4. Une matrice ligne est une matrice ayant une seule ligne :

Exemples 4:

$M_1 = (213)$ $M_2 = (3202)$

5. Une matrice colonne est une matrice ayant une seulecolonne :

(a_{ij}) , $1 \leq i \leq p$ et , $j = 1$.

Exemples 5:

$$M_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \quad M_2 = \begin{pmatrix} 0 \\ 2 \\ 3 \\ 4 \end{pmatrix}$$

Rang d'une matrice3:

Définition 1:

On appelle rang d'une matrice $A = (a_{ij})$ le rang de l'application linéaire associée a cette matrice.

Matrices équivalentes , matrices semblables 3 :

Définition 1:

Deux matrice A et B de même type $p \times q$ sont équivalentes s'il existe deux matrices carrées

inversibles P et Q

telle que $B = PAQ$ • Avec P d'ordre p est Q d'ordre q.

Proposition 2:

La relation binaire R définie sur l'espace vectoriel $H(p,q)$ des matrices de type $p \times q$ par «ARB»équivalent à «$B = PAQ$» pour deux matrices carrées inversibles P et Q est une relation d'équivalences.

Preuve :

Tout matrice $A \in M(p,q)$ vérifie $A = I_q AIp$ donc «R» est reflexive .

Soit deux matrices équivalentes A et B, alors $B = P.A.Q$:P et Q etant inversibles , on endéduit que :

$P^{-1}BQ^{-1} = A$, donc «R» est symetrique .

Soit trois matrices A, B et C telle que ARB et BRC .Alors $B = PAQ$ et $C = GBS$, d'ou

$C = G(PAQ)S = (GP).A.(QS)$:comme (GP) et (QS) sont inversibles ,il en résulte que «R» est transitive .

Donc c'est une relation d'équivalence sur l'espace vectoriel $M(p,q)$. ◇

Exemples 1 :

$$A = \begin{pmatrix} 2 & 10 & 0 & -6 & 12 \\ 18 & 4 & 13 & 9 & 2 \\ 10 & 4 & 11 & 3 & -2 \\ 6 & 8 & 4 & -2 & -8 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

A est équivalentes à la matrice B, elle verifie

$A = PBQ.$ avec .

$$P = \begin{pmatrix} 2 & -1 & 3 & 1 \\ 2 & 3 & 0 & -1 \\ 2 & 1 & 0 & 5 \\ 2 & 0 & 2 & 0 \end{pmatrix} \text{ et } Q = \begin{pmatrix} 3 & 2 & 5 & 0 & -2 \\ 4 & 0 & 1 & 3 & 2 \\ 0 & 2 & -3 & -1 & -2 \\ 2 & 4 & 1 & 1 & -1 \\ 0 & 3 & -2 & 4 & 0 \end{pmatrix}$$

Matrices semblables 3:

Définition 1:

Deux matrices carrées d'ordre n sont semblables s'il existe une matrice inversible P telle que $B = PAP^{-1}$

Puisque $A = PAP^{-1}$, la relation est reflexive .

Puisque $B = PAP^{-1}$ entraine $A = P^{-1}AP$, la relation est symetrique .

Puisque «$B = PAP^{-1}$ et $C = QBQ^{-1}$ » entraine $C = (PQ)A(PQ)^{-1}$, la relation est transitive .

Donc la relation similitude des matrices carrées d'ordre n es une relation d'équivalence dans l'anneau des matrices carrées M_n .

Exemples 1:

Soit les deux matrices $A = \begin{pmatrix} 23 & 21 \\ 14 & 13 \end{pmatrix}$ et $B = \begin{pmatrix} -17 & 36 \\ -11 & 23 \end{pmatrix}$

Verifient bien la relation de similitude avec: $B = PAP^{-1}$, $P = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$

Transposé d'une matrice 4:

Définition 1:

On appelle transposée d'une matrice $A(a_i,j)$ de type (p,q) la matrice $B = (b_{ij})$ de type $q \times p$, obtenu en echangeant lignes et colonnes de A: $a_{i,j} = b_{ij}$

on note par $B = {}^t A = {}^t (a_{ij}) = (a_{ji})$.

Exemples 1 :

$$A = (210), {}^tA = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}$$

$$A = \begin{pmatrix} 4 & 1 \\ 5 & 3 \end{pmatrix}, {}^tA = \begin{pmatrix} 4 & 5 \\ 1 & 3 \end{pmatrix}$$

Echelonnement d'une matrice 5:

De façon generale, les méthodes directes (méthode de pivot par exemple) visent essentiellement, la transformation d'un systeme lineaire dans le but de le resourdre par un systeme lineaire échelonné equivalent et qui facilite la resolution .

Exemple1:

Soit La matrice A/ telque:

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 9 & 27 \\ 2 & 4 & 8 \end{bmatrix} A^{(2)} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 6 & 24 \\ 0 & 2 & 6 \end{bmatrix} A^{(3)} = \begin{bmatrix} 1 & 0 & -3 \\ 0 & 1 & 4 \\ 0 & 0 & -2 \end{bmatrix} A^{(1)} = \begin{bmatrix} 1 & 0 & -3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}$$

$$A^{(4)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Matrices échelonnées 6:

Soit A une matrice de type $p \times q$. On note L_i ses lignes pour $1 \leq i \leq p$.

Une matrice est dite échelonnée si les deux conditions suivantes sont vérifiées.

1. Toutes les lignes nulles sont situées en bas de la matrice.
2. Chaque élément distingué est situé à droite (strictement) de l'élément distingué de la ligne précédente.

Ainsi $A = (a_{ij})$ est une matrice échelonnée, s'il existe des éléments non nuls

$$a_{1j_1}, a_{2j_2}, \ldots, a_{rj_r} \text{ ou } j_1 < j_2 < \ldots < j_r$$

avec la propriété suivante

$$a_{ij} = 0 \text{ pour } (i)\ i \leq r, j < j_i \text{ et } (ii)\ i > r$$

Dans ce cas $a_{1j_1}, a_{2j_2}, \ldots, a_{rj_r}$ sont les éléments distingués de A.

Une matrice échelonnée A est dite sous forme canonique ligne si les deux conditions supplémentaires suivantes sont vérifiées:

1. Chaque élément distingué est égal à 1.
2. Chaque élément distingué est l'unique élément non nul dans toute sa colonne.

Méthode de GAUSS 7:

La méthode suivante permet de réduire par les lignes une matrice $A = (a_{ij})$ à la forme échelonnée.

1. Appeler j_1 la première colonne contenant un élément non nul.
2. Echanger les lignes de telles sorte que ce premier élément non nul apparaisse dans la première ligne, dans la j-ème colonne, c'est-à-dire tel que $a_{1j_1} \neq 0$.
3. Utiliser a_{1j_1} comme pivot pour obtenir des zéros en dessous de a_{1j_1}: c'est-à-dire, pour chaque $i > 1$, appliquer l'opération élémentaire.

$$-a_{ij_1} L_1 + a_{1j_1} L_i \rightarrow L_i \text{ ou } -\frac{a_{ij_1}}{a_{1j_1}} L_1 + L_i \rightarrow L_i$$

4. Répéter les étapes 1,2 et 3 avec la sous-matrice formée de toutes les lignes, à l'exception

de la premiére.

5. Continuer le procédé jusq'à ce que la matrice soit mise sous forme échelonnée.

Exemples 5.6.3:

Soit la matrice A/ telque

$$A^{(1)} = \begin{bmatrix} 1 & 1 & 1 \\ 3 & 9 & 27 \\ 2 & 4 & 8 \end{bmatrix} \quad A^{(2)} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 6 & 24 \\ 0 & 2 & 6 \end{bmatrix} \quad A^{(3)} = \begin{bmatrix} 1 & 0 & -3 \\ 0 & 1 & 4 \\ 0 & 0 & -2 \end{bmatrix}$$

$$A^{(4)} = \begin{bmatrix} 1 & 0 & -3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix} \quad A^{(5)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

CHAPITRE II

Les codes (le but des codes correcteurs d'erreurs)

1. INTRODUCTION

Les codes correcteurs d'érreurs sont utilisés pour corriger des érreurs quand des messages sont transmis par le biais d'un canal de communication comportant des parasites.

Par exemple nous pourrions vouloir transmettre une information binaire (un flot de os et de $1s$).

A travers un canal parasité aussi rapidement et aussi surement que possible.

Le canal peut être une ligne téléphonique, une liaison de communication par satelite, une liaison radio haute fréquence.

La perturbation (le parasite) pourrait être une erreur humaine, foudre, parasite thermal, imperfection des équipements etc... et pourait conduire à des érreurs de telle sorte que l'information reçue est différante de celle transmise.

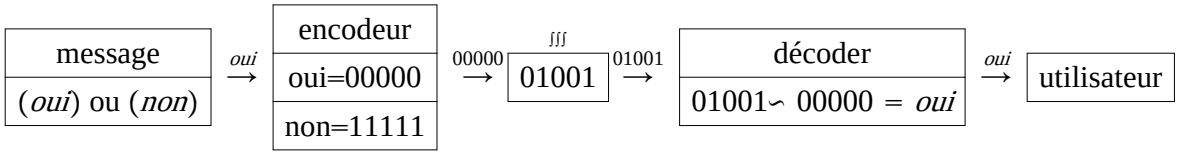
L'objectif d'un code correcteur d'erreurs est d'encoder (coder) les données, par le rajout d'une certaine quantité (volume) de redondonce au méssage, de telle maniere que le méssage oroginal peut être récuperé ci quelques erreurs se produisent un système général de communication numérique est reproduit dans le chémat 1.1 le même modèle peut être utulisé pour décrire un systeme d'information stockées ou (mise en mémoire) si l'accumulation moyenne est considirée comme un canal.

Un exemple typique est une unité de bande magnétique comportant des en-tête écrits et lus. Voir fig$_{(1)}$.

sourcedu *bruit*

Méssage →Méssage encoder mot de passe canal →vecteur recu décoder →Méssage décoder utilisation

Observons un exemple trés semple dans le quel les seuls messages que mous transméttons sont "oui" ou "non" représentivement par 0 et 1.



Ici deux erreurs se sont prodiutes et le décodeur a décodé le vecteur recu 01001 comme le mot de passe le plus "proche" qui et 00000 ou "oui".

fig(1)

Définitions et propriétés 1:

Soit $\mathbb{F}$ un ensemble fini dit alphabet

Un code C sur $\mathbb{F}$ de longueur n est un sous ensemble de $\mathbb{F}^n$. Un élément de C sera dit types de code de longueur n.

2. LES CODES

Définition 1:

- Si $\mathbb{F}$ est un groupe additif , alors C est un code additif s'il est un sous groupe additif de $\mathbb{F}^n$
- Si $\mathbb{F}$ est un anneau , alors C est un code linéaire s'il est un sous groupe additif de $\mathbb{F}^n$ et stable par rapport à la mutiplication par un élément de $\mathbb{F}^n$ (supposons que la multiplication dans $\mathbb{F}$ est commutative).
- Si $\mathbb{F}$ est un corps alors C est un code linéaire de longueur n et de dimension k s'il est sous espace vectoriel de dimension k de $\mathbb{F}^n$.

Notations :

On notera un mot de code $(x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ par concatenation sous le forme $x_1 x_2 \ldots x_n$.

Exemple 1:

Soit l'alphabet $\mathbb{F} = \{1, 3\}$

La partie $C = (133, 311, 111)$ de $\mathbb{F}^3$ est un code de longueur 3 sur $\mathbb{F}$.

Codage 2 :

Soit $\mathbb{F}_q$ un corps fini, on appelle codage une application injective, $\phi_C : \mathbb{F}_q^k \to \mathbb{F}_q^n$

Dont le code C est l'image de ϕ_C i.e

$$\underbrace{x_1 \quad x_2 \quad \dots \quad x_k}_{k} \xrightarrow{\phi_C} \underbrace{x_1 \quad x_2 \quad \dots \quad x_k}_{k} \underbrace{x_{k+1} \quad \dots \quad x_n}_{n-k}$$

cette application associe à un bloc de longeur k, son mot de code de longeur n de la manière suivante :

les k premier symboles sont les symboles d'information, et les $n-k$ symboles restants sont dits symboles de contrôle.

Exemple 1:

Soit l'application injective $\phi_C : \mathbb{F}_2^1 \to \mathbb{F}_2^3$

$$0 \to 000$$
$$1 \to 111$$

dont l'image ($\mathrm{Im}\,\phi_C$) est le code $C = \{000, 111\} \subset \mathbb{F}_2^3$, qui est dit code de répétition.

Distance de Hamming 3:

Définition 1:

La distance de Hamming entre deux mots $x = (x_1 x_2 \dots . x_n)$ et $y = (y_1 y_2 \dots . . y_n)$ de $\mathbb{F}^n$, que l'on notera $d(x, y)$, est le nombre d'indices $i \in \{1, \dots, n\}$ telle que x_i différent de y_i i.e

$$d(x, y) = |\ \{i \in \{1, \dots, n\} / x_i \neq y_i\}\ |$$

Exemple 1:

- Soit $F = \{0, 1\}, x = 101, y = 010, d(x, y) = 3.$
- Soit $F = \{1, 3\}, x = 133, y = 111, d(x, y) = 2$
- Soit $F = \{a, b\}, x = aaaa, y = aabb, d(x, y) = 2..$

Le poids de Hamming 4:

Définition 1:

le poids de hamming d'un mot $x = (x_1, x_2, \dots, x_n)$ de $\mathbb{F}_q^n$ de longueur n, noté $w(x)$, est le nombre de ses composantes non nulles. $w(x) = |\{i / x_i \neq 0\}|$.

Exemple 1:

Dans $\mathbb{F}_2^4$, on a $w(1101) = 3, w(0011) = 2.$

Distance minimale d'un code 5:

La distance minimale d'un code C est la plus petite distance entre deux mots distinct de ce code, on la note par $d = \min\{d(x, y) / x, y \in C \text{ et } x \neq y\}$.

Theoreme [4] **1:**

Un code C de distance minimale d corrige au plus $e = \left[\frac{d-1}{2}\right]$ erreurs et en détecte $d - 1$.

Preuve:

Le code C ne corrige pas t erreurs si et seulement si: $\exists x \in \mathbb{F}^n,\ \exists c, \grave{c} \in C, c \neq \grave{c}, d(x, y) \leqslant t$ et $d(x, \grave{c}) \leqslant t$ (1)

et cela entraine $d \leqslant d(c, \grave{c}) \leqslant d(c, x) + d(x, \grave{c}) \leqslant 2t$, soit $d \leqslant 2t$ (2)

Laréciproque est vraie, en affet, si (2) est verifiée, on peu toujours trouver deux mots de code c et $\grave{c}$ situes a la distance d l'un de l'autre, et les noter $c = (c_1, c_2, \dots, c_n)$ et $\grave{c} = (\grave{c}_1, \grave{c}_2, \dots, \grave{c}_d, \grave{c}_{d+1}, \dots, \grave{c}_n)$ quitte à permuter les coordonnées. Il existe deux entiers naturels p et q inferieurs ou egaux à t tel que $d = p + q \leqslant 2t$, et le mot $x = (\grave{c}_1, \grave{c}_2, \dots, \grave{c}_p, \grave{c}_{p+1}, \dots, \grave{c}_{p+q}, c_d, \dots, c_n)$ verifie bien $d(x, c) = p \leqslant t$ et $d(x, \grave{c}) = q \leqslant t$ cela preuve (1).

En conclusion C corrige t erreurs si et seulement si $2t \leqslant d$, et cela équivant a $t \leqslant \left[\frac{d-1}{2}\right]$.

◇

3. CODES LINEAIRES:

Dans cette partie, on s'interesse a une classe de codes ayant une propriété importante, la linéarité en d'autre mots l'application $\phi c : \mathbb{F}_q^k \to \mathbb{F}_q^n$ (ϕc est lineaire) ce qui permet d'endéduire par la linéarité que: $\phi c : \mathbb{F}_q^k \to \mathbb{F}_q^n \Rightarrow C = \mathrm{Im}(\phi c) \subset \mathbb{F}_q^n$.

Définition 1:

Un code linéaire de longueur n est un sous espace vectoriel $C \subset \mathbb{F}_q^n$, on notera k la dimension de C.

Un code linéaire C de longueur n, de dimension k, et distance minimale d est souvent noté $C(n, k, d)$.

Comme C est un espace vectorial de $\mathbb{F}_q^n$, si $x \in C, y \in C$, alors $x - y \in C$, il en résulte que la distance minimale du code C est

$$d = \min\{d(x,y) = w(x-y)/x, y \in C, x \neq y\} = \min\left\{w(x)/x \in C \text{ et } x \neq 0\right\}.$$

Discription matricielle des codes linéaires 2:

Matrice génératrice 1:

Soit $C = C(n, k)$ un code linéaire sur $\mathbb{F}_q$, une matrice génératrice G de C est une matrice dont les lignes forment une base de C, une matrice génératrice G est donc de type $k \times n$ et de rang k.

Si $\{c_1, c_2, \ldots . c_n\}$ est une base de C, alors tous les éléments du code linéaire C s'écrivent sous la forme:

$C = \{c \in \mathbb{F}_q^n : c = a.G, a \in \mathbb{F}_q^k\}$

Une matrice G de type $k \times n$

$$G = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix}, a = (a_0, a_1, \ldots, a_{k-1})$$

$$G = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

Soit $a = (a_0, a_1, \ldots, a_{k-1})/\ a \cdot G = (a_0, a_1, \ldots, a_{k-1}) \begin{bmatrix} g_{00} & \cdots & g_{0,n-1} \\ \vdots & \vdots & \vdots \\ g_{k,0} & \cdots & g_{k-1,n-1} \end{bmatrix}$

$= a_0 g_0 + a_1 g_1 + \ldots + a_{k-1} g_{k-1}$.

Exemple 1:

Soit $\{1100, 0111, 1010\}$ une base d'un code linéaire $C \subset \mathbb{F}_2^4$. Alors

$G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$. et la matrice génératrice du code C.

Exemple 2:

Soit G la matrice génératrice du code binaire C telque $G = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$ pour déterminer les mots de code C on utilise l'application φ définie par:

$\varphi : \mathbb{F}_2^2 \to \mathbb{F}_2^5$

$(x_1, x_2) \to (x_1, x_2) \cdot \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$

$C = \text{Im}(\varphi) \subset \mathbb{F}_2^5 = \{00000, 01111, 10010, 11101\}$ ainsi le code C est de paramétres $[5, 2, 2]$.

Et on a par exemple, le méssage 11 est codé par $c = 11 \cdot G = 11101$.

Matrice de contrôle 2:

Définition 1:

Une matrice de contrôle H d'un code linéaire C est une matrice de type $(n-k) \times n$ et de rang $(n-k)$ vérifiant : $C = \left\{ c \in \mathbb{F}_q^n / H.{}^t c = 0 \right\}$ on tire de la définition, que $C = \ker(H)$ et $rang(H) = n-k$, avec k la dimension de C sur $\mathbb{F}_q$.

$$H = \begin{bmatrix} h_0 \\ \vdots \\ \vdots \\ h_{n-k-1} \end{bmatrix} = \begin{bmatrix} h_{00} & \dots & h_{0,n-1} \\ h_{10} & \dots & h_{1,n-1} \\ \vdots & \vdots & \vdots \\ h_{n-k-1,0} & \dots & h_{n-k-1,n-1} \end{bmatrix}$$

Exemple 1:

supposons $q = 2, n = 6, k = 3 \quad (\text{donc } M = 2^3 = 8)$

C le code linéaire de paramètres $[6,3]$ dont la matrice de contrôle est donnée par :

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

Comme $C = \ker H$, $c = \{c_1, c_2, c_3, c_4, c_5, c_6\} \in H \Leftrightarrow H\,{}^t c = 0 \Leftrightarrow$

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

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

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

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

$\Leftrightarrow c = c_1 v_1 + c_2 v_2 + c_3 v_3$

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 mots de code correspond est $c = 011110$.

Le code C contient 2^3 mots de code

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

Exemple 2:

Soit l'ensemble $\{1100, 0111, 1010\}$ une basse d'un code linéaire

on a $C \subset \mathbb{F}_2^4$ de matrice génératrice G est $G = \begin{vmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{vmatrix}$

Donc l'application associée est définie par :

$\varnothing_g : \mathbb{F}_2^3 \to \mathbb{F}_2^4$

$$\varnothing_g : (x_1, x_2, x_3) \to (x_1, x_2, x_3) \begin{vmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{vmatrix}$$

$\varnothing_g(x_1, x_2, x_3) = (x_1 + x_3, x_1 + x_2, x_2 + x_3, x_2)$

D'ou $C = \text{Im}\,\varnothing_g(\mathbb{F}_2^3) = \{0000, 0110, 0111, 1010, 1011, 1101, 0001\}$

Pour obtenir le code C àpartir de la matrice de contrôle H en calcule tout d'abord l'espace nul de G.

Soit $y \in \mathbb{F}_2^4$,on a $y \in$ nul de G si seulement si $G.{}^t y = 0$

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = 0 \Leftrightarrow \begin{bmatrix} y_1 + y_2 = 0 \\ y_2 + y_3 + y_4 = 0 \\ y_1 + y_3 = 0 \end{bmatrix}$$

les solutions du système est $\{0000, 1110\} \subset \mathbb{F}_2^4$,donc la basse est l'élément (1110) donc la matrice $H = [1110]$.

Soit $\varnothing_h : \mathbb{F}_2^4 \to \mathbb{F}_2^1$

$$(x_1, x_2, x_3, x_4) \to [1110]\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = x_1 + x_2 + x_3$$

Et par conséquent , on a

$C = \ker(\varnothing_h) = \{x \in \mathbb{F}_2^4 \ : x_1 + x_2 + x_3 = 0\}$

On a par exemple : $0111 \in C$ car $\varnothing_h(0111) = 1 + 1 = 0$

$(1111) \notin C$ car $1 + 1 + 1 \neq 0$

4. CODES SYSTEMATIQUES

Achaque mots $x = (x_1, x_2, \ldots, x_k)$ du message on adjoint $n - k$ symboles: $x_{k+1}, x_{k+2} \ldots\ldots x_n$ dépendant linéairement des x_i pour obtenir le mot de code $c = f(x)$, les symboles ajoutés son appelé bits de contrôle .

On a $c = x \cdot G = (x_1 x_2 \ldots . x_k) \cdot \left(I_k / A\right)$

Où $\left(I_k / A\right)$ désigne la matrice $k \times n$ obtenus en écrivant cote à cote la matrice identité I_k de taille k et une matrice quelconque A .

$$c = x \cdot G = (x_1 x_2 \ldots . x_k) \cdot \left[\begin{array}{cccc|ccc} 1 & 0 & \ldots & 0 & a_{00} & \ldots & a_{0,n-k-1} \\ \vdots & \ddots & \ldots & \vdots & a_{10} & \ddots & a_{1,n-k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & \ldots & 1 & a_{k-1,0} & \ldots & a_{k-1,n-k-1} \end{array}\right]$$

$= (x_1 x_2 \ldots . x_k x_{k+1} \ldots x_n)$

Définition 1:

Un code C sera dit systématique, s'il possède une matrice génératice de la forme $G = \left(I_k / A\right)$

Comme $c \in C \Leftrightarrow \exists\, x \in \mathbb{F}_q^k : c = xG = x\left(I_k / A\right)$

on aura $c \in C \Rightarrow (-{}^t A / I_{n-k}) \cdot {}^t c = (-{}^t A / I_{n-k}) \cdot \begin{pmatrix} I_k \\ {}^t A \end{pmatrix} {}^t x = -{}^t A\, {}^t x + {}^t A\, {}^t x = 0.$

Autrement dit C est inclus dans le noyau de l'application lineaire de matrice $H = (-A^t / I_{n-k})$.

On notra $C \subset \ker(H)$

Comme H est une matrice de rang $n - k$, on aura $\dim C = \dim \ker H = k$ et $C = \ker H$.

On vient donc de montrer que la matrice H est une matrice de contrôle de C.

$$G = (I_k/A) = G = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} = \left[\begin{array}{c|c} \underbrace{\begin{matrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & 1 \end{matrix}}_{I_k} & \underbrace{\begin{matrix} a_{00} & \dots & \dots & a_{0,n-k-1} \\ \vdots & \ddots & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & \dots & \dots & a_{k-1,n-k-1} \end{matrix}}_{A} \end{array} \right]$$

Donc $H = (-A^t/I_{n-k}) = H = \left[\begin{array}{c|c} \underbrace{\begin{matrix} -a_{00} & \dots & \dots & -a_{k-1,0} \\ \vdots & \ddots & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ -a_{0,n-k} & \dots & \dots & -a_{k-1,n-k-1} \end{matrix}}_{-A^t} & \underbrace{\begin{matrix} 1 & 0 & \dots & 0 \\ \vdots & \ddots & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & 1 \end{matrix}}_{I_{n-k}} \end{array} \right]$

Exemple 1:

Soit C le code défini par sa matrice génératrice $G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$ on applique l'algorithme de GAUSS à G.

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \overset{L_2 \to L_1 + L_2}{\longrightarrow} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \overset{L_1 \to L_1 + L_2}{\longrightarrow} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$\overset{L_1 \to L_1 + L_3}{\longrightarrow} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Exemple 2:

L'encodage $f(x_1, x_2, x_3) = (x_1, x_2, x_3, x_1 + x_3, x_2 + x_3, x_1 + x_2 + x_3, x_3)$ définit un code systèmatique C de paramétres $[7,3]$ sur $\mathbb{F}_2$

l'écriture $(c_1, c_2, \dots, c_7) = (x_1, x_2, x_3) \cdot \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

Met en evidence une matrice génératrice de C et l'on déduit la matrice de contrôle.

$$H = \left[\begin{array}{ccc|cccc} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array} \right]$$

Exemple 3:

Soit C le code lineaire de parametres $[7,4,3]$ dont la matrice génératice est donnée par:

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \backsim G_1 = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right] = [\underbrace{I_4}_{} \mid \underbrace{A}_{}]$$

D'ou la matrice de contrôle est donnée par:

$$H = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right] = [\underbrace{-A^t}_{} \mid \underbrace{I_3}_{}]$$

5. CONSTRUCTIONS DE NOUVEAUX CODES

Parfois il est interéssant de trouver des nouveaux codes à partir de codes déja connus, pour améliorer les paramétres du code original, c'est le cas des codes étendus (extented code) des codes poinçonnées (tronqués) (punctured code), et des codes raccourcis (shorted code).

Le code etendu 1:

Soit $C(n, k, d)$ un code lineaire. On considére le code lineaire etendu $\hat{C}(n+1, k)$ de distance minimale d ou $d+1$, où chaque mot de code $\hat{C} = (c_1, c_2, \ldots, c_n, c_{n+1})$ est telque $c = (c_1, c_2, \ldots, c_n) \in C$ et $\sum_{i=1}^{n+1} c_i = 0$, on a alors tous les mots code de $\hat{C}$ de poids pair.

La matrice de contrôle $\hat{H}$ de $\hat{C}$ s'obtient en ajoutant à la matrice de contrôle H de C une ligne de 1 et un colonne avec un 0 danc les $n-k$ premiers positions et un 1 dans les $n-k+1^{ieme}$.

Exemple 1:

Soit $C = C(7,3,4)$ un code de matrice génératrice $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$ et de matrice de contrôle $H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$ alore $\hat{C} = \hat{C}(8,3,4)$ telque

$$\hat{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

$$\hat{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Exemple 2:

Soit $C = C(4,2,3)$ un code sur $\mathbb{F}_3$ de matrice génératrice $G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}$ et de matrice de contrôle $H = \begin{bmatrix} -1 & -1 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{bmatrix}$ alôre $\hat{C} = \hat{C}(5,2,3)$ telque $\hat{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & -1 & -1 \end{bmatrix}$ et $\hat{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 1 & 0 \end{bmatrix}$.

2. Le code poinçonné (tranqué) (punctured code) parapport à T, $T \subset \{1,2,\ldots,n\}$ noté C^T: le code de longueur $n-|T|$ obtenu en supprimant les coordonnées indicées par les éléments de T.

3. Le code raccourci (shorted code) parrapport à T, noté C_T : le code de longueur $n-|T|$ obtenu en utilisant l'ensemble des mots de C nul sur T, et en suprimant les coordonnées dans T.

Exemple 3:

Considerons le code binaire $C[6,3,2]$ de matrice génératrice $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$ est choisisons $T = \{4,5\}$, evidamment, la matrice du code C^T est $G^T = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$.

Pour déterminer C_T, nous devons isoler les mots de code C dont la $4^{éme}$ et la $5^{éme}$ cordonnées sont nul. On exclu aisément les lignes de G et la somme de ces trois lignes.

Il reste l'ensemble $\{(000000),(110000),(101000),(011000)\}$ puisque les mots de C sont $\{000000,111111,100111,001111,101000,011000,110000,010111\}$.

En suppriment les cordonnées dans T, nous obtenons le code engendré par:

$G_T = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$

6. DUALITE

Notons $x = (x_1, x_2, \ldots, x_n)$ et $y = (y_1, y_2, \ldots, y_n)$ deux mots de $\mathbb{F}_q^n$, avec $n \geqslant 1$.

Définition 1:

Le produit scalaire euclidien sur $\mathbb{F}_q^n$ est la forme bilinéaire symétrique qui à tout x et y de $\mathbb{F}_q^n$ associé l'élément

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i \text{ de } \mathbb{F}_q$$

Exemple 1:

le produit scalaire euclidien sur $\mathbb{F}_2^4$ de $x = 1101$ et $y = 1111$ est :

$\langle x, y \rangle = 1.1 + 1.1 + 0.1 + 1.1 = 1$

Définition 2:

1- Deux mots x, y de $\mathbb{F}_q^n$ sont dit 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 :

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

Pour un code linéaire C le dual $C^{\perp}$ est aussi un code linéaire sur $\mathbb{F}_q$ si de plus C est de matrice génératique G, et de matrice de contrôle H alors $C^{\perp}$ serait de matrice génératrice H et de matrice contrôle G l'orthogonalité permet de déduire que

$$G\ {}^tH = H\ {}^tG\ = 0$$

Enfin remarquons que si C est un code $\lceil n, k \rceil$ alors $C^{\perp}$ est un code $\lceil n, n-k \rceil$, car :

$$\dim C + \dim C^{\perp} = n.$$

Propriétés 3:

Soit C_1 et C_2 deux codes.

1. $(C_1^{\perp})^{\perp} = C_1$.
2. $(C_1 + C_2)^{\perp} = C_1^{\perp} \cap C_2^{\perp}$ 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 $C^{\perp}$ contienr C.

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

Si $C = C^{\perp}$, alors C est appelé un code auto-dual.

Exemple1:

Soit le code $C = \{000, 011, 101, 110\}$ de longueur 3 sur $\mathbb{F}_2$ le dual $C^{\perp}$ de C est

$C^{\perp} = \{y \in \mathbb{F}_2^3, y = abc, \forall c \in C, \langle c, y \rangle = 0\}$

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

donc $y_1 = 111, y_2 = 000$ d'ou $C^{\perp} = \{111, 000\}$

Exemple 2:

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

$\grave{C}^{\perp} = \{0000, 1100, 0011, 1111\}$ on remarque que $C^{\perp} = \grave{C}$.

7. POLYNÔME ENUMERATEUR DES POIDS

soit $C = C(n, k)$ un code linéaire , le polynôme homogéne de deux variables x , y suivant :

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

est appelé polynôme énumérateur des poids de C

En effet :

$$W_C(x, y) = \sum_{c \in C} x^{n - w(c)} y^{w(c)} = \sum_{i=1}^{n} A_i x^{n-i} y^i$$

Où A_i designe le nombre des mots de poids i dans C.

La suite $A_0, A_1, \ldots A_n$ est appelée distribution des poids du code C.

Si nous remplaçans 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.

Exemple 1:

Soit $C = \{000, 011, 101, 110\}$ de longueur 3sur $\mathbb{F}_2$.

Le dual $C^{\perp}$ de C est $C^{\perp} = \{000, 111\}$ et les polynômes énumérateur sont respectivement :

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

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

Exemple 2:

Le code $\grave{C} = \{00, 11\}$ de longueur 2 sur $\mathbb{F}_2$, est auto-dual car $\grave{C} = \grave{C}^{\perp}$ et

$W_{\grave{C}}(x, y) = W_{\grave{C}^{\perp}}(x, y) = x^2 + y^2$.

Exemple 3:[16]

Soit G_{24} le code de Golay de matrice génératrice $G = [I_{12}, A]$ défini par:

$$G = \left[\begin{array}{cccccccccccc|cccccccccccc}
1 & & & & & & & & & & & & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 & 1 & & & & & & & & & & & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
 & & 1 & & & & & & & & & & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
 & & & 1 & & & & & & 0 & & & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
 & & & & 1 & & & & & & & & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
 & & & & & 1 & & & & & & & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
 & & & & & & 1 & & & & & & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
 & & & & & & & 1 & & & & & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & 0 & & & & & & & 1 & & & & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
 & & & & & & & & & 1 & & & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
 & & & & & & & & & & 1 & & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
 & & & & & & & & & & & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1
\end{array}\right]$$

On remarque que $G_{24}^{\perp} = G_{24}$ donc G_{24} est auto-dual, en appliquant la formule le plus étulisé

$W_C(y) = \sum_{c=1}^{i=n} A_c y^i$

On a : $W_{G_{24}}(y) = 1 + 759y^8 + 257y^{12} + 759y^{16} + y^{24}$

CHAPITRE III

Détermination de l'équivalence entre deux codes

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 incité à nous intéresser à la détermination de l'équivalence de code.

2. GROUPE DE PERMUTATIONS DES CODES

Soient n un entier positive non nul et q une puissance d'un nombre premier ; soit I un ensmble ordonné de cardinal n utilisé pour indexer les coordonnées des mots de $\mathbb{F}_q^n$ (dans la suite nous prenons $I = \{1, 2, \ldots, n\}$)

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 mots de $\mathbb{F}_q^n$, alors :

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

Notation 1:

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 : $\sigma(C) = C$

$Perm(C) = \{\sigma \in S_n : \sigma(C) = C\}$.

Proposition 2:

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

Preuve:

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

Si $\sigma_1, \sigma_2 \in Perm(C)$, nous avons

$\sigma_1 \cdot \sigma_2 (C) = \sigma_1(\sigma_2(C))$

$= \sigma_1(C) car \sigma_2 \in Perm(C)$.

$= C car \sigma_1 \in Perm(C)$.

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

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

$\sigma_1^{-1}(\sigma_1(C)) = \sigma_1^{-1}(C) \Leftrightarrow \sigma_1^{-1}\sigma_1(C) = \sigma_1^{-1}(C)$.

$\Leftrightarrow id(C) = \sigma_1^{-1}(C)$.

$\Leftrightarrow C = \sigma_1^{-1}(C)$.

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

Définition 3:

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

Exemple 1:

a- Soit C le code $[3,2]$ défini sur $\mathbb{F}_2$ par sa matrice génératrice G avec $G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$

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_1

$G_1 = [101]$

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

Déterminations $\sigma(C_1)$, 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 $Perm(C_1) = \{id, (13)\}$.

Permutation monomiales 4:

Définition:(matrice de permutations) 1:

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.

Exemple 1:

a- La matrice $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ est une matrice de permutation sur $\mathbb{F}_3$

b- La matrice $\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$ 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 produi $c.P$ donne un mots de $\mathbb{F}_q^n$ qui est égal en fait à c avec des coordonnées permutées , c'est la raison pour laqulle les matrices de cette sorte dit matrices de permutation .

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

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

Matrice monomiale 5:

Définition 1:

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.

Exemple 1:

a- La matrice $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ est une matrice monomiale sur $\mathbb{F}_7$

b- Soit σ une permutation telque $\sigma \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

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

la matrice de permutation P

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

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

Groupe D'automorphisme 6 :

Définition 1:

Soient σ une permutation de $\{1, 2, \ldots, n\}$ et

$\pi_i : \mathbb{F}_q \rightarrow \mathbb{F}_q$

$s \mapsto \pi_i(s) = \alpha_i \cdot s$ où $\alpha_i \in \mathbb{F}_q^*, \forall i = 1, 2 \ldots, n$

Alort l'application:

$\Gamma : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$

$(c_1, c_2, \ldots, c_n) \mapsto \Gamma(c_1, c_2, \ldots, c_n) = \pi_1(c_{\sigma_{(1)}})\pi_2(c_{\sigma_{(2)}}) \ldots \pi_n(c_{\sigma_{(n)}})$

est appelée une permutation monômiale 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 de codes équivalents à un code donné .

Définition 2:

Soit C un code de longeur n sur $\mathbb{F}_q$, le groupe d'automorphismes de C noté $Aut(C)$, est

l'ensemble de toutes les permutations monômiales Γ de degré n telque : $\forall c \in C, \Gamma(c) \in C$

Exemple 3:

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

$Aut(C) = \{(id), (2134), (1234), (2143), (4321), (3412), (1324), (1432)\}$.

3. EQUIVALENCE DES CODES LINEAIRES

La définition de l'équivalence des codes linéaires est basé à l'aide des permutations de symboles qui sont donnée par multiplication par a non zéro scalaire, donc deux codes linéaires sont équivalents si l'un peut obtenir de l'autre par l'opération de combinaison de types suivant :

a- les positions de la permutation de code .

b- les symboles de multiplication apparente dans une position fixée par un non-zéro scalaire.

Théorème [16] **1:**

Deux matrices génératrices de types $k \times n$ de deux codes linéaires sont équivalents si l'une des matrices peut être obtenue a partir de l'autre par l'une des opérations suivantes:

(R_1) permutations des lignes .

(R_2) multiplication des lignes par un non-zéro scalaire .

(R_3) l'addition de scalaire multiple d'une ligne à autre .

(C_1) permutation des colonnes .

(C_2) multiplication de n'importe quelle collonne par un non zéro scalaire .

Preuve :

$(R_1), (R_2), (R_3)$ préserve la linéaire indépendants des ligne de la matrice génératrice est out simplement on remplace une base par un autre du même code.

Les opérations de type $(C_1), (C_2)$ transforment la matrice génératrice à l'un des codes équivalents .

Proposition [10] **2:**

Si G est une matrice génératrice de C, code lineaire (n, k), alors :

1. Les matrices génératrices de C sont de la forme $A \times G$, où A est une matrice carrée inversible $k \times k$ sur $\mathbb{F}_q$.
2. Le code C est l'ensemble des mots de la forme $c = \left\{(u_1, u_2, \ldots, u_k) \cdot G, \quad (u_1, u_2, \ldots, u_k) \in \mathbb{F}_q^k\right\}$.
3. Si $c_1, c_2, \ldots, c_n$ sont les vecteurs colonnes de G, les mots du code C sont tous aux de la forme $C = \{\langle c_1, u\rangle, \langle c_2, u\rangle, \ldots, \langle c_n, u\rangle\}$ avec $u \in \mathbb{F}_q^k$ et $\langle ., . \rangle$ designant le produit scalaire usuel de $\mathbb{F}_q^n$.

Lemme [15] **3:**

Soit C un $[n, k, d]_q$-code et $G = (a_{ij})$, $1 \leqslant i \leqslant k$,$1 \leqslant j \leqslant n$ une matrice génératrice de C. Le code est systématique si et seulement si le déterminant de la matrice $G_k = (a_{ij})$ $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant k$ est non nul .

Preuve :

si le déterminant de la matrice G_k est non nul , la méthode de pivot de GAUSS sur les ligne donnera une matrice génératrice de C sous forme standard , réciproquement, si C est systématique C a une matrice génératrice sous forme standard $\left(I_k / B\right)$ quivérifie la propiété demendée .

Proposition [15] **4:**

Tout code linéaire est équivalent à un code systématique.

Preuve:

Supposons que C ne soit pas un code systématique.

Soit G une matrice génératrice du code C.

Comme Le rang de G est égal a k, il existe un mineur $k \times k$ non nul. Par une permutation des colonnes de G on amène ce mineur aux k premières colonnes.

On obtient une matrice génératrice d'un code équivalent et qui lui est systématique.

Exemple 1:

a- Soit C_1 le code de matrice génératice G_1 : on applique l'algorithme de GAUSS à G_1.

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[l_3 \to l_3 - l_1]{l_2 \to l_2 - l_1} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow[l_4 \to l_4 - l_2]{l_1 \to l_1 - l_2} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$\xrightarrow{l_2 \to l_2 - l_3} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$\xrightarrow{l_3 \to l_3 - l_4} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Donc G_2 est une matrice génératrice de code C_2 équivalent à C_1. le code C_2 est systématique

.

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

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

une permutation de colonne $N°4$ par la colonne $N°1$ on obtient G_2.

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 0 & 2 & 1 & 1 & 1 \end{bmatrix}$$ En permutant la colonne $N°4$ par la colonne $N°3$ on obtient G_3.

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 2 & 1 & 1 \end{bmatrix}$$ donc G_3 est une matrice génératrice du code C.

C équivalent à C_1.

c- Soit C un code linéaire de longueur 6 et de matrice génératrice G.

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

le premier mineur $4 \times 4 \begin{vmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{vmatrix}$ est nul car la somme des deux premieres colonnes est égale à la troisieme par contre

$\begin{vmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{vmatrix} \neq 0$, on déduit que $rang(G) = 4$, donc G est la matrice de $\left[6, 4, d\right]_2$ code linéaire C mais à cause de la remarque du debut C n'est pat systématique, on permute les colonnes (pour amener le mineur non nul aux 4 premieres colonnes) par :

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{bmatrix}$$

D'où la matrice :

$$G' = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Puis , on fait le pivot de GAUSS sur les lignes de G' et on obtient :

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$, qui est la matrice génératrice d'un code systématique équivalence à C.

d- soit C le code linéaire de l'exemple (a) de matrice génératrice sous forme standard $G = \left[I_4 \ / A\right]$ telle que :

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

soit C' le code linéaire de matrice génératrice G' telle que:

$$G' = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \xrightarrow[l_2 \to l_2 - l_3]{l_1 \to l_1 - l_4} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\xrightarrow[l_3 \to l_1 - l_3]{l_2 \to l_2 - l_4} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\xrightarrow[l_4 \to l_2 - l_4]{l_1 \to l_1 - l_3} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\xrightarrow{l_3 \to l_3 + l_4} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

donc $G' = \left[I_4 \ / A' \right]$ telle que :

$$A' = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

On utilise le théorème 3.3.1 , suivant (R_1) sur les lignes de A on choisit une permutation

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix} \text{ donc } A \to A_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

On choisit une deuxième permutation σ_2

$$\sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{bmatrix} \text{ donc } A_1 \to A' = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

donc les deux codes C et C' sont équivalents .

Proposition 5:

Soit C_1, C_2 deux codes linéaires de matrice génératrice G_1 et G_2, on dit que les codes C_1, C_2 sont équivalents

s'il exise une permutation σ tel que :

$C_2 = \sigma(C_1)$,cela est équivalent à dire qu'il existe une matrice de permutation $M\sigma$ et une matrice $K \times K.P$ acoefficients dans $\mathbb{F}_q$ et inversible telles que :

$G_2 = P.G_1.M\sigma$

Exemple 1:

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \quad G_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

soit : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix}$

$$M\sigma = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}, \quad P = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

On a $G_2 = P.G_1.M\sigma$ donc C_1, C_2 sont équivalents

Définition 1:

Deux codes sur $\mathbb{F}_q$ de longueur n, sont dit équivalent, si on peut obtenir l'un de l'autre par les opérations suivantes.

1. permutation des positions du code.
2. permutation des symboles figurant en position fixés.

Exemple 1:

Soit les codes C et C' de parametres $[9,4,3]_3$ telleque :

$C = \{0000, 0111, 0222, 1021, 1102, 1210, 2012, 2120, 2201\}$

$C' = \{0012, 0101, 0220, 1021, 1110, 1202, 2000, 2122, 2211\}$

Les codes C et C' sont équivalents.

Pour obtenir C' de C.

Premierement on utilisent la permutation σ définie par $\sigma\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

deuxiement en échange de coordonnées valeurs 0 et 1 dans tous les coordonner a charge sauf la derniere.

Lemme [16] **6:**

Tout code C sur $\mathbb{F}_q$; $C = C(n,k;d)$ est équivalent à un code $C' = C'(n,k,d)$ sur $\mathbb{F}_q$ qui contient le mot de composante nul $(00\ldots0)$.

Preuve:

En choisit n'importe quel mot de code $c \in C, (c = x_1x_2\ldots x_n)$ pour tout $x_i \neq 0$, en applique la permutation $\begin{pmatrix} 0 & x_i & j \\ \downarrow & \downarrow & \downarrow \\ x_i & 0 & j \end{pmatrix}, \forall j \neq 0, x_i$ à la position du symbole i.

Exemple 1:

Soit le code C défini sur $\mathbb{F}_2$ par $C = \{00100, 00011, 11111, 11000\}$ est équivalent à $C' = \{00000, 01101, 10110, 11011\}$ par les opération suivante.

1. L'utilisation du permutation $\begin{pmatrix} 0 & 1 \\ \downarrow & \downarrow \\ 1 & 0 \end{pmatrix}$ sur les symboles de la $3^{éme}$ position.
2. Un changement entre la $2^{éme}$ et la $4^{éme}$ position.

Theorème [16] **7:**

Tout code C sur $\mathbb{F}_q$, $C = C(n,k,n)$ est équivalent à un code de répétition.

Preuve:

Soit $C = C(n,k,n)$ sur $\mathbb{F}_q = \{1,2,\ldots,q\}$ et G une matrice génératrice de C, ou les lignes de G sont les mots de code C.

Comme on a $d(C) = n$, donc les q éléments d'une colonne de G doit être distinct et aussi précisement les symboles $1,2,\ldots,q$ dans un ordre quel conque.

Pour tout colonne de G, appropriée une permutation des symboles pour donner G sous la forme $G = \begin{bmatrix} 11 & \ldots & 1 \\ 22 & \ldots & 2 \\ \vdots & \vdots & \vdots \\ qq & \ldots & q \end{bmatrix}$.

Exemple 1:

Soit C un code linéaire de longueur 3 défini sur $\mathbb{F}_3$ par $C = \{012, 120, 201\}$.

On ramarque que $C = (3,3,3)$ car on a:

$d(012,120) = d(012,201) = d(120,201) = 3$ donc $d(C) = 3$.

Le code C est équivalent à un code de répétition $C' = \{000, 111, 222\}$ par les opérations suivantes:

1. L'utilisation de la permutation $\begin{pmatrix} 0 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ 2 & 0 & 1 \end{pmatrix}$ sur les symboles de la $2^{éme}$ position du code C.
2. L'utilisation de la permutation $\begin{pmatrix} 0 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 0 \end{pmatrix}$ sur les symboles de la $3^{éme}$ position du code C.

Theoreme 8:

Le nombre des codes binaires inéquivalents de longueur n contenant seulement deux mots est égal à n.

Preuve:

Un tel code C est équivalents à $\{00\ldots0, 11\ldots100\ldots0\}$ où le nombre de 1s dans le deuxieme mot est l'un des $1,2,\ldots,n$.

Equivalence par permutation 9:

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

Pour tout $x \in \mathbb{F}_q^n$ notons $x = (x_1, x_2, \ldots, x_n)$ou simplement :

$$x = x_1 x_2 \ldots . x_n.$$

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

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

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

une permutation $\sigma \in S_n$ sera notée

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

Soit ζ_n l'ensemble des codes le longueur n sur $\mathbb{F}_q$ donc ζ_n est une partie de $P(\mathbb{F}_q^n)$ l'ensemble de toutes les parrties de $\mathbb{F}_q^n$.

Soient $\sigma \in S_n$ et C un code de ζ_n, difinissons l'application φ de $S_n \times \zeta_n$ dans ζ_n par: $\varphi(\sigma, C) = \sigma(C)$ avec:

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

Proposition 10:

L'application φ définie une opération de S_n sur ζ_n (c'est-à-dire S_n opére sur ζ_n).

Preuve:

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

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

puisque

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

Donc

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

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 opére sur ζ_n par: $(\sigma, C) \to \sigma C$

L'opération φ permet de définir une relation d'équivalence sur ζ_n.

En effet; soit $\sim$ la relation sur ζ_n définie par:

pour deux codes C et C' de ζ_n;

$$C \backsim C' \Leftrightarrow \exists \sigma \in S_n, C' = \sigma(C)$$

Proposition 11:

La relation $\backsim$ définie sur ζ_n, est une relation d'équivalence

1. $\sim$ est réflexive car : pour tout code C de ζ_n;

$$C = id(C)$$

Ce qui entraîne que : $C \sim C$.

2. $\sim$ est symétrique: soient C et C' de ζ_n tels que $C \sim C'$.

nous anons:

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

Or

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

donc

$$C' = \sigma(C) \Leftrightarrow \overset{-1}{\sigma}(C') = \overset{-1}{\sigma}(\sigma(C)) \Leftrightarrow \overset{-1}{\sigma}(C') = \left(\overset{-1}{\sigma}\sigma\right)(C)$$

$$\Leftrightarrow \overset{-1}{\sigma}(C') = id(C) \Leftrightarrow \overset{-1}{\sigma}(C') = C \Leftrightarrow C' \sim C$$

3. $\sim$ est transitive : soient C, C' et C'' de ζ_n tels que: $C \sim C'$ et $C' \sim C''$

$C \sim C'$ et $C' \sim C'' \Leftrightarrow \exists \sigma \in S_n, \exists \tau \in S_n : C' = \sigma(C)$ 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: $C \sim C''$ $\diamond$

Définition 1:

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

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

Exemple 1:

1. le code C défini dans l'exemple 3.2.3 .(a) est équivalent par s_3 a lui-même.
   De l'éxemple 3.2.3 (b).:
2. le code C_1 lui-même déduit par les permutation id et (13)
3. le code C_2 déduit de C_1 par (12)et (123).
4. le code C_3 déduit de C_1 par (23)et (132).

Proposition 12:

le nombre de codes équivalents par permutation à un code C de longueur n est $\frac{n!}{|perm(C)|}$

Preuve :

Soit $\overline{C}$ l'orbitede de C selon l'action de S_n sur ζ_n. .

Soit $(S_n/perm(C))_g$ l'ensemble des classes à gauche de S_n modulu $perm(C)$ définition l'application $g : \overline{C} \to \left(S_n / perm(C)\right)_g$ définie comme suit :

Pour tout $C_1 = \pi(C)$ de $\overline{C}$, $g(C_1) = \pi \cdot perm(C)$

Montrons que g est une bigection :

Soit C_1, C_2 deux codes de $\overline{C}$ tels que $C_1 = C_2$, alors il existe deux permutations. $\pi_1, \pi_2 \in S_n$ tellesque:

$C_1 = \pi_1(C), C_2 = \pi_2(C)$

$C_1 = C_2 \Leftrightarrow \pi_1(C) = \pi_2(C)$

$\Leftrightarrow \pi_2^{-1}\pi_1(C) = C$

$\Leftrightarrow \pi_2^{-1}\pi_1 \in perm(C).$

$\Leftrightarrow \pi_1\, perm(C) = \pi_2 perm(C).$

Ce qui prouve que g es une application injective il reste à montré qu'il est surjectif .

Soit $\sigma perm(C) \in \left(S_n / perm(C)\right)_g$ alors $\sigma(C)$ est un code équivalent par permutation à C et $g(\sigma(C) = \sigma perm(C))$

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

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

$|\overline{C}| = \left|\left(S_n / perm(C)\right)_g\right| = [S_n : perm(C)]$

$\frac{|S_n|}{|perm(C)|} = \frac{n!}{|perm(C)|}$ = (théorème de lagrange)

Exemple 1:

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 $\frac{n!}{|perm(C)|}$, donc: C posséde 3 codes équivalents .

Méthode pour déterminer les codes équivalents a C et les permutations 13

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

•soit $\sigma = (123)$, alors le premier code équivalent à C est:

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

• On calcule l'ensemble $E_1 = \{\sigma 0\ perm(C)\}$.

$E_1 = \{(123), (132)\} \circ \{(12)\} = \{(123), (132)\}.$

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

• soit $\sigma = (13)$, alors le deuxiéme code équivalent à C est :

$$\sigma(C) = (13)(C) = \{000, 010, 111, 100\} = C_2.$$

• On calcule l'ensemble $E_2 = \{\sigma 0\ perm(C)\}$.

$$E_2 = \{(13), (123)\} \circ \{(12)\} = \{(13), (132)\}.$$

Donc les trois codes équivalents à C sont C, C_1, 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 $E_1 = \{(132), (23)\}$.

On a $(132)(C) = C_1$.

$(23)(C) = C_1$

l'ensemble $E_2 = \{(13), (123)\}$

On a $(13)(C) = C_2$

$(123)(C) = C_2$

$$perm(C) = \{id, 12\} \left| \begin{array}{l} (id)(C) = C \\ (12)(C) = C \end{array} \right.$$

4.INVARIANTS:

la notion d'invariant que nous utiliserons sera liée à celle d'équivalence , il s'agit de toutes propriétés d'un code qui ne changera pas lorsque l'on appliquera une permutation .

Définition 1:

Un invariant sur E est une application $\upsilon : \zeta \rightarrow E$. ζ : l'ensemble de tous les codes sur $\mathbb{F}_q$.

Telle que deux codes équivalents prennent la même valeur par υ, c'est a à dire

$$\forall C \in \zeta_n, \forall \sigma \in S_n : \upsilon(\sigma(C)) = \upsilon(C)$$

Exemple 1:

soit C est $\grave{C}$ deux codes équivalents ,telle que :

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

comme invariant ,nous prenons le polynôme énumérateurdes poids.

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

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

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 donc la distance minimale est égale à 1

$d(1011, 1101) = 2$

Hull d'un code lineaire 2:

Définition 1:

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

Proposition 2:

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

Alors :

1. $H(\sigma(C)) = \sigma(H(C))$

2. Si v est invariant, l'application $C \rightarrow v(H(C))$ est aussi un invariant.

Preuve:

pour 1) il suffit de remarquer que:

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

Pour 2) il suffit d'appliquet 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 ou 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 le polynôme énumérateur, la longueur ... etc. Pour ces raisons nous allons définir une propriété locale d'un code est une de ses positions.

Exemple 1:

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 $H(C) = C \cap C^{\perp} = \{000\}$.

5. SIGNATURES:

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 tout permutation σ de S_n et pour tout i de I_n

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

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.

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'aplication définie par :

$S(C, i) = v(C_i)$,ou (C_i) le code poinçonné en i.

6. Un Algorithme Pour Trouver la permutation entre deux codes équivalents

Soient C et C' deux codes de même longueur. Nous voulons savoir s'il sont équivalents et, dans l'affirmative, calculer une permutation σ telle que $C' = \sigma(C)$.

Dans le cas où C et C' sont équivalents, et que de plus nous connaissons une signature totalement discriminante pour C, l'utilisation de l'Algorithme permet d'obtenir la permutation.

Algorithme [13]**:**

Soient C et C' deux codes équivalents de longueur n et soit S une signature totalement discriminante pour C

Procédure : code C, C' : signature S

pour i dans I_n, pour j dans I_n

si :

$S(C, i) = S(C', j)$

$\sigma(i) \leftarrow j$

retourner (σ).

Exemple 1:

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 :

$v(C) = W_C(x) = \sum_{c \in C} x^{w(c)} = W(C_i)$ et comme signature nous prenons la signature suivant:

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

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

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

Voyons que la signature S et totalement discriminante pour C.

pour le code C' nous avons:

$C'_1 = \{0011, 0101\} \rightarrow W(C'_1) = 2x^2$
$C'_2 = \{0011, 1011, 1001\} \rightarrow W(C'_2) = 2x^2 + x^3$
$C'_3 = \{0001, 1001, 1101\} \rightarrow W(C'_3) = x + x^2 + x^3$
$C'_4 = \{0010, 1010, 1100\} \rightarrow W(C'_4) = x + 2x^2$

Nous voyons que la signature S et toralement discriminante pour C' 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 obtenons donc immédiatement la permutation σ telque $C' = \sigma(C)$.

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

C'est à dire que la permutation σ est déterminée est définie par:

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

CONCLUSION

Nous avons présenté dans ce travial une étude sur l'équivalence entre deux codes correcteurs d'erreurs de même longueur.

Elle est basée sur les notions de groupe de permutation, matrices,invariant et de signature.

Notre travail consiste à étudier l'équivalence entre deux codes correcteurs d'erreurs d'une part, et d'autre part de détèrminer la permutation qui définit l'équivalence.

Dans ce travail, on a présenté une étude capable de déterminer cette permutation dans des cas particuliers. Plus précisement ;

- En utilisant les matrices génératrices des deux codes sous formes standard.
- En utilisant les permutations sur les positions.
- En utilisant la notion de signature définie par Nicolas SENDRIER(INRIA, France), sous l'hypothèse que cette signature est totalement discriminante.

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

BIBLIOGRAPHIE

[1] A.POUGAM,M-Coste,R,Quarez "*Code Correcteurs*" Juin 2002.
[2] CARMEN-SIMONA NEDELOIA "*Etude des enumerateurs des poids des codes linéaires utilisant des formes de composées des matrices génératrices*".
These de doctorat -2005- (Université de limoges), P 3-10.
[3] CHRISTINE BACHOC "*Cours des codes (UE code,signal)*"
Université Bordeaux, Master CSI2-2004-2005, P9
[4] DANY-JACK MARCIER "*Utilisation de l'algèbre dans les systemes d'information*"
IUFM des Antilles et de Guyane, 15 Mais 2001, P1-11.
[5] FJ.MACWILIAMS and NJA Sloane. "*The théory of error-correcting codes*". North

Holland 1977.
[6] GINTARAS SKERSYS "*Calcule de groupe d'automorphismes des codes. Détermination de l'équivalance des code*"
These doctorat -1999- (Université de Limoges), P19-30.
[7] HARLODN-WARD.JAYA.WOOD "*Characters and the équivalence of codes*"
Journal of combinatorial theory, Séries A73,348-352 (1996) Article N°0027,
P348-349.
[8] JORGE CASTNEIRA MARIERA, PATRIK GUY FARREL "*Essentials of error -Control coding*"
JOHN WILEY & SONS, LTD 2006, P45-48.
[9] LADJELAT.LAHCENE "*Etude de l'quivalance de deux codes sur un corps finis*".
Mémoire présente pour l'obtention du diplôme de MAGISTER -2004- Université de M'SILA.
[10] M.DEMAZURE "*Cours d'algèbre*". Cassiné 1997.
[11] MOHAMED ZITOUNI "*Algèbre*".
Reimpression 1993 OFFICE des publications Universitaires, P165-175.
[12] NICOLAS SENDRIER "*Crypto systeme à clé public basé sur les codes correcteurs d'erreurs*".
INRIA- Rocquencourt. Mémoire d'Habilitation adiriger des recherches, Mars 2002, P10-13.
[13] NICOLAS SENDRIER "*Un Algorithme pour trouver la premutation entre deux codes binaires équivalants*".
INRIA- Rocquencourt. Rapport de recherche N°2853, Avril 1996, P5-6.
[14] O.PAPINI ET J.WOLLFMAN "*Algèbre discréte et codes correcteurs*"
P107-108.
[15] P.V,KOSELEFF " *Codes correcteurs d'erreurs*".
MIAC24-M_3-Résumé du cour -V-2004, P45-48.
[16] RAYMOND HILL "*Afirst course in coding theory*".
Clarendon PRESS. OXFORD 1996, P50-54.
[17] V,PLESS "*Introduction to the theory of error correcting codes*".
3rd, ed, WILEY, NEWYORK 1998, P36-38.
[18] V, PLESS, W.C.HUFFMAN ET R. A- BRUALDI "*An Introduction to algebra codes*".
HUND BOOK OF CODING THEORY, ed,V.S. Pless and W.C HUFFMAN NORTH HOLLAND.
[19] W.CARY HUFFMAN, VERA PLESS " *Fundamentals of error- Correcting codes*"
Conbridge University .Press 2003. P3-17.