UNIVERSITÉD'ANTANANARIVO

Faculté des Sciences

Département des Mathématiques et Informatique

Mémoire de fin d'études en vue de l'obtention du

Diplôme d'Études Approfondies

Option : MATHÉMATIQUESAPPLIQUÉES

Spécialité : GRANDES DÉVIATIONS ET ALGÈBRE APPLIQUÉES

DECODAGE ALGEBRIQUE DES CODES CYCLIQUES

Soutenu publiquement par **RASAMIMANANA Ravotina Clément**

le 25 Mars 2014

Président : Monsieur RABEHERIMANANA TOUSSAINT JOSEPH
Professeur à l'Université d'Antananarivo

Rapporteur : Monsieur ANDRIATAHINY Harinaivo
Maître de Conférences à l'Université d'Antananarivo

Examinateu : Monsieur RAMAHAZOSOA Irrish Parker
Maître de Conférences à l'Université d'Antananarivo

Monsieur ANDRIAMIFIDISOA Ramamonjy
Maître de Conférences à l'Université d'Antananarivo

DÉCODAGE ALGÉBRIQUE DES CODES CYCLIQUES

Ravotina

Remerciements

Mon premier remerciement est adressé à Dieu qui m'a donné la vie, sans lui ce mémoire n'aurait pu être mené à son terme.

Mon deuxième remerciement est adressé à Monsieur **ANDRIATAHINY Harinaivo**, Maître de Conférences, qui m'a encadré et m'a accordé de son temps et sa confiance pour ce travail. Ses conseils, ses encouragements et sa rigueur m'ont été d'une aide considérable et efficace. Veuillez agréer mes sincères remerciements.

Ensuite, je tiens à exprimer toute ma reconnaissance et toute ma gratitude envers Monsieur **RABEHERIMANANA Toussaint Joseph**, Professeur titulaire, qui a accepté de présider ce mémoire de DEA mais qui est aussi notre professeur de Grande Déviation durant notre première année de DEA. Veuillez accepter mes vifs remerciements.

Je voudrais aussi remercier Monsieur **RAMAHAZOSOA Irrish Parker**, Maître de Conférences, d'accepter de faire parti du jury en tant qu'examinateur. Veuillez accepter mes sentiments respectueux.

Je remercie aussi Monsieur **ANDRIAMIFIDISOA Ramamonjy**, Maître de Conférences, d'avoir accepté de prendre part à ce jury en tant qu'examinateur, veuillez accepter l'expression de mes remerciements.

Je ne saurais oublier tous les enseignants et les responsables du Département de Mathématiques et Informatique de la Faculté des Sciences de l'Université d'Antananarivo : Merci.

Enfin, il me reste à adresser un grand merci à mes parents, mes frères, mes sœurs, et le reste de la famille pour l'appui inconditionnel dont j'ai bénéficié de leur part.

Table des matières

Introduction **4**

1 Rappels sur les codes cycliques **6**
1.1 codes linéaires 6
1.2 Codes cycliques 8
1.3 Polynôme localisateur d'erreur et syndromes 12
1.4 Identité de Newton 14

2 Notions sur les bases de Groebner **16**
2.1 Introduction 16
2.2 Ordre sur les monômes de $K[x_1, \ldots, x_n]$ 17
2.3 Algorithme de division dans $K[x_1, \ldots, x_n]$ 19
2.4 Idéaux monômiaux et Lemme de Dickson. 21
2.5 Théorème de la base de Hilbert et Bases de Groebner 22
2.6 Propriétés des bases de Groebner 25
2.7 Algorithme de Buchberger 30

3 Décodage des codes cycliques généraux **33**
3.1 Introduction 33
3.2 Décodage des codes cycliques avec l'identité de Newton . . . 34
3.3 Exemple de décodage des codes cycliques en utilisant l'identité de Newton 34
3.4 Décodage des codes cycliques en utilisant la base de Groebner 37

Conclusion **46**

Annexe A : Rappels sur les polynômes, Idéaux, et Variétés affines **47**
A.1.Polynôme et espace affine 47
A.2.Variétés affines 48
A.3.Idéal 48
A.4.Hilbert Nullstellensatz 50

Annexe B : Quelques exemples des codes cycliques **52**
B.1.Code BCH (Bose-Chaudhuri-Hocqenghem) 52
B.2.Code Reed-Solomon (RS) 53
B.3.Code Reed-Muller (RM) 54

Bibliographie **55**

Introduction

Le codage correcteur d'erreurs dont l'origine remonte à la fin des années 40, permet de transmettre de façon fiable l'information. On souhaite transmettre des informations via un canal de transmission. Celui-ci ne pouvant être parfait, l'information reçue par le destinataire peut être inexploitable ou erronée. Pour réduire au maximum la probabilité d'erreur, on construit une procédure de *codage* − *décodage* de l'information à transmettre qui, au prix d'éléments transmis supplémentaires, va permettre de détecter puis de corriger les altérations du message dues à l'imperfection du canal. On se base pour ceci essentiellement sur l'étude des corps finis et des polynômes sur ceux-ci.
L'objet de la théorie de l'information est la description et l'étude de système de communication, où l'information est considérée comme une grandeur mathématique, à partir du travail de Claude Shannon (1948) "The mathematical theory of communication".
Le modèle général d'un système de communication comportant une protection contre les erreurs de transmission est le suivant :

$$\underline{\textbf{[Source]}} \longrightarrow \underset{\uparrow\, u}{\underline{\textbf{[Encodeur]}}} \longrightarrow \underset{\uparrow\, c}{\underset{\updownarrow\, e}{\underline{\textbf{[Canal]}}}} \longrightarrow \underset{\uparrow\, r = c + e}{\underline{\textbf{[Décodeur]}}} \longrightarrow \underset{\uparrow\, u'}{\underline{\textbf{[Recepteur]}}}$$

u : *message émis*
c : *mot de code émis* (*message codé*)
e : *erreur*
r : *mot reçu*
u' : *message corrigé*

Le message à transmettre est un bloc de symboles tous issus d'un même alphabet.
En tant que décodage algébrique, le travail est alors basé sur une méthode algébrique, c'est-à-dire qu'on a besoin de maîtriser la manipulation des polynômes à plusieurs variables, les idéaux, et surtout la résolution de systèmes

d'équations polynômiaux. Il faut introduire les bases de Groebner, puisque ce sont des outils fondamentaux de l'algèbre commutative pour l'étude des systèmes polynômiaux, elles permettent de résoudre nombreux problèmes concernant les systèmes polynômiaux : appartenance à un idéal, dimension et degré de l'espace des solutions, nombre de solutions dans le cas d'un nombre fini de solutions, calculs de ces solutions, etc...

Dans ce mémoire, on présente la théorie des codes correcteurs d'erreurs, en particulier les codes cycliques et nous explicitons le décodage algébrique des codes cycliques et les liens avec la détermination des bases de Groebner. Le plan général de ce mémoire est alors comme suit : dans le premier chapitre, les fondements mathématiques permettant la construction de codes avec un rendement garanti sont présentés, en particulier les codes cycliques.
On verra dans le chapitre deux quelques notions générales à propos de la base de Groebner.
Le résultat de mon mémoire sera présenté dans le dernier chapitre, c'est le décodage des codes cycliques généraux et quelques exemples concrets.

Chapitre 1

Rappels sur les codes cycliques

1.1 codes linéaires

Définition 1.1. Un ensemble $\mathbb{K}$ muni de deux lois de composition interne $+$ et $\bullet$ est un *corps* si :
- $(\mathbb{K}, +, \bullet)$ est un anneau ;
- $(\mathbb{K}^*, \bullet)$ est un groupe où $\mathbb{K}^*$=$\mathbb{K} - \{0\}$.

Si la loi $\bullet$ est commutatif, on dit que le *corps* est commutatif. Si le cardinal de $\mathbb{K}$ est fini, alors le *corps* est dit $fini$. On rappelle que si p est premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps (voir [15]).

Notation 1. Soient $p \in \mathbb{P}$ (p premier), $l \in \mathbb{N}^*$, et $q = p^l$. Un *corps* fini de cardinal q est noté $\mathbb{F}_q$.

Définition 1.2. Soient $\mathbb{F}_q$ un corps fini et $n \in \mathbb{N}^*$ tels que (n, q) =1. Le plus petit entier positif m tel que $n|q^m - 1$ est appelé *ordre de q modulo n* et on écrit $m = \mathcal{O}_q[n]$.
Dans la théorie de codage, on utilise le corps fini à q éléments $\mathbb{F}_q$ comme alphabet et le plus utilisé est $\mathbb{F}_2$.

Pour transmettre des messages, qui sont de longueur k, c'est-à-dire des vecteurs $u = (u_1, u_2, ..., u_k) \in (\mathbb{F}_q)^k$, on fait passer d'abord ces messages dans un encodeur qui est une application injective

$$\mathrm{E} : (\mathbb{F}_q)^k \longrightarrow (\mathbb{F}_q)^n \text{ avec } n > k.$$

L'image $\mathcal{C}$=E($(\mathbb{F}_q)^k$) s'appelle le *code utilisé* et les éléments $x = (x_1, x_2, ..., x_n)$ $\in \mathcal{C}$ sont des *mots de code*. On sait que le nombre de mots de code est q^k.
Si E est linéaire, le sous espace vectoriel $\mathcal{C}$ de $(\mathbb{F}_q)^n$ est appelé *code linéaire*

de dimension k, de longueur n, et de redondance $n-k$.
Plus précisément $\mathcal{C}$ est un *code linéaire* si et seulement si

$$\forall\ m_1, m_2 \in \mathcal{C}; \forall\ a_1, a_2 \in \mathbb{F}_q, a_1 m_1 + a_2 m_2 \in \mathcal{C}.$$

Le *poids* d'un mot $x = (x_1, x_2, ..., x_n) \in (\mathbb{F}_q)^n$ est défini par

$$|x| = \text{card}\ \{\ i\ /x_i \neq 0\ ;\ 1 \leq i \leq n\} \tag{1.1}$$

Définition 1.3. (cf. [15]) La *distance de Hamming* entre deux points $x, y \in (\mathbb{F}_q)^n$ $(x \neq y)$ est définie par

$$d(x, y) = |x - y| \tag{1.2}$$

Définition 1.4. (cf. [15]) la *distance minimale* d'un code linéaire $\mathcal{C}$ est définie par

$$\begin{aligned} d &= min\{d(x, y)/x, y \in \mathcal{C}, x \neq y\} \\ &= min\{|x|/x \in \mathcal{C}, x \neq 0\} \end{aligned} \tag{1.3}$$

On transmet le *mot de code* $x \in \mathcal{C}$ à travers un canal bruité, et à la sortie du canal, on reçoit un vecteur $y \in (\mathbb{F}_q)^n$. La différence $z = y - x$ est appelée *erreur commise*.
Si $\mathcal{C}$ est un *code linéaire* de longueur n, de dimension k, et de distance minimale d sur $\mathbb{F}_q$, alors $\mathcal{C}$ est appelé code du type $(n, k, d)_q$.
Il y a deux manières de représenter un code linéaire à l'aide de matrices : soit on introduit 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 obtient ainsi la notion de *matrice de contrôle*.

Pour connaitre le code en tant que sous espace vectoriel de $(\mathbb{F}_q)^n$, il suffit d'en avoir une base. Soit $(m_1, m_2, ..., m_k)$ une base de $\mathcal{C}$, chaque m_i est ainsi composé de n lettres : on les note sous la forme de vecteurs ligne. Tous les mots de $\mathcal{C}$ peuvent ainsi s'écrire comme combinaison linéaire des m_i.

Définition 1.5. (Matrice génératrice)
Soit $(m_1, m_2, ..., m_k)$ une base de $\mathcal{C}$ dans $(\mathbb{F}_q)^n$, la matrice

$$G = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix}$$

de $(\mathbb{F}_q)^{k*n}$ est appelée *matrice génératrice* de $\mathcal{C}$.

Pour former un mot de code, on calcule le produit d'un vecteur ligne $(u_1, \ldots, u_k)$ et de la matrice génératrice. Ainsi,

$$m \in \mathcal{C} \Longleftrightarrow \exists\ u \in (\mathbb{F}_q)^k,\ m = u.G \tag{1.4}$$

Remarque 1.1. Soit $\mathcal{C}$ un code linéaire du type $(n, k, d)_q$. L'encodage se fait en multipliant le mot source par la matrice génératrice du code. Le mot source doit être de longueur k. La redondance est de $n - k$ symboles.

Une autre façon de définir un code linéaire est de donner une application linéaire dont il est le noyau. On obtient ainsi une matrice H telle que

$$\mathcal{C} = \{(x_1, \ldots, x_n); H * \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0\}$$

où 0 désigne le vecteur nul.

Définition 1.6. (Matrice de contrôle) (cf. [13])
H est une *matrice de contrôle* pour le code $\mathcal{C}$ si elle vérifie

$$\forall\ m \in (\mathbb{F}_q)^n,\ (m \in \mathcal{C} \Longleftrightarrow m.H^T = 0) \tag{1.5}$$

Remarque 1.2. (cf.[13]) Le rang de cette matrice de contrôle est $n - k$.

Définition 1.7. (Code dual)(cf. [15])
Soit $\mathcal{C} \subset (\mathbb{F}_q)^n$ un code linéaire. On définit le *code dual* de $\mathcal{C}$ par

$$\mathcal{C}^{\perp} = \{y \in (\mathbb{F}_q)^n / < x, y >= 0, \forall\ x \in \mathcal{C}\} \tag{1.6}$$

où

$$< x, y >= x_1y_1 + x_2y_2 + ... + x_ny_n$$

avec $x = (x_1, x_2, ..., x_n)$ et $y = (y_1, y_2, ..., y_n)$.

Si $\mathcal{C} = \mathcal{C}^{\perp}$, on dit que $\mathcal{C}$ est un code *auto-dual*.

Lemme 1.1. *Soit $\mathcal{C}$ un code de matrice génératrice G et de matrice de contrôle H. Son code dual $\mathcal{C}^{\perp}$ est engendré par H et admet G comme matrice de contrôle.*

1.2 Codes cycliques

Les codes cycliques forment une sous classe des codes linéaires, et ils sont les plus utilisés en pratique. Ils conjuguent en effet de nombreux avantages : leur mise en œuvre(codage /décodage) est facile, ils offrent une gamme étendue de codes, avec de nombreux choix de paramètres (n, k, d), et enfin permettent de corriger différents types d'erreurs, isolées ou par paquets.

Définition 1.8. (voir [2] ou [15]) Un code linéaire $\mathcal{C} \subseteq (\mathbb{F}_q)^n$ est dit *cyclique* si pour tout $(c_0, c_1, ..., c_{n-1}) \in \mathcal{C}$, on a $(c_{n-1}, c_0, c_1, ..., c_{n-2}) \in \mathcal{C}$, c'est-à-dire s'il est stable par permutation circulaire des lettres dans chaque mot.

Il est commode de représenter $(\mathbb{F}_q)^n$ par l'anneau (cf. [15])

$$\begin{aligned} A &= \mathbb{F}_q[X]/(X^n - 1) \\ &= \mathbb{F}_q + \mathbb{F}_q X + ... + \mathbb{F}_q X^{n-1} \\ &= \{a_0 + a_1 X + ... + a_{n-1} X^{n-1} / a_i \in \mathbb{F}_q\} \end{aligned}$$

On utilise alors l'identification

$$(a_0, a_1, ..., a_{n-1}) \in (\mathbb{F}_q)^n \leftrightarrow a_0 + a_1 X + ... + a_{n-1} X^{n-1} \in A$$

Théorème 1.2. *([2] ou [15]) Un code linéaire $\mathcal{C} \subset (\mathbb{F}_q)^n$ est cyclique si est seulement si $\mathcal{C}$ est un idéal de A.*

Démonstration. ($\Rightarrow$) Supposons que $\mathcal{C}$ est cyclique.
Soit $c = (c_0, c_1, ..., c_{n-1}) \in \mathcal{C}$, alors $(c_{n-1}, c_0, c_1, ..., c_{n-2}) \in \mathcal{C}$
Dans A, ce fait se traduit par
$c(X) = c_0 + c_1 X + ... + c_{n-1} X^{n-1} \in \mathcal{C}$ implique
$X.c(X) = c_{n-1} + c_0 X + ... + c_{n-2} X^{n-1} \in \mathcal{C}$
Et d'une manière générale, on a

$$X^i.c(X) \in \mathcal{C}, \text{ pour tout i}$$

Et comme $\mathcal{C}$ est linéaire, alors

$$f(X).c(X) \in \mathcal{C}, \forall\ f(X) \in A$$

Ainsi, $\mathcal{C}$ est un idéal de A.
($\Leftarrow$) Supposons que $\mathcal{C}$ est un idéal de A et soit

$$c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \in \mathcal{C}$$

On a alors

$$X.c(X) \in \mathcal{C}$$

or

$$X.c(X) = c_{n-1} + c_0 X + ... + c_{n-2} X^{n-1} \in \mathcal{C}$$

D'où $\mathcal{C}$ est cyclique. □

Tout idéal de $\mathbb{F}_q[X]/(X^n - 1)$ est engendré par un seul élément [15] ; cela tient à l'existence d'une division euclidienne dans cet anneau.

Définition 1.9. (Polynôme générateur)
Le *polynôme générateur* du code cyclique $\mathcal{C}$ est le polynôme normalisé de plus bas degré de $\mathcal{C}$. On le note génériquement $g(X)$.

Normalisé signifie que le coefficient du monôme de plus haut degré vaut 1. Cette normalisation garantit l'unicité de $g(X)$. Noter que $g(X)$ ne peut pas être le polynôme nul avec cette définition.

Théorème 1.3. *(voir [2]) L'unique polynôme unitaire $g(X)$ de degré minimal dans un idéal I de l'anneau $A = \mathbb{F}_q[X]/(X^n - 1)$ est un générateur de I et divise $X^n - 1$. La dimension de I est $n - deg(g(X))$.*
Inversement, tout diviseur de $X^n - 1$ est un générateur d'un idéal de A.

Démonstration. Soit $c(X) \in I$, par l'algorithme de la division euclidienne, on a :

$$c(X) = q(X).g(X) + r(X) \text{ avec } deg(r(X)) < deg(g(X))$$

Comme I est un idéal, alors

$$c(X) - g(X).q(X) \in I$$

D'où

$$r(X) \in I$$

Et d'après le degré de g qui est minimal dans I, on a $r = 0$.
Donc, on a

$$g(X)|c(X),$$

et ainsi

$$\mathcal{C} = A.g(X)$$

En appliquant le même argument au polynôme $X^n - 1$, on a

$$X^n - 1 = q_1(X).g(X) + r_1(X) \text{ avec } deg(r_1) < deg(g)$$

D'où $r_1(X) \in I$ et ainsi $r_1 = 0$
On a alors

$$g(X)|X^n - 1$$

Supposons que $deg(g(X)) = n - k$. Alors les éléments $g(X), Xg(X), \ldots,$ $X^{k-1}g(x)$ sont linéairement indépendants dans I. Comme tout élément de l'idéal I est de la forme $a(X).g(X)$ avec $deg(a(X)) < k$ alors ces éléments engendrent l'idéal I. D'où $dimI = k$.
Soit $g(X)$ un polynôme unitaire tel que $g(X)|X^n - 1$. Considérons l'idéal $I = A.g(X) = (g(X))$. Soit $c(X) \in I$, alors $c(X) = a(X)g(X)mod(X^n - 1)$, c'est-à-dire $c(X) = a(X)g(X) + b(X)(X^n - 1)$
Comme $g(X)|X^n - 1$, alors $g(X)|c(X)$. □

Lemme 1.4. *(cf. [15]) Soit $\mathcal{C}$ un code cyclique de $(\mathbb{F}_q)^n$, de polynôme générateur*

$$g(X) = g_0 + g_1X + g_2X^2 + ... + g_{n-k}X^{n-k},$$

on obtient une matrice génératrice de $\mathcal{C}$ définie par

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_{n-k} \end{pmatrix} \in (\mathbb{F}_q)^{k*n}$$

Cette matrice est appelée *matrice de Hadamard (ou matrice circulante).* On observe que G est bien de rang k, car la sous matrice $k * k$ de droite est tridiagonale, avec des 1 sur la diagonale.(car $g(X)$ est unitaire)

Définition 1.10. (Classes cyclotomiques)
Soient n et q deux entiers naturels tels que $(n, q) = 1$.
La relation $\Re$ définie sur l'ensemble des entiers modulo n par

$$i\Re j \Leftrightarrow i \equiv q^k j[n]$$

pour un certain entier naturel k définit une relation d'équivalence. On établit ainsi une partition de $\{0, 1, 2, ..., n-1\}$ en des classes d'équivalence appelées *classes cyclotomiques de q modulo n.*

$$cl(i) = \{i, iq, iq^2, ..., iq^{s-1}\}$$

où s est le plus petit entier tel que $\overline{i} = \overline{iq^s}$.

Exemple 1.1. Supposons $q = 2$ et $n = 15$. Les classes cyclotomiques de 2 modulo 15 sont alors

$$\begin{aligned} cl(0) &= \{0\} \\ cl(1) &= \{1, 2, 4, 8\} \\ cl(3) &= \{3, 6, 12, 9\} \\ cl(5) &= \{5, 10\} \\ cl(7) &= \{7, 14, 13, 11\} \end{aligned}$$

Définition 1.11. (Ensemble de définition)
Soit $n = q^m - 1$ où $q = p^l$ $(p \in \mathbb{P}, l \in \mathbb{N}^*)$
Soit α un élément primitif de $\mathbb{F}_{q^m}$.
Soit $\mathcal{C}$ un code cyclique de longueur n sur $\mathbb{F}_q$, et de polynôme générateur $g(x)$.
On appelle *ensemble de définition* de $\mathcal{C}$ l'ensemble défini par

$$\mathcal{Q} = \{i \in \{1, 2, \dots, q^m - 2\} / \ g(\alpha^i) = 0\}.$$

Exemple 1.2. Construction d'un code cyclique $(7, 4)$, c'est-à-dire de longueur 7 et de dimension 4. Considérons la décomposition de $X^7 - 1$ dans $\mathbb{F}_2[X]$. Les classes cyclotomiques et les polynômes irréductibles associés sont

alors :
$\star$ pour $i = 0 : cl_0 = \{0\}$. D'où $g_0 = X - \alpha^0 = X - 1$.
$\star$ pour $i = 1 : cl_1 = \{1, 2, 4\}$. D'où $g_1 = (X - \alpha^1)(X - \alpha^2)(X - \alpha^4)$
$\star$ pour $i = 3 : cl_3 = \{3, 6, 5\}$. D'où $g_3 = (X - \alpha^3)(X - \alpha^5)(X - \alpha^6)$
En fait, on montre que $\mathbb{F}_2[X]$ n'admet que deux polynômes irréductibles de degré 3 : $1 + X + X^3$ et $1 + X^2 + X^3$. Ces deux polynômes sont donc g_1 et g_3. Le polynôme $g(X) = 1 + X^2 + X^3$ est donc le polynôme générateur d'un code cyclique de longueur 7 et de dimension 4 (car g est de degré 3). La matrice génératrice de ce code est :

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

Plus généralement, la factorisation de $X^7 - 1$ permet d'exhiber 6 diviseurs non triviaux de $X^7 - 1$ qui définissent chacun un code cyclique :
$\bullet g_1 = X - 1$:code cyclique (7,6)
$\bullet g_2 = X^3 + X + 1$:code cyclique (7,4)
$\bullet g_3 = X^3 + X^2 + 1$:code cyclique (7,4)
$\bullet g_4 = (X - 1)(X^3 + X + 1)$:code cyclique (7,3)
$\bullet g_5 = (X - 1)(X^3 + X^2 + 1)$:code cyclique (7,3)
$\bullet g_6 = (X^3 + X + 1)(X^3 + X^2 + 1)$:code cyclique (7,1)

1.3 Polynôme localisateur d'erreur et syndromes

Un code cyclique $\mathcal{C}$ de longueur n, de dimension k, et de distance minimale d sur $\mathbb{F}_q$ est défini par :

$$\mathcal{C} = \{c(x)/c(\alpha^i) = 0, \forall i \in \mathcal{Q}\}, \tag{1.7}$$

où α est un élément primitif de $\mathbb{F}_{q^m}$ (α est une racine primitive $n^{ième}$ de l'unité), avec m est l'ordre de q modulo n (cf. définition 1.2), et $\mathcal{Q}$ est l'ensemble de définition de $\mathcal{C}(\mathcal{Q} \subset I_n = \{0, 1, \ldots, n-1\})$. Soit $c(x)$ un mot de code à transmettre à travers un canal bruité, on obtient le mot de code reçu $r(x)$ de la forme $r(x) = c(x) + e(x)$, où $e(x)$ est l'*erreur*. On peut calculer les syndromes s_i par :

$$s_i = r(\alpha^i) = c(\alpha^i) + e(\alpha^i) = e(\alpha^i) \tag{1.8}$$

pour $i \in \mathcal{Q}$. Ces syndromes s_i peuvent aussi être exprimés de la façon suivante :

$$s_i = Y_1 Z_1^i + Y_2 Z_2^i + \cdots + Y_v Z_v^i, i \in \mathcal{Q}, s_i \in \mathbb{F}_{q^m} \tag{1.9}$$

où v est le nombre d'erreurs, $Y_j \in \mathbb{F}_q - \{0\}$ pour $j = 1, 2, \ldots, v$ sont les valeurs de l'erreur, et

$$Z_j = \alpha^{r_j},\ \textit{pour}\ j = 1, \ldots, v \tag{1.10}$$

où les r_j sont des entiers $\in I_n$ qu'on appelle indices de localisation des erreurs.

Définition 1.12. Polynômes syndromes
Soient s_i, pour $i \in \mathcal{Q}$, des syndromes qui sont déjà connus, l'ensemble des polynômes syndromes F est définie par :

$$f_i = \quad Y_1 Z_1^i + Y_2 Z_2^i + \cdots + Y_v Z_v^i - s_i, i \in \mathcal{Q}, \tag{1.11}$$
$$h_j = \quad Z_j^n - 1 \text{ et } l_j = Y_j^{q-1} - 1,\ 1 \leq j \leq v. \tag{1.12}$$

On peut remplacer l'ensemble $\mathcal{Q}$ dans (1.11) par l'ensemble des représentants des classes cyclotomiques (on note par $\mathcal{R}$ cet ensemble)(voir [11] ou [5]).

Théorème 1.5. *Les syndromes $s_i,\ i \in \mathcal{Q}$, sont uniques pour chaque erreur de poids $v \leq t$ avec $t = [(d-1)/2]$.*

Théorème 1.6. *Soit t le plus grand entier tel que $2t+1 \leq d$. On suppose que les erreurs ont toujours un poids $\leq t$. Alors, à chaque vecteur reçu $y \in (\mathbb{F}_q)^n$, on peut associer un seul mot de code $x \in \mathcal{C}$ tel que $|y - x| \leq t$.*

Démonstration. Si on avait $x' \in \mathcal{C}$ tel que $|y - x'| \leq t$, on aurait

$$\begin{aligned} |x - x'| &\leq |y - x| + |y - x'| \ (\textit{Inégalité triangulaire}) \\ &\leq 2t \\ &< d \end{aligned}$$

alors $x = x'$ d'après la définition de d. □

Les racines des polynômes définis dans (1.11) et (1.12) satisfont le polynôme localisateur d'erreur $L(z)$.

Définition 1.13. (cf. [5]) Le *polynôme localisateur d'erreur* est défini par :

$$L(z) = \prod_{i=1}^{v} (z - Z_i) = z^v + \sum_{j=1}^{v} \sigma_j z^{v-j}, \tag{1.13}$$

où les Z_i, pour $i = 1, \ldots, v$, sont définies dans l'équation (1.9) et

$$\sigma_i = (-1)^i \sum_{1 \leq j_1 < j_2 < \cdots < j_i \leq v} Z_{j_1} Z_{j_2} \cdots Z_{j_i},\ 1 \leq i \leq v \tag{1.14}$$

sont les fonctions élémentaires symétriques de Z_j.

1.4 Identité de Newton

Les syndromes s_i et les coefficients σ_j de $L(z)$ sont reliés par le théorème important suivant (voir [11]) :

Théorème 1.7. *"**Les identités de Newton**" Les fonctions somme*

$$s_i = \sum_{j=1}^{v} Y_j Z_j^i$$

et

$$\sigma_i = (-1)^i \sum_{1 \le j_1 < j_2 < \cdots < j_i \le v} Z_{j_1} Z_{j_2} \cdots Z_{j_i},\ 1 \le i \le v.$$

satisfont les identités suivantes :

$$s_i + \sum_{j=1}^{v} \sigma_j s_{i-j} = 0, \quad v < i < n. \tag{1.15}$$

Démonstration. Dans l'équation (1.13), nous avons

$$\begin{aligned} \prod_{i=1}^{v}(z - Z_i) &= z^v + \sum_{j=1}^{v} \sigma_j z^{v-j} \\ &= z^v + \sigma_1 z^{v-1} + \sigma_2 z^{v-2} + \cdots + \sigma_v \end{aligned}$$

En changeant z par Z_i, on obtient

$$Z_i^v + \sigma_1 Z_i^{v-1} + \sigma_2 Z_i^{v-2} + \cdots + \sigma_v = 0 \tag{1.16}$$

En multipliant les 2 membres de cette dernière équation par $Y_i Z_i$, on a

$$Y_i Z_i^{v+1} + \sigma_1 Y_i Z_i^v + \cdots + \sigma_v Y_i Z_i = 0.$$

Ensuite, en faisant la sommation des équations suivantes :

$$\begin{aligned} Y_1 Z_1^{v+1} + \sigma_1 Y_1 Z_1^v + \cdots + \sigma_v Y_1 Z_1 &= 0 \\ Y_2 Z_2^{v+1} + \sigma_1 Y_2 Z_2^v + \cdots + \sigma_v Y_2 Z_2 &= 0 \\ &\vdots \\ Y_v Z_v^{v+1} + \sigma_1 Y_v Z_v^v + \cdots + \sigma_v Y_2 Z_2 &= 0 \end{aligned}$$

on a

$$s_{v+1} + \sum_{j=1}^{v} \sigma_j s_{v+1-j} = 0.$$

D'une façon analogue mais on multiplie l'équation (1.16) par $Y_i Z_i^2$, on obtient

$$s_{v+2} + \sum_{j=1}^{v} \sigma_j s_{v+2-j} = 0.$$

Raisonnement analogue pour avoir tous les résultats. □

Remarque 1.3. Dans le cas $2v \leq n$ (cf. [12]), on peut déterminer directement le polynôme localisateur d'erreur à partir de l'ensemble des équations dans (1.15).

On verra l'application de cette remarque dans le chapitre 3.

Chapitre 2

Notions sur les bases de Groebner

2.1 Introduction

Dans ce chapitre, on suppose que K soit un corps arbitraire. Du fait de leur nature géométrique, les idéaux des anneaux de polynômes à plusieurs variables sur K sont des objets particulièrement intéressants. Parmi les problèmes que l'on rencontre, ceux qui suivent sont de première importance :
-**Générateurs d'un idéal** : Est-ce que tout idéal $I \subset K[x_1, ..., x_n]$ admet un nombre fini de générateurs ? Et si oui comment peut-on les trouver à partir de la donnée de I ? Existe-t-il un système de générateurs plus intéressant que les autres ?
-**Problème d'appartenance à un idéal** : Étant donné $f \in K[x_1, ..., x_n]$ et $I = \langle f_1, ..., f_s \rangle \subset K[x_1, ..., x_n]$, déterminer (efficacement) si $f \in I$?
-**Zéros d'un système d'équations polynômiales** : Soient $f_1, ..., f_s$ une famille de polynômes de $K[x_1, ..., x_n]$. Comment trouver effectivement les solutions d'un système d'équations

$$\begin{cases} f_1(x_1, ..., x_n) = 0 \\ \vdots \\ f_s(x_1, ..., x_n) = 0 \end{cases}$$

-**Présentation implicite et présentation paramétrée** : Supposons que l'on ait un paramétrage $t_i = f_i(x_1, ..., x_m)$ décrivant un sous ensemble de K^n, pour $i \in \{1, ..., n\}$ et $f_i \in K[x_1, ..., x_m]$. Comment trouver des polynômes $g_1, ..., g_s$ de $K[t_1, ..., t_n]$, tel que cet ensemble de points soit solution du système

$$\begin{cases} g_1(t_1, ..., t_n) = 0 \\ \vdots \\ g_s(t_1, ..., t_n) = 0 \end{cases}$$

2.2 Ordre sur les monômes de $K[x_1, \ldots, x_n]$

Dans ce qui suit, n est un entier naturel non nul. Nous appellerons *multi-indice* (et s'il n'y a pas d'ambiguïté, tout simplement *indice*) un *n-uplet* de $\mathbb{N}^n$. Si $\nu = (\nu_1, \ldots, \nu_n)$ est un tel *multi-indice*, nous désignerons par x^ν le monôme $x_1^{\nu_1} \ldots x_n^{\nu_n}$ de $K[x_1, \ldots, x_n]$ (Voir l'annexe A). Ainsi l'ensemble des monômes de $K[x_1, \ldots, x_n]$ s'identifie à $\mathbb{N}^n$.(il est implicite que l'on utilise la convention $x_i^0 = 1$). De ce fait, se donner un ordre(i.e une relation d'ordre) sur $\mathbb{N}^n$ équivaudra à se donner un ordre sur les monômes de $K[x_1, \ldots, x_n]$. Néanmoins, seuls les ordres "compatibles" avec la structure algébrique des polynômes seront intéressants de notre point de vue. Commençons par définir ce type d'ordre :

Définition 2.1. (cf [7] ou [9]) On appelle *ordre monômial* sur $K[x_1, \ldots, x_n]$ toute relation d'ordre totale $\succ$ sur $\mathbb{N}^n$, telle que $\mathbb{N}^n$ soit *bien ordonné* et satisfaisant à la propriété suivante : *si* $\alpha, \beta, et\ \gamma \in \mathbb{N}^n$ *avec* $\alpha \succ \beta$ *alors* $\alpha + \gamma \succ \beta + \gamma$.

Remarque 2.1. On rappelle qu'un ensemble ordonné E est dit *bien ordonné* si toute partie non vide de E possède un plus petit élément (pour l'ordre considéré). Le problème est de savoir quand un ordre est un "*bon ordre*".

Lemme 2.1. *"Critère de bon ordre" (cf [7] ou [9])*
Une relation d'ordre $\succ$ sur $\mathbb{N}^n$ est un bon ordre si et seulement si toute suite strictement décroissante de $\mathbb{N}^n$ est stationnaire.

Démonstration. Il suffit de prouver que $\succ$ n'est pas un bon ordre *ssi* il existe une suite infinie strictement décroissante dans $\mathbb{N}^n$.
Si $\succ$ n'est pas un bon ordre, alors il existe un sous-ensemble non vide $S \subset \mathbb{N}^n$ qui n'admet pas de plus petit élément,
soit $\alpha(1) \in S$, $\alpha(1)$ n'est pas un plus petit élément, donc on peut trouver $\alpha(2) \in S$ tel que $\alpha(1) \succ \alpha(2)$. $\alpha(2)$ n'est pas aussi un plus petit élément, de même manière, il existe $\alpha(3) \in S$ tel que $\alpha(2) \succ \alpha(3)$. En continuant cette démarche, on obtient une suite infinie strictement décroissante

$$\alpha(1) \succ \alpha(2) \succ \alpha(3) \succ \cdots$$

Réciproquement, en donnant une telle suite infinie, alors $\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ est un sous ensemble non vide de $\mathbb{N}^n$ qui n'admet pas de plus petit élément, donc $\succ$ n'est pas un bon ordre. □

Voici quelques exemples fondamentaux d'ordres monômiaux.

Définition 2.2. (L'ordre lexicographique, cf. [4], [7], [9])
Soient $\alpha = (\alpha_1, \ldots, \alpha_n)$ et $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. On dit que $\alpha \succ_{lex} \beta$ si la première composante non nulle du vecteur $(\alpha - \beta)$ en partant de la gauche est positive.

Exemple 2.1.

$$(1,2,0) \succ_{lex} (0,3,4) \ ; \ (3,2,4) \succ_{lex} (3,2,1)$$

Les variables $x_1, \ldots, x_n$ sont ordonnées de la manière usuelle

$$(1,0,\ldots,0) \succ_{lex} (0,1,0,\ldots,0) \succ_{lex} \cdots \succ_{lex} (0,\ldots,0,1)$$

soit

$$x_1 \succ_{lex} x_2 \succ_{lex} \cdots \succ_{lex} x_n$$

Une variante de l'ordre *lex* est l'ordre lexicographique gradué($grlex$) qui tient compte des degrés totaux (voir l'annexe A) des monômes. Dans ce qui suit, $|.|$ désigne le degré total d'un monôme.

Définition 2.3. (L'ordre lexicographique gradué) (cf. [4], [7], [9])
Soient $\alpha = (\alpha_1, \ldots, \alpha_n)$ et $\beta = (\beta_1, \ldots, \beta_n)$ deux *n-uplet* de $\mathbb{N}^n$. On dira que $\alpha \succ_{grlex} \beta$ si $|\alpha| > |\beta|$ ou $|\alpha| = |\beta|$ *et* $\alpha \succ_{lex} \beta$.

Exemple 2.2.

$$(1,2,3) \succ_{grlex} (3,2,0) \ ; \ (1,2,4) \succ_{grlex} (1,1,5)$$

Nous avons aussi $x_1 \succ_{grlex} x_2 \succ_{grlex} \cdots \succ_{grlex} x_n$.
Il y a de nombreuses possibilités de construire des ordres monômiaux. Un autre ordre qui peut s'avérer utile en certaine occasion est l'*ordre lexicographique gradué retourné*.

Définition 2.4. (L'ordre lexicographique gradué retourné) (cf. [4], [7], [9])
Soient $\alpha = (\alpha_1, \ldots, \alpha_n)$ et $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. On dira que $\alpha \succ_{grevlex} \beta$ si $|\alpha| > |\beta|$ ou $|\alpha| = |\beta|$ et la première composante non nulle du vecteur $(\alpha - \beta)$ en partant de la droite est négative.

Exemple 2.3.

$$(4,7,1) \succ_{grevlex} (4,3,2) \ ; \ (1,5,2) \succ_{grevlex} (4,1,3)$$

Il est facile de voir que $x_1 \succ_{grevlex} x_2 \succ_{grevlex} \ldots \succ_{grevlex} x_n$.

Proposition 2.2. *Les ordres* $\succ_{lex}, \succ_{grlex}$, *et* $\succ_{grevlex}$ *sont monômiaux.*

Démonstration. Voir [7] pour la preuve. □

Pour faciliter la manipulation des polynômes à plusieurs variables, nous allons introduire un peu de *terminologie*.

Définition 2.5. Soit $P = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$ un polynôme de $K[x_1, \ldots, x_n]$ et soit $\succ$ un ordre monômial.

1. Le *multidegré* de P est $multideg(P) = max\{\alpha \in \mathbb{N}^n, a_\alpha \neq 0\}$ où le maximum est pris relativement avec l'ordre $\succ$;

2. Le *coefficient de plus haut degré* (*leading coefficient*) de P est $LC(P) = a_{multideg(P)}$;
3. le *monôme de plus haut degré*(*leading monômial*) de P est $LM(P) = x^{multideg(P)}$;
4. Le *terme de plus haut degré*(*leading term*) de P est $LT(P) = LC(P).LM(P)$.

On peut vérifier les résultats suivants qui généralisent les propriétés classiques.

Lemme 2.3. *(cf [9]) Soient $f, g \in K[x_1, \ldots, x_n]$ des polynômes non nuls. Alors*
i) nous avons $multideg(fg) = multideg(f) + multideg(g)$.
ii) si $f + g \neq 0$, alors $multideg(f + g) \preceq max(multideg(f), multideg(g))$. L'égalité étant réalisée si les multidegrés sont distincts.

2.3 Algorithme de division dans $K[x_1, \ldots, x_n]$

En général, le but est de diviser un polynôme $f \in K[x_1, \ldots, x_n]$ par $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. Comme nous verrons, cela veut dire exprimer f sous la forme

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

où les *quotients* $a_1, \ldots, a_s$ et le reste r appartiennent à $K[x_1, \ldots, x_n]$.

Exemple 2.4. On divisera $f = xy^2 + 1$ par $f_1 = xy + 1$ et $f_2 = y + 1$, en utilisant l'ordre *lexicographique* avec $x \succ_{lex} y$. Nous voulons employer le plan comme pour la division de polynôme à une variable, mais la différence est que, ici il existe plusieurs diviseurs et quotients.
On écrit verticalement les diviseurs f_1, f_2 et les quotients a_1, a_2 comme suit :

$$\begin{array}{cc} a_1 : & \\ a_2 : & \\ xy+1 & \overline{| \; xy^2+1} \\ y+1 & \end{array}$$

Les termes de plus haut degré (leading term) $LT(f_1) = xy$ et $LT(f_2) = y$ divisent le terme de plus haut degré de f, car $LT(f) = xy^2$. Puis, on inscrit f_1 en premier et on l'utilisera. Donc, pour éliminer xy^2, on multiplie xy par y et on fait la différence entre f et $y.f_1$
on a

$$\begin{array}{cc} a_1 : & y \\ a_2 : & \\ xy+1 & \overline{| \; xy^2+1} \\ y+1 & \underline{xy^2+y} \\ & -y+1 \end{array}$$

Maintenant, on répète le même processus pour $-y+1$, et on utilise f_2 car $LT(f_1) = xy$ ne divise pas $LT(-y+1) = -y$. On obtient

$$\begin{array}{rr} a_1 : & y \\ a_2 : & -1 \\ \hline xy+1 & \mid\ xy^2+1 \\ y+1 & \underline{xy^2+y} \\ & -y+1 \\ & \underline{-y-1} \\ & 2 \end{array}$$

On voit que ni $LT(f_1)$, ni $LT(f_2)$ ne divise 2, le reste est alors $r = 2$.
Donc on peut écrire

$$\begin{aligned} f &= xy^2+1 \\ &= y(xy+1)+(-1)(y+1)+2 \\ &= yf_1+(-1)f_2+r \end{aligned}$$

Théorème 2.4. *Fixons un ordre monômial sur $\mathbb{N}^n$. Soit $F = (f_1, \ldots, f_s) \in K[x_1, \ldots, x_n]^s$. Alors tout polynôme f de $K[x_1, \ldots, x_n]$ peut s'écrire sous la forme*

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

où $a_i, r \in K[x_1, \ldots, x_n]$ et, soit $r = 0$, ou alors r est une combinaison linéaire des monômes dont aucun n'est divisible par $LT(f_1), \ldots, LT(f_s)$.
r est le reste (remainder) de la division de f par F.
Si de plus $a_i f_i \neq 0$, alors $multideg(f) \succeq multideg(a_i f_i)$.

Démonstration. Voir [7] page 62-63. La base de la preuve est l'algorithme de division ci-dessous. □

Le reste r que l'on trouve dépend de nombreux facteurs, bien évidemment l'ordre monômial, mais aussi l'ordonnancement des variables une fois le type d'ordre monômial choisi. Plus encore, si on se fixe un algorithme pour calculer r et les a_i, ces derniers peuvent changer si l'on modifie l'ordre des f_i, voir les choix que l'on fait dans les réductions. De ce fait si $r = 0$, on a bien $f \in (f_1, \ldots, f_s)$. Mais ce n'est pas une condition nécessaire, comme le montre l'exemple suivant :
Soit $f_1 = xy+1$, $f_2 = y^2-1$ des polynômes de $K[x, y]$ avec l'ordre *lex*. On pose $F = (f_1, f_2)$ et $f = xy^2 - x$. On obtient

$$xy^2 - x = y(xy+1) + 0(y^2-1) - x - y.$$

Mais on a aussi

$$xy^2 - x = 0(xy+1) + x(y^2-1) + 0.$$

On verra plus loin qu'il s'agit de l'algorithme suivant appliqué à $F = (f_1, f_2)$.

Algorithme de division (*Voir* [7] *ou* [9])

Paramètres d'entrée : $f, f_1, \ldots, f_s$.
Sortie : $a_1, \ldots, a_s, r$.
$a_1 := 0; \ldots; a_s := 0; r := 0$;
$p := f$;
TANT QUE $p <> 0$
FAIRE
SI $LT(f_i)$ divise $LT(p)$ pour un certain i de $\{1, \ldots, s\}$
ALORS
{
$a_i := a_i + LT(p)/LT(f_i)$;
$p := p - (LT(p)/LT(f_i)) * f_i$;
}
SINON
{ $r := r + LT(p)$;
$p := p - LT(p)$;
}
FIN SI
FIN FAIRE

2.4 Idéaux monômiaux et Lemme de Dickson.

Définition 2.6. Soit I un idéal de $K[x_1, \ldots, x_n]$ (cf annexe A.3). On dit que I est monômial s'il existe une partie A de $\mathbb{N}^n$ (A peut être infinie) tel que I soit constitué de tous les polynômes s'exprimant comme des sommes finies de la forme $\sum_{\alpha \in A} h_\alpha x^\alpha$, où $h_\alpha \in K[x_1, \ldots, x_n]$. Dans ce cas, on écrit $I = \langle x^\alpha \rangle_{\alpha \in A}$.

Exemple 2.5.

$$I = \langle x^4y^2, x^3y^4, x^2y^2 \rangle \subset K[x, y].$$

Lemme 2.5. *Soit $I = \langle x^\alpha \rangle_{\alpha \in A}$ un idéal monômial. Alors un monôme x^β appartient à I ssi x^β est divisible par x^α pour quelques $\alpha \in A$.*

Démonstration. Si x^β est multiple de x^α pour certain $\alpha \in A$, alors $x^\beta \in I$ par définition d'un idéal.
Réciproquement, si $x^\beta \in I$ alors $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, avec $h_i \in K[x_1, \ldots, x_n]$ et $\alpha(i) \in A$. Si on développe chaque h_i comme une combinaison linéaire des monômes, on voit que chaque terme de la côté droite de l'équation est divisible par certain $x^{\alpha(i)}$. D'où x^β doit avoir la même propriété. □

Lemme 2.6. *Soit I un idéal monômial, et soit $f \in K[x_1, \ldots, x_n]$. Alors les assertions suivantes sont équivalentes :*

i) $f \in I$;
ii) tous termes de f appartiennent à I ;
iii) f est une combinaison K-linéaire des monômes de I.

Démonstration. Les implications *iii)⇒ii)⇒i)* sont triviaux. La preuve de *i)⇒iii)* est similaire au preuve du *lemme* précédent. □

Corollaire 2.7. *Deux idéaux monômiaux sont égaux ssi ils contiennent les mêmes monômes.*

Le résultat crucial suivant est connu sous le nom de "Lemme de Dickson".

Théorème 2.8. *(**Lemme de Dickson**, voir [7] ou [9]) Soit $I = \langle x^\alpha \rangle_{\alpha \in A} \subset K[x_1, \ldots, x_n]$. Alors I peut s'ecrire sous la forme $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ avec $\alpha(1), \ldots, \alpha(s) \in A$. En particulier, I admet une base finie.*

Démonstration. Voir [7] page 69.

□

2.5 Théorème de la base de Hilbert et Bases de Groebner

Définition 2.7. Soit I un idéal non nul de $K[x_1, \ldots, x_n]$.

i) On note par $LT(I)$ l'ensemble des termes de plus haut degré (*leading terms*) des éléments de I. Donc,

$$LT(I) = \{cx^\alpha : \exists\ f \in I \text{ tel que } LT(f) = cx^\alpha\}.$$

ii) On note par $\langle LT(I) \rangle$ l'idéal engendré par les éléments de $LT(I)$.

On a déjà vu que le "leading term" joue un rôle important dans l'algorithme de division. Cela amène un point subtil mais important à propos de $\langle LT(I) \rangle$. A savoir, si on a un ensemble de générateur fini pour I, on écrit $I = \langle f_1, \ldots, f_s \rangle$, et les idéaux $\langle LT(f_1), \ldots, LT(f_s) \rangle$ et $\langle LT(I) \rangle$ peuvent être différents. Par définition, on a $LT(f_i) \in LT(I) \subset \langle LT(I) \rangle$, cela implique $\langle LT(f_1), \ldots, LT(f_s) \rangle \subset \langle LT(I) \rangle$. Cependant, $\langle LT(I) \rangle$ peut strictement plus grand que $\langle LT(f_1), \ldots, LT(f_s) \rangle$.Pour voir cela, considérons l'exemple suivant :

Exemple 2.6. Soit $I = \langle f_1, f_2 \rangle$, où $f_1 = x^3 - 2xy$ et $f_2 = x^2y - 2y^2 + x$, et on utilise l'ordre monômial *grlex* dans $K[x, y]$.
On a,

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

Donc $x^2 \in I$ et $x^2 = LT(x^2) \in \langle LT(I)\rangle$.
Or x^2 n'est pas divisible par $LT(f_1) = x^3$ ou $LT(f_2) = x^2y$ donc
$x^2 \notin \langle LT(f_1), LT(f_2)\rangle$ d'après lemme 2.5

Proposition 2.9. *Soit $I \subset K[x_1, \ldots, x_n]$ un idéal. Alors*

i) $\langle LT(I)\rangle$ est un idéal monômial.
ii) Il existe $g_1, \ldots, g_t \in I$ tel que $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$.

Démonstration. i) Le *leading monomial* (monôme de plus haut degré) $LM(g)$ d'un élément $g \in I - \{0\}$ engendre l'idéal monômial $\langle LM(g) : g \in I - \{0\}\rangle$. Puisque $LM(g)$ et $LT(g)$ se diffèrent par une constante non nulle, cet idéal est $\langle LT(g) : g \in I - \{0\}\rangle = \langle LT(I)\rangle$. Donc $\langle LT(I)\rangle$ est un idéal monômial.
ii) Puisque $\langle LT(I)\rangle$ est engendré par les monômes $LM(g)$ pour $g \in I - \{0\}$, le *lemme de Dickson* nous dit que $\langle LT(I)\rangle = \langle LM(g_1), \ldots, LM(g_t)\rangle$ pour certain $g_1, \ldots, g_t \in I$ (avec t fini). Puisque $LM(g_i)$ et $LT(g_i)$ se diffèrent par une constante non nulle, donc $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. □

Théorème 2.10. ***(Théorème de la base de Hilbert)*** *(cf. [7])*
Tout idéal I de $K[x_1, \ldots, x_n]$ admet un nombre fini de générateur. En d'autre terme $I = \langle g_1, \ldots, g_t\rangle$ pour certains $g_1, \ldots, g_t$ de $K[x_1, \ldots, x_n]$.

Démonstration. Si $I = \{0\}$, on prend $\{0\}$ comme ensemble de générateur, qui est certainement fini. Si I contient quelques polynômes non nuls, alors un ensemble générateur $g_1, \ldots, g_t$ pour I peut construire comme la suivante. D'après la proposition précédente, il existe $g_1, \ldots, g_t \in I$ tel que $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. On veut montrer que $I = \langle g_1, \ldots, g_t\rangle$.
Il est clair que $\langle g_1, \ldots, g_t\rangle \subset I$ puisque chaque $g_i \in I$.
Réciproquement, soit $f \in I$ un polynôme. Si on applique l'algorithme de division pour diviser f par $\langle g_1, \ldots, g_t\rangle$, alors on a l'expression suivante

$$f = a_1g_1 + \cdots + a_tg_t + r$$

où dans l'expression de r il n'existe pas de terme divisible par $LT(g_1), \ldots, LT(g_t)$. On voulait alors montrer que $r = 0$. Pour voir cela, noter que

$$r = f - a_1g_1 - \cdots - a_tg_t \in I.$$

Si $r \neq 0$, alors $LT(r) \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$, et d'après *lemme 2.5* , il suit que $LT(r)$ peut être divisible par un certain $LT(g_i)$. Par conséquence, cette contradiction montre que r peut être égale à 0. Donc,

$$f = a_1g_1 + \cdots + a_tg_t + 0 \in \langle g_1, \ldots, g_t\rangle,$$

qui montre que $I \subset \langle g_1, \ldots, g_t\rangle$, cela complète la preuve. □

Définition 2.8. Fixons un ordre monômial. On dit qu'un sous ensemble fini $G = \{g_1, \ldots, g_t\}$ d'un idéal I est une *base de Groebner* (ou base standard) si

$$\langle LT(g_1), \ldots, LT(g_t)\rangle = \langle LT(I)\rangle.$$

Autrement dit, un ensemble $\{g_1, \ldots, g_t\} \subset I$ est une base de Groebner de I si les leading term de chaque éléments de I est divisible par un certain $LT(g_t)$.

Corollaire 2.11. *Fixons un ordre monômial. Tout idéal I de $K[x_1, \ldots, x_n]$ différent de $\{0\}$ admet une base de Groebner. En outre, une base de Groebner d'un idéal I est une base de I.*

Démonstration. Etant donné un idéal non nul, l'ensemble $G = \{g_1, \ldots, g_t\}$ construit dans le preuve du *théorème 2.10* est une base de Groebner par construction. Pour la deuxième assertion, noter que si $\langle LT(g_1), \ldots, LT(g_t)\rangle = \langle LT(I)\rangle$, alors l'argument donné dans le théorème 2.10 montre que $I = \langle g_1, \ldots, g_t\rangle$, pour que G soit une base de I. □

Pour terminer cette section, on donne deux applications du théorème de la base de Hilbert. La première est une conséquence algébrique à propos des idéals dans $K[x_1, \ldots, x_n]$.

Théorème 2.12. ***(Condition des Chaînes Ascendantes)*** *(ACC) Soit*

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

une suite croissante d'idéaux dans $K[x_1, \ldots, x_n]$. Alors il existe $N \geq 1$ tel que

$$I_N = I_{N+1} = I_{N+3} = \cdots.$$

Démonstration. Soit une suite croissante d'idéaux $I_1 \subset I_2 \subset I_3 \subset \cdots$, considérons l'ensemble $I = \bigcup_{i=1}^{\infty} I_i$. On commence par montrer que I est aussi un idéal de $K[x_1, \ldots, x_n]$. D'abord, $0 \in I$ puisque $0 \in I_i$ pour tout i. Ensuite, si $f, g \in I$, alors par définition, $f \in I_i$ et $g \in I_j$ pour certain i et j (possible différent). En plus, puisque les idéaux I_i forment une suite croissante, si on suppose que $i \leq j$, alors $f, g \in I_j$. Puisque I_j est un idéal, il suit que $f + g \in I_j$, et alors $f + g \in I$. De même façon, si $f \in I$ et $r \in K[x_1, \ldots, x_n]$, alors $f \in I_i$ pour un certain i, et $r.f \in I_i \subset I$. D'où I est un idéal.
D'après le théorème de la base de Hilbert, l'idéal I admet un ensemble de générateur fini, c'est-à-dire $I = \langle f_1, \ldots, f_s\rangle$. Or chaque élément de ce générateur est contenu dans un idéal I_j, c'est-à-dire $f_i \in I_{j_i}$ pour certain j_i, ($avec\ i = 1, \ldots, s$). On choisit $N = max\{j_i\}$. Alors $f_i \in I_N$ pour tout i. Finalement, nous avons $I = \langle f_1, \ldots, f_s\rangle \subset I_N \subset I_{N+1} \subset \cdots \subset I$. □

La deuxième conséquence du *théorème da la base de Hilbert* serait géométrique. On sait que :

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in K^n : f_i(a_1, \ldots, a_n) = 0 \textit{ pour tout } i\}.$$

(Voir l'annexe A)

Définition 2.9. Soit I un idéal de $K[x_1, \ldots, x_n]$. On note par $V(I)$ l'ensemble

$$V(I) = \{(a_1, \ldots, a_n) \in K^n : f(a_1, \ldots, a_n) = 0 \textit{ pour tout} f \in I\}.$$

Proposition 2.13. *$V(I)$ est une variété affine. En particulier, si $I = \langle f_1, \ldots, f_s \rangle$, alors $V(I) = V(f_1, \ldots, f_s)$.*

Démonstration. D'après le *théorème de la base de Hilbert*, il existe $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ tel que $I = \langle f_1, \ldots, f_s \rangle$. Le but est de montrer que $V(I) = V(f_1, \ldots, f_s)$. Premièrement, puisque les $f_i \in I$, et par définition $f(a_1, \ldots, a_n) = 0$ pour tout $f \in I$, alors $f_i(a_1, \ldots, a_n) = 0$, et $V(I) \subset V(f_1, \ldots, f_s)$.
D'autre part, soit $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$ et soit $f \in I$. Puisque $I = \langle f_1, \ldots, f_s \rangle$, on peut écrire

$$f = \sum_{i=1}^{s} h_i f_i$$

pour certain $h_i \in K[x_1, \ldots, x_n]$. Alors

$$\begin{aligned} f(a_1, \ldots, a_n) &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) \\ &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n).o \\ &= 0 \end{aligned}$$

Donc $V(f_1, \ldots, f_s) \subset V(I)$. □

2.6 Propriétés des bases de Groebner

On a déjà montrer que tout idéal non nul $I \subset K[x_1, \ldots, x_n]$ admet une base de Groebner. Dans cette section, nous étudierons les propriétés des bases de Groebner et apprenons comment détecter quand une base donnée est une base de Groebner.

Proposition 2.14. *"Unicité du reste"*
Soit $G = \{g_1, \ldots, g_t\}$ une base de Groebner d'un idéal I de $K[x_1, \ldots, x_n]$ et soit $f \in K[x_1, \ldots, x_n]$. Alors il existe un unique $r \in K[x_1, \ldots, x_n]$ ayant les propriétés suivantes :

i) Aucun terme de r n'est divisible par l'un des $LT(g_1), \ldots, LT(g_t)$,
ii) Il existe $g \in I$ tel que $f = g + r$.

Le polynôme r est le reste de la division de f par G et ce indépendamment de l'ordre des éléments de G et de l'ordre monômial choisi.

Démonstration. L'algorithme de division donne $f = a_1g_1 + \cdots + a_tg_t + r$, avec r satisfait $i)$. On peut aussi en satisfaire $ii)$ en mettant $g = a_1g_1 + \cdots + a_tg_t \in I$. Cela montre l'existence de r.
Pour prouver l'unicité, supposons que $f = g + r = g' + r'$ satisfaisant $i)$ et $ii)$. Alors $r - r' = g' - g \in I$, alors que si $r \neq r'$, alors $LT(r - r') \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. D'après *Lemme*2.5, il suit que $LT(r - r')$ est divisible par quelque $LT(g_i)$. C'est impossible car il n'y a pas de terme de r ou de r' divisible par l'un des $LT(g_1), \ldots, LT(g_t)$. Donc $r - r'$ doit être zéro, et on a prouvé l'unicité.
La dernière partie de la proposition découle de l'unicité de r. □

Le reste r est appelé quelquefois la *forme normale de f*. Comme conséquence nous obtenons un moyen de savoir si un polynôme appartient ou non à un idéal.

Proposition 2.15. *Soit $G = \{g_1, \ldots, g_t\}$ une base de Groebner d'un idéal I de $K[x_1, \ldots, x_n]$ et soit $f \in K[x_1, \ldots, x_n]$. Alors $f \in I$ si et seulement si le reste de la division de f par G est zéro.*

Démonstration. Si le reste est zéro, alors on a déjà observé que $f \in I$. Inversement, soit $f \in I$, alors $f = f + 0$ satisfait le deux propriétés du *proposition*2.14. Il suit que 0 est le reste de la division de f par G. □

Définition 2.10. On écrit $\overline{f}^F$ le reste de la division de f par le s-uplet ordonné $F = (f_1, \ldots, f_s)$. Si F est une base de Groebner de $\langle f_1, \ldots, f_s\rangle$, alors on peut considérer F comme un ensemble d'après la *proposition*.2.14

Par exemple, soit $F = (x^2y - y^2, x^4y^2 - y^2) \subset K[x, y]$, en utilisant l'ordre *lex*, nous avons

$$\overline{x^5y}^F = xy^3$$

en effet, l'algorithme de division donne

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0.(x^4y^2 - y^2) + xy^3.$$

Définition 2.11. Soient $f, g \in K[x_1, \ldots, x_n]$ des polynômes non nuls.
i) Si $multideg(f) = \alpha$ et $multideg(g) = \beta$, alors soit $\gamma = (\gamma_1, \ldots, \gamma_n)$, où $\gamma_i = max(\alpha_i, \beta_i)$ pour chaque i. On dit que x^γ est le plus petit commun multiple (**least common multiple**) de $LM(f)$ et $LM(g)$, et on écrit

$$x^\gamma = PPCM(LM(f), LM(g)).$$

ii) On définit le *S-polynôme* de f et g, noté $S(f,g)$, comme étant

$$S(f,g) = \frac{x^\gamma}{LT(f)}.f - \frac{x^\gamma}{LT(g)}.g.$$

Par exemple, soient $f = x^3y^2 - x^2y^3 + x$ et $g = 3x^4y + y^2$ dans $\mathbb{R}[x,y]$ avec l'ordre *grlex*. Alors $\gamma = (4,2)$ et

$$\begin{aligned} S(f,g) &= \frac{x^4y^2}{x^3y^2}.f - \frac{x^4y^2}{3x^4y}.g \\ &= x.f - (1/3).y.g \\ &= -x^3y^3 + x^2 - (1/3)y^3. \end{aligned}$$

Lemme 2.16. *Considérons la somme $\sum_{i=1}^s c_i f_i$, où $c_i \in K$ et $multideg(f_i) = \delta \in \mathbb{N}^n$ pour tout i. Si $multideg(\sum_{i=1}^s c_i f_i) \prec \delta$, alors $\sum_{i=1}^s c_i f_i$ est une combinaison linéaire, à coefficient dans K, des S-polynômes $S(f_j, f_k)$ pour $1 \leq j,k \leq s$. De plus, chaque $S(f_j,f_k)$ admet de multidegré $\prec \delta$.*

Démonstration. Soit $d_i = LC(f_i)$, alors que le leading coefficient de $c_i f_i$ est $c_i d_i$. Puisque $multideg(c_i f_i) = \delta$ et le multidegré de leur somme est strictement plus petit, alors $\sum_{i=1}^s c_i d_i = 0$.
Définissons $p_i = f_i/d_i$, et notons que le leading coefficient de p_i est 1. Considérons la somme

$$\begin{aligned} \sum_{i=1}^s c_i f_i = \sum_{i=1}^s c_i d_i p_i = c_1d_1(p_1 - p_2) + (c_1d_1 + c_2d_2)(p_2 - p_3) + \cdots + \\ (c_1d_1 + \cdots + c_{s-1}d_{s-1})(p_{s-1} - p_s) + (c_1d_1 + \cdots + c_sd_s)p_s. \quad (2.1) \end{aligned}$$

Par hypothèse, $LT(f_i) = d_i x^\delta$, qui implique que le plus petit commun multiple (LCM) de $LM(f_j)$ et $LM(f_k)$ est x^δ. Donc

$$S(f_j,f_k) = \frac{x^\delta}{LT(f_j)}f_j - \frac{x^\delta}{LT(f_k)}f_k = \frac{x^\delta}{d_j x^\delta}f_j - \frac{x^\delta}{d_k x^\delta}f_k = p_j - p_k. \quad (2.2)$$

En utilisant cette équation et l'égalité $\sum_{i=1}^s c_i d_i = 0$, la somme (2.1) au dessus dévient

$$\begin{aligned} \sum_{i=1}^s c_i f_i = c_1d_1S(f_1,f_2) + (c_1d_1 + c_2d_2)S(f_2,f_3) \\ + \cdots + (c_1d_1 + \cdots + c_{s-1}d_{s-1})S(f_{s-1},f_s). \end{aligned}$$

Puisque p_j et p_k admettent de multidegré δ et de leading coefficient 1, alors la différence $p_j - p_k$ admet de multidegré $\prec \delta$. En observant l'équation (2.2), l'égalité est vrai pour $S(f_j,f_k)$, et on a prouvé le lemme. □

Théorème 2.17. *Soit I un idéal polynômial. Alors une base $G = \{g_1,\ldots,g_t\}$ de I est une base de Groebner de I si et seulement si pour toute paire $i \neq j$, le reste de la division de $S(g_i,g_j)$ par G est zéro.*

Démonstration. ($\Rightarrow$) : Si G est une base de Groebner, alors $S(g_i, g_j) \in I$, donc le reste de la division de $S(g_i, g_j)$ par G est zéro d'après la proposition 2.15.
($\Leftarrow$) : Soit $f \in I$ un polynôme non nul. Nous devons montrer que si les restes de la division de tout *S-polynôme* par G sont des 0, alors $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$. Avant de donner les détails, on va résumer la stratégie de la preuve.
Soit $f \in I = \langle g_1, \ldots, g_t\rangle$, il existe des polynômes $h_i \in K[x_1, \ldots, x_n]$ tel que

$$f = \sum_{i=1}^{t} h_i g_i. \tag{2.3}$$

D'après lemme 2.3, on a

$$multideg(f) \preceq max(multideg(h_i g_i)). \tag{2.4}$$

Si on n'a pas l'égalité, alors quelque annulation doit se produire parmi les leading terms de (2.3). Le lemme 2.16 nous permettra de réécrire ceci dans le terme de *S-polynôme*. Alors l'hypothèse : les restes des *S-polynôme* sont des zéros nous permettra de remplacer les *S-polynômes* par des expressions qui entrainent moins d'annulation. Donc, on obtiendra une expression de f qui a moins d'annulation de leading terms . En continuant cette méthode, nous obtiendrons en fin une expression de f tel que on a l'égalité dans (2.4). Alors $multideg(f) = multideg(h_i g_i)$ pour certain i, et on aura que $LT(f)$ soit divisible par $LT(g_i)$. Cela montrera que $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$, ce que nous voulons prouver.
Maintenant, on donne le détails de la preuve. En donnant l'expression (2.3) pour f, soit $m(i) = multideg(h_i g_i)$, et on pose $\delta = max(m(1), \ldots, m(t)$. Alors l'inégalité (2.4) devient

$$multideg(f) \preceq \delta.$$

Considérons toutes les façons possibles pour que f puisse s'écrire sous la forme (2.3). Pour chaque expression, on peut avoir différents δ. Puisque l'ordre monômial est un bon ordre, on peut choisir une expression de f tel que δ soit minimal.
Nous montrerons qu'une fois cette valeur minimale de δ est choisie, on a $multideg(f) = \delta$. Alors on a égalité dans (2.4), et comme nous avons observé, il suit que $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$. Cela prouve le théorème.
Il reste à montrer que $multideg(f) = \delta$. On prouvera cela par contradiction. Supposons que $multideg(f) \prec \delta$. Pour isoler les termes de multidegré δ, on va écrire f sous la forme :

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)\prec\delta} h_i g_i \\ &= \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{m(i)\prec\delta} h_i g_i. \end{aligned} \tag{2.5}$$

Les monômes apparaissent dans le deuxième et troisième sommes de la deuxième ligne sont de multidegré $\prec \delta$. Donc, l'hypothèse $multideg(f) \prec \delta$ veut dire que la première somme admet aussi de multidegré $\prec \delta$.
Soit $LT(h_i) = c_i x^{\alpha(i)}$. Alors la première somme
$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ admet exactement la forme décrite dans lemme 2.16 avec $f_i = x^{\alpha(i)} g_i$. Donc le lemme 2.16 implique que cette somme est une combinaison linéaire des *S-polynômes* $S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k)$. Cependant,

$$\begin{aligned} S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k) &= \frac{x^\delta}{x^{\alpha(j)}LT(g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(k)}LT(g_k)} x^{\alpha(k)} g_k \\ &= x^{\delta - \gamma_{jk}} S(g_j, g_k), \end{aligned}$$

où $x^{\gamma jk} = LCM(LM(g_j), LM(g_k))$. Donc il existe des constantes $c_{jk} \in K$ tel que

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k). \tag{2.6}$$

L'étape suivante utilise l'hypothèse : le reste de la division de $S(g_j, g_k)$ par $g_1, \ldots, g_t$ est nul. En utilisant l'algorithme de division, cela veut dire que chaque *S-polynôme* peut s'écrire sous la forme

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i, \tag{2.7}$$

où $a_{ijk} \in K[x_1, \ldots, x_n]$. L'algorithme de division entraine aussi

$$multideg(a_{ijk}g_i) \preceq multideg(S(g_j, g_k)) \tag{2.8}$$

pour tout i, j, k (voir théorème 2.4). Intuitivement, cela dit que quand le reste est zéro, on peut chercher une expression de $S(g_j, g_k)$ dans les termes de G où les leading terms ne sont pas tous annuler. Pour exploiter ceci, multiplions l'expression de $S(g_j, g_k)$ par $x^{\delta - \gamma_{jk}}$ pour obtenir

$$x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i,$$

où $b_{ijk} = x^{\delta - \gamma_{jk}} a_{ijk}$. Alors (2.8) et lemme 2.16 implique

$$multideg(b_{ijk}g_i) \preceq multideg(x^{\delta - \gamma_{jk}} S(g_j, g_k)) \prec \delta. \tag{2.9}$$

Si on remplace l'expression de $x^{\delta - \gamma_{jk}} S(g_j, g_k)$ dans l'équation (2.6), on obtient une équation

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum_{j,k} c_{jk} (\sum_i b_{ijk} g_i) = \sum_i \widetilde{h}_i g_i$$

tel que , d'après (2.9), pour tout i, on a la propriété

$$multideg(\widetilde{h}_i g_i) \prec \delta.$$

Comme dernière étape de la preuve, remplaçons $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_i \widetilde{h}_i g_i$ dans l'équation (2.5) pour obtenir une expression de f comme un polynôme combinaison des g_i où tous les termes qui admettent de multidegré $\prec \delta$. Cela contredit le minimalité de δ et complète la démonstration du théorème. □

2.7 Algorithme de Buchberger

D'après Corollaire.2.9, on sait que tout idéal non nul dans $K[x_1, \ldots, x_n]$ admet une base de Groebner. Malheureusement, la preuve donnée était non constructive dans le sens qu'il n'a pas dit comment produire une base de Groebner. Donc maintenant, si on a un idéal $I \subset K[x_1, \ldots, x_n]$, le but est de répondre à la question : "Comment construire une base de Groebner pour I ?"
Le premier algorithme de calcul de base de Groebner à été donné par Buchberger dans sa thèse. L'un des principaux outils de cet algorithme est la notion de *S-polynôme* (voir définition 2.11).

Exemple 2.7. Considérons l'anneau de polynôme $K[x, y]$ avec l'ordre $grlex$, et soit $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$. Rappelons que $\{f_1, f_2\}$ n'est pas une base de Groebner pour I, en effet

$$LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2)\rangle.$$

Pour produire une base de Groebner, une idée naturelle est d'essayer en premier d'étendre l'ensemble générateur original à une base de Groebner en ajoutant plus de polynômes dans I.
Quels nouveaux générateurs devrions nous ajouter ? Pour cela, on a introduit le *S-polynôme*. Nous avons $S(f_1, f_2) = -x^2 \in I$, et son reste dans la division par $F = (f_1, f_2)$ est $-x^2$, qui est différent de 0. D'où, nous devrions inclure ce reste dans l'ensemble de générateur, on pose $f_3 = -x^2$. Si on pose $F = (f_1, f_2, f_3)$, On peut utiliser le théorème 2.17 pour tester si cet ensemble est une base de Groebner de I. On calcule

$$S(f_1, f_2) = f_3,$$

donc $\overline{S(f_1, f_2)}^F = 0$,

$$S(f_1, f_3) = (x^3 - 2xy) - (-x)(-x^2) = -2xy,$$

on a $\overline{S(f_1,f_3)}^F = -2xy \neq 0$.
D'où, on doit ajouter $f_4 = -2xy$ dans l'ensemble de générateur. Si on pose $F = (f_1, f_2, f_3, f_4)$, alors

$$\begin{aligned}
\overline{S(f_1,f_2)}^F &= \overline{S(f_1,f_3)}^F = 0, \\
S(f_1,f_4) &= y(x^3 - 2xy) - (-1/2)x^2(-2xy) = -2xy = yf_4, donc \\
\overline{S(f_1,f_4)}^F &= 0, \\
S(f_2,f_3) &= (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \\
\overline{S(f_2,f_3)}^F &= -2y^2 + x \neq 0.
\end{aligned}$$

Donc, on doit aussi introduire $f_5 = -2y^2 + x$ dans l'ensemble de générateur. Fixons $F = \{f_1, f_2, f_3, f_4, f_5\}$, on peut calculer que

$$\overline{S(f_i,f_j)}^F = 0 \text{ pour tout } 1 \leq i \leq j \leq 5.$$

D'après théorème 2.17 , il suit qu'une base de Groebner de I, avec l'ordre $grlex$, est donné par

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

Théorème 2.18. *(cf [7]) Soit $I = \langle f_1, \ldots, f_s\rangle \neq \{0\}$ un idéal polynômial. Alors on peut construire une base de Groebner de I dans un nombre fini de "pas" par l'algorithme suivant :*

Entrée : $F = (f_1, \ldots, f_s)$
Sortie : une base de Groebner $G = (g_1, \ldots, g_t)$ de I, avec $F \subset G$
G :=F
REPETER
G' :=G
POUR chaque paire $\{p, q\}$,$p \neq q$ dans G'
FAIRE $S := \overline{S(p,q)}^{G'}$
SI $S \neq 0$ ALORS $G := G \cup \{S\}$
JUSQU'A G :=G'

Démonstration. Avant de commencer la preuve, on a besoin de définir les notations fréquemment utilisées suivantes. Si $G = \{g_1, \ldots, g_t\}$, on note

$$\begin{aligned}
\langle G\rangle &= \langle g_1, \ldots, g_t\rangle \\
\langle LT(G)\rangle &= \langle LT(g_1), \ldots, LT(g_t)\rangle.
\end{aligned}$$

Nous montrons en premier que $G \subset I$ à chaque étape de l'algorithme. Ceci est vrai à l'initiale, et à chaque fois qu'on agrandisse G, en ajoutant le reste $S := \overline{S(p,q)}^{G'}$ pour p et $q \in G$. Donc, si $G \subset I$, alors p, q, et $S(p,q) \in I$, et puisque nous divisons par $G' \subset I$, on obtient $G \bigcup \{S\} \subset I$. Notons aussi que

$F \subset G$ avec F est une base de I, donc G est aussi une base de I.
L'algorithme se termine quand $G = G'$, qui veut dire que $S := \overline{S(p,q)}^{G'} = 0$ pour tout $p, q \in G$. D'où G est une base de Groebner de $\langle G \rangle = I$ d'après le théorème 2.17. Il reste à montrer que l'algorithme est terminé. On a besoin de considérer ce qui se passe après chaque passage à travers la boucle principale. L'ensemble G est constitué par G' (c'est l'ancien G) avec les restes non nul de la division des *S-polynômes* de tout élément de G' par G'. Alors

$$\langle LT(G') \rangle \subset \langle LT(G) \rangle \tag{2.10}$$

puisque $G' \subset G$. En plus, si $G' \neq G$ nous réclamons que $\langle LT(G') \rangle$ est strictement plus petit que $\langle LT(G) \rangle$. Pour voir cela, supposons qu'un reste non nul r d'un *s-polynôme* a été ajouté à G. Puisque r est un reste de la division par G', $LT(r)$ n'est pas divisible par les leading terms des éléments de G', donc $LT(r) \notin \langle LT(G') \rangle$. Cependant $LT(r) \in \langle LT(G') \rangle$, cela prouve notre réclamation. D'après (2.10), les idéaux $\langle LT(G') \rangle$ à partir d'itérations successives de la boucle forment une suite croissante d'idéaux dans $K[x_1, \ldots, x_n]$. Donc, l'A.C.C(cf. théorème 2.12) implique qu'après un nombre fini d'itérations, la suite sera constante, donc on obtient $\langle LT(G') \rangle = \langle LT(G) \rangle$. Finalement, d'après la section précédente, on a $G = G'$, et que l'algorithme soit terminé après un nombre fini de pas. □

Lemme 2.19. *Soit G une base de Groebner d'un idéal polynômial I. Soit $p \in G$ un polynôme tel que $LT(p) \in \langle LT(G - \{p\}) \rangle$. Alors $G - \{p\}$ est aussi une base de Groebner de I.*

Démonstration. On sait que $\langle LT(G) \rangle = \langle LT(I) \rangle$. Si $LT(p) \in \langle LT(G - \{p\}) \rangle$, alors $\langle LT(G - \{p\}) \rangle = \langle LT(G) \rangle$. Par définition, il suit que $G - \{p\}$ est aussi une base de Groebner de I. □

Définition 2.12. Une **base de Groebner minimale** d'un idéal polynômial I est une base de Groebner G de I tels que :
i) $LC(p) = 1$ pour tout $p \in G$.
ii) Pour tout $p \in G$, $LT(p) \notin \langle LT(G - \{p\}) \rangle$.

On peut construire une base de Groebner minimale d'un idéal non nul donné en appliquant l'algorithme du théorème 2.18 et en utilisant le lemme 2.19 pour éliminer les générateurs inutiles.

Définition 2.13. Une **base de Groebner réduite** d'un idéal polynômial I est une base de Groebner G de I tels que :
i) $LC(p) = 1$ pour tout $p \in G$.
ii) Pour tout $p \in G$, aucun monôme de p n'appartient à $\langle LT(G - \{p\}) \rangle$.

Proposition 2.20. *Soit $I \neq \{0\}$ un idéal polynômial. Alors, pour un ordre monômial donné, I admet une unique base de Groebner réduite.*

Démonstration. voir [7] page 90. □

Chapitre 3

Décodage des codes cycliques généraux

Ce chapitre est consacré au décodage des codes cycliques généraux, jusqu'à et au delà de la capacité de correction $t = [(d-1)/2]$, en utilisant la théorie de l'élimination et les bases de Groebner.
Le problème est, à partir des syndromes de l'erreur, de trouver l'erreur, ou plus précisément le polynôme localisateur d'erreur.

3.1 Introduction

Soient $\mathbb{F}_q$ le corps à q éléments et n un entier premier avec q. Dans le cas de certains énoncés généraux, on notera $\mathbb{F}$ le corps de base, non nécessairement fini. Les énoncés les plus significatifs en terme de codage seront obtenus sur $\mathbb{F}_2$.
Un code cyclique $\mathcal{C}$ de longueur n sur $\mathbb{F}_q$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$ (cf. théorème 1.2). L'anneau $\mathbb{F}_q[X]/(X^n-1)$ étant principal, donc tout code cyclique $\mathcal{C}$ admet un polynôme générateur $g(X)$, qui divise X^n-1. En se donnant une racine primitive *n-ième* de l'unité α sur $\mathbb{F}_q$, avec $\alpha \in \mathbb{F}_{q^m} = K$, on définit l'ensemble de définition $\mathcal{Q}$ du code $\mathcal{C}$ par :

$$\mathcal{Q} = \{i \in I_n = \{0, 1, \ldots, n-1\}; g(\alpha^i) = 0\} \tag{3.1}$$

On a alors

$$c \in \mathcal{C} \Leftrightarrow c(\alpha^i) = 0, \forall\ i \in \mathcal{Q}. \tag{3.2}$$

Soit $c(x) = a(x)g(x)$ un *mot de code* à transmettre à travers un canal bruité, on obtient le *mot de code reçu* de la forme $r(x) = c(x) + e(x)$ où c étant le *mot de code émis* et e l'*erreur commise*. Alors en calculant $r(\alpha^i)$, on obtient

$$r(\alpha^i) = c(\alpha^i) + e(\alpha^i) = e(\alpha^i)\ \textit{pour}\ i \in \mathcal{Q} \tag{3.3}$$

Ainsi, le décodeur connait les $e(\alpha^i)$ pour $i \in \mathcal{Q}$ que l'on appelle *syndromes* de l'erreur. On les note $s_i, i \in \mathcal{Q}$. On peut aussi exprimer ces syndromes s_i comme suit :

$$s_i = Y_1 Z_1^i + Y_2 Z_2^i + \cdots + Y_v Z_v^i,\ i \in \mathcal{Q},\ s_i \in K \tag{3.4}$$

où v est le nombre d'erreurs, $Y_j \in \mathbb{F}_q - \{0\}$ pour $j = 1, 2, \ldots, v$ sont les *valeurs de l'erreur*, et

$$Z_j = \alpha^{r_j},\ \textit{pour}\ j = 1, 2, \ldots, v, \tag{3.5}$$

où les entiers $r_j \in I_n$ soient les *indices de localisation des erreurs.*
Le but du processus de décodage est de trouver les v emplacements de l'erreur inconnus et les v valeurs de l'erreur correspondantes à partir des syndromes connus s_i pour $i \in \mathcal{Q}$.

3.2 Décodage des codes cycliques avec l'identité de Newton

Soit $\mathcal{C}$ un code cyclique de polynôme générateur g et soient c le message émis et r le message reçu. Supposons qu'au plus t erreurs se produisent, et on note v le nombre exacte d'erreurs, $v \leq t$ où v est sous la condition $2v \leq n$ (cf. remarque 1.3, voir [12]). Le polynôme d'erreur qu'on veut chercher est de la forme $e(x) = \sum_{i=1}^{v} e_i x^{r_i}$, où les r_i sont tous différentes dans $0, 1, \ldots, n-1$, et e_i sont les valeurs d'erreurs. Pour déterminer ce polynôme d'erreur, on a toujours besoin de calculer le polynôme localisateur d'erreur $L(z)$ (cf. chapitre 1). On utilise les identités de Newton pour déterminer les coefficients σ_j du polynôme localisateur d'erreur pour $1 \leq j \leq v$. Il y a 4 étapes à suivre pour cette méthode :
$1^{\text{ère}}$ **étape** : Déterminer les syndromes s_i en calculant $r(\alpha^i)$.
$2^{ème}$ **étape** : Trouver les coefficients σ_j du polynôme localisateur d'erreur en utilisant l'*identité de Newton.*
$3^{ème}$ **étape** : Chercher les racines de $L(z)$ en testant les différentes puissances de α pour déterminer les localisateurs d'erreur α^i.
$4^{ème}$ **étape** : Remplacer les α^i par leurs valeurs dans l'expression de s_j pour déterminer les valeurs des erreurs e_i (cas non binaire seulement). On obtient ainsi le polynôme erreur $e(x)$ et on peut décoder par $c = r - e$.

3.3 Exemple de décodage des codes cycliques en utilisant l'identité de Newton

Exemple 3.1. Soit α un élément primitif de $\mathbb{F}_{16}$, racine du polynôme $x^4 + x + 1$ sur $\mathbb{F}_2$ (où $x^4 + x + 1$ est irréductible sur $\mathbb{F}_2$), c'est-à-dire $\alpha^4 + \alpha + 1 = 0$. Tous les puissances de α sont :

$$\begin{array}{lll}
\alpha^0 = \alpha^{15} = 1 & \alpha^5 = \alpha + \alpha^2 & \alpha^{10} = 1 + \alpha + \alpha^2 \\
\alpha^1 = \alpha & \alpha^6 = \alpha^2 + \alpha^3 & \alpha^{11} = \alpha + \alpha^2 + \alpha^3 \\
\alpha^2 & \alpha^7 = 1 + \alpha + \alpha^3 & \alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3 \\
\alpha^3 & \alpha^8 = 1 + \alpha^2 & \alpha^{13} = 1 + \alpha^2 + \alpha^3 \\
\alpha^4 = 1 + \alpha & \alpha^9 = \alpha + \alpha^3 & \alpha^{14} = 1 + \alpha^3
\end{array}$$

Soit $\mathcal{C}$ un code cyclique de longueur 15 sur $\mathbb{F}_2$ de polynôme générateur $g(x) = (x^4+x+1)(x^4+x^3+x^2+x+1) = x^8+x^7+x^6+x^4+1$ et d'ensemble de définition $\mathcal{Q} = \{1, 2, 3, 4, 6, 8, 9, 12\}$. $\mathcal{C}$ est alors de dimension $k = 7$ et de distance minimale $d = 5$. On peut corriger $t = [\frac{5-1}{2}] = 2$ erreurs maximum. Soit, par exemple, le mot reçu $r = (100111000000000)$ ou bien $r(x) = 1 + x^3 + x^4 + x^5$ et on suppose qu'il y a exactement 2 erreurs (i.e $v = 2$). D'après le **Chapitre 1**, le polynôme localisateur d'erreur $L(z)$ est définie par : $L(z) = (z - Z_1)(z - Z_2) = z^2 + \sigma_1 z + \sigma_2$ et la clé du décodage est de trouver les coefficients σ_1 et σ_2. On a

$$\begin{aligned}
s_1 &= r(\alpha^1) = \alpha^6 \\
s_2 &= r(\alpha^2) = \alpha^{12} \\
s_3 &= r(\alpha^3) = \alpha^8 \\
s_4 &= r(\alpha^4) = \alpha^9
\end{aligned}$$

D'après l'identité de Newton, on obtient le système d' équations (d'inconnus σ_1 et σ_2) suivant :

$$\begin{cases} s_3 + \sigma_1 s_2 + \sigma_2 s_1 = 0 \\ s_4 + \sigma_1 s_3 + \sigma_2 s_2 = 0 \end{cases}$$

ou encore

$$\begin{cases} \alpha^{12}\sigma_1 + \alpha^6\sigma_2 = \alpha^8 \\ \alpha^8\sigma_1 + \alpha^{12}\sigma_2 = \alpha^9 \end{cases}$$

en résolvant ce système, on obtient $\sigma_1 = \alpha^6$ et $\sigma_2 = \alpha^7$,
donc $L(z) = z^2 + \alpha^6 z + \alpha^7 = (z - Z_1)(z - Z_2)$.
En testant les différentes puissances de α, on trouve $Z_1 = \alpha^{r_1} = \alpha^8$ et $Z_2 = \alpha^{r_2} = \alpha^{14}$. Le polynôme d'erreur est alors $e(x) = x^8 + x^{14}$. Donc le mot transmis était $c(x) = r(x) - e(x) = 1 + x^3 + x^4 + x^5 + x^8 + x^{14}$ ou bien $c = (100111001000001)$.
On décode ce mot par la division de ce polynôme par le polynôme générateur $g(x)$. On obtient le polynôme $1 + x^3 + x^5 + x^6$ et le reste est nul. Alors le message initial était $a(x) = c(x)/g(x) = 1 + x^3 + x^5 + x^6$ ou $a = (1001011)$.

Exemple 3.2. Soit α une racine du polynôme $x^2 + x + 2$ irréductible sur $\mathbb{F}_3$. On dit que α est un élément primitif de $\mathbb{F}_{3^2} = \mathbb{F}_9$ et les puissances de α sont :

$$\begin{aligned}
&\alpha^1 = \alpha,\ \alpha^2 = 1 + 2\alpha,\ \alpha^3 = 2 + 2\alpha,\ \alpha^4 = 2, \\
&\alpha^5 = 2,\ \alpha^6 = 2 + \alpha,\ \alpha^7 = 1 + \alpha,\ \alpha^8 = 1.
\end{aligned}$$

En outre, on sait que les classes cyclotomiques de 3 modulo 8 sont :

$$\begin{aligned} cl(0) &= \{0\} \\ cl(1) &= \{1,3\} \\ cl(2) &= \{2,6\} \\ cl(4) &= \{4\} \\ cl(5) &= \{5,7\} \end{aligned}$$

On considère le code cyclique de longueur 8 sur $\mathbb{F}_3$ de polynôme générateur $g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^6) = (x^2+1)(x^2+x+2)(x+1)$ divisible par le polynôme minimal de α et possède comme racines α, α^2, α^3, α^4 et α^6. (i.e $\mathcal{Q} = \{1,2,3,4,6\}$)
Supposons que le mot reçu est $r = (02100112)$ (ou bien $r(x) = 2x + x^2 + x^5 + x^6 + 2x^7$) et on suppose que deux erreurs ont été commises.
Ensuite, on a

$$\begin{aligned} s_1 &= Y_1Z_1 + Y_2Z_2 = r(\alpha) = 2\alpha + \alpha^2 + \alpha^5 + \alpha^6 + 2\alpha^7 = 2 = \alpha^4 \\ s_2 &= Y_1Z_1^2 + Y_2Z_2^2 = r(\alpha^2) = 2\alpha^2 + \alpha^4 + \alpha^2 + \alpha^4 + 2\alpha^6 = \alpha^3 \\ s_3 &= Y_1Z_1^3 + Y_2Z_2^3 = r(\alpha^3) = \alpha^4 \\ s_4 &= Y_1Z_1^4 + Y_2Z_2^4 = r(\alpha^4) = 0 \\ s_6 &= Y_1Z_1^6 + Y_2Z_2^6 = r(\alpha^6) = \alpha \end{aligned}$$

avec $Y_1,\ Y_2 \in \mathbb{F}_3 - \{0\}$ sont les valeurs des erreurs et $Z_1 = \alpha^{r_1}$ et $Z_2 = \alpha^{r_2}$ où r_1 et r_2 sont des indices de localisations des erreurs.
On sait que le polynôme localisateur d'erreur soit de la forme

$$\begin{aligned} L(z) &= (z - Z_1)(z - Z_2) \\ &= z^2 - (Z_1 + Z_2)z + Z_1Z_2 \\ &= z^2 + \sigma_1 z + \sigma_2 \end{aligned}$$

En utilisant l'identité de Newton, on obtient le système d'équations suivant

$$\begin{cases} s_3 + \sigma_1 s_2 + \sigma_2 s_1 = 0 \\ s_4 + \sigma_1 s_3 + \sigma_2 s_2 = 0 \end{cases}$$

où les inconnus sont σ_1 et σ_2. En suite, on a

$$\begin{cases} \alpha^3\sigma_1 + \alpha^4\sigma_2 = -\alpha^4 \\ \alpha^4\sigma_1 + \alpha^3\sigma_2 = 0 \end{cases}$$

alors $\sigma_1 = \alpha^4 = 2$ et $\sigma_2 = \alpha$. Donc $L(z) = z^2 + 2z + \alpha$.
En testant les différentes puissances de α, on trouve $L(\alpha^3) = L(\alpha^6) = 0$,

c'est-à-dire $Z_1 = \alpha^3$ et $Z_2 = \alpha^6$. Pour trouver les valeurs d'erreurs Y_1 etY_2, il suffit de résoudre le système d'équations suivant :

$$\begin{cases} \alpha^3 Y_1 + \alpha^6 Y_2 = \alpha^4 \\ \alpha^6 Y_1 + \alpha^4 Y_2 = \alpha^3 \end{cases}$$

Alors

$$\begin{cases} Y_1 = \alpha^4 = 2 \\ Y_2 = \alpha^4 = 2 \end{cases}$$

Ces valeurs de Y_1 et Y_2 sont aussi solutions pour les trois autres égalités. Le polynôme d'erreur est donc $e(x) = 2x^3 + 2x^6$ et le mot envoyé était $c(x) = r(x) - e(x) = 2x + x^2 + x^3 + x^5 + 2x^6 + 2x^7$. (ou bien $c = (02110122)$). La division de $c(x)$ par $g(x)$ donne bien le mot décodé $m(x) = 2x^2 + x$, qui correspond à $m = (012)$.

3.4 Décodage des codes cycliques en utilisant la base de Groebner

Le premier plan du décodage est basé sur une méthode de recherche des zéros communs de l'ensemble des polynômes syndromes F définis par :

$$f_i = Y_1 Z_1^i + Y_2 Z_2^i + \cdots + Y_v Z_v^i - s_i, \ i \in \mathcal{Q}, \tag{3.6}$$

$$h_j = Z_j^n - 1, \quad \text{et } l_j = Y_j^{q-1} - 1, \ 1 \leq j \leq v. \tag{3.7}$$

On peut remplacer l'ensemble $\mathcal{Q}$ dans (3.6) par l'ensemble $\mathcal{R}$ des représentants des classes cyclotomiques.
Soit $V(F)$ l'ensemble des zéros communs de $F \subset K[Z_1, \ldots, Z_v, Y_1, \ldots, Y_v]$ dans la clôture algébrique $\overline{K}$ de K.

D'après la proposition 2.13, si on note $I(F)$ l'idéal engendré par F, alors $V(I(F)) = V(F)$.
Soient $z_1^*, z_2^*, \ldots, z_v^*$ les localisations des erreurs et $y_1^*, y_2^*, \ldots, y_v^*$ les valeurs des erreurs correspondantes. Alors il est clair que
$Z = (z_1^*, z_2^*, \ldots, z_v^*, y_1^*, y_2^*, \ldots, y_v^*) \in V(F)$ et $0 < |V(F)| < \infty$. En effet, par définition de s_i, on a $s_i = Y_1 Z_1^i + Y_2 Z_2^i + \cdots + Y_v Z_v^i$ donc on peut vérifier facilement que Z est racine de toutes les f_i. Ensuite, d'après une propriété d'un corps fini, on voit que Z annule aussi les h_j et l_j.
D'après le **théorème.1.4**, pour le cas $v \leq t = [\frac{d-1}{2}]$, il suit que $V(F)$ est constitué seulement de Z et de tous les points qu'on obtient par application d'une permutation arbitraire des v premières composantes de Z et la même permutation pour les v dernières composantes. Les zéros des polynômes **(3.6)** et **(3.7)** satisfont le polynôme localisateur d'erreur $L(z)$ qu'on a déjà défini dans le **chapitre 1**.
La clé du processus de décodage des codes cycliques est de chercher le

polynôme localisateur d'erreur $L(z)$. Dans ce mémoire, je présente deux théorèmes pour déterminer $L(z)$. Voir [1], [6]
Considérons l'ensemble des polynômes syndromes $F \subset K[Z_1, \ldots, Z_v, Y_1, \ldots, Y_v]$ défini dans **(3.6)** et **(3.7)**. Notons que pour un j donné $(1 \leq j \leq v)$, $I(F) \cap K[Z_j]$ est un idéal de $K[Z_j]$. C'est aussi un idéal principal puisque tout idéal de $K[Z_j]$ est principal.
Pour chercher les localisations possibles des erreurs, on a besoin de définir E_j pour $j = 1, \ldots, v$ qui est l'ensemble de toutes les j-ème composantes des zéros de F. Soit $Z = (z_1^*, z_2^*, \ldots, z_v^*, y_1^*, y_2^*, \ldots, y_v^*)$ un zéro de F, où $z_j^* \in K$ et $y_j^* \in \mathbb{F}_q - \{0\}$ sont, respectivement, les localisations des erreurs et les valeurs des erreurs pour $j = 1, \ldots, v$. Alors

$$E_j = \{z_j^* / (z_1^*, z_2^*, \ldots, z_v^*, y_1^*, y_2^*, \ldots, y_v^*) \in V(F)\} \tag{3.8}$$

pour $1 \leq j \leq v$.

Théorème 3.1. *Soit $g_j(Z_j) \in K[Z_j]$ le polynôme unitaire générateur de l'idéal $I(F) \cap K[Z_j]$ pour $j = 1, 2, \ldots, v$. Alors*

$$g_1(z) = g_2(z) = \cdots = g_v(z) = L(z), \tag{3.9}$$

où $L(z)$ est le polynôme localisateur d'erreur.

Démonstration. Considérons l'ensemble
$E_j = \{z_j^* / (z_1^*, z_2^*, \ldots, z_v^*, y_1^*, y_2^*, \ldots, y_v^*) \in V(F)\}$. Remarquons que
$E_1 = E_2 = \cdots = E_v = E = \{\beta / (z_1^*, z_2^*, \ldots, \beta, \ldots, z_v^*, y_1^*, y_2^*, \ldots, y_v^*)\}$, c'est-à-dire l'ensemble E est constitué par les v premières composantes de Z pour tout $Z \in V(F)$. En effet, les éléments de $V(F)$ sont $Z = (z_1^*, z_2^*, \ldots, z_v^*, y_1^*, y_2^*, \ldots, y_v^*)$ et tous les points obtenus par application d'une permutation arbitraire des v-premières composantes de Z et la même permutation pour les v-dernières composantes.
Par définition,

$$L(z) = \prod_{i=1}^{v} (z - Z_i) \tag{3.10}$$

donc les racines de $L(z)$ sont les Z_i qui sont des composantes de Z.
Soit $\beta \in E$, il existe $Z \in V(F)$ tel que β soit l'une de ses composantes, donc il existe j tel que $g_j(\beta) = 0$.
Or, par hypothèse $g_j(Zj)$ est le polynôme unitaire générateur de l'idéal principal $I(F) \cap K[Z_j]$.
Soit $\mathcal{L}(Z_i) = \prod_{\beta \in E}(Z_i - \beta)$. Alors, on peut exprimer $g_j(Z_j)$ sous la forme

$$g_j(Z_j) = a(Z_j)\mathcal{L}(Z_j)$$

En plus, puisque $Z_j^n - 1 \in I(F) \cap K[Z_j]$, il suit qu'il existe un polynôme $b(Z_j)$ tel que

$$Z_j^n - 1 = b(Z_j)g_j(Z_j) = b(Z_j)a(Z_j)\mathcal{L}(Z_j).$$

Puisque n, le longueur du code cyclique, satisfait $n|q^m - 1$, donc

$$PGCD(a(Z_j), \mathcal{L}(Z_j)) = 1,$$

en effet $Z_j^n - 1 = \prod_{i=0}^{n-1}(Z_j - \alpha^i)$.
Ensuite, puisque $Z_j^n - 1 | Z_j^{q^m-1} - 1$ (car $n|q^m - 1$) pour $1 \leq j \leq v$, toutes les composantes des éléments de $V(F)$ sont dans $K \subset \overline{K}$. Or, d'après **proposition 2.13** $V(F) = V(I(F))$, donc tout zéro de $I(F)$ dans $\overline{K}$ peut aussi élément de K.
Par définition de E, toutes les composantes des éléments de $V(F)$ sont dans E. Donc, tout zéro de $I(F)$ dans $\overline{K}$ satisfait $\mathcal{L}(Z_j)$. Alors, d'après le théorème d'**Hilbert Nullstellenzatz** (voir l'annexe A), il existe $l > 0$ tel que $\mathcal{L}^l(Z_j) \in I(F)$. D'où, il existe un polynôme $c(Z_j)$ tel que

$$\mathcal{L}^l(Z_j) = c(Z_j)g_j(Z_j) = c(Z_j)a(Z_j)\mathcal{L}(Z_j).$$

En outre, puisque

$$PGCD(a(Z_j), \mathcal{L}(Z_j)) = 1$$

et $g_j(Z_j)$ est un polynôme unitaire, on a $a(Z_j) = 1$,
donc

$$g_j(Z_j) = \mathcal{L}(Z_j)$$

Or,

$$\mathcal{L}(Z_j) = \prod_{\beta \in E}(Z_j - \beta) = \prod_{i=1}^{v}(Z_j - Z_i^*) = L(Z_j).$$

Finalement, on a

$$g_1(z) = g_2(z) = \cdots = g_v(z) = L(z).$$

□

Ce théorème peut être utilisé pour chercher directement le polynôme localisateur d'erreur à partir des équations syndromes (3.6) et (3.7), en utilisant l'algorithme de Buchberger pour calculer une base de Groebner de F.
Voici deux exemples concrets, comme application de ce théorème.

Exemple 3.3. Reprenons l'**exemple 3.1**
Soit α un élément primitif de $\mathbb{F}_{16}$ racine du polynôme $x^4 + x + 1$ sur $\mathbb{F}_2$. Tous les puissances de α sont déjà définies dans l'exemple 3.1.
Soit $\mathcal{C}$ un code cyclique de longueur 15, de dimension 7, de distance minimale $d = 5$ sur $\mathbb{F}_2$, et de polynôme générateur $g(x) = x^8 + x^7 + x^6 + x^5 + 1$. L'ensemble de définition de $\mathcal{C}$ est $\mathcal{Q} = \{1, 2, 3, 4, 6, 8, 9, 12\}$ et on peut corriger $t = [\frac{d-1}{2}] = 2$ erreurs maximum.

Supposons que le mot reçu est $r(x) = 1 + x^3 + x^4 + x^5$ et il y a 2 erreurs. Les syndromes sont :

$$s_1 = r(\alpha^1) = \alpha^6$$
$$s_3 = r(\alpha^3) = \alpha^8$$

Les polynômes syndromes sont :

$$\begin{aligned} f_1 &= Z_1 + Z_2 - s_1 = Z_1 + Z_2 + \alpha^6 \\ f_3 &= Z_1^3 + Z_2^3 - s_3 = Z_1^3 + Z_2^3 + \alpha^8 \\ h_1 &= Z_1^{15} - 1 = Z_1^{15} + 1 \\ h_2 &= Z_2^{15} - 1 = Z_2^{15} + 1 \end{aligned}$$

On utilise l'**algorithme de Buchberger** pour calculer une base de Groebner de $F = \{f_1, f_3, h_1, h_2\}$. Pour faciliter les calcules, on pose $F = \{f_1, f_2, f_3, f_4\}$ avec $f_1 = Z_1 + Z_2 + \alpha^6$, $f_2 = Z_1^3 + Z_2^3 + \alpha^8$, $f_3 = Z_1^{15} + 1$, et $f_4 = Z_2^{15} + 1$ et on utilise l'*ordre lexicographique* avec $Z_2 \succ_{lex} Z_1$.
Posons $G = F = \{f_1, f_2, f_3, f_4\}$

$$\begin{aligned} S(f_1, f_2) &= \frac{Z_2^3}{Z_2}(Z_2 + Z_1 + \alpha^6) + \frac{Z_2^3}{Z_2^3}(Z_1^3 + Z_2^3 + \alpha^8) \\ &= Z_2^3 + Z_1 Z_2^2 + \alpha^6 Z_2^2 + Z_1^3 + Z_2^3 + \alpha^8 \\ &= Z_1 Z_2^2 + \alpha^6 Z_2^2 + Z_1^3 + \alpha^8 \end{aligned}$$

ensuite, on a

$$\overline{S(f_1, f_2)}^G = \alpha^6 Z_1^2 + \alpha^{12} Z_1 + \alpha^{13}.$$

En effet, $S(f_1, f_2) = (Z_1 Z_2 + \alpha^6 Z_2 + Z_1^2 + \alpha^{12}) f_1 + \alpha^6 Z_1^2 + \alpha^{12} Z_1 + \alpha^{13}$.
Posons $f_5 = \overline{S(f_1, f_2)}^G = \alpha^6 Z_1^2 + \alpha^{12} Z_1 + \alpha^{13}$ et G devient
$G = \{f_1, f_2, f_3, f_4, f_5\}$. Maintenant, on a $\overline{S(f_1, f_2)}^G = 0$

$$\begin{aligned} S(f_1, f_3) &= \frac{Z_1^{15} Z_2}{Z_2}(Z_2 + Z_1 + \alpha^6) + \frac{Z_1^{15} Z_2}{Z_1^{15}}(Z_1^{15} + 1) \\ &= Z_1^{16} + \alpha^6 Z_1^{15} + Z_2 \end{aligned}$$

on a aussi

$$\overline{S(f_1, f_3)}^G = 0$$

En effet, $S(f_1, f_3) = f_1 + (Z_1 + \alpha^6) f_3$.

$$\begin{aligned} S(f_1, f_5) &= \frac{Z_1^2 Z_2}{Z_2}(Z_2 + Z_1 + \alpha^6) + \frac{Z_1^2 Z_2}{\alpha^6 Z_1^2}(\alpha^6 Z_1^2 + \alpha^{12} Z_1 + \alpha^{13}) \\ &= \alpha^6 Z_1 Z_2 + \alpha^7 Z_2 + Z_1^3 + \alpha^6 Z_1^2 \end{aligned}$$

et on a

$$\overline{S(f_1, f_5)}^G = 0$$

En effet, $S(f_1, f_5) = (\alpha^6 Z_1 + \alpha^7) f_1 + \alpha^9 Z_1 f_5$.
De même manière, on a

$$\begin{aligned} S(f_2, f_5) &= \frac{Z_1^2 Z_2^3}{Z_2^3}(Z_2^3 + Z_1^3 + \alpha^8) + \frac{Z_1^2 Z_2^3}{\alpha^6 Z_1^2}(\alpha^6 Z_1^2 + \alpha^{12} Z_1 + \alpha^{13}) \\ &= \alpha^6 Z_1 Z_2^3 + \alpha^7 Z_2^3 + Z_1^5 + \alpha^8 Z_1^2 \end{aligned}$$

On voit

$$\overline{S(f_2, f_5)}^G = 0$$

En effet, $S(f_2, f_5) = (\alpha^6 Z_1 + \alpha^7) f_2 + (\alpha^9 Z_1^3 + \alpha^2) f_5$.
On peut vérifier facilement que pour tout $i, j \in \{1, \ldots, 5\}$ avec $i \neq j$,

$$\overline{S(f_i, f_j)}^G = 0$$

donc, d'après le **théorème 2.16**, $G = \{f_1, f_2, f_3, f_4, f_5\}$ est une base de Groebner de F.L'ensemble $G_N = \{Z_1 + Z_2 + \alpha^6, Z_1^3 + Z_2^3 + \alpha^8, Z_1^{15} + 1, Z_2^{15} + 1, Z_1^2 + \alpha^6 Z_1 + \alpha^7\}$ est aussi une base de Groebner de F.
Donc, d'après le **théorème 3.1**, le polynôme localisateur d'erreur est

$$L(z) = z^2 + \alpha^6 z + \alpha^7$$

Exemple 3.4. (voir [5] et [11]) Soit α un élément primitif de $\mathbb{F}_{2^5} = \mathbb{F}_{32}$ racine du polynôme $x^5 + x^2 + 1$ sur $\mathbb{F}_2$. Tous les éléments de $\mathbb{F}_{32}$ sont
0
$\alpha^0 = 1$
α
α^2
α^3
α^4
$\alpha^5 = 1 + \alpha^2$
$\alpha^6 = \alpha + \alpha^3$
$\alpha^7 = \alpha^2 + \alpha^4$
$\alpha^8 = 1 + \alpha^2 + \alpha^3$
$\alpha^9 = \alpha + \alpha^3 + \alpha^4$
$\alpha^{10} = 1 + \alpha^4$
$\alpha^{11} = 1 + \alpha + \alpha^2$
$\alpha^{12} = \alpha + \alpha^2 \alpha^3$
$\alpha^{13} = \alpha^2 + \alpha^3 + \alpha^4$
$\alpha^{14} = 1 + \alpha^2 + \alpha^3 + \alpha^4$
$\alpha^{15} = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$

$\alpha^{16} = 1 + \alpha + \alpha^3 + \alpha^4$
$\alpha^{17} = 1 + \alpha + \alpha^4$
$\alpha^{18} = 1 + \alpha$
$\alpha^{19} = \alpha + \alpha^2$
$\alpha^{20} = \alpha^2 + \alpha^3$
$\alpha^{21} = \alpha^3 + \alpha^4$
$\alpha^{22} = 1 + \alpha^2 + \alpha^4$
$\alpha^{23} = 1 + \alpha + \alpha^2 + \alpha^3$
$\alpha^{24} = \alpha + \alpha^2 + \alpha^3 + \alpha^4$
$\alpha^{25} = 1 + \alpha^3 + \alpha^4$
$\alpha^{26} = 1 + \alpha + \alpha^2 + \alpha^4$
$\alpha^{27} = 1 + \alpha + \alpha^3$
$\alpha^{28} = \alpha + \alpha^2 + \alpha^4$
$\alpha^{29} = 1 + \alpha^3$
$\alpha^{30} = \alpha + \alpha^4$
Considérons le code cyclique binaire d'ensemble de définition $\mathcal{Q} = \{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}$ et l'ensemble des représentants de classes cyclotomiques est $\mathcal{R} = \{1, 5, 7\}$. Le polynôme générateur de ce code est alors défini par
$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16})(x-\alpha^5)(x-\alpha^{10})(x-\alpha^{20})(x-\alpha^9)(x-\alpha^{18})(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{28})(x-\alpha^{25})(x-\alpha^{19})$
C'est un code cyclique du type $(31, 16, 7)_2$, donc on peut détecter au maximum 3 erreurs ($t = [\frac{7-1}{2}] = 3$).
Supposons que le mot reçu est $r(x) = x^3 + x^5$ et il y a exactement 2 erreurs. Les syndromes sont $s_1 = r(\alpha^1) = \alpha^8$, $s_5 = r(\alpha^5) = \alpha^{19}$, $s_7 = r(\alpha^7) = \alpha^3$, et l'ensemble des polynômes syndromes est

$$F = \{Z_2 + Z_1 + \alpha^8, Z_2^5 + Z_1^5 + \alpha^{19}, Z_2^7 + Z_1^7 + \alpha^3, Z_1^{32} + Z_1, Z_2^{32} + Z_2\}.$$

Pour calculer une base de Groebner de F, on utilise l'ordre lexicographique avec $Z_2 \succ_{lex} Z_1$. Posons $f_1 = Z_2 + Z_1 + \alpha^8$, $f_2 = Z_2^5 + Z_1^5 + \alpha^{19}$, $f_3 = Z_2^7 + Z_1^7 + \alpha^3$, $f_4 =, Z_1^{32} + Z_1$, $f_5 = Z_2^{32} + Z_2$, et $G = F = \{f_1, f_2, f_3, f_4, f_5\}$. On a

$$\begin{aligned} S(f_1, f_2) &= \frac{Z_2^5}{Z_2}(Z_2 + Z_1 + \alpha^8) + \frac{Z_2^5}{Z_2^5}(Z_2^5 + Z_1^5 + \alpha^{19}) \\ &= Z_1 Z_2^4 + \alpha^8 Z_2^4 + Z_1^5 + \alpha^{19} \end{aligned}$$

alors

$$\overline{S(f_1, f_2)}^G = \alpha^8 Z_1^4 + \alpha Z_1 + \alpha^{13}.$$

En effet $S(f_1, f_2) = (Z_1 Z_2^3 + \alpha^8 Z_2^3 + Z_1^2 Z_2^2 + \alpha^{16} Z_2^2 + Z_1^3 Z_2 + \alpha^8 Z_1^2 Z_2 + \alpha^{16} Z_1 Z_2 + \alpha^{24} Z_2 + Z_1^4 + \alpha) f_1 + \alpha^8 Z_1^4 + \alpha Z_1 + \alpha^{13}$.
On pose $f_6 = \alpha^8 Z_1^4 + \alpha Z_1 + \alpha^{13}$ et on ajoute f_6 à G donc G dévient

$G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ et $\overline{S(f_1, f_2)}^G = 0$. Ensuite,

$$\begin{aligned} S(f_2, f_3) &= \frac{Z_2^7}{Z_2^5}(Z_2^5 + Z_1^5 + \alpha^{19}) + \frac{Z_2^7}{Z_2^7}(Z_2^7 + Z_1^7 + \alpha^3) \\ &= Z_1^5 Z_2^2 + \alpha^{19} Z_2^2 + Z_1^7 + \alpha^3 \end{aligned}$$

et

$$\overline{S(f_2, f_3)}^G = \alpha^{13} Z_1^2 + \alpha^{21} Z_1 + \alpha^{21}.$$

En effet $S(f_2, f_3) = (Z_1^5 Z_2 + \alpha^{19} Z_2 + Z_1^6 + \alpha^8 Z_1^5 + \alpha^{19} Z_1 + \alpha^{27}) f_1 + \alpha^8 Z_1 f_6 + \alpha^{13} Z_1^2 + \alpha^{21} Z_1 + \alpha^{21}$.
On ajoute $f_7 = \alpha^{13} Z_1^2 + \alpha^{21} Z_1 + \alpha^{21}$ à G et on obtient $G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7\}$.
Des calculs analogues au précédent montrent que pour tout $i, j \in \{1, 2, \ldots, 7\}$ avec $i \neq j$, on a $\overline{S(f_i, f_j)}^G = 0$ donc G est une base de Groebner de F. En outre, l'ensemble

$$\begin{aligned} G_N = \{&Z_2 + Z_1 + \alpha^8, Z_2^5 + Z_1^5 + \alpha^{19}, Z_2^7 + Z_1^7 + \alpha^3, Z_1^{32} + Z_1, \\ &Z_2^{32} + Z_2, Z_1^4 + \alpha^{24} Z_1 + \alpha^5, Z_1^2 + \alpha^8 Z_1 + \alpha^8\} \end{aligned}$$

est aussi une base de Groebner de F et d'après le **théorème 3.1**, le polynôme localisateur d'erreur est

$$L(z) = z^2 + \alpha^8 z + \alpha^8$$

Or $L(z) = (z - \alpha^{r_1})(z - \alpha^{r_2})$ et en testant les différentes puissances de α, on voit $r_1 = 3$ et $r_2 = 5$. Donc l'erreur est $e(x) = x^3 + x^5$ et le mot transmis était $c(x) = r(x) - e(x) = 0$.
Supposons maintenant qu'il y a 3 erreurs et le mot reçu est $r(x) = 1 + x^5 + x^{15}$. Les syndromes sont $s_1 = r(\alpha^1) = \alpha^{16}$, $s_5 = r(\alpha^5) = \alpha^2$, $s_7 = r(\alpha^7) = \alpha^{15}$ et l'ensemble des polynômes syndromes est

$$\begin{aligned} F = \{&Z_3 + Z_2 + Z_1 + \alpha^{16}, Z_3^5 + Z_2^5 + Z_1^5 + \alpha^2, \\ &Z_3^7 + Z_2^7 + Z_1^7 + \alpha^{15}, Z_1^{32} + Z_1, Z_2^{32} + Z_2, Z_3^{32} + Z_3\}. \end{aligned}$$

En utilisant l'algorithme de Buchberger pour trouver une base de Groebner de F, avec l'ordre *lex* où $Z_3 \succ_{lex} Z_2 \succ_{lex} Z_1$, on obtient le polynôme localisateur d'erreur $L(z) = z^3 + \alpha^{16} z^2 + \alpha^{28} z + \alpha^{20}$.

Dans la suite, on développera un autre processus de décodage. On définit l'ensemble $\mathcal{I}_n - \mathcal{Q} = \{i / i \notin \mathcal{Q}\}$ et soit $\mathcal{R}' = \{r_1, r_2, \ldots, r_l\} \subset \mathcal{I}_n - \mathcal{Q}$ l'ensemble des représentants des classes cyclotomiques de $\mathcal{I}_n - \mathcal{Q}$. On a besoin de définir aussi un autre ensemble des polynômes syndromes F' du

code comme l'ensemble des polynômes suivants :

$$f'_i = s_i + \sum_{j=1}^{v} \sigma_j s_{i-j}, \qquad v < i < n, \tag{3.11}$$

$$h'_j = \sigma_j^{q^m} - \sigma_j, \qquad 1 \leq j \leq v, \tag{3.12}$$

$$l'_{r_j} = s_{r_j}^{q^m} - s_{r_j}, \qquad 1 \leq j \leq l, \tag{3.13}$$

où σ_j et s_{r_j} sont des variables dans K pour $1 \leq j \leq v$ et $1 \leq j \leq l$,respectivement, et les s_i dans (3.11) pour $i \in \mathcal{I}_n - \mathcal{Q}$ sont représentés par les s_r pour $r \in \mathcal{R}'$.
Considérons l'ensemble des polynômes syndrome $F' \subset K[\sigma_1, \sigma_2, \ldots, \sigma_v, s_{r_1}, s_{r_2}, \ldots, s_{r_l}]$ avec $v \leq t$ soit le nombre d'erreurs. Alors $0 < |V(F')| < \infty$. Pour trouver les localisations des erreurs, on a besoin de définir Σ_j pour $j = 1, 2, \ldots, v$ qui est l'ensemble de toutes les j-ème composantes des zéros de F'. Soit $Z = (\sigma_1^*, \sigma_2^*, \ldots, \sigma_v^*, s_{r_1}^*, s_{r_2}^*, \ldots, s_{r_l}^*) \in V(F')$. Alors pour chaque $j \leq v$, on a

$$\Sigma_j = \{\sigma_j^* / (\sigma_1^*, \sigma_2^*, \ldots, \sigma_v^*, s_{r_1}^*, s_{r_2}^*, \ldots, s_{r_l}^*) \in V(F')\}, \tag{3.14}$$

c'est-à-dire, Σ_j contient toutes les j-è*me* composantes de Z pour tout $Z \in V(F')$. Notons que Σ_j dépend de l'entier j pour $1 \leq j \leq v$.

Théorème 3.2. *Soit $g_j(\sigma_j) \in K[\sigma_j]$ le polynôme unitaire générateur de l'idéal principal $I(F') \cap K[\sigma_j]$. Si $v \leq t$, alors*

$$g_j(\sigma_j) = \sigma_j - \sigma_j^* \tag{3.15}$$

où $L(z) = z^v + \sum_{j=1}^{v} \sigma_j^* z^{v-j}$ est le polynôme localisateur d'erreur.

Démonstration. Pour prouver ce théorème, on va montrer premièrement que

$$g_j(\sigma_j) = \prod_{\beta \in \Sigma_j} (\sigma_j - \beta), \tag{3.16}$$

où l'ensemble Σ_j est défini dans $(*)$ pour $j = 1, 2, \ldots, v$. Puisque $g_j(\sigma_j)$ est le polynôme unitaire générateur de l'idéal principal $I(F') \cap K[\sigma_j]$, il suit que $g_j(\beta) = 0$ pour tout $\beta \in \Sigma_j$.En suite, soit $L_j(\sigma_j) = \prod_{\beta \in \Sigma_j} (\sigma_j - \beta)$. Alors on peut exprimer $g_j(\sigma_j)$ sous la forme $g_j(\sigma_j) = a_j(\sigma_j) L_j(\sigma_j)$ pour quelque polynôme $a_j(\sigma_j)$.
En plus, puisque $\sigma_j^{q^m} - \sigma_j \in I(F') \cap K[\sigma_j]$, donc $g_j(\sigma_j) | \sigma_j^{q^m} - \sigma_j$. Or, d'après la propriété du corps finis $\mathbb{F}_{q^m}$, toute racine de $\sigma_j^{q^m} - \sigma_j$ est de multiplicité 1 (car $\sigma_j \in \mathbb{F}_{q^m}$), donc $PGCD(a_j(\sigma_j), L_j(\sigma_j)) = 1$. En outre, tout élément de $V(F')$ admet toutes ses composantes dans $K \subset \overline{K}$. Par définition de Σ_j, les $j-$è*me* composantes de tout élément de $V(F')$ appartiennent à Σ_j. En plus, tout zéro de $I(F')$ dans $\overline{K}$ satisfait $L_j(\sigma_j) = 0$. D'après le **théorème**

d'Hilbert Nullstelensatz, il existe un entier $h > 0$ tel que $L_j^h(\sigma_j) \in I(F')$. Donc il existe un polynôme $c_j(\sigma_j)$ tel que

$$L_j^h(\sigma_j) = c_j(\sigma_j)g_j(\sigma_j) = c_j(\sigma_j)a_j(\sigma_j)L_j(\sigma_j)$$

Puisque $PGCD(a_j(\sigma_j), L_j(\sigma_j)) = 1$ et $g_j(\sigma_j)$ est un polynôme unitaire, nécessairement $a_j(\sigma_j) = 1$. Donc $g_j(\sigma_j) = L_j(\sigma_j)$.
Finalement, les **théorèmes 1.5, et 1.7** montrent que les zéros dans $V(F')$ sont uniques. Donc $\Sigma_j = \{\sigma_j^*\}$, $L_j(\sigma_j) = \sigma_j - \sigma_j^*$, et $g_j(\sigma_j) = L_j(\sigma_j) = \sigma_j - \sigma_j^*$ pour $j = 1, 2, \ldots, v$ □

Exemple 3.5. Reprenons l'exemple 3.2.
Soit α une racine du polynôme $x^2 + x + 2$ irréductible sur $\mathbb{F}_3$, donc α est un élément primitif de $\mathbb{F}_9$. Les puissances de α sont déjà définies dans l'exemple 3.2.
Considérons le code cyclique de longueur 8 sur $\mathbb{F}_3$, de polynôme générateur $g(x) = x^5 + 2x^4 + x^3 + x^2 + 2$, et d'ensemble de définition $\mathcal{Q} = \{1, 2, 3, 4, 6\}$, donc $I_8 - \mathcal{Q} = \{5, 7\}$ et $\mathcal{R}' = \{5\}$
On voit que $d = 5$ et alors on peur corriger 2 erreurs au maximum. On suppose que le mot reçu est $r(x) = 2x + x^2 + x^5 + x^6 + 2x^7$ avec 2 erreurs ($v = 2$).
On a déjà calculé tous les syndromes s_i pour $i \in \mathcal{Q}$ (Voir exemple 3.2).
Les éléments de l'ensemble des polynômes syndromes F' sont :
$f_3' = s_3 + \sigma_1 s_2 + \sigma_2 s_1 = \alpha^4 + \alpha^3\sigma_1 + \alpha^4\sigma_2$,
$f_4' = s_4 + \sigma_1 s_3 + \sigma_2 s_2 = \alpha^4\sigma_1 + \alpha^3\sigma_2$,
$f_5' = s_5 + \sigma_1 s_4 + \sigma_2 s_3 = s_5 + \alpha^4\sigma_2$,
$f_6' = s_6 + \sigma_1 s_5 + \sigma_2 s_4 = \alpha + \sigma_1 s_5$,
$f_7' = s_7 + \sigma_1 s_6 + \sigma_2 s_5 = s_5^3 + \alpha\sigma_1 + \sigma_2 s_5$,
(en effet, $s_7 = s_{3.5} = r(\alpha^{3.5}) = r(\alpha^5)^3 = s_5^3$)
$h_1' = \sigma_1^9 - \sigma_1$,
$h_2' = \sigma_2^9 - \sigma_2$,
$l_5' = s_5^9 - s_5$.
Pour calculer la base de Groebner réduite de F', on utilise l'ordre *lex* et on pose $\sigma_1 \prec \sigma_2 \prec s_5$. Quand on fait le calcul avec MAPLE, on voit les polynômes $\sigma_1 - \alpha^4$ et $\sigma_2 - \alpha$ dans la base de Groebner réduite de F'.
Donc, d'après le théorème 3.2, le polynôme localisateur d'erreur est $L(z) = z^2 + \alpha^4 z + \alpha = z^2 + 2z + \alpha$
Voir l'exemple 3.2 pour la suite du processus de décodage.

Conclusion

Dans ce mémoire, on a montré que les bases de Groebner forment un outil essentiel pour le décodage des codes cycliques. On a présenté dans ce mémoire des méthodes de décodage algébrique des codes cycliques à l'aide de calcul de base de Groebner.
D'abord, on peut dire que le premier travail à faire est de calculer les syndromes connus (qui sont les s_i tel que $i \in \mathcal{Q}$) et plus précisément de formuler l'ensemble de polynômes syndromes. Remarquons qu'il y a deux ensembles des polynômes syndromes différents (F et F'), mais l'objectif est de trouver le polynôme localisateur d'erreur $L(z)$.

D'après les **théorème 3.1** et **théorème 3.2**, on peut déterminer $L(z)$ en cherchant le générateur unitaire de l'idéal $I(F) \cap K[Z_j]$ ou de l'idéal $I(F') \cap K[\sigma_j]$. On a montré que le générateur unitaire d'un idéal polynômial dans $K[Z_j]$ ou $K[\sigma_j]$ peut être déterminé à partir des algorithmes pour le calcul des bases de Groebner.

Enfin, on peut conclure que l'algorithme de décodage des codes cycliques est basé sur les **théorème 3.1** et **théorème 3.2**, et l'utilisation de la base de Groebner.

Annexe A : Rappels sur les polynômes, Idéaux, et Variétés affines

A.1.Polynôme et espace affine

Je pense que le lecteur soit certainement familier avec les polynômes à une ou à deux variables, mais nous aurons besoin d'être familier avec les polynômes à n variables $x_1, \ldots, x_n$ à coefficient dans un corps arbitraire K. On commence par la définition de monôme.

Définition A 1. (cf [7]) Un monôme à plusieurs variables $x_1, \ldots, x_n$ est un produit de la forme

$$x_1^{\alpha_1}.x_2^{\alpha_2}\ldots x_n^{\alpha_n},$$

où les exposants $\alpha_1, \ldots, \alpha_n$ sont des entiers non négatifs. De plus, la somme $\alpha_1 + \cdots + \alpha_n$ est appelée *degré total*.

On peut simplifier la notation d'un monôme comme suit : soit $\alpha = (\alpha_1, \ldots, \alpha_n)$ un $n - uplet$ de $\mathbb{N}^n$, on pose

$$x^\alpha = x_1^{\alpha_1}.x_2^{\alpha_2}\ldots x_n^{\alpha_n},$$

et $|\alpha| = \alpha_1 + \cdots + \alpha_n$ le degré total du monôme.

Définition A 2. (cf. [7]) Un polynôme f à n variables $x_1, \ldots, x_n$ et à coefficient dans K est une combinaison linéaire finie des monômes. On notera un polynôme f sous la forme

$$f = \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in K,$$

où la somme se fait sous un nombre fini des $n - uplets$ $\alpha = (\alpha_1, \ldots, \alpha_n)$. L'ensemble de tout polynômes à n variables $x_1, \ldots, x_n$ et à coefficient dans K est noté $K[x_1, \ldots, x_n]$.

On utilise la terminologie suivante quand on parle de polynôme :

Définition A 3. soit $f = \sum_\alpha a_\alpha x^\alpha$ un polynôme dans $K[x_1, \ldots, x_n]$.
i)a_α est appelé coefficient du monôme x^α.
ii)Si $a_\alpha \neq 0$, alors $a_\alpha x^\alpha$ est un terme de f.
iii)Le degré total de f, noté **deg(f)**, est le maximum $|\alpha|$ tel que le coefficient $a_\alpha \neq 0$.

Définition A 4. Étant donné un corps K et un entier positif n, on définit l'espace affine à $n - dimension$ sur K par l'ensemble

$$K^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in K\}$$

A.2.Variétés affines

Définition A 5. Soient K un corps et $f_1, \ldots, f_s$ des polynômes dans $K[x_1, \ldots, x_n]$. On pose

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in K^n : f_i(a_1, \ldots, a_n) = 0 \textit{ pour tout } 1 \leq i \leq s\},$$

$V(f_1, \ldots, f_s)$ est appelée *variété affine* définie par $f_1, \ldots, f_s$.

Autrement dit, une variété affine $V(f_1, \ldots, f_s) \subset K^n$ est l'ensemble de toutes les solutions du système d'équations

$$\begin{cases} f_1(x_1, ..., x_n) = 0 \\ \vdots \\ f_s(x_1, ..., x_n) = 0 \end{cases}$$

Exemple 3.6. On prend $K = \mathbb{R}$ et $n = 2$. La variété $V(x^2 + y^2 - 1)$ est le cercle de rayon 1 centré à l'origine.

A.3.Idéal

Définition A 6. Un sous ensemble $I \subset K[x_1, \ldots, x_n]$ est un idéal s'il satisfait les conditions :
(i) $0 \in I$,
(ii) Si $f, g \in I$, alors $f + g \in I$,
(iii) Si $f \in I$ et $h \in K[x_1, \ldots, x_n]$, alors $hf \in I$.

Définition A 7. Soient $f_1, \ldots, f_s$ des polynômes dans $K[x_1, \ldots, x_n]$, on pose

$$\langle f_1, \ldots, f_s \rangle = \{\sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in K[x_1, \ldots, x_n]\}.$$

Lemme A 1. *Si $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, alors $\langle f_1, \ldots, f_s \rangle$ est un idéal de $K[x_1, \ldots, x_n]$ qu'on appelle idéal engendré par $f_1, \ldots, f_s$.*

Démonstration. Il vérifie la condition (i), en effet $0 = \sum_{i=1}^{s} 0 f_i \in \langle f_1, \ldots, f_s \rangle$. Ensuite, supposons que $f = \sum_{i=1}^{s} p_i f_i$ et $g = \sum_{i=1}^{s} q_i f_i$, et soit $h \in K[x_1, \ldots, x_n]$, alors les équations

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i,$$

$$hf = \sum_{i=1}^{s} (hp_i) f_i$$

complètent la démonstration pour que $\langle f_1, \ldots, f_s \rangle$ soit un idéal. □

Proposition A 1. *Si $f_1, \ldots, f_s$ et $g_1, \ldots, g_t$ sont des bases d'un même idéal de $K[x_1, \ldots, x_n]$ (c'est-à-dire $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$), alors*

$$V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$$

.

Démonstration. voir [7] □

Définition A 8. Soit $V \subset K^n$ une variété affine, on définit l'ensemble

$$I(V) = \{f \in K[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ pour tout } (a_1, \ldots, a_n) \in V\}.$$

Lemme A 2. *Si $V \subset K^n$ est une variété affine, alors $I(V) \subset K[x_1, \ldots, x_n]$ est un idéal qu'on appelle idéal de V.*

Démonstration. Il est clair que $0 \in I(V)$, en effet le polynôme nul s'annule en tout point de K^n, et en particulier sur V. Ensuite, supposons que $f, g \in I(V)$ et $h \in K[x_1, \ldots, x_n]$. Soit $(a_1, \ldots, a_n) \in V$ (un point arbitraire). Alors $f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0$ et $h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) * 0 = 0$. □

Remarque A 1. Quand on parle de polynôme, idéal, et variété, on obtient le diagramme suivant :

$$\begin{array}{ccccc} \textit{Polynômes} & & \textit{Variété} & & \textit{Idéal} \\ f_1, \ldots, f_s & \longrightarrow & V(f_1, \ldots, f_s) & \longrightarrow & I(V(f_1, \ldots, f_s)). \end{array}$$

Lemme A 3. *Si $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, alors*

$$\langle f_1, \ldots, f_s \rangle \subset I(V(f_1, \ldots, f_s)).$$

Démonstration. Soit $f \in \langle f_1, \ldots, f_s \rangle$, c'est-à-dire $f = \sum_{i=1}^{s} h_i f_i$ pour quelques polynômes $h_1, \ldots, h_s \in K[x_1, \ldots, x_n]$. Puisque $f_1, \ldots, f_s$ s'annulent sur $V(f_1, \ldots, f_s)$, alors $\sum_{i=1}^{s} h_i f_i = 0$ sur $V(f_1, \ldots, f_s)$. Donc f s'annule sur $V(f_1, \ldots, f_s)$, qui montre que $f \in I(V(f_1, \ldots, f_s))$. □

Proposition A 2. *Soient V et W des variétés affines dans K^n. alors :*
(i) $V \subset W$ *ssi* $I(V) \supset I(W)$,
(ii) $V = W$ *ssi*$I(V) = I(W)$.

Démonstration. (i) Supposons que $V \subset W$, alors tout polynôme qui s'annule sur W s'annule aussi sur V, donc $I(W) \subset I(V)$. En suite, on suppose que $I(W) \subset I(V)$. On sait que W est la variété définie par quelques polynômes $g_1, \ldots, g_t \in K[x_1, \ldots, x_n]$. alors $g_1, \ldots, g_t \in I(W) \subset I(V)$, et les $g_i (1 \leq i \leq t)$ s'annulent sur V. Puisque W est constitué par tous les zéros commun des g_i, donc $V \subset W$.
(ii) est une conséquence directe de (i). □

A.4.Hilbert Nullstellensatz

Nous avons déjà vu le diagramme :

$$\begin{array}{ccc} Variété\ affine & & Idéal \\ V & \longrightarrow & I(V). \end{array}$$

Réciproquement, étant donné un idéal $I \subset K[x_1, \ldots, x_n]$, on peut définir l'ensemble

$$V(I) = \{x \in K^n : f(x) = 0 \text{ pour tout } f \in I\}.$$

Le théorème de la base de Hilbert assure que $V(I)$ soit une variété affine, en effet ce théorème dit qu'il existe un ensemble fini des polynômes $f_1, \ldots, f_s \in I$ tel que $I = \langle f_1, \ldots, f_s \rangle$, et on a prouvé dans la proposition 2.13 que $V(I)$ est l'ensemble des zéros commun de ces polynômes. Donc, on a aussi le diagramme

$$\begin{array}{ccc} Idéal & & Variété\ affine \\ I & \longrightarrow & V(I). \end{array}$$

Ces deux diagrammes nous donnent une correspondance entre idéaux et variétés.

Théorème A 1. ***(the weak Nullstellensatz)*** *Soit K un corps algébriquement clos et soit $I \subset K[x_1, \ldots, x_n]$ un idéal satisfaisant $V(I) = \emptyset$. Alors $I = K[x_1, \ldots, x_n]$.*

Démonstration. Voir [7] page 168-169 □

Théorème A 2. ***(Théorème d'Hilbert Nullstellensatz)***
Soit K un corps algébriquement clos. Si $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ tel que $f \in I(V(f_1, \ldots, f_s))$, alors il existe un entier $m \geq 1$ tel que

$$f^m \in \langle f_1, \ldots, f_s \rangle$$

(et réciproquement)

Démonstration. (cf [7]) Étant donné un polynôme f qui s'annule pour tout zéro commun des polynômes $f_1, \ldots, f_s$, il suffit de montrer qu'il existe un entier $m \geq 1$ et des polynômes $A_1, \ldots, A_s$ tel que

$$f^m = \sum_{i=1}^{s} A_i f_i.$$

Considérons l'idéal $\widetilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset K[x_1, \ldots, x_n, y]$, où $f, f_1, \ldots, f_s$ sont comme au dessus. On va montrer que $V(\widetilde{I}) = \emptyset$.
Soit $(a_1, \ldots, a_n, a_{n+1}) \in K^{n+1}$, alors deux cas sont possibles :
$1^{\text{èr}}$ *cas* : $(a_1, \ldots, a_n)$ est un zéro commun de $f_1, \ldots, f_s$.
$2^{\text{ème}}$ *cas* : $(a_1, \ldots, a_n)$ n'est pas un zéro commun de $f_1, \ldots, f_s$.
Pour le premier cas, on a $f(a_1, \ldots, a_n) = 0$ puisque f s'annule en tout zéro commun de $f_1, \ldots, f_s$. Donc le polynôme $1 - yf$ prend la valeur $1 - a_{n-1} f(a_1, \ldots, a_n) = 1 \neq 0$ au point $(a_1, \ldots, a_n, a_{n+1})$. En particulier, $(a_1, \ldots, a_n, a_{n+1}) \notin V(\widetilde{I})$.
Dans le deuxième cas, pour un i quelconque $(1 \leq i \leq s)$, on peut avoir $f_i(a_1, \ldots, a_n) \neq 0$. Supposons que f_i est une fonction à $n+1$ variables qui ne dépend pas de la dernière variable, on a alors $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$. En particulier, on peut conclure que $(a_1, \ldots, a_n, a_{n+1}) \notin V(\widetilde{I})$. Ensuite, puisque $(a_1, \ldots, a_n, a_{n+1}) \in K^{n+1}$ est arbitraire, alors $V(\widetilde{I}) = \emptyset$.
Maintenant, en utilisant le théorème précédent (the weak Nullstellensatz), on a $1 \in \widetilde{I}$. C'est-à-dire

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf) \qquad (A.1)$$

pour certains polynômes $p_i, q \in K[x_1, \ldots, x_n, y]$.
Ensuite, posons $y = 1/f(x_1, \ldots, x_n)$, alors la relation $(A.1)$ devient

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, \frac{1}{f}) f_i \qquad (A.2)$$

Multiplions les deux membres de cette équation par une fonction puissance f^m où m est choisi suffisamment grand pour effacer tous les dénominateurs. Cela donne

$$f^m = \sum_{i=1}^{s} A_i f_i,$$

pour quelques polynômes $A_i \in K[x_1, \ldots, x_n]$. □

Annexe B : Quelques exemples des codes cycliques

B.1.Code BCH (Bose-Chaudhuri-Hocqenghem)

Ces codes ont été définis en 1959/60. Ils sont à l'origine de la définition générale des codes cycliques. Les codes BCH sont les codes cycliques de plus grande dimension pour une capacité de correction donnée ; cette capacité est assurée par une borne sur leur distance minimale, qu'on appelle la *borne BCH*. Celle-ci assure que la distance minimale d'un code BCH est minorée par une valeur appelée *distance construite (ou distance désignée)* du code.
Soient p un nombre premier, et $q = p^e$ ($e \in \mathbb{N}^*$), soit $n \in \mathbb{N}^*$ tel que $(n, q) = 1$.
Soient $m = \mathcal{O}_q[n]$ (voir définition 1.2), et $l \in \mathbb{N}^*$ tel que $n.l = q^m - 1$.
Soit γ un générateur de $\mathbb{F}_{q^m}^*$, on a donc $\gamma^{q^m-1} = 1$. Soit $\omega = \gamma^l$, on a $\omega^n = 1$.
ω est une racine primitive $n - ième$ de l'unité dans $\mathbb{F}_{q^m}$.

Définition B 1. (cf. [15]) Soient $s \in \mathbb{N}$ et $\delta \in \mathbb{N}^*$ tel que $s + \delta - 2 \leq n - 1$. Un code BCH de longueur n et de distance désignée δ sur $\mathbb{F}_q$ est un code cyclique de longueur n sur $\mathbb{F}_q$ dont le polynôme générateur $g(x)$ est le p.p.c.m des polynômes minimaux de $\omega^s, \omega^{s+1}, \ldots, \omega^{s+\delta-2}$.
Si $n = q^m - 1$, le code BCH est dit $primitif$.

Remarque B 1. on a :

$$\begin{aligned}\mathcal{C}_{BCH} &= \{c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}/c_i \in \mathbb{F}_q, c(\omega^i) = 0, \\ &\qquad\qquad \forall i \in \{s, s+1, \ldots, s+\delta-2\}\} \\ &= \{c = (c_0, c_1, \ldots, c_{n-1}) \in (\mathbb{F}_q)^n / H.c^t = 0\}\end{aligned}$$

où H est une matrice de contrôle du code.

Propriété B 1. (cf. [15]) Soit $\mathcal{C}$ un code BCH de distance désignée δ et de distance minimale d. Alors, on a $\delta \leq d$.

Exemple B 1. Prenons $p = q = 2$, $n = 2^3 - 1 = 7$ ($m = 3$), on a $X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$.

Considérons $f(X) = X^3 + X + 1$ et soit ω une racine de $f(X)$ dans $\mathbb{F}_8$. Alors

$$\mathbb{F}_8^* = (\omega) \; etX^7 - 1 = \prod_{j=0}^{6} (X - \omega^j).$$

Prenons $s = 1,\ \delta = 3$, le code BCH de longueur 7 sur $\mathbb{F}_2$ et de distance désignée $\delta = 3$ a pour polynôme générateur $g(X)$ qui est le ppcm des polynômes minimaux de ω^1, ω^2.
Comme $f(X) = X^3 + X + 1 = (X - \omega)(X - \omega^2)(X - \omega^4)$, alors $g(x) = f(X)$.

Remarque B 2. Un code BCH de distance désignée de la forme $\delta = 2t + 1$ ($t \in \mathbb{N}$) est $t-$correcteur car $\delta = 2t + 1 \leq d$.

B.2.Code Reed-Solomon (RS)

Définition B 2. (voir [15]) Soient $q = p^e$ ($p \in \mathbb{P},\ e \in \mathbb{N}^*$); $n = q - 1$. Les codes BCH correspondant à ce cas spécial s'appellent codes Reed-Solomon. Soit δ la distance désignée et prenons $s = n - (\delta - 1)$. Les racines consécutives sont alors $\omega^{n-\delta+1}, \omega^{n-\delta+2}, \ldots, \omega^{n-1}$ où ω est un élément générateur de $\mathbb{F}_q^*$. Le code RS est :

$$\mathcal{C}_{RS} = \{c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} / c_i \in \mathbb{F}_q,\ c(\omega^j) = 0 \\ \forall\ j \in \{n - \delta + 1, n - \delta + 2, \ldots, n - 1\}\}.$$

Remarque B 3. Le polynôme générateur du code RS prend la forme

$$g(X) = \prod_{i=n-\delta+1}^{n-1} (X - \omega^i)$$

Propriété B 2. Soit $\mathcal{C}$ un code linéaire du type $(n, k, d)_q$, alors $k + d \leq n + 1$. Cette rélation est appelée *borne de Singleton.*

Définition B 3. Un code linéaire du type $(n, k, d)_q$ tel que k+d=n+1 est appelé code MDS (Maximum Distance Séparable).

Proposition B 1. *(cf. [15]) Un code RS est un code MDS.*

Démonstration. D'après la borne BCH, on a $\delta \leq d$.
Par ailleurs, on a $k = dim(\mathcal{C}) = n - deg(g) = n - \delta + 1$. D'où $\delta = n - k + 1$.
D'après la borne de Singleton, on a $k + d \leq n + 1$, donc $d \leq n - k + 1$.
Ainsi, on a $n - k + 1 \leq d \leq n - k + 1$.
Alors $d = n - k + 1$ ou encore $d + k = n + 1$ □

Bibliographie

Bibliographie

[1] E.R.Berlekamp, *Algebraic coding theory.* New York : McGraw-hill, 1968

[2] I.F. Blake, R.C. Mullin *"The Mathematical Theory of Coding"* Academic Press New York San Francisco London 1975.

[3] B.Buchberger, *"Grobner bases : An algorithmic method in polynomial ideal theory,"* in Multidimensional systems theory, N.K.Bose, Ed. ppP 184-232, Dordrecht Reidel, 1985.

[4] S. Bulygin and R. Pellikaan, *"Decoding and finding the minimum distance with Groebner bases : history and new insights".* In series on Coding Theory and Cryptology vol.7 pp.585-622, World scientific, 2010.

[5] X Chen, I.S. Reed,T. Helleseth, and Truong, *Use of Grobner bases TO decode binary cyclic codes up to the minimum distance,* IEEE Trans. Inform. Theory, April 1993.

[6] R. T. Chien, *"Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes,"* IEEE Trans. Inform. Theory, vol. IT-10, pp 357-363, Oct. 1964

[7] D. A. Cox, J. B. Little, and D. O'Shea. *"Ideals, Varieties, and algorithms : an introduction to computational algebraic geometry and commutative algebra."* Springer, 1997.

[8] Daniel Augot. *"Décodage des codes algébriques et cryptographie"*Univérsité Pierre et Marie Curie-Paris VI.2007.

[9] P. Elbaz, Vincent. *Bases de Groebner et leurs applications* Version 2.1

[10] S. Lang, *Algebra, 2nd ed.* Menlo Park, CA : Addison-Wesley, 1984.

[11] F. J. MacWilliams and N. J. A. Sloane, *nThe theory of error-correcting codes.* Amsterdam : North Holland, 1977.

[12] J. L. Massey. *"Shift-register synthesis and BCH decoding,"* IEEE Trans. Inform. Theory, vol. IT-15, pp. 122-127, Jan 1969.

[13] A. A. Pantchichkine. Mathématiques des codes correcteurs d'erreurs. *"Cryptologie, Sécurité, et Codage d'information,"*2004-2005.

[14] A. Poli and L. Huguet, *Error correcting codes : Theory and applications.* Englewood Cliffs, NJ : Prenttice Hall International (UK) Ltd., 1992.

[15] J.H. Van Lint, *"Introduction to coding theory"* 3^{rd} Edition, Springer-Verlag Berlin Heidelberg 1999.

Candidat : RASAMIMANANA Ravotina Clément
e-mail : dart90rasamy@gmail.com
Mobile : (+261)33 71 959 64

Titre : Décodage algébrique des codes cycliques.

Résumé : L'intérêt de ce mémoire portent sur le décodage algébrique des codes cycliques généraux. Ce mémoire fournit deux théorèmes pour décoder tous les types de codes cycliques à partir du travail de X.Chen, I.S.Reed, T.Helleseth, et T.K.Truong (IEEE TRANSACTIONS ON INFORMATION THEORY. VOL 40, NO. 5, SEPTEMBER 1994). On a prouvé que le problème fondamentale du décodage est la détermination du polynôme localisateur d'erreur $L(z)$ en utilisant l'algorithme de Buchberger pour calculer les bases de Groebner de l'ensemble des polynômes syndrome F ou F'.

Mots clés : Théorie des codes, codes cycliques, algorithme de Buchberger et bases de Groebner, théorème d'Hilbert Nullstellensatz, décodage.

Abstract : The interest of this book is about the algebraic decoding of the general cyclic codes. This book provides two theorems for decoding all types of cyclic codes from the work of X.Chen, I.S.Reed, T.Helleseth, and T.K.Truong (IEEE TRANSACTIONS ONE INFORMATION THEORY. VOL 40, NO. 5, SEPTEMBER 1994). It is shown that the fundamental problem of the decoding is the determination of the error-locator polynomial $L(z)$ using the Buchberger's algorithm for computig Groebner bases of the set of syndrome polynomials F or F'.

Key Words : Coding theory, cyclic codes, Buchberger's algorirhm and Groebner bases, Hilbert's Nullstellensatz theorem, decoding.

Encadreur : Mr ANDRIATAHINY Harinaivo, Maître de Conférences
Département de Mathématiques et Informatique
Faculté des Sciences
Université d'Antananarivo
e-mail : aharinaivo@yahoo.fr
Mobile : (+261)32 04 607 57