REPUBLIQUE ALGERIENNE DEMOQRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche scientifique

Université Laarbi Ben M'hidi OUM EL BOUAGHI

Faculté des Sciences Exactes

et

des Sciences de la Nature et de la Vie

Département de Mathématiques et informatique

$N°$ d'ordre :

$N°$ de série :

Mémoire

En vue de l'obtention du diplome de :

MAGISTER

Option : ELEMENT D'ARITHMETIQUE

Présenté par :

SAHRAOUI ALA EDDINE

SUR LES CODES SIMPLEXES

Soutenu le : 19/11/2013

Devant le jury composé de :

Mr.Abdelhamid Ayadi	*Président*	*Professeur*	*Université d'Oum El Bouaghi*
Mr.Lemnouar Noui	*Rapporteur*	*Professeur*	*Université de Batna*
Mr.Said Guedjiba	*Examinateur*	*Professeur*	*Université de Batna*
Mr.Abdelkrim Aliouche	*Examinateur*	*M.C.A*	*Université d'Oum El Bouaghi*
Mr.Toufik Zaimi	*Invité*	*M.C.A*	*Université d'Oum El Bouaghi*

Dédicace et remerciement

A la mémoire de mon père, pour toute la tendresse, pour tous les sacrifices, pour tout l'enseignement qu'il m'a transmis depuis le B A BAS.

En témoignage de mon éternelle reconnaissance RAHIMAHOU ALLAH.

A ma mère qui croit toujours en moi, que ce travail soit une marque de mon amour éternel et de toute ma reconnaissance.

A mes frères et ma soeur.

A ma famille et mes amis pour tous les encouragements.

A mon directeur de thèse :

Que Monsieur le professeur NOUI LEMNOUAR ,reçoive toute l'expression de ma reconnaissance de m'avoir proposé ce sujet de thèse, de sa disponibilité malgré ses lourdes taches professionnelles,de ses compétences scientifique qui m'ont permis de mener à terme ce travail.

A monsieur le président du jury le professeur Abdelhamid Ayadi.

A messieurs les membres du jury le professeur Said Guedjiba, le docteur Abd elkrim Aliouche.

Qui ont accepté d'évaluer mon travail, veillez trouver ici le témoignage de ma gratitude et de mon profond respect.

A monsieur Zaimi Toufik qui m' a encouragé et qui m' a apporté son soutien depuis la première mouture je dois le remercier de la disponibilité dont il a fait preuve au moment ou lui même était très occupé.

A mon professeur Zekraoui Hanifa qui m' a encouragé .

Je tiens à remercier particulièrement le professeur "Jennifer .D.Key " de l'université " Western Cape" du sud Afrique de m'avoir mis à ma disposition des documents et des logicielle afin de pouvoir démarrer ce travail, et de m'avoir procurer toutes les réponses à mes questions à propos de son article,dont j'en avais besoin,pour pouvoir terminer mon travail.
Ainsi que le professeur "Arrigo Bonisoli " de l'université "Università degli Studi di Modena e Reggio Emilia " d'Italie qui a contribuer à l'élaboration de ce travail.

Table des matières

Notation

q : un nombre premier.

$\mathbb{F}_q$: le corps $\frac{\mathbb{Z}}{q\mathbb{Z}}$.

$\langle ., . \rangle$: le produit scalaire.

$C[n, k, d]$: un code de longueur n , de dimension k et de distance minimale d .

$C^{\perp}$: le code orthogonale de C .

$\mathcal{S}_n(\mathbb{F}_2)$: Code simplexe binaire.

$\mathcal{H}_n(\mathbb{F}_2)$: Code de $Hamming$ binaire.

G : matrice génératrice .

H : matrice de contrôle.

$wt(x)$: le poids du vecteur x.

$d(., .)$: distance de $Hamming$.

$d(C)$: distance minimale du code C.

e : nombre d'erreur.

R : le taux de transmission.

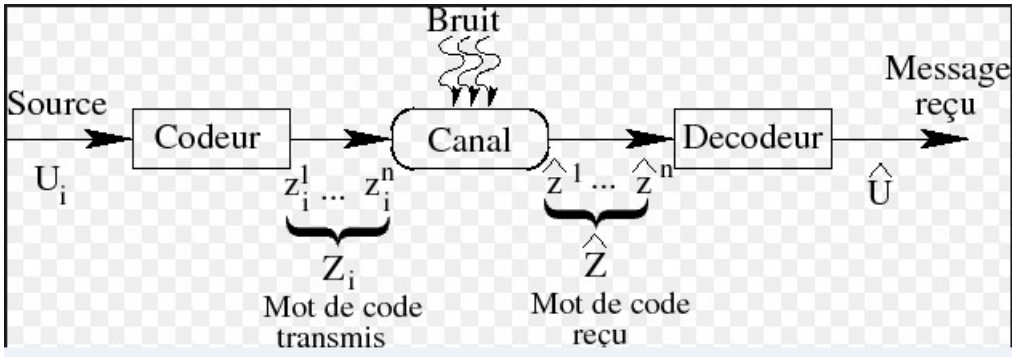
Introduction

la théorie des codes s'est développée pour répondre au problème de la correction des erreurs introduites dans un système de transmission de l'information, fondée en 1948 par *Claude Shannon*.

Dans les années 1940 *Richard Hamming* a reconnu que l'évolution futur d'ordinateur requis une plus grande fiabilité. En particulier la capacité à détecter et à corriger les erreurs, il a crée les codes de *Hamming*, les codes Parfaits et les codes correcteurs d'une seul erreur.

L'échange de l'information effective d'un émetteur vers un récepteur à travers un canal bruité lors de la transmission de l'information des perturbations et parasites extérieurs peuvent modifier le contenu de l'information.

Le problème est comment retrouver le message d'origine ?



La théorie des codes est une science qui consiste à élaborer des stratégies mathématiques pour détecter et corriger des erreurs.

L'objectif de ce travail est l'étude des codes simplexes.

Chapitre 1

Notions fondamentales d'algèbre

Dans ce chapitre on rappelle les notions fondamentales d'algèbres, notions utiles pour l'étude des codes linéaires.

1.1 Groupes

Définition 1.1.1 *Soit G un ensemble non vide, et $*$ une application :*

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a,b) & \longmapsto & a*b, \end{array}$$

Alors, on dit que $(G,*)$ est un groupe si :

1) $*$ est associative, *i.e* .$\forall a,b,c \in G, a*(b*c) = (a*b)*c$;

2) G possède un élément neutre e pour $*$, $\exists e \in G, \forall a \in G, a*e = e*a = a$;

3) Tout $a \in G$ admet un symétrique, *i.e* . $\forall a \in G, \exists b \in G, a*b = b*a = e$.

Exemple

Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis de l'addition usuelle sont des groupes. De même les ensembles $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ munis de la multiplication usuelle.

Si de plus la loi $*$ est commutative , *i.e*.$\forall a,b \in G, a*b = b*a$, alors on dit que G est un groupe commutatif ou abélien.

Les exemples ci-dessus sont des groupes abéliens. Dans ce qui suit on note multiplicativement la loi du groupe et dans ce cas le symétrique d'un élément a (qui est unique) est noté a^{-1}.

1.1.1 Propriétés immédiates

1) L'élément neutre d'un groupe est unique ;

2) Le symétrique d'un élément est unique ;

3) $\forall a; b \in G, (ab)^{-1} = b^{-1}a^{-1}$, si la loi est multiplicative (.).

1.1.2 Sous-groupes

Définition 1.1.2 *Soit $H \subset G$ un sous-ensemble non vide, on dit que H est un sous groupe de G si :*

1)$\forall a; b \in H \Longrightarrow ab \in H$;

2)$\forall a \in H \Longrightarrow a^{-1} \in H$,

Les deux conditions ci-dessus sont équivalentes à l'unique condition :
$\forall a, b \in H \Longrightarrow ab^{-1} \in H$.
Un groupe ayant un nombre fini n d'éléments est dit groupe fini d'ordre n. Sinon il est dit d'ordre infini. Par exemple $\mathbb{Z}$ est d'ordre infini.

Théorème 1.1.1 *Théorème de Lagrange* [1]
L'ordre $|H|$ d'un sous-groupe H d'un groupe fini G divise l'ordre $|G|$ de G, l'indice $[G : H]$ divise aussi $|G|$ et :

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

Définition 1.1.3 *Un sous-groupe H de G est distingué (on note $H \lhd G$) si pour tout $g \in G$, $Hg = gH$, ((on dit aussi : invariant ou normal))*

Remarque 1.1.1 *Evidement, dans un groupe commutatif , tout sous-groupe est distingué.*

1.1.3 Sous-groupe engendré par une partie

Définition 1.1.4 *Soit X un sous-ensemble d'un groupe G , l'intersection de tous les sous-groupes de G contenant X est un sous-groupe appelé sous-groupes engendré par X , on le notera $\langle X \rangle$*

Il est clair que $\langle X \rangle$ est le plus petit sous-groupe de G contenant X.

Définition 1.1.5 *Un groupe G est monogène si G admet un unique générateur $a \in G$ $.i.e, G = \langle a \rangle$ et cyclique si de plus G est fini .*

Définition 1.1.6 *Soit G un groupe fini et soit $g \in G$, l'ordre de g est l'ordre du sous groupe engendré par g .*

1.1.4 Homomorphismes, Isomorphismes de groupes

Définition 1.1.7 *Une application $f : G \longrightarrow G'$ d'un groupe $(G, .)$ dans un groupe $(G', .)$ est un homomorphisme de groupe si :*

$$\forall x, y \in G, f(xy) = f(x)f(y)$$

Définition 1.1.8 *Un homomorphisme de groupes $f : G \longrightarrow G'$ est dit isomorphisme de groupes si f est bijectif.*

Dans ce cas on dit que G et G' sont isomorphes.
Un isomorphisme de G dans lui même est appelé automorphisme .

1.2 Anneaux

Définition 1.2.1 *On appelle anneau la donnée d'un triplet $(A, +, .)$ où A est un ensemble, $+$ et $.$ sont deux lois de composition interne sur A vérifiant :*
1)$(A, +)$ *est un groupe abélien ,*
2) $(.)$ *est une loi associative,*
3) $\forall a, b, c \in A; a.(b + c) = a.b + a.c$ *et* $(b + c).a = b.a + c.a$
On dit que $(.)$ *est distributive par rapport à* $(+)$.

Si la loi (.) est commutative , on dit que l'anneau est commutatif .
Si la loi (.) possède un neutre bilatère , on dit que l'anneau est unitaire .

Définition 1.2.2 *Soit A un anneau, on appelle sous-anneau de A toute partie non vide $B \subset A$ vérifiante les conditions suivantes :*
1)B *est un sous-groupe du groupe additif A.*
2)B *est stable pour multiplication .*

1.2.1 Anneaux intègres

Définition 1.2.3 *Un élément a d'un anneau A est un diviseur de zéro s'il est non nul et s'il existe $b \in A$ non nul tel que : $a.b = 0$*

Définition 1.2.4 *Un anneaux A est intègre ssi $A \neq \{0\}$ et si A n'a pas de diviseur de zéro , autrement dit si on a :*

$$a.b = 0 \Longrightarrow (a = 0) \quad ou \quad (b = 0).$$

1.2.2 Homomorphismes d'anneaux

Définition 1.2.5 *Une application f d'un anneau A dans un anneau B est un homomorphisme d'anneau ssi :*
$1) f(1_A) = 1_B$,
$2) \forall (x, y) \in A \times A : f(x + y) = f(x) + f(y)$,
$3) \forall (x, y) \in A \times A : f(x.y) = f(x).f(y)$.

Si de plus f est bijective, on dit que f est un isomorphisme d'anneaux.

1.3 Corps

Définition 1.3.1 *On dit qu'un ensemble $\mathbb{K}$ muni de deux lois de composition internes $(+)$ et $(.)$ est un corps si :*
$1)(\mathbb{K}, +, .)$ *est un anneau ;*$1_{\mathbb{K}} \neq 0$,
$2) \forall x \in \mathbb{K}^*, \exists x' \in \mathbb{K}, xx' = x'x = 1_{\mathbb{K}}$.

Si de plus la multiplication est commutative, on dit que $\mathbb{K}$ est un corps commutatif.

Exemples

1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps commutatif pour les lois usuelles,
$2)\mathbb{Z}/p\mathbb{Z}$ est un corps ssi p est premier,
3) Tout corps fini est commutatif.

Définition 1.3.2 *Soit $\mathbb{K}$ un corps et $\mathbb{F}$ une partie de $\mathbb{K}$ .On dit que $\mathbb{F}$ est un sous corps de $\mathbb{K}$ si :*

1)$\mathbb{F}$ *est un sous-anneaux de* $\mathbb{K}$ *;*

2)$\forall a \in \mathbb{K}^*, a^{-1} \in \mathbb{K}^*$

1.4 Espaces vectoriels

Définition 1.4.1 *On appelle espace vectoriel sur K , tout ensemble E muni de deux lois :*

1) *Une loi interne appelée addition , notée $+$ tel que $(E,+)$ soit un groupe abélien.*

2) *Une loi externe qui à tout couple $(\lambda, x) \in \mathbb{K} \times \mathbb{E}$ fait correspondre un élément de $\mathbb{E}$ noté $\lambda.x$, cette loi vérifiant les quatre propriétés suivantes :*

1)$\forall x \in \mathbb{E}, 1.x = x$,

2)$\forall \lambda \in \mathbb{K}, \forall x, y \in \mathbb{E}; \lambda.(x+y) = \lambda.x + \lambda.y$,

3)$\forall \lambda, \mu \in \mathbb{K}, \forall x \in \mathbb{E}, (\lambda+\mu).x = \lambda.x + \mu.x$,

4)$\forall \lambda, \mu \in \mathbb{K}, \forall x \in \mathbb{E}, (\lambda.\mu).x = \lambda.(\mu.x)$.

Les éléments de $\mathbb{E}$ s'appellent vecteurs , ceux de $\mathbb{K}$ scalaires.

1.4.1 Sous-espaces vectoriels

Définition 1.4.2 *Soit $(E,+,.)$ un espace vectoriel sur $\mathbb{K}$ et $\mathbb{F}$ une partie non vide de $\mathbb{E}$. On dira que $\mathbb{F}$ est un sous-espace vectoriel de $\mathbb{E}$ si :*

F muni des deux lois induites $(+)$ et $(.)$ est un $\mathbb{K}$ espace vectoriel.

Proposition 1.4.1 [2]

soit $(E,+,.)$ un espace vectoriel sur $\mathbb{K}$ et $\mathbb{F}$ une partie non vide est un sous espace de E si , les deux conditions suivantes sont réalisées :

1)$(\mathbb{F},+)$ *est un sous-groupe de* $(\mathbb{E},+)$

2)$\forall \lambda \in \mathbb{K}, \forall x \in \mathbb{F}, \lambda.x \in \mathbb{F}$.

Proposition 1.4.2 [2]

Soit $\mathbb{F}$ *une partie non vide d'un* $\mathbb{K}$ *espace vectoriel* $\mathbb{E}$.

Les propositions suivantes sont équivalentes :

1)$\mathbb{F}$ *est un sous-espace vectoriel de* $\mathbb{E}$.

2)$\forall x, y \in \mathbb{E}, \forall \lambda, \mu \in \mathbb{K}, \lambda x + \mu y \in \mathbb{F}$.

Définition 1.4.3 *On dit qu'un système fini* $(x_1, x_2, ..., x_n)$ *de vecteurs d'un* $\mathbb{K}$ *espace vectoriel* $\mathbb{E}$ *est libre si toute combinaison linéaire de* $x_1, x_2, ..., x_n$ *est triviale :*

Si $\lambda_1, \lambda_2, ..., \lambda_n \in \mathbb{K}$, *tels que :* $\lambda_1 x_1 + \lambda_2 x_2 + ...\lambda_n x_n = 0$, *alors :* $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$;

On dit qu'un système fini $(x_1, x_2, ..., x_n)$ *de vecteurs d'un* $\mathbb{K}$ *espace vectoriel* $\mathbb{E}$ *est lié s'il n'est pas libre . Ce qui revient à dire qu'il existe des scalaire* $\lambda_1, \lambda_2, ..., \lambda_n$ *non tous nuls tels que* $\lambda_1 x_1 + \lambda_2 x_2 + ...\lambda_n x_n = 0$

Définition 1.4.4 *On appelle espace vectoriel de dimension finie tout espace vectoriel engendré par un système fini de vecteurs. Dans le cas contraire on dit que l'espace vectoriel est de dimension infinie.*

Un système $(x_1, x_2, ..., x_n)$ *de vecteurs d'un* $\mathbb{K}$ *espace vectoriel* $\mathbb{E}$ *est dit base de* $\mathbb{E}$ *si* $(x_1, x_2, ..., x_n)$ *est libre et générateur de* $\mathbb{E}$.

Exemples

1) Une base de $\mathbb{K}^n$ est $(1, 0, ..., 0), (0, 1, ..., 0), ..., (0, 0, ..., 1)$ dite une base canonique.

2) Les polynômes $1, x, x^2, ..., x^n$ forment une base de l'espace vectoriel $\mathbb{K}^n[x]$ des polynômes de degré inférieur ou égal à n.

Définition 1.4.5 *Soient* $\mathbb{E}$, $\mathbb{E}'$ *deux espaces vectoriels sur* $\mathbb{K}$ *et* f *une application de* $\mathbb{E}$ *dans* $\mathbb{E}'$. *On dit que* f *est linéaire, si :*

1)$f(v + w) = f(v) + f(w); \forall v, w \in \mathbb{E}$,

2)$f(\lambda v) = \lambda f(v), \forall v \in E, \forall \lambda \in \mathbb{K}$.

Remarque 1.4.1 *Pour toute application linéaire* f, *on a* $f(0) = 0$ *puis-que* f *est un homomorphisme de groupes.*

1.5 Matrices associées aux application linéaires

Soient $\mathbb{E}$ et $\mathbb{E}'$ deux espaces vectoriels sur $\mathbb{K}$, de dimension n et p respectivement et $f : \mathbb{E} \longrightarrow \mathbb{E}'$ une application linéaires. Choisissons $\{(e_1, e_2, ..., e_n)\}$ une base de $\mathbb{E}$ et $\{(e'_1, e'_2, ..., e'_p)\}$ une base de $\mathbb{E}'$, les images par f des vecteurs $e_1, e_2, ..., e_n$ se décomposent sur la base $(e'_1, e'_2, ..., e'_n)$:

$f(e_1) = a_{11}e'_1 + a_{21}e'_2 + ... + a_{p1}e'_p,$

$f(e_2) = a_{12}e'_1 + a_{22}e'_2 + ... + a_{p2}e'_p,$

.....

$f(e_n) = a_{1n}e'_1 + a_{2n}e'_2 + ... + a_{pn}e'_p.$

Définition 1.5.1 *On appelle matrice de f dans les bases $(e_1, e_2, ..., e_n)$, $(e'_1, e'_2, ..., e'_n)$ la matrice notée $M(f)$ dont les colonnes sont les composantes des vecteurs $f(e_1), f(e_2), ..., f(e_n)$ dans la base $(e'_1, e'_2, ..., e'_p)$*

$$M(f) = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{p1} & a_{p2} & ... & a_{pn} \end{pmatrix}$$

Il est claire que la matrice associée à f dépend du choix des bases de $\mathbb{E}$ et $\mathbb{E}'$.

Exemples

1) Soit $\mathbb{E}$ un espace vectoriel de dimension n finie et $id_{\mathbb{E}} : \mathbb{E} \longrightarrow \mathbb{E}$ l'application qui associe x à x ,on considère une base $\{(e_i, i = 1, ..., n)\}$ de $\mathbb{E}$.

On a :

$$M(id_{\mathbb{K}}) = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & 1 \end{pmatrix} = I_n$$

Cette matrice est dite la matrice d'unité de $\mathcal{M}_n(\mathbb{K})$ l'espace des matrices carrées.

Définition 1.5.2 *Une matrice carrée est une matrice dont le nombre de lignes est égal au nombre de colonnes. Ce nombre s'appelle l'ordre de la matrice.*

Notons $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices carrée d'ordre n à coefficients dans $\mathbb{K}$

$\mathcal{M}_n(\mathbb{K})$ est un espace vectoriel sur $\mathbb{K}$; de plus le produit de deux matrices carrée d'ordre n est toujours défini et c'est une matrice carrée d'ordre n.

Définition 1.5.3 *Soit $A \in \mathcal{M}_n(\mathbb{K})$, s'il existe une matrice $B \in \mathcal{M}_n(\mathbb{K})$ telle que : $AB = I_n$; la matrice A est dit inversible.*

Définition 1.5.4 *La transposé d'une matrice A , notée A^T ou ${}^tA$ est la matrice dont les lignes sont les colonnes de A.*

1.6 Extension de corps

Définition 1.6.1 *Soit $\mathbb{K}$ un corps, une extension de $\mathbb{K}$ est couple $(\mathbb{L}, i)$ où $\mathbb{L}$ est un corps et $i : \mathbb{K} \longrightarrow \mathbb{L}$ un morphisme d'anneaux unitaire. Évidement, on omet presque systématiquement le i et on note $(\mathbb{L} : \mathbb{K})$ pour dire que $\mathbb{L}$ est une extension de $\mathbb{K}$.*

Exemple

$\mathbb{C}$ est une extension de $\mathbb{R}$; $\mathbb{R}(t)$ est une extension de $\mathbb{R}$, si $\mathbb{K}$ est un sous corps de $\mathbb{L}$ alors $\mathbb{L}$ est une extension de $\mathbb{K}$ et le morphisme associé est simplement l'inclusion.

1.6.1 Rappels sur $\mathbb{Z}/p\mathbb{Z}$

Soit p un nombre premier. Nous savons que l'anneau $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p est dans ce cas un corps. C'est-à-dire que tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible.
Si on décrit les classes de $\mathbb{Z}/p\mathbb{Z}$ par leur représentant appartenant à l'intervalle d'entiers :

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, ..., p-1\}.$$

Alors on voit que tout élément non nul $a \in \mathbb{Z}/p\mathbb{Z}$ vérifie $a^{p-1} \equiv 1[p]$

1.6.2 Le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$

Les éléments générateurs

Nous avons vu que lorsque p est premier, le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ est égal à $\mathbb{Z}/p\mathbb{Z} - \{0\}$, ce groupe est cyclique, plus précisément .

Théorème 1.6.1 *Soit p un nombre premier. Alors, le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique. c'est-à-dire ce groupe peut être engendré par un élément générateur " dit aussi élément primitif" il existe un élément α tel que :*

$$\mathbb{Z}/p\mathbb{Z}^* = \{1, \alpha, \alpha^2, ..., \alpha^{p-2}\}.$$

1.6.3 Polynôme Irréductible

Soit $\mathbb{F}_2[x]$ l'ensemble des polynômes en x à coefficient dans $\mathbb{F}_2$, un polynôme $g(x)$ de $\mathbb{F}_2[x]$ est dit irréductible sur $\mathbb{F}_p$, s'il ne se décompose pas en un produit de polynômes non triviaux, c'est-à-dire polynômes de degrés strictement positifs de $\mathbb{F}_p[x]$.

Exemples

Le polynôme $p(x) = 1 + x + x^2$ est irréductible sur $\mathbb{F}_2$.
Le polynôme $f(x) = x + x^3$ n' est pas irréductible sur $\mathbb{F}_2$ car $f(x) = x(1 + x^2)$.

1.6.4 Période d'un polynôme

Tout polynôme à une période, est la période d'un polynôme irréductible de degré n est $2^m - 1$.
Tout polynôme irréductible sur $\mathbb{F}_2$ de degré m divise $x^l + 1$ avec $l = 2^m - 1$.

Exemple

$x^3 + x + 1$ divise $x^7 + 1$ on effet , $2^3 - 1 = 7$, $x^7 + 1 = (x^4 + x^2 + x + 1)(x^3 + x + 1)$.

1.6.5 Polynôme primitif

Un polynôme $p(x)$ de degré m est dit primitif si le plus petit entier n pour que $g(x)$ divise $x^n + 1$ est $n = 2^m - 1$.

1.7 Les racines primitives dans les extensions finies des corps finis

Soit $q = p^n$ une puissance d'un nombre premier p. Soit $\mathbb{F}_q$ le corps fini à q éléments, si m est entier $\geqslant 2$, le corps fini $\mathbb{F}_{q^m}$ est une extension de degré m de $\mathbb{F}_q$.

Soit α un élément primitif de $\mathbb{F}_q^m$ et $p(x) \in \mathbb{F}_p[x]$ le polynôme primitif " de degré mn " qui est le polynôme minimal sur $\mathbb{F}_p$ de α.

Posons $\gamma = 1 + q + ... + q^{m-1}$, ainsi : $q^m - 1 = (q-1)\gamma$.

Remarquons que $\mathbb{F}_q^m = \mathbb{F}_p(\alpha)$, on a donc aussi : $\mathbb{F}_q^m = \mathbb{F}_q(\alpha)$, la dimension de l'extension algébrique simple $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$ sur $\mathbb{F}_q$ est m, par suite $(1, \alpha, ..., \alpha^{m-1})$ est une base de $\mathbb{F}_{q^m}$.

1.7.1 Lien entre racines primitives

Posons $\beta = \alpha^\gamma$ alors :

$$\beta^{q-1} = 1$$

, donc $\beta \in \mathbb{F}_q$, alors β est un élément primitif de $\mathbb{F}_q$.

1.7.2 Polynômes q- primitifs

Rappelons que $p(x) \in \mathbb{F}_p[x]$ est le polynome primitif " de degré nm " associé à α.

Notons alors $\prod(x) \in \mathbb{F}_q[x]$ le polynome minimal de α dans l'extension $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$.

Un tel polynome sera appelé q- primitif. La question est de savoir quels sont les liens entre $p(x)$ et $\prod(x)$.

Rappelons que si u est racine dans un corps fini $\mathbb{F}_s$ d'un polynome, $N(x) \in \mathbb{F}_s[x]$, alors u est aussi racine de $N(x)$.

En conséquence les racines de $p(x)$ sont : $\alpha, \alpha^p, \alpha^{p^2}, ..., \alpha^{p^{mn-1}}$, les racines de $\prod(x)$ sont : $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$.

Posons alors :

$$\begin{aligned}
\prod\nolimits_1(x) &= \prod(x) = (x-\alpha)...(x-\alpha^{q^{m-1}}) \\
\prod\nolimits_2(x) &= (x-\alpha^p)...(x-\alpha^{pq^{m-1}}) \\
\prod\nolimits_j(x) &= (x-\alpha^{p^{j-1}})...(x-\alpha^{p^{j-1}q^{m-1}}) \\
\prod\nolimits_n(x) &= (x-\alpha^{p^{n-1}})...(x-\alpha^{p^{n-1}q^{m-1}}),
\end{aligned}$$

avec ces notations alors on a :

$$p(x) = \prod_{1}(x) \prod_{2}(x) ... \prod_{n}(x).$$

Remarquons que $\prod_j(x)$ est le polynome q- primitif associé à l'élément primitif αp^{j-1}.

Chapitre 2

Codes,codes linéaires, codes de *Hamming*

Richard Wesley Hamming, né le 11 février 1915 à Chicago (Illinois) et décédé le 7 janvier 1998 à Monterey (Californie) est un mathématicien célèbre à qui on doit les codes de Hamming et la distance de Hamming. Il reçut le Prix Turing en 1968.

Dans ce chapitre, nous allons étudier les codes linéaires sur un corps fini $\mathbb{F}_q$. Même si l'on ne s'intéresse ultérieurement qu'aux codes binaires, il est nécessaire de considérer dans certaines constructions des codes sur des corps finis plus généraux.

2.1 Poids et distance de *Hamming*

Introduites par *Hamming* en 1950, ces notions sont fondamentales pour estimer l'efficacité d'un code dans le cadre d' un canal où les variables aléatoires définies par les coordonnées sont indépendantes et égales.

Définition 2.1.1 *Soit* $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_q^n$ *, le poids de Hamming de* x*, noté* $wt(x)$ *est*

égal au nombre de coordonnées non nulles de x .

$$wt(x) = card\{i : 1 \leq i \leq n / x_i \neq 0\}$$

On définit une application :

$$\begin{array}{rcl} d : \mathbb{F}_q^n \times \mathbb{F}_q^n & \longrightarrow & \mathbb{R}_+ \\ (x, y) & \longmapsto & d(x, y) \end{array}$$

$d(x, y) = card\{i : / x_i \neq y_i\}$ est le nombre d'indice pour lequel les composantes de x et y sont distinctes.

Cet distance est appelée la distance de *Hamming* .

alors :

$$d(x, y) = wt(x - y) = card\{i : 1 \leq i \leq n / x_i \neq y_i\}$$

Le support d'un élément $x \in \mathbb{F}_q^n$ est l'ensemble des indices i tels que $x_i \neq 0$.

Le poids de x est donc le cardinal de son support, il faut remarquer que la distance de *Hamming* est une vrai distance au sens métrique du terme.

Rappelons brèvement les propriétés d'une distance $d(x, y)$.

$d(x, y) = 0 \Longleftrightarrow x = y$.

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

$d(x, z) \leq d(x, y) + d(y, z)$.

La boule de centre x et de rayon r est par définition l'ensemble :

$$B(x, r) = \{y : y \in \mathbb{F}_q^n / d(x, y) \leq r\}$$

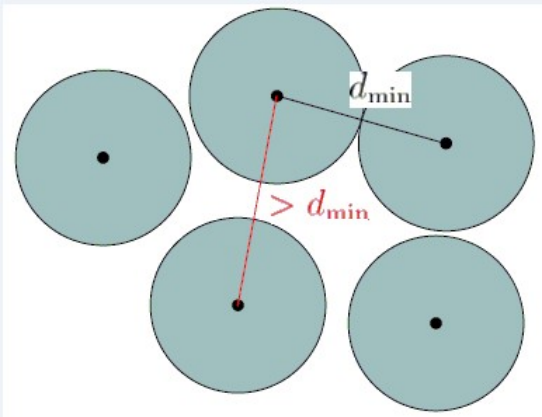
On peut remarquer que : $y \in B(x, r) \Longleftrightarrow y - x \in B(0, r)$.

Alors :

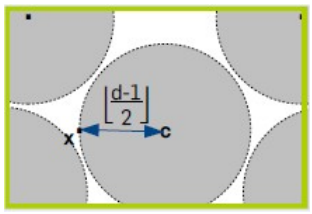
$$card(B(x, r)) = \sum_{k=0}^{r} C_k^n (q-1)^k.$$

Définition 2.1.2 *Un code de longueur n est un sous-ensemble de $\mathbb{F}_q^n$, la distance minimale de C notée $d(c)$ est le minimum des distances entre deux éléments distincts de C*

$$d(C) = \min_{x,y \in C, x \neq y} d(x,y).$$



Proposition 2.1.1 [10] *Notons $e = [\frac{d-1}{2}]$, les boules $B(x,e)$ avec $x \in C$ sont deux à deux disjointes, et e est la valeur maximale du rayon pour cette propriété.*
On dit que C détecte $d-1$ erreurs et corrige $e = [\frac{d-1}{2}]$



Remarque 2.1.1 *Si le nombre d'erreurs est inférieur à e, C corrige les erreurs.*
Si le nombre d'erreurs dépasse e, C ne peut pas corriger les erreurs car il peut exister plusieurs éléments de C approchent de x le vecteur reçu.

2.2 Codes linéaires

Définition 2.2.1 *Soit $\mathbb{K}$ un corps fini et soit $n > 0$, le $\mathbb{K}$ espace vectoriel $\mathbb{K}^n$ est muni de la métrique de Hamming.*

Un code linéaire est un $\mathbb{K}$ espace vectoriel de $\mathbb{K}^n$ .Ses paramètres sont :

Sa longueur n , sa dimension k , sa distance minimale d .

On dit que le code C est un code $[n, k, d]$.

Le nombre de mots de code linéaire est $|\mathbb{K}|^k$.

$R = \frac{k}{n}$ représente le taux de transmission (vitesse) et $\frac{d}{n}$ la fiabilité de transmission.

Si C est linéaire, on peut remarquer que, si x et y sont dans C , alors $x - y$ appartient également à C. Comme $d(x, y) = wt(x-y)$, la distance minimale de C est égale au minimum des poids des éléments non nuls de C . On a :

$$d = \min_{x,y \in C}\{wt(x - y), x \neq y\} = \min_{x,y \in C}\{d(x - y, 0)|x \neq y\} = \min_{x \in C^*}\{wt(x)\}.$$

2.3 Matrice génératrice , de contrôle de parité

On a deux façons de représenter un code linéaire à l'aide des matrices. Soit en utilisant un homomorphisme dont le code est l'espace vectoriel image , on obtient ainsi la notion de matrice génératrice.

Soit on introduit un homomorphisme dont le code est le noyau , on aura ainsi la notion de matrice contrôle.

Matrice génératrice

Pour connaitre le code en tant que sous espace , il suffit de lui déterminer une base, celle ci est le plus souvent représentée sous la forme d'une matrice $k \times n$ sur $\mathbb{K}$, la matrice génératrice du code , dont les lignes sont les vecteurs de cette base.

Propriétés

Soit C un code linéaire sur un corps $\mathbb{K}$.

1/ On dit qu'une matrice est une matrice génératrice de C si et seulement si elle est matrice $k \times n$ sur $\mathbb{K}$, avec $k \leqslant n$ dont le rang est k.

2/ Un code possède plusieurs matrices génératrices.

3/ Les mots de C sont tout les combinaisons linéaires des lignes d'une matrice génératrice.

Si G est une matrice génératrice de $C[n, k, d]$ sur $\mathbb{K}$, alors :

4/ les matrices génératrices de C sont de la forme $A \times G$, où A est une matrice carré inversible $k \times k$ sur $\mathbb{K}$.

5/ si $c_1, c_2, ..., c_n$ sont les vecteurs colonnes de G les mots du code C sont tous sous la forme :

$$m_u = (\langle c_1, u\rangle, \langle c_2, u\rangle, ..., \langle c_n, u\rangle),$$

avec $u \in \mathbb{K}^k$ et $\langle ., .\rangle$ désigne le produit scalaire usuel de $\mathbb{K}^k$

Remarque 2.3.1 *Soit C un code linéaire $[n, k, d]$, l'encodage se fait en multipliant le mot source par la matrice génératrice du code*

Définition 2.3.1 *Une matrice génératrice d'un code C est normalisée ou canonique si la matrice formée par les k première colonnes est la matrice d'unité : $G = [I_k|A]$.*
Si un code est définit par une matrice génératrice normalisée , on dit que ce code est systématique

Remarque 2.3.2 *Tout code linéaire est équivalent à un code linéaire systématique.*

Code dual et matrice de contrôle

Une autre manière pour définir un code linéaire est de donner une application linéaire dont il est le noyau.

On obtient ainsi une matrice H telle que :

$$C = \{(x_1, ..., x_n); H \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0\}.$$

Le code dual du code C est son espace orthogonal , on désigne par $\langle ., .\rangle$ le produit scalaire usuel : $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$.

$$C^{\perp} = \{y : y \in \mathbb{K}^n / \forall x \in C, \langle x, y \rangle\}$$

Une matrice de contrôle de parité de C est une matrice $(n-k) \times n$ génératrice de $C^{\perp}$.

Remarque

1/ Le dual de $C^{\perp}$ est C lui même ,

2/ Un code est dit auto dual s'il est égal à son dual.

Proposition 2.3.1 [8] *Soit C un code linéaire de matrice génératrice G, supposons que G soit de la forme dite canonique ou systématique $G = [I_k|A]$, alors une matrice de contrôle de parité est $H = [-A^t|I_{n-k}]$.*

Conséquences

G est une matrice génératrice de C alors :

1/ si H une matrice de contrôle de parité de C , alors : $G^t H = 0$.

2/ $c_1, ..., c_n$ colonnes de H, alors : $H \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 c_1 + ... + x_n c_n = 0$

Donc C contient un mot de poids au plus d, ssi 'l existe une combinaison linéaire à coefficients non-nulles de d colonnes de H qui est elle même nulle.

3/ Ainsi, un code C est de poids d si et seulement si, il existe d colonnes de sa matrice de contrôle de parité linéairement dépendante, tandis que $d-1$ colonnes quelconques sont indépendantes.

2.4 Les codes de *Hamming*

Dans ce paragraphe ,on construit une famille des codes qui ont pour propriété de corriger une erreur.

On travaille dans $\mathbb{F}_2^k$.

Définition 2.4.1 *Le code de Hamming est un code linéaire défini par sa matrice de contrôle de parité dont les colonnes sont tous les vecteurs de* $\mathbb{F}_2^k - \{0\}$.

donc on peux définir le code de Hamming de longueur $2^k - 1$ *par une matrice de contrôle dont les colonnes sont les vecteurs de* $\mathbb{F}_2^k - \{0\}$ *ordonnés par l'ordre lexicographique*

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

alors :

$H \in \mathcal{M}_{k\times(2^k-1)}$.

Exemple :

pour $k = 3$, on obtient pour matrice de contrôle :

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \textit{ donc } H' = \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right)$$

Alors la matrice génératrice est :

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

Alors $C = [7, 4, 3]$ donc $C^\perp = [7, 3, 4]$. Le code C est :

$$\begin{array}{rlll} C = & \{(0000000); & (1000011); & (0100101); \\ & (0001111); & (0011001); & (0010011); \\ & (0010110); & (0110011); & (0110111) \\ & (0101111); & (1000011); & (1011010) \\ & (1110000); & (1001100); & (1100110); (1111111)\} \end{array}$$

Proposition 2.4.1 *Pour tout $k \geq 3$, le code de Hamming est de distance minimale égale à 3.*

Par conséquent il est capable de corriger une seule erreur.

Preuve: Supposons x, y deux mots dans code binaire de *Hamming* , soit H sa matrice de contrôle, comme C est un code linéaire alors $x - y \in C$.

Supposons que $d(x, y) = 1$, alors $x - y$ est un vecteur de la base canonique donc $H(x - y)$ est un colonne de H , comme$x - y \neq 0$ car tous les colonnes de H sont non nulle , mais $x - y \in C$, alors $H(x - y) = 0$ contradiction.

Supposons que $d(x, y) = 2$, alors $H(x - y) = 0$ si et seulement s'il existe deux colonnes de H qui sont linéairement dépendants.

Ce n'est pas le cas d'où $d(x, y) \geqslant 3$, pour tous les mots de code x, y.

Tout matrice de contrôle d'un code binaire de *Hamming* aura trois colonnes qui sont linéairement dépendante , donc en fait des mots de code sont de distance 3 □

Conséquence

Le code binaire de *Hamming* est capable de corriger une seul erreur.

2.4.1 Décodage par syndrome

Soit C un $[n, k, d]$ code linéaire sur $\mathbb{K}$, Soit H une matrice de contrôle de C.

Définition 2.4.2 *Pour $x \in \mathbb{K}^n$, xH^T est appelé Syndrome de x .*

On défini une relation d'équivalence dans $\mathbb{K}^n$ par : $x\mathcal{R}y \Longleftrightarrow (x - y)H^T = 0$;

alors :

$$\begin{array}{rcl} xH^T = yH^T & \Longleftrightarrow & (x - y)H^T = 0 \\ x\mathcal{R}y & \Longleftrightarrow & x - y \in C. \end{array}$$

L'ensemble des classes est $\dfrac{\mathbb{K}^n}{C} = \{x + c | x \in \mathbb{K}\}$, alors : $|\dfrac{\mathbb{K}^n}{C}| = \dfrac{|\mathbb{K}^n|}{|C|} = \dfrac{q^n}{q^k} = q^{n-k} = m.$

Soit u un représentons de la classe $\bar{x} = x + c$ de poids minimum , u est appelé le leader de $\bar{x}$.

Soit $\{u_1, u_2, ..., u_m\}$ l'ensemble des leaders dans $\mathbb{K}^n$.

Principe de décodage par syndrome

1/ On détermine les leaders $u_1, u_2, ..., u_m$.

2/ On construit le tableau standard :

leader	$u_1 = 0$	u_2	.....	u_m
syndrome	$S(u_1) = u_1 H^T$	$S(u_2) = u_2 H^T$	.....	$S(u_m) = u_m H^T$

3/ Soit $y \in \mathcal{K}^n$ le message reçu , y affecte au moins de e erreurs.

4/ On calcule $S(y) = yH^T$.

5/ On cherche u_i un leader d'une classe de même syndrome que y.

6/ On décode le mot reçu pour $x = y - u_i$.

Exemple

Soit C un code de longueur 6 de matrice génératrice
$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$; alors $H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$,
$d = 3$; alors $e = 1$

leader	0	e_1	e_2	e_3	e_4	e_5	e_6	$e_4 + e_5$
syndrome	(000)	(101)	(111)	(011)	(100)	(010)	(001)	(110)

Soit $y(011111)$ un mot reçu

$$S(y) = yH^T = (011111) \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (011),$$

$x = y - u_i$ alors $x = (011111) - (001000) = (010111)$

Cas où il y a au plus d'une erreur

Soit C le mot envoyé et x le mot reçu, $d(x, c)$ = nombre d'erreurs.

$x - c = \lambda e_i$, e_i étant un élément de la base canonique.

$(x - c)H^T = xH^T - cH^T = xH^T = \lambda e_i H^T$ car $c \in C$.

alors :

$$\lambda e_i H^T = \lambda c_i$$

tel que : c_i est la i ème colonne dans H, donc l'erreur est commise dans la i ème colonne

Exemple sur code de *Hamming*

Soit le code binaire de *Hamming* , $C[7,4,3]$.

Soit $v=(1001) \in \mathbb{F}_2^4$, soit G une matrice génératrice de ce code tel que :

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

donc $vG=c\in C$,alors :

$$vG=(1001)\left(\begin{array}{cccc|ccc} 1&0&0&0&0&1&1\\ 0&1&0&0&1&0&1\\ 0&0&1&0&1&1&0\\ 0&0&0&1&1&1&1 \end{array}\right)=(1001100).$$

La matrice de contrôle H qui convient à G est

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

Sachant que le mot reçu est $x=(0001100)$, alors on obtient le mot envoyée comme ci dessus :

$$xH^T=(0001100)\left(\begin{array}{ccc} 0&1&1\\ 1&0&1\\ 1&1&0\\ 1&1&1\\ 1&0&0\\ 0&1&0\\ 0&0&1 \end{array}\right)=(011)$$

,

donc c'est la 1 ère colonne de la matrice de contrôle H , alors l'erreur est commise à la première position .

Donc le message envoyé est $c=(1001)$

Chapitre 3

Codes simplexes

Dans ce chapitre , on va traiter l'article de $D.G.Hoffman$ qui parle sur la relation entre les codes linéaires et les poids.[5]

Soit K un corps fini à q éléments donc " $K = \mathbb{F}_q$ est commutatif " .

On appelle un code linéaire de longueur n de dimension k sur $\mathbb{F}_q$ tout sous espace vectoriel de $\mathbb{F}_q^n$.

On dit que C est de cardinal q^k , de dimension k et de longueur n.

Comme C est un espace vectoriel de $\mathbb{F}_q^n$, C hérite certains propriétés métriques.

Soit $v \in \mathbb{F}_q^n$, on appelle poids de v le nombre $wt(v) = |\{i/v_i \neq 0\}|$.

La distance entre deux vecteurs est le poids de leur différence, on déduit :

1)$d(u, v) = wt(u - v)$.

2)$wt(u) = 0 \Longleftrightarrow u = 0$.

3)$wt(\lambda u) = wt(u), \lambda \in \mathbb{F}_q - \{0\}$.

4)$wt(u + v) \leq wt(u) + wt(v)$.

l'interaction entre la structure algébrique de C et de la structure métrique induite par la fonction de poids est au coeur de la théorie du codage.

3.1 Code équidistant

Définition 3.1.1 *Un code $\mathcal{C}$ à poids fixe, est un code dont ses mots non nulle ont le même poids :*

$$\forall x \neq y \in \mathcal{C}, x \neq 0, y \neq 0; wt(x) = wt(y).$$

Définition 3.1.2 *Un code $\mathcal{C}$ équidistant , c'est un code où la distance entre deux mots différent est fixe :*

$$\forall x \neq y \in \mathcal{C}, d(x, y) = fixe.$$

Proposition 3.1.1 *Soit $\mathcal{C}$ un code linéaire , alors : $\mathcal{C}$ est équidistant si et seulement si $\mathcal{C}$ est à poids fixe.*

Preuve: Soit $\mathcal{C}$ un code linéaire équidistant donc $d(x, y) = cst$ alors :

pour $y = 0$, $d(x, 0) = cst$, donc $wt(x) = cst$ donc $\mathcal{C}$ est à poids fixe.

La réciproque :

Soit $\mathcal{C}$ un code linéaire à poids fixe alors :

$\forall x, y \in \mathcal{C}, d(x,y) = wt(x-y)$,

posons $z = x - y \in \mathcal{C}$ donc $wt(z) = cst = d(x,y)$.

Alors : $\mathcal{C}$ est un code à poids fixe.

□

Remarque 3.1.1 *La proposition* 3.1.1 *est vrai seulement pour les codes linéaire . Voici un contre exemple :*

$$\mathcal{C} = \{x = (110100); y = (001011); z = (111000)\}$$

$\mathcal{C}$ *est un code non linéaire de poids fixe* $wt(x) = wt(y) = wt(z) = 3$ *mais :*

$d(x,y) = 6, d(y,z) = 4$

L'inégalité triangulaire $wt(u+v) \leq wt(u) + wt(v)$ détient , mais comme l'exemple suivant montre qu'il est trop faible pour raconter toute l'histoire .

v	0	v_1	v_2	v_3	v_1+v_2	v_1+v_3	v_2+v_3	$v_1+v_2+v_3$
$wt(v)$	0	1	1	1	2	2	2	1

les huit vecteurs d'un code linéaire de dimension 3 par défaut.

L'inégalité triangulaire est réalisé mais dommage, il n'y a pas ce code.

Cet exemple illustre notre premier objectif, soit V un espace vectoriel sur $\mathbb{F}_q$ et ω une fonction de V dans les entiers non négative, dans quelles conditions pouvons réaliser V comme sous-espace "concrète" de certain $\mathbb{F}_q^n$, de sorte que ω devient la fonction de poids ?

La première théorème répond à cette question.

Théorème 3.1.1 [5] *soit* V *un sous espace sur* $\mathbb{F}$ *de dimension* k*, et pour* $v \in V$*, soit* $\omega(v)$ *est un entier non négative, alors les trois énoncés suivants sont équivalents :*

1) *Pour un certains* n*, il y a une transformation linéaire* T *de* V *dans* $\mathbb{F}_q^n$ *satisfait :*

$$wt(T(v)) = \omega(v), \forall v \in V.$$

2)$\omega(0) = 0, \omega(\alpha v) = \omega(v), \forall v \in V; \alpha \neq 0, \alpha \in \mathbb{F}_q$*, ainsi, si* W *est sous espace de* V *, alors :*

$$\sum_{w \in W} \omega(w) \text{ est divisible par } (q-1)q^{t-1},$$

tel que t est la dimension de W, et si X est un sous-ensemble de $W \subset V$ alors :

$$\sum_{w \in W} \omega(w) \leq \sum_{w \in X} \omega(w),$$

à la différence de multiple de q^t.

3)$\omega(0) = 0, \omega(\alpha v) = \omega(v), \forall v \in V; \alpha \neq 0, \alpha \in \mathbb{F}_q$, *ainsi, si H est sous espace de V de dimension $k-1$ alors :*

$$q \sum_{w \in H} \omega(w) \equiv \sum_{v \in V} \omega(v) (mod\ q^{k-1}),$$

et

$$q \sum_{w \in H} \omega(w) \leq \sum_{v \in V} \omega(v).$$

Preuve: Supposons (1) et prouver (2).

$\omega(0) = wt(T(0)) = wt(0) = 0$. car T est une fonction linéaire.

$\omega(\alpha v) = wt(T(\alpha v)) = wt(\alpha T(v)) = wt(T(v)) = \omega(v)$.

Pour chaque $S \subseteq V$, nous formons $|S|$ par n matrice $M(S)$ comme ci dessus :

Les rangées de $M(S)$ sont indexées par les éléments de S, et pour chaque $v \in S, T(v)$ est la rangée correspondante de $M(S)$. Notons que chaque des q éléments de corps se produit exactement q^{t-1} fois dans chaque colonne non nul de $M(W)$.

Alors, si x est le nombre de ces colonnes donc :

$$\sum_{w \in W} \omega(w) = x(q-1)q^{t-1}.$$

Si X est le sous-espace $W + u$,puis $M(W)$ en ajoutant $T(u)$ à chaque ligne de $M(W)$, ce processus permute simplement les entrées de la x non nulles colonnes de $M(W)$.

Cependant, une colonne nulle de $M(W)$ est une constante colonne dans $M(X)$, et si cette constante n'est pas nulle alors $M(X)$ gagne de poids, ainsi :

$$\sum_{w \in W} \omega(w) \leq \sum_{w \in X} \omega(w),$$

La différence est divisible par q^t.

Évidemment (2) implique (3), depuis les q sous ensemble de H dans V

$$\begin{aligned}
\sum_{w\in H}\omega(w) &= x(q-1)q^{k-2}\\
q\sum_{w\in H}\omega(w) &= x(q-1)q^{k-1}\\
\sum_{v\in V}\omega(v) &= x'(q-1)q^{k-1}\\
q\sum_{w\in H}\omega(w) &= \sum_{v\in V}\omega(v)+(x-x')(q-1)q^{k-1}\\
q\sum_{w\in H}\omega(w) &\equiv \sum_{v\in V}\omega(v)[q^{k-1}]
\end{aligned}$$

(3) $\Longrightarrow$ (1)

On peut supposer que $V=\mathbb{F}^k$, avec des élément écrits comme vecteurs lignes.Ainsi, la transformation T que nous cherchons, sera de la forme : $T(v)=v.G$, pour une matrice appropriée G avec k ligne.

Nous procédons de construire G.

Soit R le groupe des touts sous espace de V de dimension $k-1$, et soit $H\in R$.

Depuis ω est constante sur les $q-1$ non nulle vecteurs de n'importe dimension sous-espace de H, $\sum_{w\in H}\omega(w)$ est divisible par $q-1$, de même que $\sum_{v\in V}\omega(v)$, par le même raisonnement.
Depuis $q-1$ et q^{k-1} sont premiers entre eux, le nombre :

$$\gamma_H \doteqdot (q-1)^{-1}q^{1-k}(\sum_{v\in V}\omega(v)-q\sum_{w\in H}\omega(w))$$

est un entier non négatif .

Soit v_H un vecteur non nul orthogonal à H.

Formons la matrice G comme suit :

Pour chaque $H\in R$, placer les copies γ_H de la transposé de v_H dans G en forme des colonnes.

Tout ce qui reste à prouver, c'est que $wt(vG)=\omega(v),\forall v\in V$ cela est évident pour $v=0$.

Alors, on suppose que $v\neq 0$, donc :

$$\begin{aligned}
wt(vG) &= \sum_{H\in R, v\notin H}\gamma_H\\
&= (q-1)^{-1}q^{1-k}[\sum_{u\in V}\omega(u)|\{H\in R, v\notin H\}|-q\sum_{w\in V}\omega(w)|\{H\in R/w\in H, v\notin H\}|]
\end{aligned}$$

Calculons : $|\{H\in R, v\notin H\}|$, $|\{H\in R/w\in H, v\notin H\}|$.

La deuxième est plus délicate, si w est dans le sous espace $\langle v\rangle$ engendré par v de dimension

égal 1,il est évident que $|\{H \in R/w \in H, v \notin H\}| = 0$.

Supposons maintenant que $w \notin \langle v \rangle$.

Rappelons que tout les non-nuls s dans V déterminent un unique élément de R, à savoir l'ensemble de tous les vecteurs orthogonaux à S, et inversement tout élément R est déterminée par $q-1$ vecteurs de S.

D'abord, nous calculons le cardinal de l'ensemble. $S = \{s \in V/s.w = 0, s.v \neq 0\}$, comme il y a q^{k-1} vecteurs orthogonal à w, et q^{k-2} d'entre eux sont aussi orthogonal à v, nous avons : $|S| = q^{k-1} - q^{k-2}$, ainsi :

$$|\{H \in R/w \in H, v \notin H\}| = \frac{q^{k-1} - q^{k-2}}{q-1}$$

La première est simple :

$S = \{s \in V/s.v \neq 0\}$, alors on a q^k vecteur dans V et on a q^{k-1} orthogonal à v alors $|S| = q^k - q^{k-1}$, donc

$$|\{H \in R/w \in H, v \notin H\}| = \frac{q^k - q^{k-1}}{q-1}$$

alors :

$$\begin{aligned}
wt(vG) &= \sum_{H \in R, v \notin H} \gamma_H \\
&= \sum_{H \in R, v \notin H} [(q-1)^{-1} q^{1-k} (\sum_{v \in V} \omega(v) - q \sum_{w \in H} \omega(w))] \\
&= (q-1)^{-1} q^{1-k} [\sum_{H \in R, v \notin H} \sum_{v \in V} \omega(v) - q \sum_{H \in R, v \notin H} \sum_{w \in H} \omega(w)] \\
&= (q-1)^{-1} q^{1-k} [\sum_{u \in V} \omega(u) |\{H \in R, v \notin H\}| - q \sum_{w \in V} \omega(w) |\{H \in R/w \in H, v \notin H\}|] \\
&= (q-1)^{-1} q^{1-k} [\frac{q^k - q^{k-1}}{q-1} \sum_{u \in V} \omega(u) - q \frac{q^{k-1} - q^{k-2}}{q-1} \sum_{w \in V; w \notin \langle v \rangle} \omega(w)] \\
&= (q-1)^{-1} q^{1-k} [\frac{q^k - q^{k-1}}{q-1} \sum_{u \in V} \omega(u) - \frac{q^k - q^{k-1}}{q-1} \sum_{w \in V; w \notin \langle v \rangle} \omega(w)] \\
&= (q-1)^{-1} q^{1-k} \frac{q^k - q^{k-1}}{q-1} [\sum_{u \in V} \omega(u) - \sum_{w \in V; w \notin \langle v \rangle} \omega(w)]
\end{aligned}$$

$$\begin{aligned}
wt(vG) &= (q-1)^{-1} \sum_{u \in \langle v \rangle} \omega(u) \\
&= (q-1)^{-1} (q-1) \omega(v) \\
&= \omega(v).
\end{aligned}$$

□

La matrice G construit au dessus est loin d'être unique.En fait, n'importe qu'elle séquence de les opérations suivantes :

a) Multiplier certaines colonnes par des éléments non nuls.

b) Se raccordent des colonnes de zéros.

c) Permuter les colonnes.

Cependant, le théorème suivante montre que tout est la liberté que nous avons, le reste est forcé.

Théorème 3.1.2 [5] *Soit $G \in M_{k\times n}$ sur $\mathbb{F}_q^k$, soit γ_H est le nombre de colonnes non-nulles de G orthogonal à H, puis :*

$$\gamma_H = (q-1)^{-1}q^{1-k}(\sum_{v\in\mathbb{F}_q^k} wt(vG) - q\sum_{w\in H} wt(wG))$$

Preuve: d'après la preuve de la théorème (1) , $\forall v \neq 0, \in \mathbb{F}_q^k$, on a :

$$wt(vG) = \sum_{J\in R, v\notin J} \gamma_J$$

puis : $\forall H \in R$.

$$\begin{aligned}
(q-1)^{-1}q^{1-k}(\sum_{v\in\mathbb{F}_q^k} wt(vG) - q\sum_{w\in H} wt(wG)) &= (q-1)^{-1}q^{1-k}(\sum_{v\in\mathbb{F}_q^k}\sum_{J\in R, v\notin J}\gamma_J - q\sum_{w\in H}\sum_{J\in R, w\notin J}\gamma_J)\\
&= (q-1)^{-1}q^{1-k}(\sum_{J\in R}\gamma_J|\{v\in V/v\notin J\}|\\
&\quad -q\sum_{J\in R}\gamma_J|\{w\in H/w\notin J\}|)\\
&= (q-1)^{-1}q^{1-k}[(q^k-q^{k-1})\sum_{J\in R}\gamma_J\\
&\quad -q(q^{k-1}-q^{k-2})\sum_{J\in R, J\neq H}\gamma_J]\\
&= (q-1)^{-1}q^{1-k}(q^k-q^{k-1})[\sum_{J\in R}\gamma_J - \sum_{J\in R, J\neq H}\gamma_J]\\
&= (q-1)^{-1}(q-1)(\gamma_H)\\
&= \gamma_H.
\end{aligned}$$

□

Un code C linéaire est un code à poids fixe si $wt(v) = wt(w)$, pour tous $v, w \in C$ non nuls.

Comme application, nous caractérisons un code à poids fixe, on donne quelque définitions.

Si C est un code linéaire de longueur n, et m est un nombre entier positif, pour chaque $v \in C$, formons le vecteur constitué par les m copies de v concaténâtes ensemble.

Le code linéaire obtenu est de longueur $n.m$ est appelée réplication de C, avec multiplicateur m.

Si β est un nombre entier non-négatif, ajoutons β zéros à la fin de chaque vecteur de C, le

résultat est un code linéaire de longueur $n+\beta$ est appelée rembourrage "*padding*" de C.
Si π est une permutation de $\{1,2,...,n\}$, et si $\alpha=(\alpha_1,\alpha_2,...,\alpha_n)$ est un vecteur de non nuls éléments sur le corps, pour chaque $v=(v_1,v_2,...,v_n)\in C$, former le vecteur $(\alpha_1 v_{\pi(1)},\alpha_2 v_{\pi(2)},...,\alpha_n v_{\pi(n)})$.
Le code linéaire résultant est dit équivalent à C.
Dans le notion du théorème (3.1.2), soit $G\in M_{k\times n}$ tel que $n=\dfrac{q^k-1}{q-1}$ satisfait $\gamma_H=1$, pour tout $H\in R$.
Le code $C:=\{vG/v\in\mathbb{F}_q^k\}$ est appelé un code dual de $Hamming$ de dimension k.

Théorème 3.1.3 [5] *Soit C un code linéaire de dimension k, alors C est équivalent à poids fixe si et seulement si C est équivalent à un rembourrage d'une réplication d'un dual de $Hamming$ de dimension k.*
Dans ce cas, tous les non-nuls $v\in C$ ont le poids mq^{k-1} où m est le multiplicateur de la réplication.

Preuve: Si C est un équivalent à rembourrage d'une réplication de dual de $Hamming$ de dimension k avec le multiplicateur m, alors, dans la notation du théorème (3.1.2).
On a $\gamma_H=m,\forall H\in R,\forall v\in\mathbb{F}^k$.
alors :

$$\begin{aligned} wt(vG)=\sum_{H\in R,v\notin H}\gamma_H &= m|\{H\in R/v\notin H\}| \\ &= m\frac{q^k-q^{k-1}}{q-1} \\ &= mq^{k-1}. \end{aligned}$$

Inversement :
Si $wt(v)=w,\forall v\neq 0/v\in C$ par le théorème (3.1.2),

$$\begin{aligned} \forall H\in R,\quad \gamma_H &= (q-1)^{-1}q^{1-k}(\sum_{v\in\mathbb{F}_q^k} wt(vG)-q\sum_{w\in H} wt(wG)), \\ &= (q-1)^{-1}q^{1-k}(\sum_{v\in C,v\neq 0} wt(v)-q\sum_{w\in H,w\neq 0} wt(w)) \\ &= (q-1)^{-1}q^{1-k}(\sum_{v\in C,v\neq 0}\omega-q\sum_{w\in H,w\neq 0}\omega) \\ &= \omega(q-1)^{-1}q^{1-k}(q^k-1-q(q^{k-1}-1)) \\ &= \omega(q-1)^{-1}q^{1-k}(q^k-1-q^k+q) \\ &= \omega q^{1-k} \end{aligned}$$

□

3.2 Caractérisation des codes équidistants

Soit $\mathcal{C}$ un code d'ordre q, de longueur n et de distance minimale d , alors on a :

$$d \leqslant \frac{n|\mathcal{C}|(q-1)}{q(|\mathcal{C}|-1)}. \text{ "}Borne\ \ de\ \ Plotkin\text{"}$$

On va prouver cet borne :

3.2.1 La borne de *Plotkin*

Corollaire 3.2.1 [29] $\forall \mathcal{C} \subset \mathbb{F}^n(q)$ *de distance* δ *, alors :*

$$R \leqslant 1 - \frac{q}{q-1}\delta + o(1).$$

tel que R *est taux de transmission.*

Preuve: On va raccourci les mots de code $\mathcal{C}$, par regrouper les mots de code de sorte qu'ils d'accord sur les premiers $n - n'$ positions tel que $n' = \lceil \frac{qd}{q-1} \rceil - 1$,

$$\forall x \in \mathbb{F}_q^{n-n'}, \mathcal{C}_x = \{(c_{n-n'+1}, ..., c_n) | (c_1, ..., c_n) \in \mathcal{C}, (c_1, ..., c_{n-n'}) = x\}.$$

On définit $d = \delta n$, $\forall x, \mathcal{C}_x$ a la distance d, comme $\mathcal{C}$ a la distance d , car :
si $\exists x; c_1 \neq c_2 \in \mathcal{C}_x, d(c_1, c_2) < d$, alors $d((x, c_1); (x, c_2)) < d$ ce qui implique que la distance de $\mathcal{C}$ est inférieur à d car $(x, c_1), (x, c_2) \in \mathcal{C}$, par définition de $\mathcal{C}_x$.
Donc :

$$n' < \frac{q}{q-1}d,$$

alors

$$\begin{aligned} d &> (1 - \frac{1}{q})n', \\ qd &> (q-1)n', \\ qd - (q-1)n' &> 0, \end{aligned}$$

donc :

$$|\mathcal{C}_x| < \frac{(q-1)n'}{qd - (q-1)n'} < \frac{qd}{qd - (q-1)n'} < qd,$$

On a

$$|\mathcal{C}| = \sum_{x \in \mathbb{F}_q^{n-n'}} |\mathcal{C}_x|,$$

alors :

$$\begin{aligned} |\mathcal{C}| &\leqslant \sum_{x \in \mathbb{F}_q^{n-n'}} qd = q^{n-n'} qd, \\ &\leqslant q^{n-\frac{q}{q-1}d+1} d, \\ &\leqslant q^{n-\frac{q}{q-1}d+1+o(n)}, \end{aligned}$$

donc

$$R \leqslant 1 - \frac{q}{q-1}d + o(n)$$

□

Résultat

$\forall \mathcal{C} \subset \mathbb{F}_q^n$ de taux R et distance relative δ , alors $R < 1 - \delta$.

Lemme 3.2.1 [29] *Soit $v_1, v_2, ..., v_s \in \mathbb{R}^n$, vecteurs non nulles .*

1) *si $\langle v_i, v_j \rangle \leqslant 0, \forall i \neq j$ alors $s \leqslant 2n$.*

2) *soit v_j vecteurs unitaires tel que $1 \leqslant i \leqslant s$, de plus si $\langle v_i, v_j \rangle \leqslant -\varepsilon \leqslant 0, \forall i \neq j$,*
alors : $s \leqslant 1 + \frac{1}{\varepsilon}$.

Lemme 3.2.2 [29] *Soit f une application tel que : $f : \mathcal{C} \longrightarrow \mathbb{R}^{nq}$, $\forall c \in \mathcal{C}; \|f(c)\| = 1$, et* $\forall c_1 \neq c_2 \in \mathcal{C}; \langle f(c_1), f(c_2) \rangle \leqslant 1 - \frac{q}{q-1}\frac{d(c_1, c_2)}{n}$

On trouve la preuve de ces lemmes dans [30]

Théorème 3.2.1 [29] " *Borne de Plotkin* "

Quelque soit un code $\mathcal{C} \subset \mathbb{F}_q^n$ *de distance* d *, alors :*

1) *si* $d = (1 - \frac{1}{q})n, |\mathcal{C}| \leqslant 2qn.$

2) *si* $d > (1 - \frac{1}{q})n, |\mathcal{C}| \leqslant \dfrac{qd}{qd - (q-1)n}.$

Preuve: Soit $\mathcal{C} = \{c_1, ..., c_s\}, \forall i \neq j,$

$$\begin{aligned} \langle f(c_i), f(c_j)\rangle &\leqslant 1 - (\frac{q}{q-1}).\frac{d(c_i, c_j)}{n}, \\ &\leqslant 1 - \frac{q}{q-1}.\frac{d}{n}. \end{aligned}$$

si $d = (1 - \dfrac{1}{q}n = \dfrac{q-1}{q}n$;alors

$$\begin{aligned} \langle f(c_i), f(c_j)\rangle &\leqslant 1 - (\frac{q}{q-1}).n.\frac{q-1}{q}.\frac{1}{n} \\ &\leqslant 0 \\ alors : m &\leqslant 2nq, \end{aligned}$$

donc :

$$|\mathcal{C}| \leqslant 2nq$$

si $d > \dfrac{q-1}{q}n$, alors :

$$\begin{aligned} \forall i \neq j \langle f(c_i), f(c_j)\rangle &\leqslant 1 - \frac{q}{q-1}.\frac{d}{n} = \frac{n(q-1) - qd}{n(q-1)} \\ \langle f(c_i), f(c_j)\rangle &\leqslant -\frac{qd - n(q-1)}{n(q-1)} \end{aligned}$$

comme : $qd - n(q-1) > 0$, alors : $\varepsilon = \dfrac{qd - n(q-1)}{n(q-1)} > 0$.

donc :

$$\begin{aligned} s = |\mathcal{C}| &\leqslant 1 + \frac{(q-1)n}{qd - (q-1)n}, \\ |\mathcal{C}| &\leqslant \frac{qd - (q-1)n + (q-1)n}{qd - (q-1)n}, \\ |\mathcal{C}| &\leqslant \frac{qd}{qd - (q-1)n}. \end{aligned}$$

alors : $|\mathcal{C}|qd - (q-1)n|\mathcal{C}| \leqslant qd$, alors : $qd(|c| - 1) \leqslant (q-1)n|\mathcal{C}|$ donc $d \leqslant \dfrac{(q-1)n|\mathcal{C}|}{q(|c|-1)}$

□

Si le code $\mathcal{C}$ est un équidistant code alors :

$$d = \frac{(q-1)n|\mathcal{C}|}{q(|\mathcal{C}|-1}, |\mathcal{C}| = q^k.$$

donc :

$$d = \frac{nq^k(q-1)}{q(q^k-1)}$$

d'où par conséquent , il doit être un entier positif m tel que :
$n = \frac{(q^k-1)m}{q-1}$, donc $d = \frac{\frac{(q^k-1)m}{q-1}(q-1)q^k}{q(q^k-1)}$ alors :

$$d = mq^{k-1}.$$

On va construire un code linéaire équidistant $\mathcal{C}[n,k,d]$, tel que :

$$n = \frac{(q^k-1)m}{q-1}, \quad d = q^{k-1}m.$$

Pour $l = 1, 2, ..., m$, soit G_l une matrice de $k(\frac{q^k-1}{q-1})$ de coefficients dans $\mathbb{F}_q$, avec la propriété que chaque deux colonnes sont linéairement indépendant.
G_l est la matrice de contrôle de code de $Hamming$ donc G_l est la matrice génératrice du dual de code de $Hamming$.
Si on définit la matrice génératrice de $\mathcal{C}$ comme $G := [G_1|G_2|...|G_m]$, nous rappelons que deux codes sont équivalent si on obtient l'un à partir de l'autre par une permutation convenable.
Si $q \neq 2$, les codes générés séparément par les matrices $G_1, ..., G_m$ ne sont pas nécessairement équivalent.
On va démontrer que si $\mathcal{C}$ est un code linéaire équidistant $\mathcal{C}[n,k,d]$, puis il existe $G_1, ..., G_m$ matrices génératrices des duals de codes de $Hamming$, tel que $\mathcal{C}$ est équivalent à un code qui a la matrice génératrice $G := [G_1|G_2|...|G_m]$ tel que $G_i; \forall i : 1 \leqslant i \leqslant m, G_i \in \mathcal{M}_{k\times\frac{q^k-1}{q-1}}$.
On va démontrer par récurrence à k.
Pour $k = 1$ le résultat est évidement.
Supposons que la propriété est vraie pour $k-1$ est soit $u_1, u_2, ..., u_k$ les lignes de la matrice génératrice A de $\mathcal{C}$, le dernier ligne u_k a $q^{k-1}m$ positions.
Parmi ceux ci il y a m positions dans laquelle les lignes $u_1, u_2, ..., u_{k-1}$ ont élément commun est le zéro , en fait ces $k-1$ lignes représentent une matrice génératrice d'un code équidistant

de dimension $k-1$ et distance $d = q^{k-2}s$ tel que $s = qm$,

alors :

$$l = \frac{s(q^{k-1}-1)}{q-1}.$$

d'où les commun zéros de $u_1, u_2, ..., u_{k-1}$ se produit $n - l = m$ positions.

Depuis la matrice A a des colonnes non nulle, alors le mot de code u_k a non null éléments ; donc , on obtient A sous la forme :

$$A = \left(\begin{array}{c|c|c} 0 & & \\ 0 & & \\ \vdots & M & N \\ 0 & & \\ \hline u & v & 0 \end{array}\right)$$

tel que : $A \in \mathcal{M}_{k\times l}$, $M \in \mathcal{M}_{(k-1)\times(q^{k-1}-1)m}$, $N \in \mathcal{M}_{(k-1)\times\frac{q^{k-1}-1}{q-1}m}$,

$u \in \mathcal{M}_{1\times m}$, $v \in \mathcal{M}_{1\times(q^{k-1}-1)m}$, les vecteurs u, v ont non nulles éléments , alors la matrice $\mathcal{M}$ est une matrice génératrice du code linéaire équidistant de dimension $k-1$ et du distance $q^{k-2}(q-1)m$, le même chose pour la matrice N , c'est une matrice génératrice d'un code linéaire équidistant de dimension $k-1$ et du distance $q^{k-2}m$.

Soit x une combinatoire linéaire non-nulle de les lignes $u_1, u_2, ..., u_{k-1}$. Les vecteurs u_k et x sont linéairement indépendant , alors u_k, x construisent un code linéaire équidistant de distance $q^{k-1}m$ et de dimension égal 2, alors la distance de ce code est de la forme qs tel que $s = q^{k-2}m$, alors le longueur de ce code est de la forme qs , tel que $s = q^{k-2}m$, alors le longueur de ce code est $\frac{s(q^2-1)}{q-1} = \frac{q^{k-2}m(q^2-1)}{q-1} = q^{k-2}m(q+1)$, que signifie qu'il y a $q^{k-2}m(q-1)$ position tel que x et u_k n'ont pas des zéros éléments donc le contribution de M à la poids de x est égal à $q^{k-2}(q-1)m$, alors que le contribution de la matrice N est $q^{k-2}m$, supposons que M de rang $h < k-1$, comme M a des colonnes non nulle, alors :

$\exists\alpha \in \mathbb{N}; (q^{k-1}-1)m = \alpha\frac{q^h-1}{q-1}$ et $q^{k-2}(q-1)m = q^{h-1}\alpha$;

donc

$$\alpha = q^k - 1 - h(q-1)m$$

alors :

$$\begin{aligned}(q^{k-1}-1)m &= q^{k-1-h}(q-1)m\frac{q^k-1}{q-1} \\ q^{k-1}-1 &= q^{k-1-h}(q^h-1)\end{aligned}$$

contradiction car q devise $q^{k-1-h}(q^h-1)$ mais q ne divise pas $q^{k-1}-1$, donc le rang de M et N égale $k-1$.

On va appliquer notre hypothèse sur les matrices génératrices M et N.

Une permutation des colonnes apporte la matrice A comme ci dessus :

$$A=\left(\begin{array}{c|c|c|c|c|c|c|c|c} 0 & & & & & & & & \\ 0 & & & & & & & & \\ \vdots & M_1 & M_2 & ... & M_{(q-1)m} & N_1 & N_2 & ... & N_m \\ 0 & & & & & & & & \\ \hline u & v_1 & v_2 & ... & v_{(q-1)m} & 0 & 0 & ... & 0 \end{array}\right)$$

les matrices M_1, M_2, ...,$M_{(q-1)m}$, N_1 , N_2 ,..., $N_m \in \mathcal{M}_{k-1\times\beta}$; tel que $\beta=\dfrac{q^{k-1}-1}{q-1}$, sont des matrices de $Hamming$ et les vecteurs $u, v_1, ..., v_{(q-1)m}$ n'ont pas des éléments nulles.

Nous voulons formuler le résultat ci dessus de manière, on peux prendre de les matrices $M_i, N_j, (i=1,...,(q-1)m; j=1,...,m)$, on regroupe les colonnes qui représentent une seul et même sous espace vectoriel de $\mathbb{F}_q^{k-1}$ de dimension 1 et on peut réorganiser les colonnes de la matrice A comme ci dessus :

$$A=\left(\begin{array}{c|c|c|c|c} 0 & & & & \\ 0 & & & & \\ \vdots & A_1 & A_2 & ... & A_\beta \\ 0 & & & & \\ \hline u & x_1 & x_2 & ... & x_\beta \end{array}\right)$$

Les matrices $A_1, A_2, ..., A_\beta \in \mathcal{M}_{k-1\times qm}$, les vecteurs $x_1, x_2, ..., x_\beta$ sont de longueur qm.

Donc, on a les propriétés suivants :

1/ Deux colonnes de la même matrice A_i sont linéairement dépendent , $\forall i=1,2,...,\beta$.

2/ Les colonnes de la matrice A_i et les colonnes de la matrice A_j ,$\forall i\neq j$ sont linéairement indépendant.

3/ Chaque vecteur $x_j=(x_{j_1}, x_{j_2}, ..., x_{j_{qm}})$ a m élément égal à 0.

4/ u est un vecteur de longueur m avec des élément non nulle.

Soit $j\in\{1,2,...,\beta\}$, soit $y_j=(y_{j_1}, y_{j_2}, ..., y_{j_{qm}})$, le premier ligne non nulle de A_j , comme A_j est de rang 1 , les éléments de y_j sont tous non nulle.

On va montrer que $\forall c\in\mathbb{F}_q$, $|\{i|x_{ji}=cy_{ji}\}|=m$.

Si $c = 0$ donc x_j a m élément égal à 0.

Si $c \neq 0$, nous considérons le vecteur $u_k - cu_l$ tel que u_l est une ligne de la matrice A, depuis ce vecteur ne réside pas dans le sous espace vectoriel engendré par $u_1, u_2, ..., u_{k-1}$, il peut substituer u_k en tant que la ligne numéro k de A .

Correspondant à A_j, nous obtenons pour $u_k - cu_l$, le vecteur x'_j avec m élément nulle.

Considérons la matrice Z_j formé par ajouter le vecteur x_j à la matrice A_j comme ligne numéro k .

Soit $\mathbb{F}_q = \{c_0, c_1, ..., c_{q-1}\}$, alors $\forall s \in \{0, 1, ..., q-1\}$ il y a m positions tel que les éléments qui occupent ces postes dans la ligne numéro k de Z_j sont obtenu en multipliant par c_s les éléments qui correspondant dans la ligne numéro l de Z_j et obtenir la matrice ci dessus :

$$A = \left(\begin{array}{c|c|c|c} ... & ... & ..... & ... \\ \hline z_{j,0} & z_{j,1} & ..... & z_{j,q-1} \\ \hline ... & ... & ..... & ... \\ \hline c_0 z_{j,0} & c_1 z_{j,1} & ..... & c_{q-1} z_{j,q-1} \end{array}\right)$$

tel que $z_{j,0}, z_{j,1}, ..., z_{j,q-1}$ sont l vecteurs de longueur m avec des éléments non nulles.

Soit Z_{js} une $k \times m$ matrice tel que $s \in \{0, 1, ..., q-1\}$ est obtenu par prendre les colonnes dans les positions $sm + 1, sm + 2, ...; sm + m$.

Donc , $\forall s \neq w$ alors les colonne de Z_{js} sont linéairement indépendant avec les colonnes de Z_{jw}.

On va répéter la procédure pour chaque $j = 1, 2, ..., \beta$ et on note Z est $k \times m$ la matrice qui a le vecteur u comme un ligne numéro k et nulle par ailleurs .

On obtient la matrice A a prés réorganisation convenable comme ci dessus :

$$A = (Z|Z_{1,0}|Z_{1,1}|...|Z_{1,q-1}|...|Z_{\beta,0}|...|Z_{\beta,q-1})$$

à partir de cette matrice , nous prenons chaque colonne dans la position i est congru à j modulo n tel que j est fixé dans $\{1, 2, ..., m\}$ et $i \in \{1, 2, ..., n\}$ à partir de ces colonnes nous formons la matrice G_j qui contient j colonne de chaque sous matrice Z et $Z_{j,s}$; $j \in \{1, ..., n\}$; $s \in \{0, 1, ..., q-1\}$, donc chaque deux colonne de G_j sont linéairement indépendant , d'où G_j est $k \times \dfrac{q^k - 1}{q - 1}$ matrice de $Hamming$ et A peut être amené sous la forme $(G_1|G_2|...|G_m)$ par une permutation des colonnes.

3.2.2 Application

Exemple 01

On donne $k = 2$, $n = 2^2 - 1 = 3$, $m = 2$, alors $d = 2^{2-1} = 2$ donc :

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

alors :

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

$n' = \dfrac{2(2^2-1)}{2-1} = 6$, $k' = 2$, $d' = (2^{2-1})2 = 4$
après une permutation convenable :

$$G' = \left(\begin{array}{cc|cc|cc} 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right)$$

On va obtenir le code $\mathcal{C}$, $\forall x = (x_1, x_2) \in \mathcal{C}, x.G' \in \mathcal{C}$; alors :

$$(x_1, x_2)\left(\begin{array}{cc|cc|cc} 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right) = (x_2, x_2, x_1 + x_2, x_1 + x_2, x_1, x_1)$$

alors : $\mathcal{C} = \{(000000); (111100); (001111); (110011)\}$

Exemple 02

On donne $k = 2$, $n = \dfrac{3^2-1}{3-1} = \dfrac{8}{2} = 4$, $m = 2$, alors $d = 3^{2-1} = 3$ donc :

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

alors :

$$G = \left(\begin{array}{cccc|cccc} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \end{array}\right)$$

$n' = \dfrac{2(3^2-1)}{3-1} = 8$, $k' = 2$, $d' = (3^{2-1})2 = 6$
après une permutation convenable :

$$G' = \left(\begin{array}{cc|cccc|cc} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 2 & 0 & 0 \end{array}\right)$$

On va obtenir le code $\mathcal{C}$, $\forall x = (x_1, x_2) \in \mathcal{C}, x.G' \in \mathcal{C}$; alors :

$$(x_1, x_2)\left(\begin{array}{cc|cccc|cc} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 2 & 0 & 0 \end{array}\right) = (x_2, x_2, x_1 + x_2, x_1 + 2x_2, x_1 + x_2, x_1 + 2x_2, x_1, x_1)$$

alors :

$$\begin{aligned} \mathcal{C} = \ & \{(00000000); (00111111); (11121200); (11202011); \\ & (11010122); (22020211); (00222222); (22212100); (22101022)\} \end{aligned}$$

Chapitre 4

Permutation de décodage du code simplexe

Dans ce chapitre , on va traiter l'article qui parle sur le décodage du code simplexe par $PD - Sets$ [4]

Définition 4.0.1 *Un code simplexe binaire $\mathcal{S}_n(\mathbb{F}_2)$ est le dual du code de Hamming binaire $\mathcal{H}_n(\mathbb{F}_2)$, alors $\mathcal{S}_n(\mathbb{F}_2)$ est de longueur $2^n - 1$ et de dimension n.*

La matrice génératrice du $\mathcal{S}_n(\mathbb{F}_2)$ est la matrice de contrôle de $\mathcal{H}_n(\mathbb{F}_2)$

Proposition 4.0.1 [4] *Tous les vecteurs non nulles du code simplexe sont de même poids, la valeur commune de leur poids est 2^{n-1} .*

Preuve: Notons H la matrice génératrice de $\mathcal{S}_n(\mathbb{F}_2)$ alors H est la matrice de contrôle de $\mathcal{H}_n(\mathbb{F}_2)$.
Soit $x \in \mathcal{S}_n(\mathbb{F}_2)$ donc, $x = uH$ tel que $x \in \mathbb{F}_2$.
Notons $c_1, c_2, ..., c_n$ les colonnes de H . Alors $x = (uc_1, uc_2, ..., uc_n)$, on sait que les colonnes $c_i \in \mathbb{F}_2^n - \{0\}$ alors :

$$wt(x) = card\{c \in \mathbb{F}_2^n - \{0\}/uc_i \neq 0\},$$

donc : $wt(x) = 2^{n-1}$.

□

$\mathcal{S}_n(\mathbb{F}_2)$ est $[2^n - 1, n, 2^{n-1}]$ code.

Définition 4.0.2 *A sous ensemble des positions de coordonnées d'un code linéaire est appelée un ensemble d'information s'il existe une matrice génératrice pour le code qui est systématique sur les colonnes de ses positions .*

La base canonique de $\mathbb{F}_2^n$ forme un ensemble d'information $\mathcal{I}_n$ pour $\mathcal{S}_n(\mathbb{F}_2)$.

Définition 4.0.3 *Soit C un code corrige t erreurs, avec un ensemble d'information $\mathcal{I}$ et H sa matrice de contrôle ,alors* $\mathbf{PD-ensemble}$ *pour C est une ensemble $\mathcal{S}$ d'automorphisme de C , tel que chaque* $\mathbf{t-ensemble}$ *des positions de coordonnées est déplacé par au moins un élément de $\mathcal{S}$ dans la matrice H.*

Pour $s \leq t$ un $\mathbf{s-PD-ensemble}$ est un ensemble d'automorphisme de C tel que chaque $\mathbf{s-ensemble}$ des positions de coordonnées est déplacé par au moins un élément de $\mathcal{S}$ dans H.

4.1 L'algorithme de permutation de décodage

On a un code $C[n,k,d]$ systématique corrige t erreurs , donc sa matrice génératrice est sous la forme $G[I_k|A]$ alors $H[-A^t|I_{n-k}]$ est sa matrice de contrôle .
Tout vecteurs v de longueur k est codé comme vG, supposons x est envoyé et y est reçu au maximum t erreur.
Soit $\mathcal{S} = \{g_1, g_2, ..., g_s\}$ est $\mathbf{PD-ensembles}$ calculons les syndromes $H(yg_i)^t$ pour
$i = 1, ..., s$, jusqu'à trouver un i tel que le poids de ce vecteur est au maximum t.
calculons le mots de code c qui possède le même symbole d'information comme yg_i et décoder y comme cg_i^{-1} .
Notez que cet algorithme utilise en fait le $\mathbf{PD-ensemble}$ comme une séquence ; ainsi , il est à propos d'indexer les élément de l'ensemble $\mathcal{S}$ par l'ensemble $\{1, 2, ..., |\mathcal{S}|\}$ de sorte que les éléments qui corrigera un petit nombre d'erreurs se produisent d'abord.
Ainsi , si $\mathbf{s-PD-ensembles}$ se trouvent imbriquées pour tous $1 < s \leq t$, alors nous pouvons commander $\mathcal{S}$ comme suit :
Trouver un $\mathbf{s-PD-ensembles}$ $\mathcal{S}$ pour chaque $0 < s \leq t$, tel que le $\mathbf{PD-ensembles}$ $\mathcal{S}$ comme une séquence dans cet ordre :

$$\mathcal{S} = [\mathcal{S}_0, (\mathcal{S}_1 - \mathcal{S}_0), (\mathcal{S}_2 - \mathcal{S}_1), ..., (\mathcal{S}_t - \mathcal{S}_{t-1})].$$

Exemple

Soit $\mathcal{S}_3(\mathbb{F}_2)$ un code de longueur 7 de matrice génératrice
$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$; alors par une permutation convenable : $1 \longmapsto 3$; $3 \longmapsto 4$; $4 \longmapsto 1$; $2 \longmapsto 2$; $5 \longmapsto 5$; $6 \longmapsto 6$; $7 \longmapsto 7$; on a :

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

alors $H = \left(\begin{array}{ccc|cccc} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$.
On va calculer les syndromes :

leader	0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
syndrome	(0000)	(0111)	(1011)	(1101)	(1000)	(0100)	(0010)	(0001)

Soit $y(1111100)$ un mot reçu

$$S(y) = yH^T = (1111100)\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = (1101),$$

$x = y - u_i$ alors $x = (1111100) - (001000) = (1101100)$

alors $c = (1101)$

Exemple

Soit $\mathcal{S}_4(\mathbb{F}_2)$ un code de longueur 15 de matrice génératrice
$G = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$;
alors par une permutation convenable :
$G' = \left(\begin{array}{cccc|ccccccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right)$;

Donc : $H = \left(\begin{array}{cccc|cccccccccccc} 1&1&1&1&1&0&0&0&0&0&0&0&0&0&0 \\ 1&0&1&1&0&1&0&0&0&0&0&0&0&0&0 \\ 1&1&0&1&0&0&1&0&0&0&0&0&0&0&0 \\ 1&1&1&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&1&1&1&0&0&0&0&1&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0&0&0&1&0&0&0&0 \\ 1&0&0&1&0&0&0&0&0&0&0&1&0&0&0 \\ 0&1&0&1&0&0&0&0&0&0&0&0&1&0&0 \\ 0&1&1&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&1&1&0&0&0&0&0&0&0&0&0&0&1 \end{array}\right)$;

Soit $\mathcal{S} = \{g_1, g_2, ..., g_s\}$ **PD − ensemble** tel que g_i est automorphismes de C représente des permutation des positions de coordonnée.

Supposons x est envoyé et y est reçu au maximum t erreur.

Alors on va calculer les syndromes $H(yg_i)^t$ pour $i = 1, 2, ..., s$, jusqu'à trouver un i tel que le poids de ce vecteur est au maximum t.

calculons le mots de code c qui possède le même symbole d'information comme yg_i et décoder y comme cg_i^{-1} .

Évidemment, il est plus compliqué pour $n > 4$.

Résultat

Si $\mathcal{S}$ est un **PD − ensembles** pour un code $C[n, k, d]$ corrige t erreurs et $r = n - k$:

$$|\mathcal{S}| \geq \lceil \frac{n}{r} \lceil \frac{n-1}{r-1} \lceil ... \lceil \frac{n-t+1}{r-t+1} \rceil ... \rceil \rceil \rceil \quad borne\ de\ Gorden - Schonheim$$

Cet résultat peut être adapté pour **s − PD − ensembles** tel que $s \leq t$ remplaçant de t dans la formule précédente.

4.2 s − PD − ensembles de cardinal $s+1$ pour $\mathcal{S}_n(\mathbb{F}_2)$

On va montrer comment trouver **s − PD − ensembles** pour $\mathcal{S}_n(\mathbb{F}_2)$ tel que satisfait la borne de $Gorden - Schonheim$ pour **s − PD − ensembles**.

On a $\mathcal{S}_n = [2^n - 1, n, 2^{n-1}]$, et $\mathcal{I}_n = \{e_1, e_2, ..., e_n\}$ l'ensemble d'information tel que $\mathcal{I}_n$ est l'ensemble d'élément du base canonique de $\mathbb{F}_2^n$.

La matrice génératrice de $\mathcal{S}_n$ a $2^n - 1$ non null vecteurs de $\mathbb{F}_2^n$, avec les éléments e_i^t de la base

canonique dans n premières positions alors : $G = [I_n|A]$.

On a $Aut(\mathcal{S}_n) = GL_n(\mathbb{F}_2)$, $GL_n(\mathbb{F}_2)$ groupe linéaire, on va écrire les vecteurs sous la forme vecteurs ligne, ainsi vA est l'image du vecteur v ou $A \in GL_n(\mathbb{F}_2)$, et pour toute A la permutation résultant des positions de coordonnées donne un automorphisme du code $\mathcal{S}_n$.

On va regarder à ce borne pour $\mathcal{S}_n$, tel que $n \geq 4$, car $\mathcal{S}_3$ corrige un seul erreur donc la permutation de décodage n'est pas nécessaire .

Posons :

$$g_n(t) = \lceil \frac{n}{r} \lceil \frac{n-1}{r-1} \lceil ... \lceil \frac{n-t+1}{r-t+1} \rceil ... \rceil \rceil \rceil.$$

Lemme 4.2.1 [4] *Pour le code simplexe binaire $\mathcal{S}_n$ et $n \geq 4$, $1 \leq s \leq t = 2^{n-2} - 1$.*

$$g_n(s) = \lceil \frac{2^n - 1}{2^n - 1 - n} \lceil \frac{2^n - 2}{2^n - 2 - n} \lceil ... \lceil \frac{2^n - s}{2^n - s - n} \rceil ... \rceil \rceil \rceil \geq s + 1.$$

En particulier : $g_n(1) = 2$, $g_n(2) = 3$, $\forall n \geq 4$.

Preuve: Le plus profond terme dans la formule pour la borne est $\lceil \frac{2^n - s}{2^n - s - n} \rceil$.

Il est claire qu'il est la valeur égal à 2 pour $n \geq 4$, $1 \leq s \leq t$, à chaque étape de la calcul du plafond, à partir de la plus interne , la fraction est supérieur à 1 , de sorte que la durée augmente en valeur au moins 1.

Donc : $g_n(s) \geq s + 1$. □

Définition 4.2.1 *Pour $\mathcal{S}_n, n \geq 4$;*

$$f_n = max\{s/2 \leq s, g_n(s) = s + 1\}.$$

Lemme 4.2.2 [4] $\forall n \geq 4$ *:*

$$f_n = \lceil \frac{2^n - 1}{n} \rceil - 1.$$

Preuve: Il y a s étapes dans le calcul de la formule de l'équation du lemme 4.2.1.
On a $\lceil \frac{2^n - s}{2^n - s - n} \rceil = 2$. Ainsi, nous devons veiller qu'a chaque étape de travail à partir de l'intérieur, l'augmentation est 1.

Alors :

$$\begin{aligned}
\lceil \frac{2^n - (s-1)}{2^n - (s-1) - n} \lceil \frac{2^n - s}{2^n - s - n} \rceil \rceil &= \lceil 2. \frac{2^n - s + 1}{2^n - s + 1 - n} \rceil \\
&= \lceil \frac{2.2^n - 2s + 2}{2^n - s + 1 - n} \rceil \\
&= \lceil \frac{2.2^n - 2s + 2 - 2n + 2n}{2^n - s + 1 - n} \rceil \\
&= \lceil \frac{2.(2^n - s + 1 - n)}{2^n - s + 1 - n} + \frac{2n}{2^n - s + 1 - n} \rceil \\
&= \lceil 2 + \frac{2n}{2^n - s + 1 - n} \rceil = 3
\end{aligned}$$

alors :

$$\frac{2n}{2^n - s + 1 - n} \leq 1,$$

donc :

$$2n \leq 2^n - s + 1 - n,$$

donc :

$$s \leq 2^n - 3n + 1$$

Pour le terme suivant "le troisième terme" on obtient : $s \leq 2^n - 4n + 2$.

Pour le l ème terme : $s \leq 2^n - (l+1)n + l - 1$.

Ainsi pour $l = s$:

$$s \leq 2^n - (s+1)n + s - 1,$$

donc

$$s + ns - s \leq 2^n - n - 1,$$

donc

$$s \leq \lceil \frac{2^n - 1}{n} \rceil - 1.$$

Alors on a $s \leq 2^n - (l+1)n + l - 1 = 2^n - ((l+1)n - (l+1) + 2)$.

On a $(l+1)n - (l+1) + 2 \geq ln - l + 2, \forall n \geq 1$.

La borne précédente $(l-1)$ ème sera également satisfaite alors :

$$f_n = max\{s/2 \leq s, g_n(s) = s+1\} = \lceil \frac{2^n - 1}{n} \rceil - 1.$$

□

Alors pour quelque soit $s \leq f_n$ un $\mathbf{s - PD - ensemble}$ de taille $s+1$ rencontrera la borne de $Gorden - Schonhein$ pour la correction des s erreurs, nous allons trouver des conditions sur des ensembles de matrices de $GL_n(\mathbb{F}_2)$.

Proposition 4.2.1 [4] *Soit $C = \mathcal{S}_n, \forall n \geq 4$, avec d'ensemble d'information $\mathcal{I}_n$,et ensemble de contrôle $\mathcal{C}_n$.*

Si $P_k = \{M_i/0 \leq i < k\}$ est un ensemble de $k+1$ matrices dans $GL_n(\mathbb{F}_2)$ tel que : $\forall M_i^{-1}, M_j^{-1}, i \neq j$ n'ont pas une rangée en commun.

Ainsi P_k est un $\mathbf{k - PD - ensemble}$ de $k+1$ élément pour C. De plus, tous sous ensemble de P_k de taille $s+1$, $1 \leq s \leq k$ est un $\mathbf{k - PD - ensemble}$ pour C .

Inversement si $R_k = \{N_i/0 \leq i < k\}$ est un $\mathbf{k - PD - ensemble}$ pour C donc il n'y a pas deux matrices N_i^{-1}, N_j^{-1} tel que $i \neq j$ ont un ligne en commun.

Preuve: Supposons $P_k = \{M_i/0 \leq i < k\}$ tel que $\forall i \neq j$, M_i^{-1} et M_j^{-1} n'ont pas un rangée en commun .

Soit $T = \{v_1, ..., v_k\}$ un ensemble de k vecteurs distinct dans $\mathbb{F}_2^n$.

Supposons que ne pouvons pas faire plonger T dans $\mathcal{C}_n$ par n'importe élément de P_k.

Ainsi $\forall i, 0 \leq i \leq k$, il y a $v_j, 1 \leq j \leq k$, tel que : $v_j M_i \in \mathcal{I}_n$, comme i a $k+1$ valeurs et j a k valeurs, alors on a $v_j M_i$ et $v_j M_l$, tel que pour $j, i \neq l$, ont le même poids égale à 1.

Supposons que $v_j M_i = e_r$ et $v_j M_l = e_i$, alors : $v_j = e_r M_i^{-1} = e_t M_l^{-1}$, la rangée numéro r dans M_i^{-1} égale à la rangée numéro t dans M_l^{-1} ; contradiction.

La réciproque :

Soit $R_k = \{N_i/0 \leq i < k\}$ une $\mathbf{k - PD - ensemble}$ pour C et soit $v \in \mathbb{F}_2^n$ est la colonne numéro r dans N_i^{-1} et v la colonne numéro t dans N_j^{-1}, donc :

$v = e_r N_i^{-1} = e_t N_j^{-1}$, alors : $vN_i = e_r$, $vN_j = e_t$.

Soit $J = \{m/0 \leq m \leq k; m \neq i, j\}$ pour chaque $m \in J$, nous choisissons une colonne v_m de

N_m^{-1}, on a une ensemble a au moins $k-1$ vecteurs v_m tel que $v_m N_m = e_t$, et donc $v_m N_m$ de poids égale à 1 .

L'ensemble $T = \{v_m/m \in J\} \cup \{v\}$ est de cardinal k, mais il n'y a pas du matrice dans R_k permettra de faire un plan de chaque éléments de T dans $\mathcal{C}_n$. contradiction avec l'hypothèse que R_k est un $\mathbf{k-PD-ensemble}$.

L'état des sous ensembles de P_k de cardinal $s+1$ est évidement car il est le même cas pour k

□

Corollaire 4.2.1 [4] $\forall n \geq 4$ *si* P_k *est de cardinal* $k+1$ *est un* $\mathbf{k-PD-ensemble}$ *pour* $\mathcal{S}_n$ *avec* $\mathcal{I}_n$ *ensemble d'information, alors n'importe quel ordre des éléments de* P_k *donne* $\mathbf{s-PD-ensemble}$ *imbriquées ;* $1 \leq s \leq k$.

On peux ordonner les éléments de P_k arbitrairement comme $[M_{i_0}, ..., M_{i_k}]$ s'il n'y a pas une erreur détecté , M_{i_0} sera décoder ; si une erreur a détecté , alors M_{i_0} et M_{i_1} seront décodé, si on a trois erreurs détecté , l'une des trois première décode, pour s erreurs des $s+1$ premières effectue le décodage.

Ainsi, les erreurs qui se produisent moins " ce qui est supposé pour un bon canal" , le plus tôt sera le vecteur sera décodé.

Corollaire 4.2.2 [4] $\forall n \geq 4$ *un c de* $k+1$ *éléments de* $GL_n(\mathbb{F}_2)$ *pour* $\mathcal{S}_n$ *avec ensemble d'information* $\mathcal{I}_n$ *doit satisfaire :*

$$k \leq \lceil \frac{2^n - 1}{n} \rceil - 1.$$

Preuve: On a de proposition 4.2.1 le $\mathbf{k-PD-ensemble}$ de $k+1$ matrices aura pour l'ensemble de ses inverses, $k+1$ matrices avec aucune ligne se produisant deux fois, ainsi, en comptant les lignes que nous avoir :

$$(k+1)n \leq 2^n - 1,$$

$$kn \leq 2^n - n - 1,$$

$$k \leq \lceil \frac{2^n - 1}{n} \rceil - 1$$

□

Définition 4.2.2 *Soit un code C a un ensemble P de coordination, un ensemble $\mathcal{L}$ d'information de C est appelé t-informations antiblocage système " t-AI-système" si $\forall t$ ensemble $T \subset P$, il y' a $B \in \mathcal{L}$ tel que $B \cap T = \Phi$.*

Corollaire 4.2.3 [4] *Supposons $n \geq 4$ et $Q_k = \{N_i / 0 \leq i \leq k\}$ tel que $k \geq 1$ est un ensemble de $k+1$ matrices dans $GL_n(\mathbb{F}_{\not=})$ tel que $\forall i \neq jN8I, N_j$ n'ont pas un ligne en commun.*
Si R_i est un ensemble des lignes de N_i pour $0 \leq i \leq k$ l'ensemble $\mathfrak{D} = \{R_i / 0 \leq i \leq k\}$ est un $k-$ informations antiblocage système de taille $k+1$ pour $\mathcal{S}_n$.
Inversement :
$\forall k$ antiblocage information système $\mathfrak{L} = \{A_i / 0 \leq i < k\}$ pour $\mathcal{S}_n$ de $k+1$ éléments doit avoir la propriété $A_i \cap A_j = \Phi, \forall i \neq j$.

Preuve: De la proposition 4.2.1 on a : $P_k = \{N_i^{-1} / 0 \leq i \leq k\}$ est un $\mathbf{k - PD - ensemble}$ pour ensemble d'information $\mathcal{I}_n$, alors $\forall k-$ ensemble des vecteurs $T = \{v_i / 1 \leq i \leq k\}$ il y a N_i^{-1} tel que $v_j N_i^{-1} \in \mathcal{C}_n, \forall 1 \leq j \leq k$, alors $T \cap R_i = \Phi$. Donc $\mathfrak{D}$ est un $k-$ informations antiblocage système pour $\mathcal{S}_n$.
Inversement :
Soit un $k - AI$ système $\mathfrak{L} = \{A_i / 0 \leq i \leq k\}$ de $k+1$ éléments pour $\mathcal{S}_n$.
Le preuve qu'il n'y a pas un vecteur en commun de deux éléments de $\mathfrak{D}$ est dans la preuve de la proposition 4.2.1 , comme quelque soit A_i contient n vecteurs forment un base pour $\mathbb{F}_2^n$, ainsi définir une matrice inversible .

□

En effet, on prend $M_0 = I_n$, pour obtenir une cas d'aucune erreur.
Pour ce cas on définit :

$$A_n = \{M / M \in GL_n(\mathbb{F}_2) / tout \ \ les \ ligne \ de \ M \ \ ont \ \ poids \ \ au \ \ moins \ \ egal \ \ 2\}.$$

Proposition 4.2.2 [4] *Soit C un code simplexe $\mathcal{S}_n$, tel que $n \geq 4$,d'ensemble d'information $\mathcal{I}_n$ d'ensemble de contrôle $\mathcal{C}_n$ .Si $P_k = \{M_0 = I_n, M_1, ..., M_k\}$ est un ensemble de $k+1$ matrice dans $GL_n(\mathbb{F}_2)$ tel que chaque pair $(i,j), i \neq j; M_i^{-1}M_j \in A_n$, alors P_k est un* **$\mathbf{k-PD-ensemble}$** *de $k+1$ élément pour C.*

Preuve: On remarque $M \in A_n \Longleftrightarrow M^{-1} \in A_n$

Supposons que $M \in A_n$, si M^{-1} a un ligne de poids égale à 1 soit e_j dans la i ème colonne, de $I_n = M^{-1}M$ est le j ème ligne de M, contradiction car M a les vecteurs ligne ont poids au minimum égale à 2 donc $M^{-1} \in A_n$.

Supposons que $M_i = M_0^{-1}M_i \in A_n; \forall i \geq 1$, on va montrer que les lignes de M_i^{-1} et M_j^{-1} tel que $i \neq j$ sont distinct.

Il est claire que les lignes de $M_i^{-1}, \forall i \geq 1$ sont distinct à de I_n, supposons que M_i^{-1} et M_j^{-1} tel que $0 \neq i \neq j \neq 0$, alors $v = e_r M_i^{-1} = e_s M_j^{-1}$ pour certain r, s donc : $vM_j = e_r M_i^{-1} M_j = e_s$; contradiction car $M_i^{-1}M_j \in A$, donc par la proposition 4.2.1 P_k est un $\mathbf{k-PD-ensemble}$ de $k+1$ éléments.

□

Maintenant on va montrer comment construire $\mathbf{s-PD-ensemble}$.

Définition 4.2.3 $\forall M \in GL_n(\mathbb{F}_2), M = [m_{ij}]$ *et* $u = (u_1, ..., u_n) \in \mathbb{F}_2^n; u \neq 0$.

Soit $M(u) = [a_{ij}]$ une matrice de $(n+1) \times (n+1)$ tel que :

$a_{11} = 1, a_{1;1+i} = u_i, \forall i, 1 \leq i \leq n, a_{i1} = 0, \forall i, 2 \leq i \leq n+1, a_{i+1;j+1} = m_{ij}, \forall i \geq 1; j \leq n.$

tel que :

$$M(u) = \left(\begin{array}{c|ccc} 1 & u_1 & ... & u_n \\ \hline 0 & & & \\ \vdots & & M & \\ 0 & & & \end{array}\right)$$

Exemple

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, u = (1,0,0,0) = e_1, \text{ alors : } M(u) = \left(\begin{array}{c|cccc} 1 & 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right)$$

Résultat

Si $Q_k = \{A_i / 0 \leq i \leq k\}$ est un ensemble des matrices dans $GL_n(\mathbb{F}_2)$ tel que les lignes de A_i sont distinct de celle $A_j, \forall i \neq j$, alors si $u_0, u_1, ..., u_k$ des vecteurs distincts dans $\mathbb{F}_2^n$.
L'ensemble $Q_k^* = \{A_i(u_i) / 0 \leq i \leq k\}$ est l'ensemble des matrices dans $GL_{n+1}(\mathbb{F}_2)$ avec les mêmes propriétés.
Pour trouver $\mathbf{k-PD-ensemble}$ de $k+1$ élément, on va trouver $k+1$ matrices $n \times n$ avec aucun ligne en commun ,*i.e.* $k+1$ ensembles de base deux à deux disjoints de $\mathbb{F}_2^n$.

Proposition 4.2.3 [4] *Si :*
$N_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$, $N_2 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$;
alors $P_3 = \{I_4, N_1^{-1}, N_2^{-1}\}$ *est* $\mathbf{2-PD-ensemble}$ *pour* $\mathcal{S}_4$ *si* $(N_1)_1 = N_1(e_1); (N_2)_1 = N_2(e_2)$ *; par récurrence* $(N_1)_r = (N_1)_{r-1}(e_1)$, $(N_2)_r = (N_2)_{r-1}(e_2), \forall r \geq 2$, *ou* e_1, e_2 *deux élément de la base canonique,*

$$\forall n \geq 5, P_3(n) = \{I_n, (N_1)_{n-4}^{-1}, (N_2)_{n-4}^{-1}\}$$

est un $\mathbf{2-PD-ensemble}$ *pour* $\mathcal{S}_n$.

Preuve: N_1, N_2 satisfont les conditions de la propositions 4.2.2, alors par la proposition 4.2.1 est $\mathbf{2-PD-ensemble}$ donc elle est correct pour $P_3(n), \forall n \geq 5$. □

Remarque 4.2.1 *La troisième matrice* N_2 *n'existe pas si les deux première matrice sont :* I_4 *et* $N_1 = I_4 + J$ *tel que* J *est la matrice ou tous ses éléments égale à* 1, *puis que tous les vecteurs restants sont de même poids et donc il y a au plus trois en un ensemble linéairement indépendant.*

Exemple

Dans la proposition 4.2.3 , $n = 6$,

$$N_1(e_1) = \left(\begin{array}{c|c|cccc} 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right), \; N_2(e_2) = \left(\begin{array}{c|c|cccc} 1 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right).$$

Corollaire 4.2.4 [4] $\forall n \geq 4$, *si* $\mathbf{k-PD-ensemble}$ *de* $k+1$ *matrices pour* $\mathcal{S}_n$, *avec un ensemble d'information* $\mathcal{I}_n$, *on peux trouver un* $\mathbf{k-PD-ensemble}$ *de* $k+1$ *matrices pour* $\mathcal{S}_m$, *avec un ensemble d'information* $\mathcal{I}_m$, $\forall m \geq n$.

Preuve: Soit $P_k = \{M_i / 0 \leq i \leq k\}$ un $\mathbf{k-PD-ensemble}$ pour $\mathcal{S}_n$.

Soit $N_i = M_i^{-1}, \forall i = 0, ..., k$, supposons que $\{u_i / 0 \leq i \leq k\}$ un ensemble de $k+1$ vecteurs distincts dans $\mathbb{F}_2^n$.

Depuis k généralement est $t = 2^{n-2} - 1$, tous les membres $i \leq k$ ont un représentation binaire non nuls dans les $n-1$premiers positions " le plus à gauche" .

Depuis la proposition 4.2.3 par récurrence $\forall r \geq 1$, on ajoutons 0 à la fin de chaque u_i à chaque étape $(N_i)_1 = N_i(u_i)$, $(N_i)_r = (N_i)_{r-1}(u_i)$ pour chaque i tel que $0 \leq i \leq k$ et $1 \leq r \leq m$, donc pour chaque $m > n$;

$$Q_k = \{(N_0)^{-1}_{m-n}, (N_1)^{-1}_{m-n}, ..., (N_k)^{-1}_{m-n}\}.$$

est un $\mathbf{k-PD-ensemble}$ imbriquée de $k+1$ éléments pour $\mathcal{S}_m$, avec ensemble d'information $\mathcal{I}_m$. □

Bibliographie

[1] P.S.Alexandroff, *Introduction A la Theorie Des Groupes* , Dunod, Paris, 1968.

[2] J.H.Van Lint, *Introduction to Coding Theory*, Springer ; 1999.

[3] Lan.F.Blake, Ronald C.Mullin, *The Mathematical Theory Of Coding* , Academic Press, 1975.

[4] Washiel Fish , Jennifer .D.Key, Eric Mwambene, *Partial Permutation Decoding For Simplex Codes*, Advences in Mathematics of Communication, Volume 6,NO ,4 , 2012 ; 505-516.

[5] D.G.Hoffman, *Linear Codes And Weights*, Australasian Journal of Combinatorics 7(1993), PP 37-45.

[6] Arrigo Bonisoli, *Every equidistant linear code is a sequence of dual Hamming codes*, Ars Combin. 18 (1984), 181-186.

[7] Nuh Ayden, *An Introduction To Coding Theory Via Hamming Codes*, NSF CCLI Grant , 2007.

[8] Todd K .Moon, *Error Correction Coding* , Wiley, 2005.

[9] R.Micheloni, A.Marelli, R.Ravasion, *Error Correcting Codes* , North Holland Publishing , 1981.

[10] F.J.Mac Williams , N.J.A.Sloane, *The Theory Of Error Correcting Codes*, North Holland Publishing, 1981.

[11] Robert H.Morelos-Zaragoza , *The Art Of Error Correcting Coding*, Second Edition , J.Wiley,Sons LTD, 2006.

[12] M.Deza, *Une Propriete Extermale Des Plans Projectifs Finis Dans Une Classe De Codes Equidistants* , Discrete Mathematics, 6(1973)-343-352.

[13] Tor Helleseth , H.F.Mattson Jr, *On The Coset Of The Simplex Code* , Discrete Ma-

thematics 56(1985)169-189.

[14] Hans-Joachim Kroll , Rita Vincenti, *PD− Sets For The Codes Related To Some Classical Varieties*, Discrete Mathematics301(2005)p 89-105.

[15] J.D. Key , P. Seneviratine, *Codes From The Line Graphs Of Complete Multipartite Graphs And PD− Sets* , Discrete Mathematics307(2007)p 2217-2225.

[16] Hans-Joachim Kroll, Rita Vincenti, *Antiblocking systems and PD− Sets* , Discrete Mathematics 308 (2008) 401 - 407.

[17] J.H.Van.Lint , *A Theorem On Equidistant Codes* , Discrete Mathematics6(1973)353-358.

[18] BENLARBI-DELAI M'HAMMED, JABBOURI ELMOSTAFA, LBEKOURRI ABOUBAKR, *Module Mathematiques II Cours d'Algebre II*, Universit´e Mohammed V-Agdal Facult´e des Sciences,2007.

[19] Jay A. Wood, *Understanding Linear Codes of Constant Weight Using Virtual Linear Codes* , Department of Mathematics and Statistics Western Michigan University.

[20] Jessy Mac Williams , *Permutation Decoding Of Systematic Codes* , The Bell System Technical Journal,1964.

[21] H.J.Landau, David Slepian,*On the Optimality Of The Regular Simplex Code*, The Bell System Technical Journal 1966.

[22] Claude Carlet, *Cours de Codes Correcteurs d'Erreurs* , thèse D E A,Bamako, 2007.

[23] Pierre Abbrugiati, *Introduction Aux Codes Correcteurs* , thèse, 2006.

[24] Odile Papini, *Introduction A La Theorie Des Codes Correcteurs D'erreurs* http ://odile.papini.perso.esil.univmed.fr/sources/CODAGE.html.

[25] Bruno Deschamps, *Groupes, Anneaux et Arithmetique* ,Le Mans 2006/2007.

[26] Navid Azizi, *Decoding The Binary Hamming Codes* , February 19, 2003.

[27] James Fiedler, *Hamming Codes* , Fall, 2004.

[28] Yunghsiang S. Han,*Introduction To Binary Linear Block Codes* , Graduate Institute of Communication Engineering, National Taipei University ,Taiwan.

[29] Atri Rudra, *Plotkin Bound* , Error Correcting Codes : Combinatorics, Algorithms And Applications , 2007.

[30] Atri Rudra, *Proof of A Geometric Lemma* , Error Correcting Codes : Combinatorics, Algorithms And Applications , 2007.

[31] Jay A. Wood, *The Structure Of Linear Codes Of Constant Weight* , Transactions Of The American Mathematical Society, Volume 354, Number 3, Pages 1007-1026.

Conclusion

Dans ce travail, on a présenté des notions sur les codes linéaires, les codes équidistants spécifiquement les codes simplexes.
On a indiqué comment décoder les codes simplexes par un logarithme qui a nous montré l'importance de ces codes.
Nous espérons que nous avons fourni un simple aperçu autour les codes simplexes du fait que la théorie des codes a été découvert récemment par rapport à d'autres théorie.

Mots clés

Code de Hamming, orthogonal, décodage, poids.

Résumé

Les télécommunications sont devenues indispensables dans notre vie quotidienne, cet échange numérique d'informations se fait par le biais de canaux de communication comme le câble, la fibre optique, le wifi, les satellites ...etc.
Ces canaux ne sont pas tous fiable 100%. la théorie des codes correcteurs d'erreurs s'est développée pour répondre à ce genre de problème.
Le premier chapitre de ce mémoire est consacré aux notions fondamentales d'algèbre .
aux deuxième chapitre on introduit la notion de codes " code linéaire, code de Hamming, matrice génératrice, matrice de contrôle, l'encodage et le décodage par syndrome.
Dans le troisième chapitre on donne une caractérisation des codes équidistants.
Le dernier chapitre est consacré au décodage des codes simplexes en utilisant un algorithme de permutation de décodage.

Abstract

Telecommunications have become indispensable in our daily life, this digital exchange of information is done through communication channels such as cable, optical fiber, wireless, satellites...

These channels are not all reliable 100%. the theory of error correcting codes was developed to meet this kind of problem.

The first chapter of this thesis is devoted to the fundamentals of algebra. the second chapter the concept of codes "linear code is introduced, Hamming code, generator matrix, matrix control, encoding and decoding syndrome. In the third chapter we give a characterization of equidistant codes. The last chapter is devoted to decoding the codes using a simplex algorithm permutation decoding.

ملخص

اصبحت الاتصَالَات السلكية و اللَاسلكية لَا غنَى عنهَا في حيَاتنَا اليومية، و يَتِم هَذَا التبَادل الرقمي لِلمعلومَات من خلَال قنوَات الَاتصَال مثل الكَابل و الَاليَاف البَصرية الويفي و الَاقمَار الَاصطنَاعية.

هذه القنوَات ليست دقيقة 100% . و بَالتَالي نظرية الترميز المصحِحة لِلَاخطَاء اكتشفت لتصحيح مثل هذه المشَاكل.

في الفصل الأول تطرقنَا لمفَاهيم اسَاسية في الجبر.

في الفصل الثَاني قمنَا بتعريف الترميز ، ترميز الخطي ، ترميز $Hamming$ ، مفهوم المصفوفة المولدة، اَلترميز و فك الترميز بوَاسطة جدول خَاص .

في الفصل الثَالث قمنَا بأعطَاء فكرة عن الترميز الذي يمتَاز بخَاصية تسَاوي المسَافة.

اخيرًا قدمنَا خوَارزمية لفك الترميز المبسط .