الجمهورية الجزائرية الديموقراطية الشعبية
PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
وزارة التعليم العالي و البحث العلمي
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
جامعة عبّاس لغرور خنشلة
ABBAS LAGHROUR-KHENCHELA UNIVERSITY
Faculty Of Sciences And Technology
Department of Mathematics and Computer Science

N^o de série :.....

Mémoire de fin d'étude

Pour l'obtention de diplome de **Master Mathématiques**

Filière :**Mathématique**

Spécialité :**Mathématique Appliquée**

Intitulé par :

Sur les codes quasi-cycliques

Réalisé Par :MALKI Walid **Dirigé par :Mr.SAHRAOUI Alaeddine**

BOUMAARAF Abdelaziz

Membres de jury :
Mr MEFTAH Yacine Président
Mr BAHRI Boubakeur Examinateur

Année universitaire 2020/2021

Remerciement

Nous remercions vivement notre encadreur, Mr Sahraoui Ala Eddine , pour nous avoir proposé ce sujet d'actualité assez passionnant ; sa patience et son organisation nous ont permis de surmonter de nombreuses difficultés liées à ce travail.

Nous tenons à lui exprimer nos sincères déférences pour son encadrement.

A monsieur le président du jury Mr MEFTAH Yacine .

A messieurs le membre du jury Mr BAHRI Boubakeur.

d'avoir accepté d'évaluer notre travail, veillez trouver ici le témoignage de notre gratitude et de notre profond respect.

Merci également à tous ceux qui ont contribué à notre formation spirituelle.

Nous tenons aussi à remercier toute l'équipe pédagogique pour nous avoir transmis leur savoir tout au long de notre cycle d'étude.

Notation

p : un nombre premier.

$\mathbb{F}_p$: le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

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

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

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

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

$\mathcal{C}_n(\mathbb{F}_2)$: Code cyclique.

G : matrice génératrice .

H : matrice de contrôle.

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

$supp(v)$ support de vecteur.

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

$d(\mathcal{C})$: distance minimale du code $\mathcal{C}$.

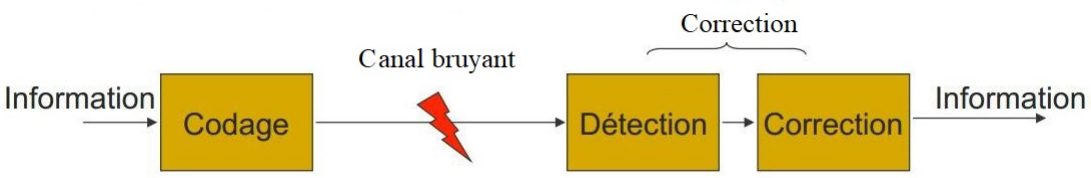
e : nombre d'erreur.

$\mathcal{M}_n(\mathbb{K})$: l'espace des matrices carrées.

$Irr(\xi_1)$ polynôme irréductible de racine ξ_1.

Introduction

La naissance de la théorie de l'information et de la théorie de codage est fondu par l'article de Claude Shannon de 1948 intitulé « A Mathematical Theory of Communication ». L'objectif principal de ces disciplines est le transfert efficace d'informations fiables. Pour être efficace, le transfert d'informations ne doit pas nécessiter beaucoup de temps et d'efforts. Pour être fiables, les données transmises et reçues doivent se ressembler. Cependant, lors de la transmission sur un canal bruyant, les informations seront endommagées. Ainsi, il est devenu nécessaire de développer des moyens de détecter quand une erreur s'est produite et de la corriger. Par exemple, on peut penser à la transmission de photos satellites prises dans l'espace et renvoyées vers la terre.



L'étude de notre présent mémoire est organisée en 3 chapitres. Le premier chapitre se consiste aux notions fondamental d'algèbre en générale, ensuite le deuxième qui décrit les codes en blocs en générale et des exemples de ces codes qui existent avec leurs principes de codage et décodage surtout les code cycliques, et enfin, Dans le troisième chapitre on donne une caractérisation des codes quasi-cycliques, une définition générale et des propriétés sur ces codes.

Table des matières

Chapitre 1

Notions fondamentales d'algèbre

1.1 Groupes

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

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

$(G\,;*)$ est un groupe si et seulement si :

- *$*$ est associative ie $\forall a,b,c \in G$: $(\ a * b\ ) * c = a * (b * c)$.*
- *G possède un élément neutre e pour $*$ tel que $\forall a \in G\ a * e = e * a = a$.*
- *tout élément $a \in G$ a un inverse $b \in G$ tel que $a * b = b * a = e$;*
  on note $b = a^{-1}$ pour la multiplication et $b = -a$ pour l'addition.

Un groupe $(G\,;*)$ s'appelle abélien si l'opération $*$ commutative :

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

Exemple

- $(\mathbb{N}\,;+\,)$ et $(\mathbb{N}\,;\,.\,)$ ne sont pas des groupes car l'opposé et l'inverse d'un nombre naturel ne sont pas des nombres naturels ;
- $(\mathbb{Z}\,;+)$, $(\mathbb{Q}\,;+)$, $(\mathbb{R}\,;+)$ et $(\mathbb{C}\,;+)$ sont des groupes abéliens avec 0 comme l'élément neutre ;
- Si on note $\mathbb{Z}^* = \mathbb{Z}\diagdown\{0\}$ (et même chose pour $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$), l'ensemble $(\mathbb{Z}^*\,;\,.\,)$ n'est pas un groupe, alors que $(\mathbb{Q}^*\,;\,.\,)$,$(\mathbb{R}^*\,;\,.\,)$ et $(\mathbb{C}^*\,;\,.\,)$ sont des groupes abéliens avec 1 comme l'élément neutre.
- $(\mathbb{Q}\,;\,.\,)$, $(\mathbb{R}\,;\,.\,)$ et $(\mathbb{C}\,;\,.\,)$ ne sont pas des groupes car 0 n'est pas inversible.

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 (.).

1.1.1 Sous-Groupes

Définition 1.1.2 *Soit $H \subseteq G$ un sous-ensemble. On dit que H est un sous-groupe de G lorsque les deux conditions suivantes sont vérifiées :*
i) H est stable pour la loi : (ce qui signifie $a.b \in H$ pour tous a ; $b \in H$),
ii) H est stable par passage à l'inverse (ce qui signifie $a^{-1} \in H$ pour tout $a \in H$).
On notera $H < G$ Dans ce cas, la restriction la loi . de G dans H définit une loi de composition interne dans H, pour laquelle H est lui-même un groupe.

Les conditions *i* et *ii* sont évidemment équivalentes à l'unique condition :
$a, b \in H \Rightarrow a.b^{-1} \in H$.
Exemple
$(2\mathbb{Z}, +) < (\mathbb{Z}, +)$, en générale les sous groupes additifs de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}, n \in \mathbb{N}$.

1.1.2 Sous-groupe engendré par une partie

Définition 1.1.3 *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 1.1.4 *Un groupe G est monogène si G admet un unique générateur $a \in G$ $.i.e, G = \langle a \rangle$,*
de plus G est fini alors G est cyclique.

1.1.3 Homomorphismes, Isomorphismes de groupes

Proposition 1.1.1 *Une application $f : G \longrightarrow G'$ d'un groupe G dans un groupe G' est un homomorphisme de groupe si :*

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

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 *Un anneau A est un ensemble non vide muni de deux lois de composition internes, l'une notée comme une addition et l'autre comme une multiplication, vérifiant les propriétés :*
- *A est un groupe abélien pour l'addition, (on note 0 son élément neutre),*
- *la multiplication est associative, c'est-à-dire :*

$$a(bc) = (ab)c, \forall a; b; c \in A.$$

- *la multiplication est distributive sur l'addition à gauche et à droite, c'est-à-dire :*

$$a(b+c) = ab + ac \text{ et } (a+b)c = ac + bc; \forall a; b; c \in A.$$

Un anneau (A ; + ; .) s'appelle commutatif si l'opération (.) est commutative.
Un anneau (A ; + ; .) s'appelle unitaire si l'opération (.) a un élément neutre noté 1 ∈ A est appelé unité de l'anneau.

Exemple
L'ensemble $\mathbb{Z}$ des entiers est un anneau commutatif unitaire. Il en est de mème de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

1.2.1 Sous-Anneaux

Définition 1.2.2 *Soit A un anneau. On appelle sous-anneau de A toute partie non-vide B de A qui vérifie les deux conditions suivantes :*
1) *B est un sous-groupe du groupe additif A.*
2) *B est stable par la multiplication de A, c'est-à-dire que l'on a :*
ab ∈ B quels que soient a ∈ B et b ∈ B.

Remarques
- Si B est un sous-anneau de A, alors B est lui-mème un anneau (pour les lois déduites de celles de A par restriction à B).
- Si B est un sous-anneau unitaire d'un anneau unitaire A, alors B est lui-mème un anneau unitaire, et on a $1_B = 1_A$.
- Si l'anneau A est commutatif, alors tout sous-anneau de A est commutatif.

1.2.2 Idéaux

Définition 1.2.3 *Soit A un anneau et I une partie de A. On dit que I est un idéal à gauche (resp. à droite) de A si :*
a) I est un sous-groupe du groupe additif A.
b) Quel que soit a ∈ A et quel que soit x ∈ I, on a ax ∈ I/(resp.xa ∈ I).
On dit que I est un idéal bilatère ou simplement un idéal de A si I est à la fois un idéal à gauche et un idéal à droite de A.
Notons que dans un anneau commutatif, tous les idéaux sont bilatères.

Exemple

Dans tout anneau A, les sous-groupes triviaux A et 0 sont des idéaux. Tout idéal de A autre que A et l'idéal nul 0 s'appelle un idéal propre de A.

1.2.3 Idéal premier

Un idéal I est dit premier si :

$$xy \in I \Longrightarrow x \in I \vee y \in I$$

1.2.4 Idéal maximal

Un idéal I est dit maximal dans l'anneau A si pour tout idéal J de A tel que $I \subseteq J$ alors $I = J \vee J = A$.

Exemple

Soit $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$;
On a $\overline{2} \neq \overline{0}, \overline{3} \neq \overline{0}$, mais $\overline{2}.\overline{3} = \overline{6} = \overline{0}$, alors $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre.
$\overline{2}, \overline{3}$ sont appelés diviseurs de 0

1.2.5 Anneaux quotient

Théorème 1.2.1 *Soient A un anneau et I un idéal bilatère de A.*
*Alors la relation définie par $x\mathcal{R}y \iff x - y \in I$ est une relation d'équivalence sur A, compatible avec les deux lois de A. L'ensemble quotient, noté A/I, muni des deux lois quotients est un anneau appelé **anneau-quotient** de A par I.*
Si, de plus, A est commutatif, l'anneau A/I est commutatif.

1.2.6 Anneaux intègres

Définition 1.2.4 *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 1.2.5 *Un anneaux A est intègre ssi $A \neq \{0\}$ et si A n'a pas de diviseur de zéro , autrement dit si on a :*

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

1.2.7 Caractéristique d'un anneau

On suppose que A est unitaire , la caractéristique de A est le plus petit entier $n \neq 0$ tel que $n.1 = 0$ et on écrit $cara(A) = n$.
Si n n'existe pas on dit que A est de caractéristique nulle.

Exemple

$$cara(\mathbb{C}) = cara(\mathbb{R}) = cara(\mathbb{Q}) = cara(\mathbb{Z}) = 0.$$
$$cara(\mathbb{Z}/n\mathbb{Z}) = n.$$

1.2.8 Homomorphismes d'anneaux

Proposition 1.2.1 *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 *Soit $\mathbb{K}$ un ensemble muni de deux loi $+$, ..*
On dit que $\mathbb{K}$ est un corps si :
- $(\mathbb{K}, +, .$ *est un anneau commutatif .*
- *tout élément non null est inversible pour le produit.*

Exemples

- $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps mais $(\mathbb{Z}, +, \times)$ n'est pas.

1.3.1 Sous- Corps

Définition 1.3.2 *Soit ($\mathbb{K}$, + , .) est un corps, un sous-corps de $(\mathbb{K}, +, .)$ est sous-anneau $\mathbb{F}$ de $\mathbb{K}$,*
tel que pour tout élément non nul x de $\mathbb{F}$, on a $x^{-1} \in \mathbb{F}$;($\mathbb{F}$, + , .) est un corps.

Propriétés
- Pour tout entier $n \geq 2$ ($\mathbb{Z}/\mathrm{n}\mathbb{Z}$ est un corps)$\Longleftrightarrow$ (n est un nombre premier).
  On note $\mathbb{F}_n = \mathbb{Z}/\mathrm{n}\mathbb{Z}$; n est un nombre premier.
- Tout corps fini est commutatif.

1.3.2 Rappels sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Soit p un nombre premier. Nous savons que l'anneau $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p dans ce cas est 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 $a \in \mathbb{F}_p$ vérifie $a^{p-1} \equiv 1[p]$

1.3.3 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 1.3.1 *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 :*

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

1.3.4 Structure des corps finis

Un corps fini est appelée en anglais Gauss Field. On connait que les corps finis avec p éléments quand p est un nombre premier : c'est le quotient $\mathbb{Z}/p\mathbb{Z}$. Étant données deux corps finis F et F' ayant tous deux p éléments avec p premier, il y a un unique isomorphisme $F \longrightarrow F'$.
Pour p premier, on notera $\mathbb{F}_p$ l'unique corps ayant p éléments.
La caractéristique d'un corps fini F est un nombre premier p, donc son sous-corps premier est $\mathbb{F}_p$. Comme F est un espace vectoriel de dimension finie sur $\mathbb{F}_p$, son nombre d'éléments est une puissance de p ; plus précisément, si s est le degré de F comme $\mathbb{F}_p$-espace vectoriel, $[F : \mathbb{F}_p] = s$, alors F a ps éléments. Ainsi le nombre d'éléments d'un corps fini est une puissance d'un nombre premier, et ce nombre premier est la caractéristique du corps.

Exemple

Soit $\mathbb{F}_4$ un corps ayant 4 éléments. Notons α un des deux éléments de $\mathbb{F}_4$ qui n'est ni 0 ni 1. L'autre doit ètre à la fois α^2 et $\alpha + 1$, donc $\alpha^2 = \alpha + 1$. Alors$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$.
les tables d'addition et de multiplication de ce corps $\mathbb{F}_4$:

$(\mathbb{F}_4, +)$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$(\mathbb{F}_4, .)$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

1.4 Espace Vectoriels

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

1. Une loi interne appelée addition, notée + tel que $(E\,;+)$ soit un groupe abélien.
2. Une loi externe qui à tout couple $(\lambda\,;x)\in$ K$\times$ E fait correspondre un élément de E noté $\lambda.x$, cette loi vérifiant les quatre propriétés suivantes :

- $\forall$ x$\in E$, 1.x = x,
- $\forall$ x,y$\in E$, $\forall\lambda \in K$;λ.(x+y)=λ.x+λ.y,
- $\forall$ x$\in E$, $\forall\lambda,\mu \in K$,(λ+μ).x=λ.x+μ.x,
- $\forall$ x$\in E$, $\forall\lambda,\mu \in K$,($\lambda.\mu$).x=λ.(μ.x),

Les éléments de E s'appelle vecteurs, ceux de k scalaires.

1.4.1 Sous-Espace Vectoriels

Proposition 1.4.1 *une partie non vide F d'un k-espace vectoriel E est un sous-espace vectoriel de E si seulement si : $\forall$ $x,y \in F$, $\forall\lambda \in k$: $x+y \in F$ et $\lambda x \in F$.*
Ou encore $\forall$ $x,y \in F$, $\forall\lambda,\mu \in k$: $\lambda x+\mu y \in F$.

Proposition 1.4.2 *Soit F une partie non vide d'un K-espace vectoriel E.*
Les propositions suivantes sont équivalentes :
1) *F est un sous-espace vectoriel de E.*
2) $\forall x, y \in E, \forall\lambda, \mu \in K, \lambda x + \mu y \in F$.

Définition 1.4.2 *On dit qu'un système fini $(x_1, x_2, ..., x_n)$ de vecteurs d'un K-espace vectoriel E est libre si toute combinaison linéaire de $x_1, x_2, ..., x_n$ est triviale :*
Si $\lambda_1, \lambda_2, ..., \lambda_n \in K$, 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 K-espace vectoriel E est lié s'il n'est pas libre . Ce qui revient à dire qu'il existe des scalaire $\lambda_1, \lambda_2, ..., \lambda_n$ tous non nuls tels que

$$\lambda_1 x_1 + \lambda_2 x_2 + ...\lambda_n x_n = 0$$

Définition 1.4.3 *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 K-espace vectoriel E est dit base de E
si $(x_1, x_2, ..., x_n)$ est libre et générateur de E.

Exemples

1) Une base de 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 $K^n[x]$ des polynômes de degré inférieur ou égal à n.

Définition 1.4.4 *Soient E, E' deux espaces vectoriels sur K et f une application de E dans E'. On dit que f est linéaire, si :*
$1) f(v+w) = f(v) + f(w);\ \forall v, w \in E,$
$2) f(\lambda v) = \lambda f(v),\ \forall v \in E, \forall \lambda \in K.$

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

1.5 Modules

La notion de module est une généralisation d la notion d'espace vectoriel.
Soit A un anneau commutatif unitaire et M un ensemble non vide.

Définition 1.5.1 *On dit que M est un module sur A si M est muni d'une addition $(+)$*

$$\begin{array}{ccc} M \times M & \longrightarrow & M \\ (x,y) & \longmapsto & x+y \end{array}$$

et d'une loi externe $(.)$

$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ (\alpha, x) & \longmapsto & \alpha.x \end{array}$$

tel que :
$1\bullet$ $(M,+)$ *est un groupe abélien.*
$2\bullet$ $(\alpha+\beta)x = \alpha x + \beta x, \forall \alpha, \beta \in A, \forall x \in M.$
$3\bullet$ $\alpha(x+y) = \alpha x + \alpha y, \forall \alpha \in A, \forall x, y \in M\ .$
$4\bullet$ $(\alpha\beta)x = \alpha(\beta x), \forall \alpha, \beta \in A, \forall x \in M\ .$
$5\bullet$ $1_A.x = x, \forall x \in M.$

Exemples 1) Tout K espace vectoriel est un module sur l'anneau K.
2) Tout groupe abélien est un $\mathbb{Z}$-module.
3) Tout idéal I d'un anneau commutatif unitaire A est un A-module.

1.5.1 Sous-module

Soit M un A-module et $M' \subset M$ une partie non vide, alors M' est dit sous-module de M si :
$1\bullet$ $x, y \in M' \Longrightarrow x - y \in M'.$
$2\bullet$ $\forall \alpha \in A, \forall x \in M' \Longrightarrow \alpha x \in M'.$

1.5.2 Module de type fini

Soit M un A-module, on dit que M est de type fini s'il est engendré par une partie finie $\{x_1, x_2, ..., x_n\}$

$$M = Ax_1 + Ax_2 + ... + Ax_n.$$

1.5.3 Module libre

Soit M un A-module, on dit que M est libre s'il admet une base $(x_i)_{i\in I}$ i.e $\forall x \in M$, x s'écrit d'une manière unique comme combinaison linéaire d'un nombre fini d'éléments de $(x_i)_{i\in I}$.

Propriété

1• Si Mest libre et de type fini, alors M admet une base finie.

2• Si M admet une base de cardinal n alors M est isomorphe à A^n, alors on dit que n est le rang de M.

Exemple

$\frac{\mathbb{Z}}{5\mathbb{Z}}$ est un $\mathbb{Z}$-module de type fini.

$\frac{\mathbb{Z}}{5\mathbb{Z}} = \langle\overline{1}\rangle$ car $\forall\overline{m} \in \frac{\mathbb{Z}}{5\mathbb{Z}}; \overline{m} = m.\overline{1}$.

1.6 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 $(e'_1, e'_2, ..., e'_n)$:

$$\begin{array}{rcl} f(e_1) & = & a_{11}e'_1 + a_{21}e'_2 + ... + a_{p1}e'_p, \\ f(e_2) & = & a_{12}e'_1 + a_{22}e'_2 + ... + a_{p2}e'_p, \\ \vdots & \vdots & \vdots \\ f(e_n) & = & a_{1n}e'_1 + a_{2n}e'_2 + ... + a_{pn}e'_p. \end{array}$$

Définition 1.6.1 *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 1.6.2 *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 $\mathbb{K}$

1.6.1 Polynôme Irréductible

Soit $\mathbb{F}_p[x]$ l'ensemble des polynômes en x à coefficient dans $\mathbb{F}_p$, un polynôme $g(x)$ de $\mathbb{F}_p[x]$ 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 $f(x) = x(1 + x^2)$.

1.6.2 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, $2^3 - 1 = 7$, $x^7 + 1 = (x^4 + x^2 + x + 1)(x^3 + x + 1)$.

1.6.3 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 $n = 2^m - 1$.

Chapitre 2

Notions de la théorie des Codes correcteurs d'erreurs

Dans ce chapitre, nous allons étudier quelques notions essentielles et utiles sur la théorie des codes correcteurs d'erreurs. 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 Code en block

En général un mot code est $x = (x_1, ..., x_n) \in \mathcal{A}^n$ de longueur n ou $\mathcal{A}$ est un ensemble appelé alphabet.
L'ensemble des mot de de code forment le code $\mathcal{C}$
pour $x \in \mathcal{C}$, si le vecteur transmit x' on dit qu'il y a erreur, pour corriger l'erreur ou on cherche un élément dans $\mathcal{C}$ qui soit le plus proche de $x' \notin \mathcal{C}$, pour cela on doit faire intervenir une distance.

Exemple

Le code $ISBN$ 'International Standard Book Number ', ce code est conçu pour simplifier le traitement des livres en ordinateur, dans ce cas le mot de code est de longueur 10,
$x = (x_1, x_2, ..., x_{10})$ ou $x_i \in 0, 1, 2, ..., 9, x$ telle que $x = 10$ à condition : $\sum_{k=1}^{10} kx_k \equiv 0[11]$
Comme un example on prend le livre de J.E et M.J BERTIN , "Algèbre linéaire et géométrie classique de " son $ISBN$ est 2-225-66693-8
Alors $(2\times1)+(2\times2)+(2\times3)+(5\times4)+(6\times5)+(6\times6)+(6\times7)+(9\times8)+(3\times9)+(8\times10) = 319 \equiv 0[11]$.

Définition 2.1.1 *soit$\mathcal{A}$ un ensemble fini et n un entier naturel $n \neq 0$; un code en bloc est une partie $\mathcal{C}$ de $\mathcal{A}^n$; $\mathcal{A}$ est appelé alphabet de $\mathcal{C}$, tout élément de $\mathcal{C}$est dit mot de code*

2.2 Distance et poids de*Hamming*

Définition 2.2.1 *Soit $x = (x_1, x_2, ..., x_n) \in \mathcal{A}^n$, on définit le support de ce vecteur par*

$$supp(x) := \{i \in 1, ..., n | x_i \neq 0\}$$

Définition 2.2.2 *Soit $x = (x_1, x_2, ..., x_n) \in \mathcal{A}^n$, le poids de Hamming de x, noté $wt(x)$ est égal au nombre de coordonnées non nulles de x.*

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

Nous allons maintenant munir l'ensemble $\mathcal{A}^n$ d'une distance, on définit une application :

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

Tel que $d(x, y) = card\{i : / x_i \neq y_i\}$ est le nombre d'indice pour lequel les composantes de x et y sont distinctes.
Cette distance vérifie les propriétés usuelles des distances :
1• $d(x, y) = 0 \Leftrightarrow x = y$
2• Symétrie : $d(x, y) = d(y, x)$
3• Positivité : $d(x, y) \geq 0$
4• Inégalité triangulaire : $d(x, y) \leq d(x, z) + d(z, y)$

Cet distance est appelée la distance de *Hamming*.
alors :

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

il faut remarquer que la distance de *Hamming* est une vrai distance au sens métrique du terme.
La boule de centre x et de rayon r est par définition l'ensemble :

$$B(x, r) = \{y : y \in \mathcal{A}^n / d(x, y) \leq r\}$$

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

Exemple

$x = (a, b, b)\,; y = (b, a, b)$ alors $d\,(x, y) = 2$

Définition 2.2.3 *Soit $\mathcal{C} \subset \mathcal{A}^n$ un code en bloc et "d" la distance de Hamming, on appelé distance minimale de $\mathcal{C}$ le nombre :*

$$d\,(\mathcal{C}) = min\,\{d\,(x, y)\,/ x \neq y; x, y \in \mathcal{C}\}$$

Exemple

Soit $\mathcal{C} = \{a, b, c\}$, tel que : $a = (1, 1, 1)$,$b = (0, 1, 0)$, $c = (1, 0, 1)$
$d(a, b) = 2$
$d(a, c) = 1$
$d(b, c) = 3$
donc $d(\mathcal{C}) = 1$

2.3 Décodage et correction

Supposons que $x = (x_1, x_2, ..., x_n) \in \mathcal{C}$ est transmis en $x' = (x'_1, x'_2, ..., x'_n)$;x' doit appartenir à C ; sinon il y a au moins un erreur, $d(x, x')$ représente le nombre d'erreurs.
pour retrouver le mot initial x ; on cherche un mot de $\mathcal{C}$ le plus proche de x'

Exemple

$\mathcal{C} = \{a, b, c\}$; $oua = (111)$, $b = (010)$, $c = (101)$,
si $x' = (100)$ est le vecteur transmis
on calcule $d(x', a)$; $d(x', b)$; $d(x', c)$
$\mathcal{C}$ est le plus proche de x', donc x' est décodé par c

Proposition 2.3.1 *Notons* $e = [\frac{d-1}{2}]$, *les boules* $B(x, e)$ *avec* $x \in \mathcal{C}$ *sont deux à deux disjointes, et* e *est la valeur maximale du rayon pour cette propriété.*
On dit que $\mathcal{C}$ *détecte* $d - 1$ *erreurs et corrige* $e = [\frac{d-1}{2}]$

Proposition 2.3.2 *Soit* $\mathcal{C}$ *un code de longueur* n *sur l'alphabet* A .
on dit que $\mathcal{C}$ *corrige* e *erreurs ,si pour tout* $x \in A^n$ *,il existe au plus un mot* c *de* $\mathcal{C}$ *tel que* $d(x, c) \leq e$.
On dit que $\mathcal{C}$ *est de capacité* e, *si* $\mathcal{C}$ *corrige* e *erreurs et ne corrige pas* $e + 1$ *erreurs.*

Remarque

Si le nombre d'erreurs est inférieur à e alors $\mathcal{C}$ corrige les erreurs.
Si le nombre d'erreurs dépasse e;$\mathcal{C}$ ne peut pas corrige les erreurs, car il peut exister plusieurs élément de $\mathcal{C}$ proches de x vecteurs reçu.

Isométrie

Définition 2.3.1 *Soit* (A^n, d) *un espace de Hamming ,une isométrie de Hamming est une application :*

$$f : A^n \longrightarrow A^n$$

tel que : $\forall (x, y) \in A^n, d(f(x), f(y)) = d(x, y)$

Exemple

Soit σ une permutation de σ_n :
$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$
soit $f : A^n \to A^n$ définie par $f(x_1, ..., x_n) = \left(x_{\sigma(1)}, ..., x_{\sigma(n)}\right)$ alors f est une isométrie

2.4 Code équivalents

Deux codes $\mathcal{C}, \mathcal{C}' \subset A^n$, sont dit équivalents,s'il existe f une isométrie de A^n,
tel que $\mathcal{C}' = f(\mathcal{C})$

Remarque

Les propriétés métriques sont conservées par équivalence ,donc deux codes équivalents ont même distance minimale don même capacité de correction

2.5 Code linéaire

Considérons le corps de base $\mathbb{F}_q$ où $q = p^m$ est une puissance d'un nombre premier.

Définition 2.5.1 *Soit $\mathbb{F}_q$ un corps fini et soit $n > 0$. Le $\mathbb{F}_q$-espace vectoriel $\mathbb{F}_q^n$ est muni de la métrique de Hamming. Un code linéaire est un $\mathbb{F}_q$-sous-espace de $\mathbb{F}_q^n$. Ses paramètres sont : sa longueur n, sa dimension k , sa distance minimale d. On dit que le code $\mathcal{C}$ est un code $[n, k, d]$;alors $\mathcal{C}$ est de cardinal q^k ; $|\mathbb{F}_q| = q$*

Exemple

1. $\mathbb{F}_2 = \{0; 1\}$
   $\mathcal{C} = \{(x_1, x_2, x_3) \in \mathbb{K}^3 / x_1 + x_2 - x_3 = 0\} \Rightarrow x_3 = x_1 + x_2$
   donc $(x_1, x_2, x_1 + x_2) = x_1(1, 0, 1) + x_2(0, 1, 1) \Rightarrow \mathcal{C} = \{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$
   $\mathcal{C}$ est $[3, 2, 2]$
2. $\mathbb{F}_q^n$; $\{0\}$ sont codes linéaires triviaux.
3. $V = \langle(1, ..., 1)\rangle = \{(a, ..., a) ; a \in \mathbb{F}_q\}$ code répétition $V = [n, 1, n]$ code linéaire.

2.6 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

Soit C un $[n,k]$-code sur $\mathbb{F}_q$. Soit $\{g_1,...,g_k\}$ une base de C. Alors la matrice

$$G := \begin{pmatrix} g_1 \\ ... \\ g_k \end{pmatrix}$$

est appelée une matrice génératrice de C.

Propriété 1

Soit G une matrice génératrice d'un code C. On dit qu'elle génère C, car tout mot de code $c \in C$ est obtenu par multiplication à gauche de G par un vecteur de $\mathbb{F}_q^k$. Pout tout $c \in C$, il existe $u \in \mathbb{F}_q^k$ tel que $u.G = c$

$$(u_1,...,u_k)\begin{pmatrix} g_{11} & g_{12} & ... & g_{1n} \\ & & ... & \\ g_{k1} & g_{k2} & ... & g_{kn} \end{pmatrix} = (c_1,...,c_n)$$

Du fait qu'un code est un sous-espace vectoriel, on peut efectuer n'importe quelle opération inversible sur les lignes de G, la matrice résultante sera toujours une matrice génératrice.

Propriété 2

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

Remarque 2.6.1 *Soit $\mathcal{C}$ un code linéaire $[n,k,d]$, l'encodage se fait en multipliant le mot source par la matrice génératrice du code*

Définition 2.6.1 *Une matrice génératrice d'un code $\mathcal{C}$ 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

Example Soit C le code linéaire binaire ayant pour matrice génératrice :

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

Remarque 2.6.2 *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 :

$$\mathcal{C} = \{(c_1, ..., c_n); H \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0\}.$$

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

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

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

Remarque

1/ Le dual de $\mathcal{C}^{\perp}$ est $\mathcal{C}$ lui même ; $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$
2/ Un code est dit auto dual s'il est égal à son dual c-à-d : $\mathcal{C}^{\perp} = \mathcal{C}$

Proposition 2.6.1 *Soit $\mathcal{C}$ 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 $\mathcal{C}$ alors :
1/ si H une matrice de contrôle de parité de $\mathcal{C}$, 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 $\mathcal{C}$ 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 $\mathcal{C}$ 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.

2.7 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 2.7.1 *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 :
$H \in \mathcal{M}_{k\times(2^k-1)}$.

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

Conséquence

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

2.8 Code équidistant

Définition 2.8.1 *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 2.8.2 *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 2.8.1 *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 2.8.1 *La proposition* (2.8.1) *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

2.9 Les codes "Maximum Distance Séparable" (MDS)

Soit $\mathcal{C}$ un code linéaire $[n,k,d]$ (i.e. de longueur n, de dimension k et de distance minimale d) sur un corps fini K. Soient H sa matrice de contrôle et G sa matrice génératrice. Alors le rang de H est égal à $n-k$. Donc il y a au plus $n-k$ colonnes dans H linéairement indépendantes. Il existe donc dans C des mots de poids $n-k+1$. On obtient :
d $\leq n-k+1$. Cette relation entre les paramètres du code $\mathcal{C}$ est la borne de Singleton.

Définition 2.9.1 *Le code* $\mathcal{C}$ *est dit "maximum distance séparable" est un code* MDS *si et seulement si* $d = n-k+1$ *; i.e. sa matrice de contrôle est de rang* $d-1$ *(ou encore sa matrice génératrice est de rang* $n-d+1$*).*
Il est dit MDS *trivial lorsque* $k = 1$ *ou* $k \geq n-1$.

Exemple
On peut aisément construire un code MDS *trivial binaire de type* $[n, n-1, 2]$ *. Nous donnons ci-après un exemple de matrice génératrice pour* $n = 6$ *; la généralisation, pour toute longueur, est évidente. Le code de matrice génératrice*

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

est MDS *trivial.*

Citons les propriétés immédiates de ces codes :
1) $\mathcal{C}$ *est* MDS *si et seulement si chaque ensemble de* $n-k$ *colonnes de sa matrice de parité* H *est de rang* $n-k$ *;*
2) *Si* $\mathcal{C}$ *est* MDS*, alors* $\mathcal{C}^{\perp}$ *l'est aussi ;*
3) $\mathcal{C}$ *est* MDS *si et seulement si chaque ensemble de* k *colonnes de sa matrice génératrice* G *est de rang* k*.*

On a certaines informations sur les codes MDS *; ainsi ils constituent une classe de codes dont on connait la distribution des poids.*

2.10 Codes cycliques

Définition 2.10.1 *Soit* $\mathbb{K}$ *un corps commutatif fini ,un code linéaire* $\mathcal{C}$ *de longueur* n *est dit cyclique si :*

$$(x_1; x_2; ...; x_n) \in \mathcal{C} \Longrightarrow (x_n; x_1; ...; x_{n-1}) \in \mathcal{C}$$

Remarque

soit P la matrice de permutation correspondante au cycle $(1; 2; ...; n)$ alors :

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

donc

$$x = (x_1; ...; x_n).P = (x_1; ...; x_n) \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & ... & 1 \\ 1 & 0 & 0 & ... & 0 \end{pmatrix} = (x_n, x_1, ..., x_{n-1})$$

$$\mathcal{C} \text{ cyclique} \Longleftrightarrow x \in \mathcal{C} \Longrightarrow x.P \in \mathcal{C}$$

Proposition 2.10.1 *soit* $\mathcal{C}$ *un code linéaire de matrice génératrice* G *et de matrice de contrôle* H *,alors :*

$$\mathcal{C} \text{ est cyclique} \Longleftrightarrow GP^tH = 0$$

2.10.1 Représentation polynomiale

Pour facilité d'étudier les propriétés algébriques de ces codes, il est plus commode d'écrire les mots d'un code cyclique sous forme polynomiale grâce à l'identification suivante :

$$c = (c_0, c_1, ..., c_{n-1}) \longleftrightarrow C(X) = c_0 + c_1.X + ... + c_{n-1}.X^{n-1}$$

Et ainsi l'action du décalage circulaire sur un mot revient à la multiplication par X modulo $X^n - 1$ sur le polynôme correspondant :

$$(c_{n-1}, c_0, ..., c_{n-2}) \longleftrightarrow XC(X) = c_{n-1} + c_0.X + ... + c_{n-2}.X^{n-1} mod[X^n - 1]$$

Définition 2.10.2 *Soit R_n l'anneau quotient défini par*

$$R_n := F_q[X]/\langle X^n - 1\rangle$$

Ainsi, un décalage circulaire sur un mot de code c correspond à une multiplication par X de c(X) dans cet anneau quotient R_n.

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

$$C \text{ est cyclique} \Longleftrightarrow C \text{ est un idéal de } R_n.$$

2.11 Polynôme générateur et polynôme de contrôle

Soit C un code cyclique de longueur n et de dimension m sur $\mathbb{F}_q$, il existe un polynôme unitaire unique g de $\mathbb{F}_q$ de degré $n - m$ divisant $x^n - 1$ tel que : C est l'idéal de $\frac{\mathbb{F}_q[X]}{\langle x^n - 1\rangle}$ engendré par $\overline{g(x)}$ donc les éléments de $\mathcal{C}$ sont des multiples de $g(x) mod[x^n - 1]$.
Le polynôme g est dit : " polynôme générateur de $\mathcal{C}$ "
Le polynôme $h(x)$ telle que $g(x)h(x) = x^n - 1$ est appelé le polynôme de contrôle $\mathcal{C}$.

Réciproquement

Tout polynôme g de dégrée $n - m$,divisant $x^n - 1$ est un polynôme générateur d'un code cyclique de longueur n est de dimension m

Remarque

pour déterminer les codes cycliques de longueur n ;il suffit de déterminer les polynômes de degré $n - m$ divisant $x^n - 1$

$$dim\mathcal{C} = n - deg(g) = n - (n - m) = m$$

Proposition 2.11.1 *soit $\mathcal{C}$ un code cyclique de longueur n et de dimension m et de polynôme générateur g ;on pose $h = \frac{x^n-1}{g}$ de degré m,alors*

$$b \in \mathcal{C} \Longleftrightarrow b.h \equiv 0[x^n - 1]$$

h est appelé polynôme de contrôle de $\mathcal{C}$

2.12 matrice génératrice et matrice de contrôle pour un code cyclique

Définition 2.12.1 *soit $\mathcal{C}$ un code cyclique de longueur n est de dimension m sur k ;*
$g(x) = g_0 + g_1x + ... + g_{n-m}x^{n-m}$, son polynôme générateur
$h(x) = h_0 + h_1x + ... + h_mx^m$, son polynôme de contrôle

alors une matrice génératrice de $\mathcal{C}$ est donnée

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-m} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & & g_{n-m} & \cdots & 0 \\ \vdots & & & \ddots & \vdots & & \vdots \\ 0 & & \cdots & g_0 & g_1 & \cdots & g_{n-m} \end{pmatrix} \in \mathcal{M}_{m\times n},$$

une matrice de contrôle de $\mathcal{C}$ est donnée pas :

$$H = \begin{pmatrix} h_m & h_{m-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_m & \cdots & & h_0 & \cdots & 0 \\ \vdots & & & \ddots & \vdots & & \vdots \\ 0 & & \cdots & h_m & h_{m-1} & \cdots & h_0 \end{pmatrix} \in \mathcal{M}_{n-m\times n},$$

Exemple
Une matrice génératrice du code cyclique sur $\mathbb{F}_2$ de longueur 7 engendré par $g(x) = x^3+x^2+1$ est

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

alors, $h(x) = (x + 1)(x^3 + x^2 + 1)$

$$= x^4 + x^2 + x + x^3 + x + 1$$

$$= x^4 + x^2 + x^3 + 1$$

donc,

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

$colonne_1 + colonne_2 + colonne_6 = 0$

$d \leqslant 3$ chaque famille de deux colonne est libre alors $d = 3$

$$C = [7; 4; 3]$$

2.13 Codes BCH

Les code BCH forment une sous-famille des codes cycliques qui on introduit par $R.C.Bose$, $K.Ray - Chaudhuri$ et $A.Hocquenghem$.

2.13.1 Racines d'un code cyclique

Soit C un code cyclique de longueur n sur $\mathbb{F}_q$ et g son polynôme générateur.
On appelle racines de C les racines de g dans le corps de décomposition de $X^n - 1$.

Proposition 2.13.1 *Soit le corps de base $\mathbb{F}_q$ de caractéristique q, soit n un entier tel que $PGCD(q, n) = 1$, on considère $\xi_1, \xi_2, ..., \xi_r$ des racines n^{eme} de l'unité, posons :*

$$H = \begin{pmatrix} 1 & \xi_1 & \xi_1^2 & ... & \xi_1^{n-1} \\ 1 & \xi_2 & \xi_2^2 & ... & \xi_2^{n-1} \\ . & . & . & . & . \\ 1 & \xi_r & \xi_r^2 & ... & \xi_r^{n-1} \end{pmatrix},$$

alors ;

$$C = \{c = (c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_q^n; c^t H = 0\}$$

est un code cyclique de longueur n et de polynôme générateur $g = PPCM(Irr(\xi_1), ..., Irr(\xi_r))$ et de dimension $n - r$.

Définition 2.13.1 *Soit ξ une racine primitive n^{eme} de l'unité .*
Soit $l, r \in \mathbb{N}$, alors tout code cyclique ayant pour racine $\xi^l, \xi^{l+1}, ..., \xi^{l+r-2}$ est appelé code BCH à $r - 1$ racine, tel que $d_{min} \geqslant r$.

Exemple Soient $n = 15, q = 2^4$ et $r = 3$.
Soit ξ une racine primitive 15^{eme} de l'unité ($\xi \in \mathbb{F}_{2^4}$ et $\xi^4 + \xi + 1 = 0$).
Posons :

$$\begin{aligned} g(X) &= PPCM(Irr(\xi_1), Irr(\xi_2), Irr(\xi_3)) \\ &= PPCM(X^4 + X + 1, X^4 + X + 1, X^4 + X^3 + X^2 + X + 1 \\ &= X^8 + X^7 + X^6 + X^4 + 1. \end{aligned}$$

Donc le code cyclique engendré par $g(X)$ est un code BCH de longueur 15 sur $\mathbb{F}_2$ de distance minimale au moins 3.

2.14 Codes de Reed-Solomon

Définition 2.14.1 *Soit $q = p^m$ une puissance d'un nombre premier. Un code de Reed-Solomon sur $\mathbb{F}_q$ de distance minimale d est un code BCH de longueur $n = q - 1 = p^m - 1$ et de distance construite d.*

Propriété Un code de Reed-Solomon est un code MDS.

Chapitre 3

Codes quasi-cycliques

Les codes quasi-cycliques étant une généralisation des codes cycliques, il est essentiel de définir un généralisation du shift, le quasi-shift.

3.1 Définitions

Définition 3.1.1 *Soit :*

$$\begin{array}{rccc} T: & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & (x_1, x_2, ..., x_n) & \longmapsto & (x_n, x_1, ..., x_{n-1}) \end{array}$$

l'application décalage circulaire dite shift.
Soit C un code de longueur n sur $\mathbb{F}_q$. Par définition :

$$C \ \ est \ \ cyclique \Longleftrightarrow \forall c \in C; T(c) \in C$$

En d'autres mots, C reste stable par shift T ou $T \in Aut(C)$.

Définition 3.1.2 *Soit $l \in \mathbb{N}^*$ tel que l divise n, soit :*

$$\begin{array}{rccc} T^l: & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & (x_1, x_2, ..., x_n) & \longmapsto & (x_l, x_{l+1}, ..., x_{l-1}) \end{array}$$

combinaison de shift T l fois , La permutation T^l est appelée quasi-shift.
Soit C un code de longueur n sur $\mathbb{F}_q$. Par définition :

$$C \ \ est \ \ l - quasi - cyclique \Longleftrightarrow \forall c \in C; T^l(c) \in C$$

En d'autres mots, C reste stable par quasi-shift T^l ou $T^l \in Aut(C)$.

Soit $\alpha \in \mathbb{F}_{q^l}$ tel que la famille $\{1, \alpha, \alpha^2, ..., \alpha^{l-1}\}$ forme un base pour l'espace vectoriel $\mathbb{F}_{q^l}$ sur le corps $\mathbb{F}_q$.
On définit le pliage par l'application linéaire suivante :

$$\begin{array}{rccc} \varphi: & \mathbb{F}_q^l & \longrightarrow & \mathbb{F}_{q^l} \\ & (a_1, a_2, ..., a_l) & \longmapsto & a_l + a_2\alpha + ... + a_l\alpha^{l-1}. \end{array}$$

On définit le dépliage par l'inverse de l'application linéaire précédente :

$$\begin{array}{rccc} \varphi^{-1}: & \mathbb{F}_{q^l} & \longrightarrow & \mathbb{F}_q^l \\ & a_l + a_2\alpha + ... + a_l\alpha^{l-1} & \longmapsto & (a_1, a_2, ..., a_l). \end{array}$$

Soit m un entier positive , soit f une application d'une ensemble E dans F.
On indique par $f^{\times m}$ l'application suivante :

$$\begin{array}{rccc} f^{\times m}: & E^m & \longrightarrow & F^m \\ & (x_1, ..., x_m) & \longmapsto & f^{\times m}(x_1, ..., x_m) = (f(x_1), ..., f(x_m)). \end{array}$$

Définition 3.1.3 *Code plié et code déplié*
Supposons que $n = ml$;on définit le code plié de C par $\varphi^{\times m}(C)$.
Soit C' un code dans $\mathbb{F}_{q^l}^m$. On définit le code déplié de C' the $(\varphi^{-1})^{\times m}(C')$.

On remarque que C est un code l-quasi-cyclique $\Longleftrightarrow$ son code plié $\varphi^{\times m}(C)$ est un code cyclique. mais pas forcement le code plié est un code linéaire sur $\mathbb{F}_{q^l}$.

3.2 Propriétés des code quasi-cyclique

3.2.1 La correspondance un à un

On a déjà vu une correspondance un à un entre les codes cyclique et les idéals de $\mathcal{R}_n = \mathbb{F}_q/\langle X^n - 1\rangle$.
Alors par [19] et [20] il y a une correspondance un à un entre l-quasi-cycliques codes et les idéals à gauche de $M_l(\mathbb{F}_q)[X]/\langle X^m - 1\rangle$.

Lemme 3.2.1 *Soit R un anneau principal commutatif et M un module libre de type finie de rang s sur R. Alors chaque sous-module N de M est engendré au plus par s éléments.*

Lemme 3.2.2 *Soit s un entier positive et R un anneau principal commutatif. Alors il y a une correspondance un à un entre les sous-modules de R^s et les idéals à gauche de $M_s(R)$.*

Notons qu'il y a un isomorphisme d'anneaux entre $M_l(\mathbb{F}_q)/\langle X^m-1\rangle$ et $M_l(\mathbb{F}_q/\langle X^m-1\rangle)$ et que $R=\mathbb{F}_q[X]/\langle X^m-1\rangle$ est un anneau principal commutatif.
Alors chaque sou-module de R^l est engendré par l éléments au plus, et chaque idéal à gauche de $M_l(\mathbb{F}_q)/\langle X^m-1\rangle$ est un idéal principale.

Théorème 3.2.1 *il y a une correspondance un à un entre l-quasi-cycliques codes sur $\mathbb{F}_q$ et les idéals à gauche de $M_l(\mathbb{F}_q[X])/\langle X^m-1\rangle$.*

Preuve: Soit g= $(g_{11},...,g_{1l},g_{21},...,g_{2l},...,g_{m1},...,g_{ml}) \in \mathbb{F}_q^{ml}$ On associe à g l'élément $\phi(g)\in(\mathbb{F}_q)[X]/\langle X^m-1\rangle)^l$ tel que :

$$\phi(g)=(g_{11}+g_{21}X+...+g_{m1}X^{m-1};g_{12}+g_{22}X+...+g_{m2}X^{m-1};...;g_{1l}+g_{2l}X+...+g_{ml}X^{m-1}).$$

Alors ϕ produit une correspondance un à un entre l-quasi-cycliques codes de longueur ml sur $\mathbb{F}_q$ est sou-module de $(\mathbb{F}_q[X]/\langle X^m-1\rangle)^l$ □

Lemme 3.2.3 *Soit C un l-quasi-cyclique code sur $\mathbb{F}_q$ de dimension k et de longueur ml. Alors il existe un entier r tel que $1\leqslant r\leqslant k$ et pour quelque soit G matrice génératrice de C et $0\leqslant i\leqslant m-1$, r est le rang de $il+1, il+2, .., (i+1)l$ colonne de G.*

On appelle l'entier r le rang de bloc de C.
Notons que r ne dépend que de C et non d'une matrice génératrice particulière de C.

3.2.2 Le polynôme générateur d'un code l-quasi-cyclique

Soit C un code l-quasi-cyclique sur F_q, si $l=1$ alors C est un code cyclique de longueur n et la matrice génératrice de C est :

$$G=\begin{pmatrix} g(X) & 0 & 0 \\ 0 & Xg(X) & 0 \\ & ... & \\ 0 & 0 & X^{n-deg(g)}g(X) \end{pmatrix}$$

tel que $g(x)\in\mathbb{F}_q[X]$ est le polynôme générateur de C.
le rang de bloc de C est l et on a vu qu'on peut écrire la matrice génératrice de C avec un seul vecteur.
La généralisation de ce résultat pour les codes quasi-cycliques est fait en utilisant le rang de bloc.

Corollaire 3.2.1 *Il existe $g_1, ..., g_r$ des vecteurs linéairement indépendants de C tel que $g_1, ..., g_r, T^l g_1, ..., T^l(g_r), ..., T^{(m-1)l}(g_1), ..., T^{(m-1)l}(g_r)$ construit C.*
Si on indique par $g_{i,j}$ la coordonnée j^eme de g_i et soit :

$$G_i = \begin{pmatrix} g_{1;il+1} & \cdots & g_{1;(i+1)l} \\ \vdots & & \vdots \\ g_{r;il+1} & \cdots & g_{r;(i+1)l} \\ & 0 & \end{pmatrix} \in M_l(\mathbb{F}_q)$$

et

$$g(X) = \frac{1}{X^\gamma} \sum_{i=0}^{m-1} G_i.X^i \in M_l(\mathbb{F}_q)[X],$$

γ est le plus petit entier tel que $G_i \neq 0$, alors C correspond à $I = \langle g(X) \rangle$ l'idéal à gauche engendré par $g(X)$.

Corollaire 3.2.2 *Le sous-module $\phi(C) \subset (\mathbb{F}_q[X]/\langle X^m - 1 \rangle)^l$ est engendré par un r éléments comme un $\mathbb{F}_q[X]/\langle X^m - 1 \rangle$ module mais ne peut pas engendré par moins de r éléments.*
Si C est un code cyclique alors on a $r = 1$ et on retrouve le résultat classique sur les codes cycliques

Définition 3.2.1 *Le polynôme*

$$g(X) = \frac{1}{X^\gamma} \sum_{i=0}^{m-1} G_i.X^i \in M_l(\mathbb{F}_q)[X],$$

est dit le polynôme générateur de C.

3.2.3 Propriété du polynôme générateur

Théorème 3.2.2 *Soit C un l-quasi-cyclique code de longueur ml sur $\mathbb{F}_q$. Soit $P(X)$ un polynôme générateur de C et soit $Q(x)$ un polynome generateur de son dual , alors ;*

$$P(X)({}^tQ^*(X)) = 0 mod[X^m - 1]$$

tel que Q^* est le polnome réciproque de Q, et ${}^tQ$ est le polynôme dont ses coefficients sont des transposées des matrices coefficients de Q.

Preuve: Comme $P(X) = \sum_{i=0}^{m-1} P_i X^i$ est un polynôme générateur de C et les colonne de la matrice $(P_0, P_1, ..., P_{m-1})$ et leur shift construisent C.
En similaire $Q(X) = \sum_{i=0}^{m-1} Q_i X^i$ et les colonne de la matrice $Q_0, Q_1, ..., Q_{m-1})$ et leur shift

construisent $C^{\perp}$.
Par définition du code dual on a

$$(P_0, P_1, ..., P_{m-1}).\begin{pmatrix} {}^tQ_0 \\ {}^tQ_1 \\ \vdots \\ {}^tQ_{m-1} \end{pmatrix} = \sum_{i=0}^{m-1} P_i({}^tQ_i) = 0$$

Comme C et $C^{\perp}$ sont des codes l-quasi-cycliques on a :

$$\sum_{i=0}^{m-1} P_i({}^tQ_{i+j \ mod \ m}) = 0 \ ; \forall j \in \mathbb{Z},$$

alors :

$$P(X)({}^tQ^*(X)) = \sum_{j=0}^{m-1}\sum_{i=0}^{m-1} P_i({}^tQ_{i-j \ mod \ m})X^j = 0 mod[X^m - 1]$$

□

3.3 Représentations des codes quasi-cycliques

On va représenter les codes quasi-cycliques par deux quasi-shift particuliers.

3.3.1 Comme concaténation de codes cycliques

On va considérer les codes quasi-cyclique comme des concaténation de plusieurs codes cycliques, alors on utilise le quasi-shift τ_1 comme ci de suite :

$$\tau_1 = (1; 2; ...; m)(m+1; m+2; ...; 2m)...((l-1)m+1; (l-1)m+2; ...; lm).$$

Alors un code C est dit quasi-cyclique si et seulement si $\tau_1 \in Aut(C)$.
On définit une matrice génératrice de ce code dans cet cas sous la forme de concaténation de blocs circulant.

$$\left(\circlearrowleft \mid \circlearrowleft \mid ... \mid \circlearrowleft \right)$$

Cette représentation permet une approche polynomiale et de façon similaire aux codes cycliques qui sont des idéaux de l'anneau $\mathbb{F}[X]/\langle X^n - 1\rangle$ alors les codes quasi-cycliques sont ici des sous-modules de R^l sur R où $R = \mathbb{F}[X]/\langle X^n - 1\rangle$.

On peut représenter le code C par la matrice polynomiale suivante :

$$\begin{pmatrix} g_{11} & g_{12} & ... & g_{1l} \\ 0 & g_{22} & ... & g_{2l} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & ... & g_{ll} \end{pmatrix}$$

où les g_{ij} sont des polynômes engendrant des codes cycliques. De plus les éléments diagonaux g_{ii} divisent $X^m - 1$.
On obtient ainsi une matrice génératrice sous forme canonique :

$$\left(\begin{array}{c|c|c|c} g_{11} & g_{12} & ... & g_{1l} \\ Xg_{11} & Xg_{12} & ... & Xg_{1l} \\ \vdots & \vdots & & \vdots \\ X^{m-deg(g_{11})-1}g_{11} & X^{m-deg(g_{11})-1}g_{12} & ... & X^{m-deg(g_{11})-1}g_{1l} \\ \hline 0 & g_{22} & ... & g_{2l} \\ 0 & Xg_{22} & ... & Xg_{2l} \\ \vdots & \vdots & & \vdots \\ 0 & X^{m-deg(g_{22})-1}g_{22} & ... & X^{m-deg(g_{22})-1}g_{2l} \\ \hline & & \ddots & \\ \hline 0 & 0 & ... & g_{ll} \\ 0 & 0 & ... & Xg_{ll} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & ... & X^{m-deg(g_{ll})-1}g_{ll} \end{array}\right)$$

où les éléments diagonaux g_{ii} divisent $X^m - 1$ et les g_{ij} , avec $i < j$ sont réduits modulo g_{jj} .

3.3.2 Comme code cyclique sur un anneau

On utilise le quasi-shift suivante :

$$\tau_2 = T^l = (1; l+1; ...; (m-1)l+1)(2; l+2; ...; (m-1)l+2)...(l; 2l; ...; ml).$$

Alors un code C est dit quasi-cyclique si et seulement si $\tau_2 \in Aut(C)$.
Cette permutation correspond à un décalage circulaire par blocs de taille l .
On définit une matrice génératrice de ce code dans cet cas sous la forme :

$$\begin{pmatrix} A_1 & A_2 & ... & A_m \\ A_m & A_1 & ... & A_{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & ... & A_1 \end{pmatrix} = \begin{pmatrix} A_1 \; A_2 \; ... \; A_m \\ \\ \circlearrowleft \\ \\ \end{pmatrix}$$

où les A_i sont des matrices de taille $j \times l$ avec$j \leqslant l$.
Dans ce cas le code est vu comme un code cyclique par blocs, cette représentation les codes quasi-cycliques sont comme codes sur l'anneau de polynômes $\mathbb{F}[X]/\langle X^m - 1\rangle$.

Bibliographie

[1] N. Bourbaki. Alg'ebre : Chapitre 8. Springer Verlag, 2011.

[2] François Dumas, ALGÈBRE : GROUPES ET ANNEAUX 1 , Université Blaise Pascal U.F.R. Sciences et Technologies ; 2007-2008.

[3] Serir Khadidja, Application des codes correcteurs d'erreurs *ReedMuller* , université Aboo Bakr Belkaid.Tlemcen ; 2011 .

[4] Claude Cartel, cours de code correcteurs d'erreurs (et fonction boolément) , D.E.A de Mathématique et Informatique de Bamako ; 2007 .

[5] Jean-Guillaume Dumas, Jean-Louis Roch,Éric Tannier, Sébastien Varrette, Théorie des codes Compression , cryptage , correction , *Dunod*, Paris ; 2007, 2013.

[6] Sahraoui Alaeddine, Les codes Simplexe , Université Laarbi Ben M'hidi Oum El-BOUAGHI ; 2013.

[7] B. Rouzeyre, Codes détecteurs et correcteurs .

[8] Structures algébriques : groupes , anneaux et corps , Maths *PCSI*.

[9] Pierre *Abbrugiati*, Introduction aux codes correcteurs d'erreurs , 23 janvier 2006.

[10] Licence Math-Info 1 ère année, Résume sur les structures algébriques des ensembles avec opérations Groupes , Université Claude Bernard Lyon 1 ; Printemps 2012.

[11] Marc Chaumont, Codes Correcteurs d'erreurs Cours 1 + Introduction + Codes linéaires en bloc ; Novembre 12, 2008

[12] Yuri Bazlov ,MATH32032 Coding Theory - 2017/18 Semester 2 ,Manchester University

[13] A. ALAMADHI , H. SBOUI, P. SOLÉ and O.YEMEN , Cyclic Codes over ($M_2(\mathbb{F}_2)$, Arxiv , 31/01/2012

[14] Nuh Aydin, An Introduction to Cording Theory via Hamming Codes :A Computational Science Model, Kenyon College, aydinn@Kenyon.edu, 8 -2007

[15] N. Aydin,T.Asamov and T. Aaron Gulliver, Some Open Problems on Quasi-Twisted and Related Code Constructions and Good Quaternary Codes,ISIT2007, Nice, France, June 24 ? June 29, 2007

[16] Christophe CHABOT,Reconnaissance de codes,structure des codes quasi-cycliques , Université de Limoges, 2009

[17] M. Barbier, C. Chabot and G. Quintin, On Quasi-Cyclic Codes as a Generalization of Cyclic Codes, arXiv 2012.

[18] F.J. MacWilliams and N.J.A. Sloane. The theory of error-correcting codes. North-Holland mathematical library. North-Holland, 1986.

[19] P.-L. Cayrel, C. Chabot, and A. Necer. Quasi-cyclic codes as codes over rings of matrices. Finite Fields and Their Applications, 16(2) :100 ?115, 2010.

[20] C. Chabot. Factorisation in M ?(Fq)[X]. Construction of quasi-cyclic codes. In WCC 2011 - Workshop on coding and cryptography, pages 209 ?218, Paris, France, apr 2011.

Résumé

La communication est un besoin fondamental de notre vie moderne. En fait, la communication est quelque chose que les humains font depuis longtemps,l'échange numérique d'informations se fait par des canaux de communication comme le câble, la fibre optique, le wifi, les satellites ...etc.
Bien sûr dans notre moderne monde numérique, toutes sortes d'entités communiquent. Les erreurs sont également présentes dans le monde numérique.

Les codes correcteurs d'erreurs sont des moyens astucieux de représenter les données afin qu'on peut récupérer les informations d'origine même si certaines parties sont corrompues. Les codes ont également des applications dans des domaines qui ne sont pas directement liés à la communication.par exemple aux supports pour le stockage comme disque compact, Pour le code cyclique défini sur $\mathbb{F}_{64}$ est plus largement utilisé pour les CD ROM.

la structure des codes quasi-cycliques considéré comme une généralisation des codes cycliques, ces codes sont utilisés en particulier en cryptographie car ils permettent d'utiliser des clés plus petites.

Notre travail est seulement une entrée sur les codes quasi-cycliques cette recherche de congé aux personnes intéressée dans ce domaine.

Abstract

Communication is a basic need of our modern life. In fact, communication is something that humans have been doing for a long time, the digital exchange of information takes place through communication channels like cable, fiber optics, wifi, satellites ... etc.
Of course in our modern digital world, all kinds of entities communicate. Errors are also present in the digital world.

Error correcting codes are nifty ways of representing data so that one can recover the original information even if some parts are corrupted. The codes also have applications in areas that are not directly related to communication ; for example to media for storage as compact disc, For the cyclic code defined at $\mathbb{F}_{64}$ is more broadly used for CD ROMs.
The structure of quasi-cyclic codes considered as a generalization of cyclic codes, these codes are used in particular in cryptography because they allow the use of smaller keys.

Our work is only one entry on quasi-cyclic codes that leave to people intersted in this area.

ملخص

التوَاصل هو حَاجة أسَاسية في حيَاتنَا الحديثة. و في الوَاقع الَاتصَالَات يقوم بهَا البشر منذ القدم.
يتم التبَادل الرقمي لِلمعلومَات من خلَال قنوَات اتصَال مثل الكَابل و الَاليَاف البَصرية الويفي و الَاقمَار الَاصطنَاعية... الخ و بَالطبع توجد هنَاك اخطَاء في نقل هذه المعلومَات .
نظرية الترميز المصحِحة لِلَاخطَاء تعتبر أحسن الطرق لتمثيل البيَانَات بحيث يمكن لِلشخص استعَادة المعلومَات الأصلية حتَى في حَالة تلف جزءٍ منهَا .
تطبق أيضَا هذه النظرية في بعض المجَالَات التي لَا ترتبط بَالَاتصَالَات، علَى سبيل المثَال أجهزة التخزين مثل اقرَاص المضغوطة و التي يستعمل من أجلهَا الترميز الدوري المعرف علَى $\mathbb{F}_{64}$.
تعتبر الترميزَات الشبه دورية بمثَابة تعميم لِلترميزَات الدورية، و تستخدم بشكل خَاص في نظرية التشفير لأنهَا تستخدم مفَاتيح أصغر.
تعتبر مذكرتنَا مَا هي إِلَا مجرد مدخل الَى هذه الترميزَات الشبه دورية ، و بهذَا نترك البحث لِلمهتمين في هذَا المجَال .