UNIVERSITE MOHAMED BOUDIAFDE M'SILA

Faculté des Mathématiques et de l'Informatique

Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du Diplôme de **MASTER**

Domaine : Mathématiques et Informatique

Filière Mathématiques**:**

Option :Algèbre et Mathématiques Discrète

Par

GACEMI Amina

Sujet

Codes et Courbes Algèbriques

Devant le jury :

Mr A. AMROUNE	Prof. Univ de M'sila	Président
Mr L. LADJELAT	Prof. Univ de M'sila	Encadreur
Mr A. SAADI	Prof. Univ de M'sila	Examinateur

Promotion : 2018 / 2019

Remerciements

Je doit remercier ALLAH qui a nous donné la force et la patience d'accomplir ce modeste travail.

Je tiens à remercier mon Encadreur de mémoire Monsieur ***L.LADJELAT*** *pour ses orientations et son accompagnement avec beaucoup de patience.*

Je tiens aussi à remercier Monsieur ***A.AMROUNE*** *pour l'intérêt qu'il a porté à mon travail. c'est pour moi un honneur qu'il a accepté de présider le jury.*

Je suis trés reconnaissant à Monsieur ***A.SAADI*** *d'avoir accepter d'examiner ce travial et de me faire l'honneur de participer au jury.*

Dédicace

A ma famille.

Notations :

- $\mathbb{F}_q$: corps fini d'ordre q
- $Car(k)$: caractéristique de $\mathbb{F}_q$
- $[K : \mathbb{F}_q]$: dimention K de sur $\mathbb{F}_q$
- I_k : matrice unitaire d'ordre k
- H^t : transposé de H
- $\mathcal{C}$: code
- C : courbe algèbrique
- $\hat{C}_f$: fermeture projective
- $C(K)$: ensemble de tous $K-$points rationnels sur C
- D : diviseur sur C

Table des matières

Introduction

Dans les années 1980, Le mathématicien russe Goppa a lié les codes aux courbes algèbriques, ce qui a conduit à une évolution de la théorie du codage, depuis lors ; l'intérêt de nombreux mathématiciens s'est tourné vers ce domaine.

Tsfasman, Vladut et Zink utilisent l'idée de Goppa pour prover l'existance de code de meilleurs paramètres que ceux assurés par la borne de Gilbert-Varshamov. Maintenant, l'essentiel des travaux sur les codes géomitriques sur des courbes algèbriques recherchent un algoritheme de codage plus rapide et efficace.

Danc ce mémoire, on s'intéresse à étudier l'utilisations du codage sur des courbes algèbriques.

Le premier chapitre est un chapitre d'introduction de corps finis et codes où présenté quelque définitions et propriétés fondamentales.

Le deuxiéme chapitre est consacré à l'étude les courbes algèbriques et on va voir certaines notions, propriétés et théorèmes qui sont plus importantes, en fin on va décrire la constraction des codes géométriques.

Chapitre 1

Notion de base sur codes et corps finis

Dans ce chapitre, nous donnons les définitions et les concepts de base, nous commençons par les corps finis, nous passerons ensuite à les codes.

1.1 Corps finis

On commence cette section par des définition de base concernant les anneaux et les corps.

Définition 1.1. *Un anneau est un triplet* $(A, +, .)$ *tel que*

(1) A *est un ensemble non vide,*

(2) l'adition " $+$ " *et multiplication* "." *sont deux lois internes dans* A *vérifiant :*

(2-1) $(A, +)$ *est un groupe commutatif ;*

(2-2) "." *est associative :* $\forall x, y, z \in A \ \ (x \cdot y) \cdot z = x \cdot (y \cdot z)$;

(2-3) "." *distributive par rapport à la loi "+"* $\forall x, y, z \in A,$

$$\begin{cases} x.(y+z) = x.y + x.z \\ (x+y).z = x.z + y.z \end{cases}$$

Remarque 1.1.

(1) 0 est l'élément neutre de $(A, +)$ appellé le zéro de A ;

(2) Si la loi "." possède un élément neutre noté "1", on dit que A est anneau **unitaire** et 1 est l'unite de A ;

(3) Si "." est commutative, on dit que l'anneau A est commutatif.

Exemple 1.1. $(\mathbb{Z}/n\mathbb{Z}, +, .)$ est l'anneau des entiers modulo n.

Définition 1.2. *Un corps est anneau unitaire non trivail (A,+,.) tels que tout élément* $x \in A \setminus \{0\}$ *est inversible.*

Définition 1.3. *Un corps finis est un corps qui possède un nombre fini d'éléments, on note un corps fini d'order q par* $\mathbb{F}_q$ *(Field of ordre q) où GF(q) (Galois field of order q).*
Un corps fini est de caractéristique premier.

Proposition 1.1. 1. *Tout corps fini de caractéristique p (premier) est extension du corps*

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

2. *Si K un corps fini d'ordre q alors* $q = p^n$ *où* $p = car(K)$ *est premier et* $n = [K : \mathbb{F}_q] \geq 1$.

3. *Si K est un corps fini d'ordre q alors* $\forall x \in K \quad x^q = x$.

Théorème 1.1. *Soit* $n, m \in \mathbb{N}^*$, *p premier* $\quad m/n \Leftrightarrow \mathbb{F}_p^m \subset \mathbb{F}_p^n$

Exemple 1.2. On détermine tous les sous corps de $\mathbb{F}_{16} = \mathbb{F}_{2^4}$

On a $\quad \mathbb{F}_{2^m} \subset \mathbb{F}_{2^4} \Leftrightarrow m/4 \Leftrightarrow m \in \{1, 2, 4\}$.

Donc les sous corps de $\mathbb{F}_{16}$ sont $\quad \mathbb{F}_2,\ \mathbb{F}_{2^2} = \mathbb{F}_4,\ \mathbb{F}_{16}$.

1.2 Codes

Nous commençons ce section par généralités sur les codes, ensuite nous passerons à les codes linéaire, et donnons les principales bornes sur les codes, enfin nous donnons la définition est les proncipales propriétés des codes cycliques.

1.2.1 Généralités sur les codes

Définition 1.4. *Soit* $\mathbb{F}$ *un ensemble fini dit* ***alphabet****, M et n deux entiers strictement positifs.*
On appele ***mot*** *de longueur n une suite* $b_1 b_2 ... b_n$, *où pour tout* $i \in 1, ..., n, b_i \in F$.
Un code est donc tout partie non vide $\mathcal{C} \subset \mathbb{F}^n$ *de cardinal* $card(\mathcal{C}) = M$, *la dimension n de* $\mathbb{F}^n$ *est appelée la longueur du code.*

Exemple 1.3. Soit $\mathcal{C} = \{101, 001\} \subset \mathbb{F}_2^3$ est un code de longueur 3 et de cardinal 2 sur $\mathbb{F}_2$.

Définition 1.5. *La distance de* ***Hamming*** *de x à y de $\mathbb{F}^n$ est le nombre $d_H(x, y)$ défini par :*

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

Exemple 1.4. Dans $\mathbb{F}_2^3$, nous avons $d_H(101, 110) = 2$.

Proposition 1.2. *L'application $d_H : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{R}$ définie par :*

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

est une distance sur $\mathbb{F}_q^n$.

Démonstration. Pour tout $x, y, z \in \mathbb{F}_q^n$

(i) $d_H(x, y) \geq 0$ et $d_H(x, y) = 0 \Leftrightarrow x = y$;

(ii) $d_H(x, y) = d_H(y, x)$;

(iii) $d_H(x, y) \leq d_H(x, z) + d_H(z, y)$.

□

Définition 1.6. *Le poids de* ***Hamming*** *d'un mot $x = x_1, x_2, ..., x_n$, est le nombre naturel :*

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

Exemple 1.5. Dans $\mathbb{F}_2^3$, nous avons $W_H(110) = 2$.

Définition 1.7. *La distance minimale d'un code $\mathcal{C}$ est la distance minimum entre deux mots distincts de code, c-à-d.*

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

.

Exemple 1.6. On prend $\mathbb{F}_q = \mathbb{F}_2$, $n = 4$.

Soit $\mathcal{C} = \{0000, 1100, 0101, 1111\} \subset \mathbb{F}_2^4$.

On a

$d_H(0000, 1100) = 2,\ d_H(1100, 0101) = 2$

$d_H(0000, 0101) = 2,\ d_H(1100, 1111) = 2$

$d_H(0000, 1111) = 4,\ d_H(0101, 1111) = 2$

donc

$$d(\mathcal{C}) = min\{2, 4\} = 2.$$

Définition 1.8. *Le poids minimal d'un code $\mathcal{C}$ est l'entier :*

$$\mathrm{W}_{min}(\mathcal{C}) = \mathrm{W}_{min} = Min\{W_H(x) : x \in \mathcal{C},\ x \neq 0\}.$$

Exemple 1.7. On prend $\mathbb{F}_q = \mathbb{F}_2,\ n = 4.$

Soit $\mathcal{C} = \{0000, 1100, 0101, 1111\} \subset \mathbb{F}_2^4$

On a $\mathrm{W}_{min}(\mathcal{C}) = 2$;

Les entiers $n,\ M,\ d$ sont appelés les paramètre de $\mathcal{C}$ et on dit que $\mathcal{C}$ est un code de type (n, M, d) sur $\mathbb{F}_q$.

Théorème 1.2. *Un code $\mathcal{C}$ de paramètre (n, M, d) peut détecter $d-1$ erreurs et corriger $[\frac{d-1}{2}]$ erreurs.*

Démonstration. 1. *Soit $x \in \mathcal{C}$ est envoyé, $y \in \mathbb{F}_q^n$* est réçu.

On a $d(\mathcal{C}) = min\{d_H(c_1, c_2) : c_1, c_2 \in \mathcal{C}, c_1 \neq c_2\}$

y ne peut être un mot de code de $\mathcal{C}$, $d_H(x, y) \leq d - 1$, dans ce cas $y \notin \mathcal{C}$ il y a au plus $d - 1$ erreurs.

2. Soit $\mathcal{C} = \{c_1, c_2, ..., c_M\}$ et considérons les boules de centre de mot code et de rayan $t = [\frac{d-1}{2}]$, $B(c_1, t),\ B(c_2, t), ...,\ B(c_M, t)$.

   Suppose $y \in \mathbb{F}_q^*$, et $d_H(x, y) \leq t$.

   $y \in B(c_1, t) \sqcup B(c_2, t) \sqcup, ..., \sqcup B(c_M, t)$ donc, il existe boule unique $B(c_{i_0}, t)$ tel que

   $y \in B(c_{i_0}, t)$ d'aprés la proposition pécédente $c_{i_0} \in \mathcal{C}$ vérifie la minimalité de la distance des mots de codes à y, donc y est décode par c_{i_0}.

□

1.2.2 codes linéaires

Définition 1.9. *Un code linéaire de longueur n sur $\mathbb{F}_q$ est un sous-espace vectoriel de $\mathbb{F}_q^n$.*

Remarque 1.2.

(i) La dimension d'un code linéaire est sa dimension comme espace vectoriel ;

(ii) $\mathcal{C}$ est un code de dimension k sur $\mathbb{F}_q$ alors $M = q^k$;

(iii) Un code linéaire de paramètres $[n, q^k, d]$ est un code de paramètres (n, q^k, d) sur $\mathbb{F}_q$.

Proposition 1.3. *La distance minimal d'un code linéaire est égale à son poids minimal.*

Matrice génératrice

Soit $\mathcal{C}$ un code linéaire de paramètre $[n, q^k, d]$ sur $\mathbb{F}_q$, $dim\mathcal{C} = k$.

Définition 1.10. *Une matrice gératrice du code $\mathcal{C}$ est une matrice de type $k \times n$ sur $\mathbb{F}_q$ dont les lignes forment une base de $\mathcal{C}$ sur $\mathbb{F}_q$.*

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & a_{k2} & \cdots & g_{kn} \end{pmatrix}$$

Proposition 1.4. *Si G est une matrice génératrice de $\mathcal{C}$ alors*

$$\mathcal{C} = \{mG/m \in \mathbb{F}_q^k\}$$

i.e, $x \in \mathcal{C} \Leftrightarrow \exists m \in \mathbb{F}_q^k : x = mG$.

Démonstration. Soient $x \in \mathbb{F}_q^n, m \in \mathrm{F}_q^k$

On a $x \in \mathcal{C} \Leftrightarrow \exists m_1, m_2, ..., m_k \in \mathbb{F}_q^k : x = m_1 g_1, m_2 g_2, ..., m_k g_k .....(*)$

$$mG = (m_1, m_2, ..., m_k) \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & a_{k2} & \cdots & g_{kn} \end{pmatrix}$$

$$\begin{aligned} mG &= (m_1 g_{11} + ... + m_k g_{k1}, ..., m_1 g1n + ... + m_k g_{kn} \\ &= m_1(g_{11}, ..., g_{1n} + ... + m_k(g_{k1}, ..., g_{kn}) \\ &= m_1 g_1 + m_2 g_2 + ... + m_k g_k. \end{aligned}$$

D'aprés $(*)$

$$x \in \mathcal{C} \Leftrightarrow \exists\, m \in \mathbb{F}_q^k : x = mG.$$

□

Exemple 1.8. Soit $\mathcal{C}$ un code linéaire de matrice génératrice $G = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

$$\begin{aligned} \mathcal{C} &= \{mG : m \in \mathbb{F}_2^2\} \\ &= \{(m_1, m_2) \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} : (m_1, m_2) \in \mathbb{F}_2^2\} \\ &= \{(m_1, m_1 + m_2, m_1 + m_2) : m_1, m_2 \in \mathbb{F}_2^2\} \\ &= \{(0,0,0), (0,1,1)(1,1,1), (1,0,0\} \end{aligned}$$

Finalement, $[n, k, d] = [3, 2, 1]$.

Définition 1.11. *Soit $\mathcal{C}$ un code linéaire de longueur n et de demension k.*

$x = x_1, x_2, ..., x_n,\ y = y_1, y_2, ..., y_n$ deux vecteurs de $\mathbb{F}_q^n$.

Le produit scalaire $< x, y >$ sur F_q défini par :

$< x, y >= x.y = x_1 y_1 + x_2 y_2 + ...x_n y_n = \sum_{k=1}^{n} x_\imath y_\imath$

x est orthogonal à y si $< x, y >= 0$, dans ce cas on écrit $x \perp y$.

Le code dual de $\mathcal{C}$ est l'ensemble $\mathcal{C}^\perp$ définie par :

$$\mathcal{C}^\perp = \{y \in \mathbb{F}_q^n :< x, y >= 0, \forall x \in \mathcal{C}\}$$

.

Matrice de controle

Définition 1.12. *Soit $\mathcal{C}$ un $[n,k]$-code, une matrice de controle H de $\mathcal{C}$ est une matrice génératrice du dual $\mathcal{C}^{\perp}$.*

Remarque 1.3. H est de type $(n-k)\times n$ sur $\mathbb{F}_q$

Proposition 1.5. *Si $\mathcal{C}$ est un code linéaire de paramètre $[n,k]$ de matrice génératrice G et de matrice de controle H alors, $GH^t = 0$*
Cas particuliere "forme standard" :

1. *Si $G = (I_k/A)$ alors $H = (-A/I_{n-k})$;*

2. *Si $H = (B/I_{n-k})$ alors $G = (I_k/A)$.*

Proposition 1.6. *Soit $\mathcal{C}$ un code linéaire de paramètre $[n,k]$ sur $\mathbb{F}_q$ et H la matrice de controle, alors on a*

$$x \in \mathcal{C} \Leftrightarrow xH^t = 0 \Leftrightarrow H^t x = 0$$

Exemple 1.9. Soit $\mathcal{C}$ un [2,4]-code sur $\mathbb{F}_3$ de matrice de controle H :

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix} = (A|I_2)$$

Alors, la matrice génératrice G de la forme *:* $G = (I_2|-A) = \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$

1.2.3 Bornes sur les codes

Théorème 1.3. *(Borne de Hamming)([7])*
Si $\mathcal{C}$ est un $(n,M,d)-$code sur $\mathbb{F}_q$ alors,

$$M \sum_{i=1}^{[\frac{d-1}{2}]} \binom{n}{i} (q-1)^i \leq q^n$$

Démonstration. Soit $\mathcal{C} = \{c_1, c_2, ..., c_M\}$, $t = [\frac{d-1}{2}]$.

On considère les boules de centre $c_1, c_2, ..., c_M$ et de rayant t i.e, les boules $B(c_1, t), B(c_2, t), ..., B(c_M, t)$.

On sait que si $c_i \neq c_j$, alors $B(c_i, t) \cap B(c_j, t) = \emptyset$.

$$|B(c_i, t)| = |B(c_j, t)| = \sum_{i=1}^{[\frac{d-1}{2}]} \binom{n}{i} (q-1)^i$$

on a

$$\bigcup_{i=1}^{M} B(c_i, t) \subseteq \mathbb{F}_q^n$$

donc

$$|\bigcup_{i=1}^{M} B(c_i, t)| \leq \mathbb{F}_q^n$$

d'où

$$M \sum_{i=1}^{[\frac{d-1}{2}]} \binom{n}{i} (q-1)^i \leq q^n$$

. □

Théorème 1.4. *(Borne de Singleton)([7])*

Si $\mathcal{C}$ est un $(n, M, d)-$code sur $\mathbb{F}_q$ alors $M \leq q^{n-d+1}$

Démonstration. Soit $C = \{c_1, c_2, ..., c_M\}$ tel que :

$c_1 = (c_{1,1}, c_{1,2}, ..., c_{1,d-1}, c_{1,d}, ..., c_{1,n})$

$c_2 = (c_{2,1}, c_{2,2}, ..., c_{2,d-1}, c_{2,d}, ..., c_{2,n})$

$\vdots$

$c_M = (c_{M,1}, c_{M,2}, ..., c_{M,d-1}, c_{M,d}, ..., c_{M,n})$

posons

$$D = \{\underbrace{c_{1,d}...c_{1,n}}_{x_1}, \underbrace{c_{2,d}...c_{2,n}}_{x_2}, ..., \underbrace{c_{M,d}...c_{M,n}}_{x_M}\}$$

les vecteur $x_1, x_2, ..., x_n$ sont des vecteur de longueur $n-d+1$ sur $\mathbb{F}_q^{n-d+1}$

les vecteur $x_1, x_2, ..., x_n$ sont deux à deux deux différents, suppposons qu'il existe $x_i = y_j$ $i \neq j$

$c_{i,d}, c_{i,d+1}, ..., c_{i,n} = c_{j,d}, c_{j,d}, ..., c_{j,n}$ ils sont correspondants à $c_i = c_{i,1}, ..., c_{i,d-1}, c_{i,d}, ..., c_{i,n}$

$c_j = c_{j,1}, ..., c_{j,d-1}, c_{j,d}, ..., c_{j,n}$

$d \leq d(c_i, c_j) \leq d-1$ (contradiction au fait que d est la distance minimal de $\mathcal{C}$.

Donc

$$|D| = M \leq |\mathbb{F}_q^{n-d+1}| = q^{n-d+1}.$$

□

Remarque 1.4. Si $\mathcal{C}$ est $(n, M, d)-$code linéaire sur $\mathbb{F}_q$, alors

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

.

Définition 1.13. (Le code de Reed − Solomon)([1], [2], [7]) *Soit* $t \in \mathrm{Z},\ 1 \leq t \leq q-1, q$ *un puissace premier*

Soit $\mathbb{F}_q[X]$ *l'anneau des polynomes à une variable sur* $\mathbb{F}_q$, *on définit l'ensemble :*

$$L_{t-1} = \{f \in \mathbb{F}_q[X] : deg(f) \leq t-1\}$$

Le code de **Reed − solomon** *définit par :*

$RS(t,q) = \{(f(\alpha_1), \ldots, f(\alpha_{q-1})) : f \in L_{t-1}, \alpha_1, ..., \alpha_{q-1} \in \mathbb{F}_q\}$

est un code linéaire de type $[q-1, t, n-t+1]$

Démonstration. 1. RS(t,q) est code lineaire (espace vectoriel) car

- Soit $x, y \in RS(t,q)$.

  $x = (f(\alpha_1), \ldots, f(\alpha_n)),\ y = (g(\alpha_1), \ldots, g(\alpha_{q-1}))$ *avec* $f, g \in L_{t-1}$.

$$\begin{aligned} x - y &= (f(\alpha_1), \ldots, f(\alpha_{q-1})) - (g(\alpha_1), \ldots, g(\alpha_{q-1})) \\ &= (f(\alpha_1) - g(\alpha_1), \ldots, f(\alpha_n) - g(\alpha_{q-1})) \\ &= ((f-g)(\alpha_1), \ldots, (f-g)(\alpha_{q-1})) \end{aligned}$$

  On a

$$\deg(f-g) \leq \max\{\deg(f), \deg(g)\}$$

$$\deg(f-g) \leq t-1 \ i.e,\ f-g \in L_{t-1}$$

  Alors

$$x - y \in RS(t,q)$$

– Soit $\lambda \in \mathbb{F}_q,\ x \in RS(t,q)$

On a

$$\begin{aligned}\lambda x &= \lambda(f(\alpha_1), \ldots, f(\alpha_{q-1})) \\ &= (\lambda f(\alpha_1), \ldots, \lambda f(\alpha_{q-1}))\end{aligned}$$

Si $\lambda = 0 \Rightarrow \lambda f = 0$ de degré $\leq t-1$

Si $\lambda \neq 0 \Rightarrow \deg(f) = \deg(\lambda f) \leq t-1$

Donc $\quad \lambda f \in L_{t-1}$, d'où $\ \lambda x \in RS(t,q)$

Finalement, $RS(t,q)$ est un code lineaire.

2. Il est claire que $RS(t,q)$ est de longueur $q-1$.

3. On montre que $\dim RS(t,q) = t$:

Soit $V \in RS(t,q)$, alors $\exists f \in L_{t-1} :\ f(x) = a_0 + a_1 x + ... + a_{t-1}x^{t-1}$ où $a_i \in \mathbb{F}_q$,

$0 \leq i \leq t-1$

On a

$$\begin{aligned}V &= (f(\alpha_1), \ldots, f(\alpha_{q-1})) \\ &= (a_0 + a_1\alpha_1 + ... + a_{t-1}\alpha_1^{t-1}, ..., a_0 + a_1\alpha_{q-1} + ... + a_{t-1}\alpha_{q-1}^{t-1}) \\ &= a_0(1, ..., 1) + a_1(\alpha_1, ..., \alpha_{q-1}) + ... + a_{t-1}(\alpha_1^{t-1}, ..., \alpha_{q-1}^{t-1})\end{aligned}$$

Si on pose :

$e_0 = (1, ..., 1)$

$e_1 = (\alpha_1, ..., \alpha_{q-1})$

$e_2 = (\alpha_1^2, ..., \alpha_{q-1}^2)$

$\vdots$

$e_{t-1} = (\alpha_1^{t-1}, ..., \alpha_{q-1}^{t-1})$

On a $v = a_0e_0 + ... + a_{t-1}e_{t-1}$

Les vecteurs $e_0, e_1, ..., e_{t-1}$ engendre $RS(t,q)$.

$\sum_{i=1}^{t-1} a_i e_i = 0 \Leftrightarrow (f(\alpha_1), ..., f(\alpha_{q-1})) = (0, ..., 0)$

Alors $f(\alpha_1) = f(\alpha_2) = ... = f(\alpha_{q-1}) = 0$, donc $\alpha_1, \alpha_2, ..., \alpha_{q-1}$ sont des racine distinct de

f, comme $\deg(f) = t-1 < t \leq q-1$, alors f est polynome nul d'où

$a_0 = a_1 = ... = a_{q-1} = 0$, donc $e_0, e_1, ..., e_{t-1}$ sont libre en plus ils forment une base de $RS(t,q)$, finalement $\dim RS(t,q) = t$.

4. la distanse minimal de $RS(t,q)$ est $d = n-t+1$ parceque, d'un part D'apres le borne de singleton :

   $d \leq n-k+1$ i,e $d \leq n-t+1$, d'autre part $\exists x \in RS(t,q),\ x \neq 0,\ W_H(x) = d$, alors $x = (0,...,0,x_{i_1},...,x_{i_2},0,...,0,...,x_{i_d},0,...,0)$ tel que $x_{i_j} \neq 0, j \in \{i_1,...,i_d\}$ et comme $x = (f(\alpha_1), f(\alpha_2), ..., f(\alpha_{i_1}), ..., f(\alpha_{i_{t-1}}))$

   donc $f(\alpha_{i_1}) = x_{i_1} \neq 0, ..., f(\alpha_{i_d}) = x_{i_d} \neq 0$ et $x_j = f(\alpha_j) = 0, j \notin \{i_1,...,i_d\}$

   f possède au moin $q-1-d$ racine dans $\mathbb{F}_q$, on a $q-1-d \leq$ le nombre des racine de f dans $\mathbb{F}_q \leq \deg(f) = t-1$, c'est implique que $n-t+1 = q-t \leq d$. Finalement $d = n-t+1$.

□

Définition 1.14. *Pour $n \in \mathbb{N}^*$, $q = |\mathbb{F}_q|$, $d \in \mathbb{N}$ on definit :*

$$A_q(n,d) = Max\{M \in \mathbb{N} | \exists\ un(n,M,d) code\ sur\ \mathbb{F}_q\}$$

Remarque 1.5. Selon le borne de singloton on a *:*

$$A_q(n,d) \leq q^{n-d+1}$$

Théorème 1.5. *(Borne de Plotkin)([2])*

Soient $\mathcal{C}$ un $(n,M,d)-$code sur $\mathbb{F}_q$, $\theta = 1-\frac{1}{q}$

Si $d > n\theta$, alors, $M \leq \frac{d}{d-n\theta}$.

Démonstration. Soient $\mathcal{C}$ un $(n,M,d)-$code sur $\mathbb{F}_q$, $\theta = 1-\frac{1}{q}$

Considérons $S = \sum_{(x,y)\in\mathcal{C}^2} d(x,y),\ A = \{(x,y) \in \mathcal{C}^2 : x \neq y\}$

On a $|A| = M(M-1)$ et $S \geq \sum_{(x,y)\in A^2 x\neq y} d = d.M(M-1)$

donc $S \geq d.M(M-1)$.....(1)

Rappelons l'inégalité de Cauchy Schwarz :

Soient $x, y \in \mathbb{R}$, on a :

$| < x,y > |^2 \leq < x,x > . < y,y >$

$|\sum_{i=1}^{q} x_i y_i|^2 \leq (\sum_{i=1}^{q} x_i^2)(\sum_{i=1}^{q} y_i^2)$.....$(CS)$

Considérons la matrice $M \times n$ dont les lignes sont les mots de code de $\mathcal{C}$:

$$\begin{pmatrix} c_1^1 & c_1^2 & \cdots & c_1^i & \cdots & c_1^n \\ c_2^1 & c_2^2 & \cdots & c_2^i & \cdots & c_2^n \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_M^1 & a_M^2 & \cdots & c_M^i & \cdots & c_M^n \end{pmatrix}$$

Pour $\alpha \in \mathbb{F}_q$, le nombre m_α est le nombre de fois qu'apparait α dans la colonne i i.e,

$m_\alpha = |\{1 \leq i \leq M : c_j^i = \alpha\}|$, on a $\sum_{\alpha \in \mathbb{F}_q} m_\alpha = M$

$\exists M - m_\alpha$ élément de $\mathbb{F}_q$ différent de α dans le colonne i.

On a

$$\begin{aligned} S &= \sum_{(x,y) \in \mathcal{A}^{\in}} d(x,y) \\ &\leq \sum_{\alpha \in \mathbb{F}_q} m_\alpha (M - m_\alpha) \\ &= \sum_{\alpha \in \mathbb{F}_q} m_\alpha M - \sum_{\alpha \in \mathbb{F}_q} m_\alpha^2 \\ &\leq M \sum_{\alpha \in \mathbb{F}_q} m_\alpha - \sum_{\alpha \in \mathbb{F}_q} m_\alpha^2 .....(*) \end{aligned}$$

On prend $x = (1, ..., 1) \in \mathbb{R}^q,\ y = (m_\alpha, ..., m_\alpha) = m_\alpha \in \mathbb{R}^q$.

appliquons (CS)

$$\begin{aligned} &Ona\ (\sum_{\alpha \in \mathbb{F}_q} m_\alpha)^2 \leq (\sum_{\alpha \mathbb{F}_q} 1)(\sum_{\alpha \in \mathbb{F}_q} m_\alpha^2) \\ &alors\ M^2 \leq q(\sum_{\alpha \in \mathbb{F}_q} m_\alpha^2) \\ &donc\ -(\sum_{\alpha \in \mathbb{F}_q} m_\alpha^2) \leq \frac{-M^2}{q} .....(**) \end{aligned}$$

de $(*)$et $(**)$ on a $S \leq M^2 - \frac{-M^2}{q} = M^2\theta$, donc $S \leq M^2\theta$.....(2)

de (1) et (2) donnent $dM(M-1) \leq s \leq M^2\theta$, alors $dM^2 - dM \leq M^2\theta$

$dM - d \leq M\theta$, donc $dM - M\theta \leq d$ d'où $M(d - n\theta) \leq M(d - \theta) \leq d$

Si $d > n\theta$, alors $M \leq \frac{d}{d - n\theta}$ □

Théorème 1.6. *(Borne de Gilbert-Varshamav)*

On a n considérant les notation précedants :

$$A_q(n,d) \geq \frac{q^n}{\sum_{i=1}^{d-1} \binom{n}{i} (q-1)^i}$$

Démonstration. Soint $\mathcal{C}$ un $(n, A_q(n,d), d)-$code sur $\mathbb{F}_q$.

pour $x \in \mathcal{C}$ on a $B_{d-1}(x) = \{y \in \mathbb{F}_q^n : d_H(x,y) \leq d-1\}$

et on a $|B_{d-1}(x)| = \sum_{i=1}^{d-1} \binom{n}{i} (q-1)^i$.

Soit $y \in \mathbb{F}_q^n$, suppose que $y \in B_{d-1}(x)$, alors $d_H(x,y) \geq d-1$ d'où $d_H(x,y) \geq d \ \ \forall x \in \mathcal{C}$

Soit $D = \mathcal{C} \bigcup \{y\} \subset \mathbb{F}_q$, on a $|D| = M+1 > M = A_q(n,d)$.

Soient $x, z \in D$

Si $x = y = z$, on a $d_H(x,z) = 0$.

Si $(x,z) \in \mathcal{C}^2$, on a $d_H(x,y) \geq d$. Si $x \in \mathcal{C}$ ou $z = y$ ou $x = y$ et $z \in \mathcal{C}$, on a $d_H(x,y) \geq d$.

Alors d(D)=d, donc D est un $(n, m+1, d)$ code sur $\mathbb{F}_q$, ce qui est contradiction avec la construction de $\mathcal{C}$. □

1.3 Les bornes asymptotique

Définition 1.15. *([2],[8]) Soit $\mathcal{C}$ un $(n, q^k, d)-$code sur $\mathbb{F}_q$.*

Le taux d'information de $\mathcal{C}$ est $R = \frac{k}{n}$.

La distance minimale ralative de $\mathcal{C}$ est $\delta = \frac{d}{n}$ tel que $0 \leq R, \delta \leq 1$

Remarque 1.6. *Si $R = \delta = 1$* on dit que $\mathcal{C}$ est code parfait.

Définition 1.16. *([7],[8]) Soit q une puisance d'un premier et $\delta \in \mathbb{R}$, $0 \leq \delta \leq 1$. on a*

$$\alpha_q(\delta) = \limsup_{n \to \infty} \frac{1}{n} \log_q A_q(n, [\delta_n])$$

.

Remarque 1.7. $\alpha_q(\delta)$ est le plus grand valeur de R tel que il existe une suite des codes sur $\mathbb{F}_q$ avec une distance minimale relative qui converge vers δ et un taux d'information qui converge vers R

Théorème 1.7. *(Borne de Plotkin asymptotique)([7])*

avec $\theta = 1 - \frac{1}{q}$ *On a*

$\alpha_q(\delta) \leq 1 - \frac{\delta}{\theta} \quad 0 \leq \delta \leq \theta\,;$

$\alpha_q(\delta) = 0 \quad \theta \leq \delta \leq 1.$

Démonstration. [7] Premiérement, on suppose que $\theta < \delta \leq 1$ d'apres la théorème 1.5

$$\begin{aligned}
\alpha_q(\delta) &= \limsup_{n\to+\infty} \frac{1}{n} \log_q A_q(n, \lfloor \delta_n \rfloor) \\
&\leq \limsup_{n\to+\infty} \frac{1}{n} \log_q (\frac{\lfloor \delta_n \rfloor}{\lfloor \delta_n \rfloor - \theta n}) \\
&= \limsup_{n\to+\infty} \frac{1}{n} \log_q A_q (\frac{\delta_n}{\delta_n - \theta n}) \\
&= 0.
\end{aligned}$$

Deuxièment, On suppose que $0 < \delta \leq \theta$ et $\{\mathcal{C}_i\}$ suite de code de longueur $\{n_i\}$, de cardinal $\{M_i\}$ et de distance minimal $\{d_i\}$, en plus elle satisfait $\lim \frac{n_i}{d_i} = \delta$, $\lim \frac{\log_q(M_i)}{n_i} = \alpha_q(\delta)$ et $n'_i = [\frac{d_i - 1}{\theta}]$ $\forall i$.

En générale, si $\mathcal{C}$ est $(n, M, d)-$code sur $\mathbb{F}_q$, par le principe de pigenhole il existe au moins $\frac{M}{q}$ mots de code qui sont terminer par le mème symbole.

On peut rendre $\mathcal{C}$ petit par prendre une partie de $\mathcal{C}$ en ses mots de codes qui se terminent par mème symbole et supprimer la dernière coordonné, on obtient un code de longueur $n-1$, de distance minmale d et de cardinal supèrieur ou égale $\frac{M}{q}$.

Si on répète cette opération $n_i - n'_i$ fois avec $\{\mathcal{C}'_i\}$, on obtient un suite de code $\{\mathcal{C}'_i\}$ de longueur n'_i avec $M'_i \geq \frac{M_i}{q^{n_i - n'_i}}$ mot de code et distance minimal $d'_i \geq d_i$ par difénition de n'_i, on a $\theta n'_i \leq d_i - 1 \leq d'_i - 1$, on applique le théorème 1.5 à ce nouveau code, on trouve $\frac{M_i}{q^{n_i - n'_i}} \leq M'_i \leq \frac{d'_i}{d'_i - \theta n'_i} \leq d'_i$, c'est implique que $M_i \leq q^{n_i - n'_i} d'_i$.

On a

$$\begin{aligned}\alpha_q(\delta) &= \limsup_{n\to+\infty} \frac{1}{n}\log_q M_i \\ &\leq \limsup_{n\to+\infty} \frac{1}{n}\log_q(q^{n_i-n_i'}d_i') \\ &= \lim_{n\to+\infty}(1-\frac{n_i'}{n_i}+\frac{\log_q d_i'}{n_i}) \\ &\leq 1-\frac{\delta}{\theta}.\end{aligned}$$

□

Définition 1.17. *(Fonction d'Entropie de Hilbert)*([2],[7],[8])

La Fonction d'Entropie de Hilbert est :

$$H_q(x) = \begin{cases} 0 \quad Si \;\; x = 0 \\ x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x) \quad 0 < x < \theta \end{cases}$$

avec $\theta = 1-\frac{1}{q},\ x \in [0,\theta]$

Lemme 1.1.

Pour tout $0 \leq \lambda \leq \theta$, on a

$$\lim_{n\to+\infty}\frac{1}{n}\log_q V_q(n,[\lambda_n]) = H_q(\lambda)$$

Théorème 1.8. *(*[2],[7],[8]*) Pour tout* $0 \leq \lambda \leq \theta$*, on a*

$$\alpha_q(\delta) \geq 1 - H_q(\delta)$$

Démonstration.

$$\begin{aligned}\alpha_q(\delta) &= \limsup_{n\to\infty}\frac{1}{n}\log_q A_q(n,\lfloor\delta_n\rfloor) \\ &\geq \limsup_{n\to\infty}\frac{1}{n}\log_q A_q(n,\lfloor\delta_n\rfloor+1) \\ &\geq \lim_{n\to\infty}\frac{1}{n}\log_q(\frac{q^n}{V_q(n,\lfloor\delta_n\rfloor)}) \\ &= \lim_{n\to\infty}(1-\frac{1}{n}\log_q V_q(n,\delta_n)) \\ &= 1 - H_q(\delta)\end{aligned}$$

□

1.4 Codes cycliques

Définition 1.18. *Un codes cyclique est un code linéaire tel que tout permutation circulaire d'un mot du code est encore un mot du code.*

Autrement dit un code linéaire $\mathcal{C}$ de longueure n est cyclique Si :

$(c_0, c_1, ..., c_{n-1}) \in \mathcal{C}$, *alors* $(c_n - 1, c_0, c_1..., c_{n-2}) \in \mathcal{C}$.

Remarque 1.8. $(c_0, c_1, ..., c_{n-1}) \in \mathcal{C} \Leftrightarrow (c_{n-1}, c_0, c_1..., c_{n-2}) \in \mathcal{C} \Leftrightarrow (c_{n-2}, c_{n-1}, c_0, c_1..., c_{n-3}) \in \mathcal{C} \Leftrightarrow \ldots \Leftrightarrow (c_0, c_1, ..., c_{n-1}) \in \mathcal{C}$

Exemple 1.10. Le code binaire $\mathcal{C} = \{000, 101, 011, 110\}$ est code cyclique.

Soit $\mathbb{F}_q[X]$ l'anneau des polynomes sur $\mathbb{F}_q$, $\mathbb{F}_q[X]/ < x^n - 1 >$ est l'anneau quotient en plus $\mathbb{F}_q[X]/ < x^n - 1 >$ possède un structure d'espace vectoriel sur $\mathbb{F}_q$ de dimension n et base $\{1, \alpha, ..., \alpha^{n-1}\} = \{\overline{1}, \overline{x}, ..., \overline{x^{n-1}}\}$.
$R_n = \mathbb{F}_q[X]/ < x^n - 1 >= \{a_0 + a_1 x + ... + a_{n-1}x^{n-1}$ modulo $x^n - 1,\ a_i \in \mathbb{F}_q\}$ Pour $\mathcal{C}$ un code de $\mathbb{F}_q$ de longueur n, on définit :

$$\begin{aligned} I_{\mathcal{C}} &= \{c_0 + c_1 x + ... + c_{n-1}x^{n-1} \text{ modulo } < x^n - 1 >: (c_0, c_1, ..., c_{n-1}) \in \mathcal{C}\} \\ &= \{c_0 + c_1 x + ... + c_{n-1}x^{n-1} + < x^n - 1 >: (c_0, c_1, ..., c_{n-1}) \in \mathcal{C}\} \end{aligned}$$

Proposition 1.7. *$\mathcal{C}$ code cyclique de longueur $n \Leftrightarrow I_{\mathcal{C}}$ ideale de R_n.*

Théorème 1.9. *Soit $\mathcal{C}$ un code cyclique de longueur n de $\mathbb{F}_q$ et $I_{\mathcal{C}} = \{c_0 + c_1 x + ... + c_{n-1}x^{n-1} + < x^n - 1 >: (c_0, c_1, ..., c_{n-1}) \in \mathcal{C}\}$ l'ideal de $R_n = \mathbb{F}_q[X]/ < x^n - 1 >$ correspondant, alors il existe une unique polynome normalise $g \in \mathbb{F}_q[X]$ de degre minimal l tel que :*

1. $I_{\mathcal{C}} =< g(x) > / < x^n - 1 >$.
2. $< g(x)/ < x^n - 1 >$ *dans* $\mathbb{F}_q[X]$.

Remarque 1.9. Le polynome $g(x)$ du théorème est appellé le polynome générateur du code cyclique $\mathcal{C}$.

Matrice générateur

Soit $\mathcal{C}$ un code cyclique de $\mathbb{F}_q^n$ de polynome générateur $g(x) = g_0 + g_1x + ... + g_lx^l$, alors la matrice générateur de $\mathcal{C}$ donnée par :

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_l & 0 & \dots & 0 & 0 \\ 0 & g_0 & g_1 & \dots & g_l & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & g_0 & g_1 & \dots & g_l \end{pmatrix}$$

Matrice de controle

Soit $\mathcal{C}$ un code cyclique de $\mathbb{F}_q^n$, engendre par $g(x)$, le polynome de controle de $\mathcal{C}$ est donnée par :
$h(x) = \frac{x^n-1}{g(x)}$ tal que $deg(h) = n - deg(g) = \dim(\mathcal{C}) = k$, donc

$$H = \begin{pmatrix} h_k & h_k - 1 & \dots & h_0 & 0 & \dots & 0 & 0 \\ 0 & h_k & h_k - 1 & \dots & k_0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & h_k & h_k - 1 & \dots & h_0 \end{pmatrix}$$

Exemple 1.11. Soit le code cyclique $\mathcal{C}$ de $\mathbb{F}_2^3$, la factorisation de $x^3 - 1$ donne : $x^3 - 1 = (x - 1)(x^2 + x + 1)$, donc $g(x) \in \{1, x - 1; x^2 + x + 1, x^3 - 1\}$
En prenant, $g(x) = x - 1$ On a $l = 1, \dim(\mathcal{C}) = 3 - 1 = 2$, Alors

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

On a $h(x) = \frac{x^3-1}{x-1} = x^2 + x + 1$, *donc* $H = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$

$$\begin{aligned} \mathcal{C} &= \{a\begin{pmatrix} 1 & 1 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 & 0 \end{pmatrix} / a, b \in \mathbb{F}_2\} \\ &= \{\begin{pmatrix} 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}\} \end{aligned}$$

Chapitre 2

Courbes et Codes géométriques

2.1 Courbes Algèbriques

Définition 2.1. *([2],[7]) Soient K un corps, $f(x, y)$ un polynome de deux variable sur K.*
L'equation $f(x, y) = 0$ défini une courbe C_f dans le plan K^2.
L'ensemble de solution de cette equation dans K^2 est noté $C_f(K)$

Exemple 2.1. Soit l'equation $x^3 + x - y = -1$.
On considère le polynome $f(x, y) = x^3+x-y+1$ définie sur $K = \mathbb{R}$, la réprésentation graphique de f donnée par la figure ci-dessous

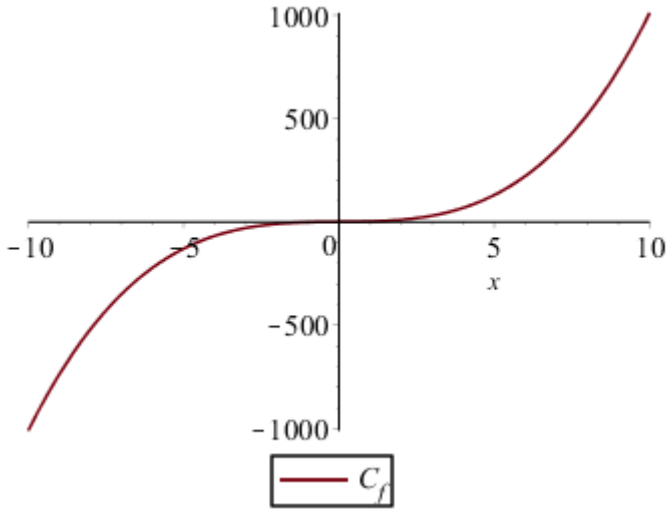

FIGURE 2.1 – Repésentation graphique de f dans $\mathbb{R}$

Si on pernd $K = \mathbb{F}_7$

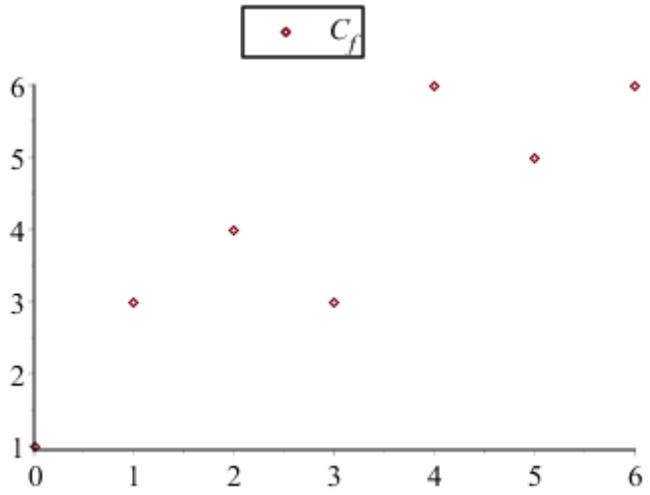

FIGURE 2.2 – Repésentation graphique de f dans $\mathbb{F}_7$

Remarque 2.1. *1.* Les solutions simultanées entre deux polynomes de deux variables sont les points d'intersecion de leur courbes .

2. En général, une courbe $C_f(K)$ tel que $f(x, y) \in K[X, Y]$ est appelé une courbe affine.

Définition 2.2. *([7],[2]) Soient K un corps, $f(x, y) \in K[X, Y]$ un polynome de degré d, C_f la courbe associées de f.*
La fermetur projective de C_f est :

$$\hat{C_f} = \{(\ X_0, Y_0, Z_0\ ) \in \mathbb{P}^2 : F(x, y, z) = 0\}$$

Tel que $d = deg(f)$ et $F(X, Y, Z) = Z^d f(\frac{X}{Z}, \frac{Y}{Z})$ est l'homogénisation de f.

Remarque 2.2.

1. $f(x_0, y_0) = 0 \Leftrightarrow F(x_0, y_0, 1) = 0$
2. Pour tout $\alpha \in K^\times$ on a :

$$F(\alpha X, \alpha Y, \alpha Z) = (\alpha Z)^d f(\frac{\alpha X}{\alpha Z}, \frac{\alpha Y}{\alpha Z}) = \alpha^d F(X, Y, Z)$$

   donc , $F(X_0, Y_0, Z_0) = 0 \Leftrightarrow F(\alpha X_0, \alpha Y_0, \alpha Z_0) = 0\ \ \forall \in K^\times$.
3. Comme F est homogénisation, $F(0, 0, 0) = 0$.

Exemple 2.2. Sur $K = \mathbb{R}$, on prend $f(x, y) = y^2 - x^3 - x - 1$.
L'homogénisation de f est

$$\begin{aligned} F(X, Y, Z) &= Z^3 f(\frac{X}{Z}, \frac{Y}{Z}) \\ &= Z^3(\frac{Y^2}{Z^2}) - Z^3(\frac{X^3}{Z^3}) - Z^3(\frac{X}{Z}) - Z^3 \\ &= ZY^2 - X^3 - Z^2X - Z^3. \end{aligned}$$

Soit K un corps, on considère la ralation $\sim$ sur K^3 définie par :
$(X_0, Y_0, Z_0) \sim (X_1, Y_1, Z_1) \Leftrightarrow \exists \alpha \in k^\times : X_1 = \alpha X_0, Y_1 = \alpha Y_0, Z_1 = \alpha Z_0$.
On montre que la relation $\sim$ est une relation d'équivalence

1. la relation $\sim$ est reflexive, en effet, pour tout $(X, Y, Z) \in K^3$ on a $X = 1X,\ Y = 1Y,\ Z = 1Z$.
2. la relation $\sim$ est symétrique, en effet, si $(X_0, Y_0, Z_0) \sim (X_1, Y_1, Z_1)$ alors $X_1 = \alpha X_0,\ Y_1 = \alpha Y_0,\ Z_1 = \alpha Z_0,$ donc comme k est corps $X_0 = \frac{1}{\alpha}X_1,\ Y_0 = \frac{1}{\alpha}Y_1,\ Z_0 = \frac{1}{\alpha}Z_1$ donc $X_0 = \beta X_1, Y_0 = \beta Y_1, Z - 0 = \beta Z_1$ d'où $(X_1, Y_1, Z_1) \sim (X_0, Y_0, Z_0)$
3. la relation $\sim$ est transitive, en effet, si$(X_0, Y_0, Z_0) \sim (X_1, Y_1, Z_1)$ et $(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$ alors $X_1 = \alpha X_0,\ Y_1 = \alpha Y_0,\ Z_1 = \alpha Z_0$. et $X_2 = \beta X_1,\ Y_2 = \beta Y_1,\ Z_2 = \beta Z_1$, donc $X_2 = \beta X_1 = \alpha X_0,\ Y_2 = \beta\alpha Y_0,\ Z_2 = \beta\alpha Z_0$ d'où $X_2 = \gamma X_0,\ Y_2 = \gamma Y_0,\ Z_2 = \gamma Z_0$.

Définition 2.3. *([7]) Soit K un corps, Le plan projectif est défini par :*

$$\mathbb{P}^2(K) = (K^3/\{(0, 0, 0)\})/\sim$$

Remarque 2.3.

(a) les points de $\mathbb{P}^2(K)$ sont classes des équivalances.

(b) $(X_0 : Y_0 : Z_0)$ est la classe d'équivalance de (X_0, Y_0, Z_0).

(c) $\mathbb{P}^2(K) = \{(X_0 : Y_0 : 1) | X_0, Y_0 \in K\} \cup \{(X_0 : 1 : 0) | X_0 \in K\} \cup \{1 : 0 : 0)\}$.
un point quelconque $(X_0 : Y_0 : Z_0)$ avec $Z_0 = 0$ est appellé un point a l'infini, tous les autres points sont appellés des points affines.

Exemple 2.3. $\mathbb{P}^2(\mathbb{Z}/2\mathbb{Z}) = \{(0:0:1),(0:1:1),(1:0:1),(0:1:0),(1:1:1),(1:1:0),(1:0:0)\}$

Théorème 2.1. *(Théorème de Bezout)([7])*

Si $f, g \in K[x,y]$ deux polynomes de degre d et e (resp)sans facteur commun, donc C_f et C_g s'intersectent au plus en de points, aussi $\hat{C}_f$ et $\hat{C}_g$ coupent exactement au points de $\mathbb{P}^2(k)$.

Exemple 2.4. Sur $\mathbb{R}$, on prend $f(x,y) = y - x^2$, $g(x,y) = x - c,\ c \in \mathbb{R}$

On peut remarquer les points d'intersection de C_f et C_g par la figure ci-dessous :

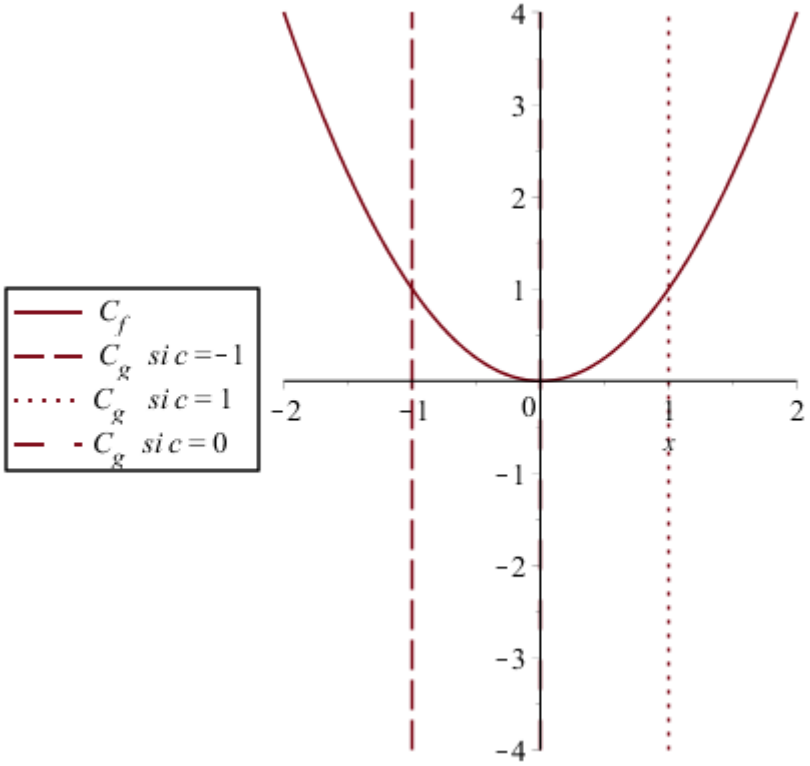

FIGURE 2.3 – Repésentation graphique de f et$g$

On a de 2.3 C_f et C_g sont s'intersectent en seul point, alors $1 \leq \deg(f)\deg(g) = 2 \cdot 1 = 2$.

Maintenant, on vas voir l'intersection de $\hat{C}_f$ et $\hat{C}_g$.

On a $F(X,Z,Y) = YZ - X^2$ et $G(X,Y,Z) = X - cZ$.

Si $Z = 1$

(a) $F(X,Y,1) = Y - X^2,\ F(X,Y,1) = 0 \Leftrightarrow Y = X^2$.

(b) $G(X,Y,1) = X - C,\ G(X,Y,1) = 0 \Leftrightarrow X = c.$

Alors $\hat{C_f} \cap \hat{C_g} = \{(c : c^2 : 1)\}$.

Si $Z = 0$

(a) $F(X,Y,0) = -X^2,\ F(X,Y,0) = 0 \Leftrightarrow X = 0.$

(b) $G(X,Y,0) = X,\ G(X,Y,0) = 0 \Leftrightarrow X = 0.$

Donc $\hat{C_f} \cap \hat{C_g} = \{(0 : 1 : 0)\}$.

Finalement, $\hat{C_f} \cap \hat{C_g} = \{(0 : 1 : 0), (c : c^2 : 1)\}$, d'où $|\hat{C_f} \cap \hat{C_g}| = 2 = \deg(f) \cdot \deg(g)$.

Définition 2.4. *Soient K corps,$f(x,y) \in K[X,Y]$ un polynome , $K = \mathbb{R}$ ou $\mathbb{C}$, La dérivée partielle de la fonction f par rapport à x en (x,y) est la dérivée de la fonction d'un seule variable $x \to f(x,y)$ où y est constant et noté $f_x(x,y)$.*

Exemple 2.5. On considère le polynome $f(x,y) = x^2 + y^3 + xy$, donc $f_x(x,y) = 2x + y,\ f_y(x,y) = 3y^2 + x$

Si $K = \mathbb{F}_2$, On trouve $f_x(x,y) = y$ et $f_y(x,y) = y^2 + x$.

Définition 2.5. *Soient K corps,$f(x,y) \in K[X,Y]$, on dit que le point (x_0,y_0) est point singulier Si $f(x_0,y_0) = f_x(x_0,y_0) = f_y(x_0,y_0) = 0$.*

Exemple 2.6. Soit $f(x,y) = x^4 + y^4 - x^3 + y^2$ sur $\mathbb{C}$.

On a $f_x(x,y) = 4x^3 - 3x^2 = x^2(-3 + 4x),\ f_y(x,y) = 4y^3 + 2y = 2y(1 + 2y^3)$. Pour (x_0,y_0) soit être un point singulier, il faut $x_0 = 0$ ou $3/4$, et $y_0 = 0,\ \frac{1}{2}i$ ou $-\frac{1}{2}i$, parmi les six pairs possibels $(0,0)$ seulmenet qu'est du courbe, donc $(0,0)$ est l'unique point singulier affine.

L'homogénisation de f est $F(X,Y,Z) = X^4 + Y^4 - ZX^3 + Z^2Y^2$, *on a* $F_X(X,Y,Z) = 4X^3 - 3ZX^2,\ F_Y(X,Y,Z) = 4Y^3 + 2Z^2Y,\ F_Z(X,Y,Z) = -X^3 + 2ZY^2$.

Il suffit trouver les points singuliers a l'infinis, on pose $Z = 0$, pour $(X_0,Y_0,0)$ est un point singulier il faut $X^4 + Y^4 = 4X^3 = 4Y^3 = -X^3 = 0$ ce vérifie si $X_0 = Y_0 = 0$, mais c'est

impossible dans $\mathbb{P}^2$ car $(0,0,0) \notin \mathbb{P}^2$.

Finalement, l'unique point singulier de $\hat{C}_f$ est $(0,0,1)$.

Remarque 2.4.

(a) La courbe C_f est non singulière (régulière) si elle ne possède aucun point singulier.

(b) Si $F(X,Y,Z)$ est l'homogénisation de $f(x,y)$, donc $(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(k)$ est point singulier de $\hat{C}_f$ si le point sur la courbe en plus $F(X_0 : Y_0 : Z_0) = F_X(X_0 : Y_0 : Z_0) = F_Y(X_0 : Y_0 : Z_0) = F_Z(X_0 : Y_0 : Z_0) = 0$

(c) La courbe $\hat{C}_f$ est non singulière si elle ne possède aucun point singulier.

Définition 2.6. *([6],[7]) Soit $f(x,y) \in K[X,Y]$ un polynome de degré d tel que $\hat{C}_f$ non singulier, donc la genre de C_f est défini par :*

$$g = \frac{(d-1)(d-2)}{2}$$

Exemple 2.7. *(a)* sur $\mathbb{R}$, on considère le polynome $f(x) = x^3 + 2x - 1$.

la genre de ce polynome est : $g = \frac{(3-1)(3-2)}{2} = 1$.

(b) Sur $\mathbb{F}_3$, on considère le polynome $h(x) = x^4 - y + 3$.

La genre de h est $g = \frac{(4-1)(4-2)}{2} = 3 = 0$.

Définition 2.7. *Soient k un corps et C une courbe projective.*

Pour toutes extensions K de k, on dit que $(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(k)$ est un $K-$point rationnel si $F(X_0, Y_0, Z_0) = 0$.

Remarque 2.5.

(a) L'ensemble de tous $K-$points rationnels sur C est notée $C(K)$.

(b) Les éléments de $C(k)$ sont appelles points simples ou points de degré un.

Exemple 2.8. On considère le polynome $f(x,y) = x^3 - y + 1$ définie sur $K = \mathbb{F}_2$.

L'homogénization de f est $F(X,Y,Z) = X^3 + Z^3 - Z^2Y$, on a $g(x) = x^2 + 1$ est polynome irreductible sur $\mathbb{F}_2$, donc le corps de composition est défini par

$$\mathbb{F}_{2^2} = \mathbb{F}_4 = \mathbb{F}_2 / < x^2 + 1 > .$$

Donc

$$\mathbb{F}_4 = \{a + b \cdot x + < x^2 + 1 > /a, b \in \mathbb{F}_2\}$$
$$= \{a + b \cdot \overline{x} \cdot / \ a, b \in \mathbb{F}_2\}$$

On pose $\alpha = \overline{x}$ avec $f(\alpha) = 0$ i.e, $\alpha^2 + 1 = 0 \Rightarrow \alpha^2 = -1 = 1$.

$\mathbb{F}_4 = \{a + b \cdot \alpha \ /a, b \in \mathbb{F}_2\} = \{0, 1, \alpha, \alpha + 1\}$.

parmi les éléments de $\mathbb{F}_4 \times \mathbb{F}_4$ on trouve $(0,1), (1,0), (\alpha, \alpha+1)$ *et* $(\alpha+1, 1)$ *sont des racine* de $F(X, Y, 1)$, alors l'ensemble des points rationnels est *:*

$$C(\mathbb{F}_4) = \{(1:0:1), (0:1:1), (\alpha:\alpha+1:1), (\alpha+1:1:1), p_\infty\}.$$

Proposition 2.1. *Soit $\mathbb{F}_q$ un corps fini de caractéristique p, l'application*

$$F : \mathbb{F}_q \to \mathbb{F}_q$$

$$x \to x^p$$

est automorphisme de $\mathbb{F}_q$ appelé Automorphiseme de Frobenius.

Définition 2.8. *(*[6],[7]*) Soit C une courbe projective non singuliere, un point de degré n sur C est ensemble $p = \{p_0, p_1, ..., p_{n-1}\}$ de n points distincts dans $C(\mathbb{F}_q^n)$ tel que $p_i = \sigma_{q,n}^i(p_0)$ pour $i = \overline{1, n-1}$*

Exemple 2.9. Revenons à notre exemple précédent 2.8 où $f(x, y) = x^3 - y + 1$, on considère Automorphiseme de Frobenius $\sigma_{2;2} : \mathbb{F}_4 \to \mathbb{F}_4$ satisfait $\sigma_{2;2}(\alpha) = \alpha^2 = 1$

On a

$C(\mathbb{F}_4) = \{(1:0:1), (0:1:1), (\alpha:\alpha+1:1), (\alpha+1:\alpha:1)\}$.

$\sigma_{2;2}(\alpha:\alpha+1:1) = (1:0:1)$

$\sigma_{2;2}(\alpha+1:1:1) = (0:1:0)$

Donc les point sont :

$Q_1 = \{(\alpha:\alpha+1:1), \ \sigma_{2;2}(\alpha:\alpha+1:1) = (1:0:1)\}$.

$Q_2 = \{(\alpha+1:\alpha:1), \ \sigma_{2;2}(\alpha+1:\alpha:1) = (0:1:0)\}$.

Définition 2.9. *([1],[2]) Soint C une courbe projective sur $\mathbb{F}_q$, Un diviseur D sur C sur $\mathbb{F}_q$ est sous forme $D = \sum n_Q Q$ où n_Q est entier et chaque Q est point de degre arbitraire sur C.*

Remarque 2.6.

(a) Si $n_Q > 0$ pour tout Q, on appelle D effective et on écrit $D \geq 0$.

(b) Le degré du diviseur D est $degD = \sum n_Q degQ$.

(c) Le support du diviseur est donne par :$SuppD = \{Q/n_Q \neq 0\}$.

(d) Le support est un ensemble fini.

(e) Le diviseur d'intersection $C \cap C'$ est diviseur effectif de degré de.

Exemple 2.10. On reste avec l'example *2.8.*
On a $Q_1 = \{(\alpha : \alpha + 1 : 1),\ \sigma_{2;2}(\alpha : \alpha + 1 : 1) = (1 : 0 : 1)\}$ *et* $Q_2 = \{(\alpha + 1 : 1 : 1),\ \sigma_{2;2}(\alpha + 1 : 1 : 1) = (0 : 1 : 0)\}$, donc $D = a \cdot Q_1 + b \cdot Q_2 + c \cdot p_\infty$ *où* $a,\ b,\ c \in \mathbb{Z}$.
Si on prend $a = -2, b = 3, c = 4$, *Alors* $D = 2Q_1 - 3Q_2 + 6p_\infty$, *avec* $degD = 2.2 - 3.2 + 6.1 = 4$ *et* $SuppD = \{Q_1, Q_2, p_\infty\}$.

On considère l'ensemble

$$\mathbb{F}_q(C) = \{\frac{g(X,Y,Z)}{h(X,Y,Z)}/g, h \in \mathbb{F}_q[X,Y,Z] \text{ sont des homogénisations de mème degré } \}$$

sur $\mathbb{F}_q[X,Y,Z]$ et $\sim$ une relation sur $\mathbb{F}_q(C)$ définie par :
$\forall g/h, g'/h' \in \mathbb{F}_q(C) \quad g/h \sim g'/h' \Leftrightarrow gh' - g'h \in < F > \subset \mathbb{F}_q[X,Y,Z]$
tel que $< F >= \{l(X,Y,Z)F(X,Y,Z) : l \in \mathbb{F}_q[X,Y,Z]\}$.
On a $\sim$ est relation d'équivalence, Car :
– Réflexivité, on a $gh - gh = 0 \in < F >$, alors $gh \sim gh$.
– Symétie, on a $g/h \sim g'/h'$, i.e, $gh' - g'h \in < F >$, alors $-(g'h - gh') \in < F >$
d'où $gh' - g'h \in < F >$ i.e, $g'/h' \sim g/h$.

– Transitivité, on a

$$\begin{cases} g/h \sim g'/h' \; i.e, \; gh' - g'h \in < F > .....(1) \\ g'/h' \sim g''/h'' \; i.e, \; g'h'' - g''h' \in < F > .....(2) \end{cases}$$

On multiple (1) par g'' et (2) par g , on obtient

$$\begin{cases} g''(gh' - g'h) = g''gh' - g''g'h.....(*) \\ g(g'h'' - g''h') = gg'h'' - gg''h'.....(**) \end{cases}$$

de $(*) + (**)$, on trouve $g''gh' - g''g'h + gg'h'' - gg''h' = gg'h'' - g''g'h = g'(gh'' - g''h)$.
comme $(gh'' - g''h)[X, Y, Z] \in \mathbb{F}_q[X, Y, Z]$ et $g' \in < F >$, donc $g'(gh'' - g''h) \in < F >$.
alors $(gh'' - g''h) \in < F >$ d'où $g/h \sim g''/h''$.

Définition 2.10. *([2],[7]) Soit $F(X, Y, Z)$ le polynome qui définit une courbe projective non singuliere sur $\mathbb{F}_q$, le corps des fonctions rationnelle sur C est*

$$\mathbb{F}_q(C) = (\{\frac{g(X, Y, Z)}{h(X, Y, Z)}/g, \; h \in \mathbb{F}_q[X, Y, Z] \text{ sont des homogénisations de mème degré }\} \cup \{0\})/\sim$$

Exemple 2.11. On reste avec l'example *2.8.*
l'homogénisation de f est $F(X, Y, Z) = X^3 + Z^3 - Z^2Y$.
On a Y/Z^2 *et* $Y^2/(X^3 + Z^3)$ sont en mème classe car $Y(X^3 + Z^3) - Y^2Z^2 = Y(X^3 + Z^3 - Z^2Y) = Y.F(X, Y, Z)$

Définition 2.11. *([2]),[7]) Soient C une courbe définit sur $\mathbb{F}_q$, $f = g/h \in \mathbb{F}_q(C)$, le diviseur de f est défini par :*

$$div(f) = \sum p - \sum q$$

tel que $\sum p$ est diviseur de $C \cap C_g$, et $\sum q$ est diviseur de $C \cap C_h$.

Définition 2.12. *([2],[8]) Soit D un diviseur sur une courbe projective non singuliere sur $\mathbb{F}_q$, l'espace de fonctions rationnelles associées à D est :*

$$L(D) = \{f \in \mathbb{F}_q(C) : div(f) + D \geq 0\} \cup \{0\}$$

.

Théorème 2.2. (Riemann − Roch)*((*[2]*),*[7]*)*
Soit C une courbe projective non siguliere de genre g définit sur $\mathbb{F}_q$ et D un diviseur sur X, alors $\dim L(D) \geq degD + 1 - g$ *en plus Si* $\deg D > 2g - 2$, *donc* $\dim L(D) = degD + 1 - g$.

2.2 Codes géométriques

Dans cette section, on utilise ce que on a vu pour décrire la constraction des codes géométriques .

Définition 2.13. *(*[7],[2]*) La droite projective est l'ensemble quotient* $(\mathbb{F}_q^2 \backslash (0,0))/\sim$ *par la relation d'équivalence* $\sim$ *définie par* $(X_0, Y_0) \sim (X_1, Y_1) \Leftrightarrow \exists \alpha \in \mathbb{F}_q^{\times} : X_1 = \alpha X_0,\ Y_1 = \alpha Y_0$.

Définition 2.14. *(*[2],[8]*) Soient X une courbe projective régulière sur $\mathbb{F}_q$, D un diviseur sur X et $p = \{p_1, ..., p_n\}$ l'esemble de n points distincts $\mathbb{F}_q-$rationnelles, le code geométrique associé à X, p et D est :*

$$C(X, p, D) = \{(f(p_1), f(p_2), ..., f(p_n))/f \in L(D)\} \subset \mathbb{F}_q^n$$

.

Théorème 2.3. *(*[2],[7],[8]*) Soient X une courbe projective régulière de genre g sur $\mathbb{F}_q$, D un diviseur sur X satisfaisant $2g - 2 < degD < n$ et $p = \{p_1, ..., p_n\}$ l'esemble de n points distincts $\mathbb{F}_q-$rationnelles, Donc le code géométrique $C(X, p, D)$ est linéaire de longueur n , dimension $k = degD + 1 - g$ et de distance minimal d tel que $d \geq n - degD$.*

preuve
On montre que $C(X, p, D)$ est linéaire de longueur n, dimension $k = degD + 1 - g$ et de distance minimal d tel que $d \geq n - degD$.
On a $\deg D > 2g - 2$, donc d'aprés le théorème 2.2 $\dim L(D) = \deg D + 1 - g$.
Soit $(f(p_1), f(p_2), ..., f(p_n)) \in \mathcal{C}$ un mot de code tel que $W_H(f(p_1), f(p_2), ..., f(p_n)) = d$, donc il existe d coordonnés non nulles, alors $f(p_{d+1}) = ... = f(p_n) = 0$ cela signifie que $dif(f) + D - p_{d+1} - ... - p_n$ est effèctive, et on a $D - p_{d+1} - .. - p_n$ doit avoir un degé non négatif, en d'autres termes, on a $\deg D - (n - d) \geq 0$ d'où $d \geq n - \deg D$.

Théorème 2.4. (Borne de Tsfasman − Vladut − Zink([5], [8])
Soit q un carré parfait, alors

$$\alpha_q(\delta) \geq -\delta + 1 - \frac{1}{\sqrt{q} - 1)}.$$

Conclusion

Dans ce travail, on a étudier d'application des courbes algèbriques dans la construction des codes géométrique, on a essayer d'utilise le théorème de Riemann-Roch, Serre et Drinfeld-Vladut pour estimer les bornes.

Bibliographie

[1] H.Chang, Linear error correcting algebraic geometry Codes, 15March2010.

[2] M.Giulietti, Notes on algebraic-geometric codes, Dipertimento di matematica, Universtà Degli studi di perugia, 06123 Perugia, Italy.

[3] Y. Ihara, "Some remarks on the number of rational points of algebraic curves over finite fields", J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (1981), pp. 721-724.

[4] G. Lachaud, Les codes géométriques de Goppa, Séminaire Bourbaki, 37ème année, 1984-85, n641, Février 1985.

[5] M. A. Tsfasman, S. G. Vladut, and Th. Zink, "Modular curves, Shimura curves, and Goppa Codes, better than the Varshamov-Gilbert bound", Math. Nachrichten, 109 (1982), pp. 21-28.

[6] S.G. Vladut et V.G. Drinfeld, "The numbre of points of an algebriac curve", Funktsional. Anal. i Prilozhen. , 17 (1983), pp 68-69. English translation in Function Anal.Appl. 17 (1983), pp.53-54.

[7] Judy L.Walker, Codes and curves, Department of Mathematics and Statistics, University of Nebraska, Lincoln, NE 68588-0323

[8] P.Zampolini, Agebraic geometric codes on curve and surfaces, Master program in Mathematics, Faculty of Science, University of Padova , Italy, 22March 2007.

ملخص

يندرج هذا العمل في إطار تطبيقات المنحنيات الجبرية في بناء التشفيرات الهندسية.

في هذا البحث نهتم بدراسة إستعمال التشفير على المنحنيات الجبرية المعرفة على حقول المنتهية وذكربعض الخواص كما نتطرق الى أهم النظريات في هذا المجال.

Résumé

Ce travail s'inscrit dans le cadre de l'application des courbes algèbriques dans la construction des codes géométrique.

Dans cette recharche, nous intéressons à étudier l'utilisations du codage sur des courbes algèbriques qui sont définies sur les corps finis et mentionnant certaines propriétés alors que nous abordons les théorèmes qui sont les plus importantes dans ce domaine.

Abstract

This work concerns the application of algebraic curves in construction of geometric codes.

In this research, we are interested in the use of the coding on algebraic curves defined on the finite field and mentioning some properties while we approach the most important theorems in this field of stady.