UNIVERSITÉ D'ANTANANARIVO

Sciences et technologies

Mention : Mathématiques
et Informatique

Mémoire en vue de l'obtention du
Diplôme de MASTER de Mathématiques

Option : Mathématiques Appliquées
Spécialité : Grandes déviations et Algèbre appliquéqs (Codage)

ALGORITHME ITERATIF FONDAMENTAL MODIFIE ET DECODAGE DES CODES HERMITIENS

Présenté par

RAKOTONINDRINA Zo Tsaratany

Le 27 Avril 2015
Devant la commission d'examen formée par les membres de Jury :

Président : Monsieur **RABEHERIMANANA Toussaint Joseph**
Professeur Titulaire
Rapporteur : Monsieur **ANDRIATAHINY Harinaivo**
Maître de conférences
Examinateurs : Monsieur **ANDRIAMIFIDISOA Ramamonjy**
Maître de conférences
Monsieur **RAMAHAZOSOA Irrish Parker**
Maître de conférences

Remerciements

Tout d'abord, nous remercions notre Père Universel de nous avoir donné la force, la volonté, la santé et le courage afin d'accomplir ce travail.

Je remercie très vivement le Professeur RABEHERIMANANA Toussaint Joseph qui m'a fait l'honneur de présider le jury de ce mémoire.

Je tiens à exprimer toute ma profonde gratitude et reconnaissance à mon encadreur Monsieur ANDRIATAHINY Harinaivo qui a proposé le thème de ce mémoire et de m'avoir sacrifié tant de temps et d'énergie du début jusqu'à la fin de cet ouvrage pour me diriger, me conseiller, et m'orienter.

Je tiens à remercier Monsieur ANDRIAMIFIDISOA Ramamonjy, d'avoir cordialement accepté de se présenter parmi les membres de jury en tant qu'examinateur.

Je tiens à remercier également Monsieur RAMAHAZOSOA Irrish Parker, qui va porter son jugement sur ce travail.

Je voudrais aussi présenter mes sincères remerciements à mes parents, ma famille et mes amis pour leur soutien morale et leurs encouragements.

Table des matières

Introduction

Le développement le plus important dans la théorie de codes correcteurs d'erreurs est, ces dernières années, l'introduction des méthodes de la géométrie algébrique pour construire des codes linéaires. Ces codes de la géométrie algébrique ont été présentés par Goppa. En 1982, Tsfasman, Vlăduţ et Zink [TVZ82] ont obtenu un résultat extrêmement passionnant : l'existence d'un ordre des codes qui dépasse la limite de Gilbert-Varshamov. C'est ainsi que beaucoup d'articles traitant des codes géométriques algébriques ont suivi [KTV84]-[Har86].

Les bonnes constructions de code sont très importantes. D'ailleurs, il est souhaitable et important de dériver les procédures simples de décodage qui peuvent corriger autant d'erreurs que possibles. Justesen et les autres [JLJ89] ont présenté pour la première fois une procédure de décodage pour les codes des courbes algébriques planes non singulières. Cette procédure de décodage peut seulement corriger $[(d^* - g - 1)/2]$ ou moins d'erreurs, où d^* est la distance minimale désignée du code et g est le genre de la courbe utilisée dans la construction. Skorobogatov et Vlăduţ [SkV90] ont généralisé leurs idées et ont donné une procédure de décodage qui peut corriger $[(d* - g - 1)/2]$ ou moins d'erreurs pour les codes des courbes algébriques arbitraires. Dans leur article, ils ont également présenté un algorithme modifié, corrigeant plus d'erreurs, mais en général, pas jusqu'à la distance minimale désignée. En utilisant des résultats profonds de la géométrie algébrique, Pellikaan [Pel89] a donné une autre procédure de décodage jusqu' à décoder $[(d^* - 1)/2]$ erreurs. Cependant, sa procédure de décodage est très complexe et n'est pas complètement efficace. Récemment, Justesen et les autres [JLJ92] ont amélioré leur procédure de décodage originale de plusieurs manières et ont donné une nouvelle procédure de décodage pour les codes des courbes planes régulières arbitraires, qui peut décoder jusqu' à $[(d^* - g/2 - 1)/2]$ erreurs.

Dans ce mémoire, nous présentons une procédure assez simple de décodage capable de décoder jusqu' à $[(d^* - 1)/2]$ erreurs. L'amélioration est obtenue en em-

ployant une forme d'arrangement de majorité pour trouver des syndromes inconnus dans l'algorithme bien connu.

Ce mémoire est organisé comme suit. Dans le premier chapitre, nous formulons d'abord deux algorithmes en donnant à chacun un exemple pour mieux comprendre leur mécanisme. Le premier c'est l'algorithme itératif fondamental (FIA) dont son but est de trouver un entier l tel que les l premières colonnes d'une matrice donnée soient linéairement dépendentes. Le second est un derivé du FIA dans lequel on fait une modification et en donnant quelques propriétés qui seront très utiles dans les autres chapitres. Dans le deuxième chapitre, nous incluons quelques notions des courbes algébriques. On présente dans le prochain chapitre la procédure de décodage pour les codes géométriques algébriques $C_\Omega(D, G)$ avec $G = mQ$. Afin de comprendre ce procédure de décodage, on termine notre étude par un exemple de décodage en prenant une courbe hérmitienne dans le dernier chapitre.

Chapitre 1

Algorithme itératif fondamental

1.1 Algorithme itératif fondamental ou FIA

Dans cette section, on va détailler brièvement l'algorithme itératif fondamental (FIA). Il ressemble à la méthode d'élimination de Gauss. Il est utilisé pour la recherche d'un entier positif l tel que les l premieres colonnes d'une matrice $M \times N$ sur un corps $\mathbb{F}$ soient linéairement dépendantes. On va considèrer la matrice A suivante et on suppose qu'elle est de rang inférieur à N.

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,N} \\ a_{2,1} & a_{2,2} & \dots & a_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ a_{M,1} & a_{M,2} & \dots & a_{M,N} \end{bmatrix}$$

Le but est de déterminer un entier l et des constantes $c_1, c_2, ..., c_l$ tel que

$$a_{i,l+1} + c_1 a_{i,l} + ... + c_l a_{i,1} = 0 \quad pour \quad i = 1, 2, ..., M. \tag{1.1}$$

On a besoin d'introduire quelques notations. Soit $C(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_l x^l$ un polynôme de degré l où $c_0 = 1$ et soient $a^{(i)}(x) = a_{i,0} + a_{i,1} x + \cdots + a_{i,N} x^N$ des polynômes où $a_{i,0} = 1$ pour $i = 1, 2, ..., M$. Le produit usuel de ces deux polynômes est donné par

$$C(x)a^{(i)}(x) = c_0 \times a_{i,0} + (c_0 \times a_{i,1} + c_1 \times a_{i,0})x + (c_0 \times a_{i,2} + c_1 \times a_{i,1} + c_2 \times a_{i,0})x^2$$

$$+ ... + (c_0 \times a_{i,n} + c_1 \times a_{i,n-1} + ... + c_n \times a_{i,0})x^n + ... + c_l \times a_{i,N} x^{l+N}$$

Pour $l + 1 \leq n \leq N$, on note par $[C(x)a^{(i)}(x)]_n$ le coefficient de x^n dans $C(x)a^{(i)}(x)$, c'est-à-dire

$$[C(x)a^{(i)}(x)]_n = c_0 a_{i,n} + c_1 a_{i,n-1} + ... + c_n a_{i,n-l} = \sum_{j=0}^{l} c_j a_{i,n-j} \tag{1.2}$$

On a alors,

$$[C(x)a^{(i)}(x)x^p]_n = [C(x)a^{(i)}(x)]_{n-p} = \sum_{j=0}^{l} c_j a_{i,n-p-j}. \tag{1.3}$$

Donc, le problème général est de chercher l'entier minimal positif l et le polynôme $C(x)$ avec $\deg C(x) \leq l$ tel que

$$[C(x)a^{(i)}(x)]_{l+1} = 0 \quad \text{pour} \quad i = 1, 2, ..., M. \tag{1.4}$$

Pour trouver la solution à ce problème, on doit construire un algorithme d'itération. Pour cela, en commençant par la première colonne, on examine successivement les éléments de toutes les colonnes de la matrice A, de la première jusqu'à la dernière ligne.

Pour chaque colonne j, on définit le polynôme

$$C^{(i-1,j)}(x) = c_0^{(i-1,j)} + c_1^{(i-1,j)}x + c_2^{(i-1,j)}x^2 + ... + c_{j-1}^{(i-1,j)}x^{j-1} = \sum_{k=0}^{j-1} c_k^{(i-1,j)}x^k \tag{1.5}$$

où $1 \leq i \leq M$ et $c_0^{(i-1,j)} = 1$, vérifiant la propriété suivante

$$[C^{(i-1,j)}(x)a^{(h)}(x)]_j = a_{h,j} + c_1^{(i-1,j)}a_{h,j-1} + ... + c_{j-1}^{(i-1,j)}a_{h,1} = 0 \quad pour \quad h \leq i-1. \tag{1.6}$$

$[C^{(i-1,j)}(x)a^{(h)}(x)]_j$ exprime le coéfficient de x^j dans $C^{(i-1,j)}(x)a^{(h)}(x)$. Par conséquent, $C^{(0,j)}(x)$ est désigné comme polynôme initial à la colonne j avec $C^{(0,1)}(x) = 1$ pour la première colonne. Soit

$$d_{i,j} = [C^{(i-1,j)}(x)a^{(i)}(x)]_j = a_{i,j} + c_1^{(i-1,j)}a_{i,j-1} + ... + c_{j-1}^{(i-1,j)}a_{i,1}. \tag{1.7}$$

.

$d_{i,j}$ s'appelle la discrépance à la ligne i et à la colonne j.

Pour chaque colonne j, si $d_{i,j} = 0$ pour $i = 1, 2, ..., r-1$, alors on a

$$C^{(0,j)}(x) = C^{(1,j)}(x) = ... = C^{(r-1,j)}(x)$$

Si on suppose que $d_{r,j} \neq 0$ et s'il n'y a aucun u, où $1 \leq u < j$ et $C^{(u)}(x) = C^{(r-1,u)}(x)$, alors on définit par $C^{(j)}(x) = C^{(r-1,j)}(x)$ le polynôme final pour la colonne j et on met un " $\times$ " sur $a_{r,j}$ pour indiquer que la discrépance n'est pas nulle à cet endroit. Dans ce cas, cette discrépance s'appelle discrépance finale à la colonne j. Toutes les discrépances sur $a_{i,j}$, pour $i < r$, sont toutes nulles. Ensuite on passe à la colonne suivante et en commençant de la première composante, on examine successivement les élément de cette colonne avec $C^{(0,j+1)}(x) = C^{(j)}(x) = C^{(r-1,j)}(x)$. Sinon, il existe un $C^{(u)}(x)$ à la colonne u, où $1 \leq u < j$ tel que $C^{(u)}(x) = C^{(r-1,u)}(x)$. Alors $C^{(r,j)}(x)$ est obtenu par le lemme suivant :

1.1.1 Lemme. *Etant donné $C^{(r-1,u)}(x)$ et $d_{r,j} \neq 0$ et s'il existe un polynôme final $C^{(u)}(x)$ à la colonne u, où $1 \leq u < j$ tel que $C^{(u)}(x) = C^{(r-1,u)}(x)$ avec $d_{r,u} \neq 0$, alors*

$$C^{(r,j)}(x) = C^{(r-1,j)}(x) - \frac{d_{r,j}}{d_{r,u}}C^{(u)}(x)x^{j-u} \tag{1.8}$$

est tel que

$$[C^{(r,j)}(x)a^{(i)}(x)]_j = 0 \quad pour \quad i = 1, 2, \ldots, r-1, r. \tag{1.9}$$

Preuve. De (1.2), (1.3), (1.8) et d'après la définition de $C^{(r-1,j)}(x)$ et de $C^{(u)}(x)$, on a

$$\begin{aligned}
[C^{(r,j)}(x)a^{(i)}(x)]_j &= [C^{(r-1,j)}(x)a^{(i)}(x)]_j - \frac{d_{r,j}}{d_{r,u}}[C^{(u)}(x)a^{(i)}(x)x^{j-u}]_j \\
&= [C^{(r-1,j)}(x)a^{(i)}(x)]_j - \frac{d_{r,j}}{d_{r,u}}[C^{(u)}(x)a^{(i)}(x)]_{j-(j-u)} \\
&= [C^{(r-1,j)}(x)a^{(i)}(x)]_j - \frac{d_{r,j}}{d_{r,u}}[C^{(u)}(x)a^{(i)}(x)]_u \\
&= \begin{cases} 0 - \frac{d_{r,j}}{d_{r,u}}0 & \text{pour } i = 1, 2, ..., r-1 \\ d_{r,j} - \frac{d_{r,j}}{d_{r,u}}d_{r,u} & \text{pour } i = r \end{cases}
\end{aligned}$$

□

1.1.2 Lemme. *Il existe un " × " dans la colonne j si est seulement si celle-ci est linéairement indépendante de ses colonnes précédentes.*

Preuve. Supposons qu'il existe $r(1), r(2), \ldots, r(s)$ tous distincts et $C^{(1)}(x) = C^{(r(1)-1,1)}(x), C^{(2)}(x) = C^{(r(2)-1,2)}(x), \ldots, C^{(s)}(x) = C^{(r(s)-1,s)}(x)$. Alors, à chaque ligne et à chaque colonne distincte de la matrice $D = [d_{i,j}]$, appelée matrice de la discrépence, avec $d_{i,j} = [C^{(j)}(x)a^{(i)}(x)]_j$, on a des $d_{r(1),1}, d_{r(2),2}, \ldots, d_{r(s-1),s-1}, d_{r(s),s}$ différentes. La sous-matrice formée par les s premières colonnes et les lignes $r(i)$ où $i = 1, \ldots, s$ est non-singulière. Ainsi, chaque colonne de D est formée par une combinaison linéaire de s premères colonnes de la matrice A et la sous-matrice correspondante dans A doit être aussi non-singulière. Par conséquent, les s premères colonnes de la matrice A sont linéairement indépendantes.

□

Ainsi, en commençant avec la première colonne, on examine les éléments dans les colonnes successives de la matrice A, un par un, de la ligne supérieure vers la ligne inférieure. Si le problème a une solution pour A, $C^{(M,l)}(x)$ est une solution. Si $d_{i,j} = 0$, alors les sous-vecteurs de i premières composanates de la colonne j est une combinaison linéaire des sous-vecteurs des i premières composantes de ses $j-1$ colonnes précédentes. Ainsi, on dit que la colonne j *est une combinaison linéaire partielle de ses colonnes précédentes avec les i premières composantes.* Les coéfficients de ce combinaison linéaire sont les coefficients de $C^{(i,j)}(x)$.

Donc,on obtient l'algorithme suivant, appelé *algorithme itératif fondamental (FIA).* Pour cela, on a besoin de deux tableaux de stockage D et C. Le tableau D est utilisé pour stocker la discrépence finale $d_{r,j}$ de la colonne j et le tableau C est utilisé pour stocker le polynôme $C^{(j)}(x)$ correspondant.

Algorithme itératif fondamental :
Etape 1) Vider les tableaux D et C, $1 \to j$, $1 \to r$, $1 \to C^{(j)}(x)$.
Etape 2) Calculer $d_{r,j} = [C^{(j)}(x)a^r(x)]_j$
Etape 3) Si $d_{r,j} = 0$, alors
  a) Si $r = M$, alors $j - 1 \to l$, $C^{(j)}(x) \to C(x)$, ARRETER ; on a la solution.
  b) Sinon $r + 1 \to r$, et retour à l'étape 2).

Etape 4) Si $d_{r,j} \neq 0$, ALORS

a) S'il existe un $d_{r,u} \in D$, pour certain $1 \leq u \prec j$,
alors

$$C^{(j)}(x) - \frac{d_{r,j}}{d_{r,u}} C^{(u)}(x) x^{j-u} \to C^{(j)}(x)$$

et retour à l'étape 3).

b) Sinon, $d_{r,j}$ est stockée dans D, $C^{(j)}(x) \to C^{(j+1)}(x)$ et $C^{(j)}(x)$ est stocké dans C, marquer un "x" à la ligne r et à la colonne j. Si $j \prec N$, alors $j+1 \to j, 1 \to r$, et retour à l' étape 2). Sinon, ARRETER, car ce probléme n'a pas de solution.

1.2 Exemple

Maintenant, on va illustrer cet algorithme à l'aide de l'exemple suivant.
On considère la matrice suivante à valeur dans le corps $\mathbb{F}_2 = \{0, 1\}$

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & \dots \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{1,4} & \dots \\ a_{M,1} & a_{M,2} & a_{M,3} & a_{1,4} & \dots \end{bmatrix}$$

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

Commençons par la première colonne, c'est-à-dire $j = 1$. Pour $r = 1$ (première ligne), on a $C^{(0,1)}(x) = 1$, et $d_{1,1} = [C^{(0,1)}(x)a^{(1)}(x)]_1 = [1 \times (1 + x + x^3 + x^4)]_1 = 1 \neq 0$. Et comme il n' y a pas de $d_{1,u}$ pour $u < 1$, on pose $C^{(1)}(x) := C^{(0,1)}(x) = 1$ dans C et on stocke $d_{1,1}$ dans le Tableau D. $C^{(0,2)}(x) := C^{(1)}(x) = 1$

Ensuite, on se déplace à la deuxième colonne, c'est-à-dire $j = 2$,

Pour $r = 1$ (première ligne), on a $d_{1,2} = [C^{(0,2)}(x)a^{(1)}(x)]_2 = [1 \times (1 + x + x^3 + x^4)]_2 = 0$, ainsi $C^{(1,2)}(x) := C^{(0,2)}(x) = 1$. On passe à la deuxième ligne :

Pour $r = 2$, $d_{2,2} = [C^{(1,2)}(x)a^{(2)}(x)]_2 = [1 \times (1 + x + x^2 + x^3)]_2 = 1 \neq 0$, et comme il n'y a pas de $d_{2,u}$ pour $1 \leq u < 2$, on pose $C^{(2)}(x) := C^{(1,2)}(x) = 1$ dans C et on stocke $d_{2,2}$ dans D. On prend $C^{(0,3)}(x) := C^{(2)}(x) = 1$

Puis, on se dèplace à la troisième colonne, c'est-à-dire $j = 3$.

Pour $r = 1$ (première ligne), on a $d_{1,3} = [C^{(0,3)}(x)a^{(1)}(x)]_3 = [1 \times (1 + x + x^3 + x^4)]_3 = 1 \neq 0$, et comme $d_{1,1} = 1 \neq 0$ existe dans D, avec $u = 1$, alors $C^{(0,3)}(x)$ est obtenu par

$$C^{(0,3)}(x) := C^{(0,3)}(x) - \frac{d_{1,3}}{d_{1,1}} C^{(x)} x^{3-1} = 1 - \frac{1}{1} x^2 = 1 + x^2$$

Maintenant, on a $C^{(0,3)}(x) = 1 + x^2$ et $d_{1,3} = [(1 + x^2) \times (1 + x + x^3 + x^4)]_3 = 2 = 0$ dans F_2, alors $C^{(1,3)}(x) := C^{(0,3)}(x) = 1 + x^2$. Par suite, pour $r = 2$, $d_{2,3} = [C^{(1,3)}(x)a^{(2)}(x)]_3 = [(1 + x^2) \times (1 + x + x^2 + x^3)]_3 = 2 = 0$ et ainsi $C^{(2,3)}(x) := C^{(0,3)}(x) = 1 + x^2$. On passe encore à la troisième ligne, et on a

$$d_{3,3} = [C^{(2,3)}(x)a^{(2)}(x)]_3 = [(1 + x^2) \times (1 + x^2 + x^3 + x^4)]_3 = 1 \neq 0,$$

Et comme il n'existe pas de $d_{3,u}$ pour $1 \leq u < 3$, alors on stocke $d_{3,3}$ dans D et on met $C^{(3)}(x) := C^{(2,3)}(x) = 1 + x^2$. dans C.

On passe à la dernière colonne ($j = 4$), et en commençant par $C^{(0,4)}(x) := C^{(3)}(x) = 1 + x^2$, on a

$$d_{1,4} = [C^{(0,4)}(x)a^{(1)}(x)]_4 = [(1 + x^2) \times (1 + x + x^3 + x^4)]_4 = 1 \neq 0.$$

Comme $d_{1,1} = 1 \neq 0$ existe, avec $u = 1$, alors

$$C^{(0,4)}(x) := C^{(0,4)}(x) - \frac{d_{1,4}}{d_{1,1}} C^{(x)} x^{4-1} = 1 + x^2 - \frac{1}{1} \times 1 \times x^3 = 1 + x^2 + x^3$$

et $d_{1,4} = [C^{(0,4)}(x)a^{(1)}(x)]_4 = [(1 + x^2 + x^3) \times (1 + x + x^3 + x^4)]_4 = 2 = 0 = d_{3,4} = d_{1,4}$, Alors $C^{(3,4)}(x) = C^{(2,4)}(x) = C^{(1,4)}(x) = C^{(0,4)}(x) = 1 + x^2 + x^3$. Et on stocke la dernière valeur de $C^{(3,4)}(x) = 1 + x^2 + x^3$ dans C.

Finalement, la solution est

$$l = j - 1 = 4 - 1 = 3$$

et

$$C(x) = 1 + x^2 + x^3.$$

La matrice de discrépance D et la matrice polynômiale correspondante sont les suivantes

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & \dots \\ . & 1 & 0 & 0 & \dots \\ . & . & 1 & 0 & \dots \end{bmatrix}$$

Et

$$C = \begin{bmatrix} 1 & . & . & . & \dots \\ . & 1 & . & . & \dots \\ . & . & 1 + x^2 & 1 + x^2 + x^3 & \dots \end{bmatrix}$$

1.3 L'Algorithme itératif fondamental modifié ou MFIA

Maintenant, on va modifier le FIA. Pour cela, soit S' la matrice comme suit

$$S' = \begin{bmatrix} s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} & s_{1,8} & s_{1,9} & s_{1,10} & s_{1,11} \\ s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} & s_{2,7} & s_{2,8} & s_{1,9} & @ & \# \\ s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} & s_{3,7} & s_{3,8} & @ & \# & \# \\ s_{4,1} & s_{4,2} & s_{4,3} & s_{4,4} & s_{4,5} & s_{4,6} & @ & \# & \# & \# & \# \\ s_{5,1} & s_{5,2} & s_{5,3} & s_{5,4} & s_{5,5} & s_{5,6} & \# & \# & \# & \# & \# \\ s_{6,1} & s_{6,2} & s_{6,3} & s_{6,4} & s_{6,5} & @ & \# & \# & \# & \# & \# \\ s_{7,1} & s_{7,2} & s_{7,3} & s_{7,4} & @ & \# & \# & \# & \# & \# & \# \\ s_{8,1} & s_{8,2} & @ & \# & \# & \# & \# & \# & \# & \# & \# \\ s_{9,1} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# \\ \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \end{bmatrix}$$

où @ et # sont toutes inconnues, et les autres sont connues. Pour chaque colonne j, si $s_{i,j}$ est @, alors les valeurs de $s_{u,j}$ sont connues pour $u < i$ et $s_{v,j}$ sont tous # pour $v > i$; s'il n'existe pas de @ et le premier $s_{i,j}$ est #, alors les éléments au-dessus de $s_{i,j}$ sont connus et les éléments $s_{i,j}$

au-dessous sont tous des #. D'une autre manière, pour chaque ligne i, si $s_{i,j}$ est @, alors les valeurs de $s_{i,u}$ sont toutes connues pour $u < j$, et $s_{i,v}$ sont des # pour $v > j$; s'il n'existe aucun @ et # est le premier $s_{i,j}$, alors les éléments à gauche de $s_{i,j}$ sont connus et les éléments à droites sont tous #.

On suppose que la colonne j est une combinaison linéaire partielle de ses colonnes précédentes avec les $i-1$ premières composantes et $s_{i,j}$ est @, on veut savoir s'il y a une unique valeur de @ dans (i, j) de telle sorte que la colonne j est une combinaison linéaire partielle de ses colonnes précédentes avec les i composantes supérieures. S'il existe, comment cette valeur unique est-elle déterminée ? L'étape principale en décodant une certaine erreur linéaire corrigeant des codes peut être réduite à ce problème (Voir section suivante) : trouver une combinaison linéaire partielle avec les R-premières composantes pour un entier R donné (s'il existe) et chercher tous les @, ceux ci sont uniquement déterminés par la condition ci-dessus.
Afin de résoudre ce probléme, on modifie le FIA comme suit :

2') L'algorithme s'arrête lorsque $C^{(R,j)}(x)$ ou $C^{(N)}(x)$ est obtenu.

2") Une fois que $C^{(R,j)}(x)$ est obtenu, où $s_{i,j}$ est @ ou #, alors l'algorithme définit le polynôme final de la colonne j,$C^{(j)}(x) = C^{(i,j)}(x)$ et on se déplace à la première composante de la colonne suivante, noté par $s_{1,j+1}$.

Ainsi, après avoir appliqué la modification de FIA,la matrice de discrépance $D = [d_{ij}]$ est obtenue et est de la forme

$$\begin{bmatrix}
\times & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
s_{2,1} & 0 & 0 & \times & 0 & 0 & 0 & 0 & 0 & @ & \# \\
s_{3,1} & 0 & \times & s_{3,4} & 0 & 0 & 0 & 0 & @ & \# & \# \\
s_{4,1} & 0 & s_{4,3} & s_{4,4} & 0 & 0 & @ & \# & \# & \# & \# \\
s_{5,1} & \times & s_{5,3} & s_{5,4} & 0 & 0 & \# & \# & \# & \# & \# \\
s_{6,1} & s_{6,2} & s_{6,3} & s_{6,4} & \times & @ & \# & \# & \# & \# & \# \\
s_{7,1} & s_{7,2} & s_{7,3} & s_{7,4} & @ & \# & \# & \# & \# & \# & \# \\
s_{8,1} & s_{8,2} & @ & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{9,1} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \#
\end{bmatrix}$$

De cette matrice, on a vu facilement que :

2a) S'il n'y a aucun " $\times$" sur la colonne j, alors la colonne j est une combinaison linéaire partielle de ses colonnes précédentes avec les $i-1$ premières composantes, où i est le plus petit entier tel que @ ou # est sur (i, j). Pour la matrice ci-dessus, $i = 6, j = 6; i = 4, j = 7$; et ainsi de suite.

2b) Si on suppose que $s_{i,j} = @$, alors @ peut être déterminé telle que la colonne j est une combinaison linéaire partielle des ses colonnes précédentes avec les i premières composantes, si est seulement si il n'y a aucun " $\times$ " sur $s_{i,u}$ pour $1 \leq u \prec j$. Par exemple, sur $(4, 7)$, on peut déterminer @.

2c) Si la valeur de @ sur (i,j) est déterminée uniquement par 2b), alors on a

$$c_0^{(i-1,j)}.@ + \sum_{h=1}^{j-1} c_h^{(i-1,j)}.s_{i,j-h} = 0$$

où

$$C^{(i-1,j)}(x) = \sum_{h=0}^{j-1} c_h^{(i-1,j)} x^h \quad \text{et} \quad c_0^{(i-1,j)} = 1,$$

on a,

$$@ = -\sum_{h=1}^{j-1} c_h^{(i-1,j)}.s_{i,j-h} \tag{1.10}$$

Maintenant on modifie formellement le FIA. On a besoin deux autres tableaux, E et F, dans lesquels on stocke respectivement les valeurs de @ uniquement déterminés par 2b) et les polynômes $C^{(i-1,j)}(x)$ correspondants. On pose $s^{(r)}(x) = 1 + s_{r,1}x + s_{r,2}x^2 + ... + s_{r,N}x^N$

L'Algorithme itératif fondamental modifié

Etape 1) Vider les tableaux D, C, E et F, $1 \to j$, $1 \to r$, $1 \to C^{(j)}(x)$.

Etape 2) Calculer $d_{r,j} = [C^{(j)}(x)s^{(r)}(x)]_j$

Etape 3) SI $d_{r,j} = 0$, ALORS

a) Si $r = R$, OU SI $j = N$, et $s_{r+1,N}$ est @ ou #, ALORS ARRETER (d'après 2')) ;

b) SI $s_{r+1,j}$ est @, $r < R$, et $j < N$, vérifier s'il n'y a pas de $s_{r+1,u} \in D$ pour $1 \leq u < j$; lorsque c'est vrai, calculer $-\sum_{h=1}^{j-1} c_h^{(j)}.s_{r+1,j-h}$, cette valeur et $C^{(j)}(x)$ sont stockés respectivement dans E et dans F ; alors $C^{(j)}(x) \to C^{(j+1)}(x), j+1 \to j, 1 \to r$ et retour à l'étape 2) (d'après (2") et 2a) - 2c)) ;

c) SI $s_{r+1,j}$ est #, $r < R$, et $j < N$, alors $C^{(j)}(x) \to C^{(j+1)}(x), j+1 \to j, 1 \to r$ et retour à l'étape 2) (d'après 2')) ;

d) sinon $r + 1 \to r$, et retour à l'ètape 2).

Etape 4) Si $d_{r,j} \neq 0$, ALORS

a) SI il existe un $d_{r,u} \in D$, pour certain $1 \leq u < j$,
ALORS

$$C^{(j)}(x) - \frac{d_{r,j}}{d_{r,u}} C^{(u)}(x) x^{j-u} \to C^{(j)}(x)$$

et retour à l'étape 3).

b) sinon, $d_{r,j}$ est stockée dans D, $C^{(j)}(x)$ est stocké dans C, marquer un "x" à la ligne r et à la colonne j,$C^{(j)}(x) \to C^{(j+1)}(x), j+1 \to j, 1 \to r$ et retour à l'étape 2).

Maintenant, on va traiter un exemple pour voir le mécanisme de l'algorithme ci-dessus. Dans cet exemple, on va faire quelques modifications de la matrice A de l'exemple de la section précédente.

1.4 Exemple

On considère la matrice S' suivante à valeur dans le corps $\mathbb{F}_2 = \{0, 1\}$ où @ et # sont des inconnues.

$$S' = \begin{bmatrix} s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} \\ s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & @ & \# \\ s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & \# & \# & \# \\ s_{4,1} & s_{4,2} & s_{4,3} & @ & \# & \# & \# \\ s_{5,1} & s_{5,2} & @ & \# & \# & \# & \# \\ s_{6,1} & @ & \# & \# & \# & \# & \# \\ s_{7,1} & \# & \# & \# & \# & \# & \# \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & @ & \# \\ 0 & 1 & 1 & 1 & \# & \# & \# \\ 1 & 0 & 1 & @ & \# & \# & \# \\ 0 & 1 & @ & \# & \# & \# & \# \\ 1 & @ & \# & \# & \# & \# & \# \\ 0 & \# & \# & \# & \# & \# & \# \end{bmatrix}$$

On va chercher la valeur de @ en utilisant le MFIA.

Commençons par la première colonne, c'est-à-dire, pour $j = 1$. Pour $r = 1$ (première ligne), on a $C^{(0,1)}(x) = 1$, et $d_{1,1} = [C^{(0,1)}(x)a^{(1)}(x)]_1 = [1 \times (1 + x + x^3 + x^4)]_1 = 1 \neq 0$. Et comme il n'a y pas de $d_{1,u}$ pour $1 \leq u < 1$, on pose $C^{(1)}(x) := C^{(0,1)}(x) = 1$ dans C et on stocke $d_{1,1}$ dans le tableau D.

Ensuite, on se déplace à la deuxième colonne, et on prend $C^{(0,2)}(x) := C^{(1)}(x) = 1$

Pour $r = 1$ (première ligne), on a $d_{1,1} = [C^{(0,2)}(x)a^{(1)}(x)]_2 = [1 \times (1 + x + x^3 + x^4)]_2 = 0$, ainsi $C^{(1,2)}(x) := C^{(0,2)}(x) = 1$. On passe à la deuxième ligne :

Pour $r = 2$, $d_{2,2} = [C^{(1,2)}(x)a^{(2)}(x)]_2 = [1 \times (1 + x + x^2 + x^3)]_2 = 1 \neq 0$, et comme il n'a y pas de $d_{2,u}$ pour $1 \leq u < 2$, on pose $C^{(2)}(x) := C^{(1,2)}(x) = 1$ dans C et on stocke $d_{2,2}$ dans D.

Puis, on se dèplace à la troisième colonne, c'est-à-dire $j = 3$. On prend $C^{(0,3)}(x) := C^{(2)}(x) = 1$

Pour $r = 1$ (première ligne), on a $d_{1,3} = [C^{(0,3)}(x)a^{(1)}(x)]_3 = [1 \times (1 + x + x^3 + x^4)]_3 = 1 \neq 0$, et comme $d_{1,1} = 1 \neq 0$ existe dans D, avec $u = 1$, alors $C^{(0,3)}(x)$ est obtenu par

$$C^{(0,3)}(x) := C^{(0,3)}(x) - \frac{d_{1,3}}{d_{1,1}} C^{(1)} x^{3-1} = 1 - \frac{1}{1} x^2 = 1 + x^2$$

Maintenant, on a $C^{(0,3)}(x) = 1 + x^2$ et $d_{1,3} = [(1 + x^2) \times (1 + x + x^3 + x^4)]_3 = 2 = 0$ dans $\mathbb{F}_2$, alors $C^{(1,3)}(x) := C^{(0,3)}(x) = 1 + x^2$. Par suite, pour $r = 2$, $d_{2,3} = [C^{(1,3)}(x)a^{(2)}(x)]_3 = [(1 + x^2) \times (1 + x +$

$x^2 + x^3)]_3 = 2 = 0$ et ainsi $C^{(2,3)}(x) := C^{(0,3)}(x) = 1 + x^2$. Et on passe encore à la troisième ligne, et on a

$$d_{3,3} = [C^{(2,3)}(x)a^{(3)}(x)]_3 = [(1 + x^2) \times (1 + x^2 + x^3 + x^4)]_3 = 1 \neq 0,$$

Et comme il n'existe pas de $d_{3,u}$ pour $1 \leq u < 3$, alors on stocke $d_{3,3}$ dans D et on met $C^{(3)}(x) := C^{(2,3)}(x) = 1 + x^2$. dans C.

On passe à la colonne suivante c'est-à-dire $j = 4$, et en commençant par $C^{(0,4)}(x) := C^{(3)}(x) = 1 + x^2$, on a

$$d_{1,4} = [C^{(0,4)}(x)a^{(1)}(x)]_4 = [(1 + x^2) \times (1 + x + x^3 + x^4)]_4 = 1 \neq 0.$$

Comme $d_{1,1} = 1 \neq 0$ existe, avec $u = 1$, alors

$$C^{(0,4)}(x) := C^{(0,4)}(x) - \frac{d_{1,4}}{d_{1,1}} C^{(1)} x^{4-1} = 1 + x^2 - \frac{1}{1} \times 1 \times x^3 = 1 + x^2 + x^3.$$

On a $d_{1,4} = [C^{(0,4)}(x)a^{(1)}(x)]_4 = [(1 + x^2 + x^3) \times (1 + x + x^3 + x^4)]_4 = 2 = 0$. De même $d_{2,4} = d_{3,4} = 0$. Ainsi, $C^{(3,4)}(x) = C^{(2,4)}(x) = C^{(1,4)}(x) = C^{(0,4)}(x) = 1 + x^2 + x^3$. Alors, on obtient $C^{(4)} = C^{(3,4)}(x) = 1 + x^2 + x^3$. Puisque $d_{3,4} = 0$ et comme il n'existe aucun $d_{4,u} \neq 0$, pour $1 \leq u < 4$, donc on peut calculer la valeur de @ sur le point $(4, 4)$. On a

$$@ = -\sum_{h=1}^{3} c_h^{(3,4)} s_{4,4-h} = c_1^{(3,4)} s_{4,3} + c_2^{(3,4)} s_{4,2} + c_3^{(3,4)} s_{4,1} = 0 \times 1 + 1 \times 0 + 1 \times 1 = 1.$$

On met respectivement la valeur de @ obtenue et son polynôme correspondant dans les tableaux E et F.

On passe maintenant à la cinquième colonne et on prend $C^{(5)}(x) = C^{(4)}(x) = 1 + x^2 + x^3$. Pour $r = 1$, on a $d_{1,5} = [C^{(5)}(x)a^{(1)}(x)]_5 = [(1 + x^2 + x^3) \times (1 + x + x^3 + x^4 + x^5)]_5 = 2 = 0$. On passe à la ligne suivante, c'est-à-dire $r = 2$, $d_{2,5} = [C^{(5)}(x)a^{(2)}(x)]_5 = [(1 + x^2 + x^3) \times (1 + x + x^2 + x^3)]_5 = 2 = 0$. On a alors $C^{(1,5)}(x) = C^{(2,5)}(x) = C^{(5)}(x) = 1 + x^2 + x^3$.Comme il existe un # sur le point $(3, 5)$ donc on se déplace à la colonne suivante. On a $C^{(6)}(x) = C^{(5)}(x) = 1 + x^2 + x^3$ et $d_{1,6} = [C^{(6)}(x)a^{(1)}(x)]_5 = [(1 + x^2 + x^3) \times (1 + x + x^3 + x^4 + x^5 + x^7)]_6 = 2 = 0$. Puisque @ se trouve sur le point $(2, 6)$ et comme $d_{2,2} = 1 \neq 0 \in D$ existe alors on ne peut pas déterminer la valeur de @ sur ce point, donc il faut passer à la colonne suivante. On a $C^{(7)}(x) = C^{(6)}(x) = 1 + x^2 + x^3$. Pour $r = 1$, on a $d_{1,7} = [C^{(7)}(x)a^{(1)}(x)]_5 = [(1 + x^2 + x^3) \times (1 + x + x^3 + x^4 + x^5 + x^7)]_7 = 3 = 1 \neq 0$. Comme $d_{1,1} = 1 \neq 0$ alors

$$C^{(7)}(x) := C^{(7)}(x) - \frac{d_{1,7}}{d_{1,1}} C^{()} x^{7-1} = 1 + x^2 + x^3 - \frac{1}{1} \times 1 \times x^6 = 1 + x^2 + x^3 + x^6.$$

on a ainsi $d_{1,7} = [C^{(7)}(x)a^{(1)}(x)]_5 = [(1 + x^2 + x^3 + x^6) \times (1 + x + x^3 + x^4 + x^5 + x^7)]_7 = 2 = 0$. Finalement, puisque $j = 7 = N$ et $s_{2,7} = \#$ alors ARRETER.

Le tabeau D de la matrice de discrépence est alors comme suit

$$D = \begin{bmatrix} x_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & x_2 & 0 & 0 & 0 & @ & \# \\ 0 & 1 & x_3 & 0 & \# & \# & \# \\ 1 & 0 & 1 & @ & \# & \# & \# \\ 0 & 1 & @ & \# & \# & \# & \# \\ 1 & @ & \# & \# & \# & \# & \# \\ 0 & \# & \# & \# & \# & \# & \# \end{bmatrix}$$

où x_1, x_2 et x_3 représentent les discrépences non nulles sur les trois premières colonnes.

Le tableau C de la matrice polynômiale est de la forme

$$C = \begin{bmatrix} 1 & . & . & . & . & 1+x^2+x^3 & 1+x^2+x^3+x^6 \\ . & 1 & . & . & 1+x^2+x^3 & . & . \\ . & . & 1+x^2 & 1+x^2+x^3 & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \end{bmatrix}$$

Après avoir calculer la valeur de @, la matrice S' devient

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

Chapitre 2

Courbes algébriques

Dans toute la suite, on suppose que $\mathbb{F}$ est un corps algébriquement clos.

2.1 Variétés affines

2.1.1 Espace affine

2.1.1 Définition. On appelle espace affine de dimension n sur $\mathbb{F}$, noté $\mathbb{A}^n(\mathbb{F})$ ou tout simplement $\mathbb{A}^n$, l'ensemble des n-uplets des éléments de $\mathbb{F}$.

$$\mathbb{A}^n = \{(a_1, \ldots, a_n)/a_i \in \mathbb{F} \quad \text{pour tout} \quad i = 1, \ldots, n\}. \tag{2.1}$$

Un élément $(a_1, \ldots, a_n)$ de $\mathbb{A}^n$ s'appelle point et $a_1, \ldots, a_n$ sont les coordonnées.

2.1.2 Exemple. Si $n = 1$, $\mathbb{A}^1(\mathbb{F})$ est appelé ligne affine et si $n = 2$, $\mathbb{A}^2(\mathbb{F})$ est appelé plan affine.

2.1.3 Définition. Soient $\mathbb{F}[X_1, \ldots, X_n]$ l'anneau de polynômes à n variables sur $\mathbb{F}$ et $F \in \mathbb{F}[X_1, \ldots, X_n]$. Un point $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(\mathbb{F})$ est un zéro de F si $F(P) = F(a_1, \ldots, a_n) = 0$. Si F n'est pas constant, l'ensemble $V(F) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n/F(a_1, \ldots, a_n) = 0\}$. est appelé hypersurface défini par F.

2.1.4 Exemple. Une courbe affine plane est un hypersurface dans $\mathbb{A}^2(\mathbb{F})$. Si F est degré un, $V(F)$ s'appelle hyperplan dans $\mathbb{A}^n(\mathbb{F})$; pour $n = 2$, $V(F)$ est une ligne.

2.1.2 Ensembles algébriques

2.1.5 Définition. Un sous-ensemble $V \subseteq \mathbb{A}^n$ est un ensemble affine algébrique ou tout simplement ensemble algébrique s'il existe un ensemble $M \subseteq \mathbb{F}[X_1, \ldots, X_n]$ tel que

$$V = \{(a_1, \ldots, a_n) \in \mathbb{A}^n/F(a_1, \ldots, a_n) = 0 \quad \text{pour tout} \quad F \in M\}. \tag{2.2}$$

Etant donné $V \subseteq \mathbb{A}^n$ un ensemble algébrique, l'ensemble des polynômes

$$I(V) = \{F \in \mathbb{A}^n/F(a_1, \ldots, a_n) = 0 \quad \text{pour tout} \quad (a_1, \ldots, a_n) \in V\}.$$

s'appelle idéal de V. $I(V)$ est évidemment un idéal de $\mathbb{F}[X_1, \ldots, X_n]$ et il est engendré par un nombre fini de polynômes $F_1, \ldots, F_r \in \mathbb{F}[X_1, \ldots, X_n]$, c'est-à-dire

$$I(V) =< F_1, \ldots, F_r >$$

Alors on a

$$V = \{P \in \mathbb{A}^n / F_1(P) = \cdots = F_r(P) = 0\}.$$

2.1.6 Définition. Un sous-ensemble $V \subseteq \mathbb{A}^n$ est dit réductible si on peut écrire sous la forme $V = V_1 \bigcup V_2$ où V_1 et V_2 sont des sous-ensemble algébriques de $\mathbb{A}^n$, et $V_i \neq V$ pour $i = 1, 2$.

Sinon $V \subseteq \mathbb{A}^n$ est dit *irréductible* c'est-à-dire V ne peut pas écrire sous la forme $V = V_1 \bigcup V_2$ où V_1 et V_2 sont des sous-ensembles algébriques propres de V.

2.1.7 Exemple. Dans $\mathbb{A}^2$ avec coordonnées x et y, on considère l'idéal principal engendré par $x^2 - y^2$. C'est une union de deux lignes droites $y = x$ et $y = -x$. Chacune de ces lignes est un ensemble algébrique irréductible dans le plan $\mathbb{A}^2$.

2.1.8 Remarque. Un idéal I est dit premier si $F \in I$ ou $G \in I$ pour tout F, G tel que $FG \in I$.

2.1.9 Proposition. *Un sous-ensemble $V \subseteq \mathbb{A}^n$ est irréductible si est seulement si $I(V)$ est un idéal premier.*

Preuve. On suppose que $I(V)$ n'est pas premier. Si $F_1F_2 \in I(V)$, $F_i \notin I(V)$ pour $i = 1, 2$ Ainsi $V = (V \bigcap V(F_1)) \bigcup (V \bigcap V(F_2))$, et $V \bigcap V(F_i) \subsetneqq V$, Donc V est réductible.

Inversement, si $V = V_1 \bigcup V_2, V_i \subsetneqq V$ avec $i = 1, 2$ alors $I(V_i) \supsetneqq I(V)$; soient $F_i \in I(V_i), F_i \notin I(V)$ pour $i = 1, 2$. Donc $F_1F_2 \in I(V)$, ainsi $I(V)$ n'est pas premier. □

2.1.10 Théorème. *Soit V un ensemble algébrique sur $\mathbb{A}^n(\mathbb{F})$. Alors il existe des ensembles algébriques irréductibles uniques $V_1, \ldots, V_m$ tel que $V = V_1 \bigcup, \ldots, \bigcup, V_m$ et $V_i \nsubseteq V_j$ pour tout $i \neq j$.*

Preuve. Soit ζ l'ensemble des ensembles algébriques $V \subset \mathbb{A}^n(\mathbb{F})$ tel que V n'est pas une réunion finie des ensembles irréductibles

On veut savoir que ζ est soit vide. Si non, soit V un élément minimal de ζ. Comme $V \in \zeta$, V n'est pas irréductible, ainsi $V = V_1 \bigcup V_2, V_i \subsetneqq V$. Alors $V_i \notin \zeta$, donc $V_i = V_{i1} \bigcup \ldots \bigcup V_{im_i}$, avec V_{ij} irréductible. Mais $V = \bigcup_{i,j} V_{ij}$, donc c'est contradiction.

Ainsi tout ensemble algébrique V peut être écrit comme $V = V_1 \bigcup \ldots \bigcup V_m$, où V_i est irréductible pour $i = 1, \ldots, m$. Pour obtenir la deuxième condition, on considère tout simplement n'importe quel V_i tels que $V_i \subset V_j$ pour $i \neq j$. Pour montrer l'unicité, soit $V = W_1 \bigcup \ldots \bigcup W_m$ une autre décomposition. Alors $V_i = \bigcup_j (W_j \bigcap V_i)$, ainsi $V_i \subset W_{j(i)}$ pour chaque $j(i)$. D'une façon similaire,$W_{j(i)} \subset V_k$ implique $i = k$, donc $V_i = W_{j(i)}$. De même chaque W_j est égal à chaque $V_{i(j)}$ □

2.1.11 Définition. Pour un idéal premier I dans l'anneau $\mathbb{F}[X_1, \ldots, X_n]$, une variété affine est un ensemble $\mathcal{X}$ de zéros de I.

2.1.12 Exemple. Pour $n = 3$, soit I l'idéal dans $\mathbb{F}[X_1, X_2, X_3]$ engendré par le polynôme $X_1^2 + X_2^2 + X_3^2 - 1$. $\mathcal{X}$ est le sphère unité dans $\mathbb{A}^3$

2.1.3 Fonctions rationnelles

2.1.13 Définition. L'anneau de coordonnées d'une variété affine $\mathcal{X} \subseteq \mathbb{A}^n$ est l'anneau $\Gamma(\mathcal{X}) = \mathbb{F}[X_1, \ldots, X_n]/I(\mathcal{X})$.

2.1.14 Remarque. Comme I est un idéal premier, l'anneau $\Gamma(\mathcal{X})$ est un domaine intègre, c'est-à-dire, pour tout $f, g \in \Gamma(\mathcal{X})$ si $fg = 0$ alors $f = 0$ ou $g = 0$. Tout élément $f = F + I \in \Gamma(\mathcal{X})$ induit une fonction $f : \mathcal{X} \longrightarrow \mathbb{F}$ qui à P associé à $f(P) = F(P)$ pour $P \in \mathcal{X}$.

2.1.15 Définition. Le corps quotient de $\mathbb{F}[\mathcal{X}]$, noté par $\mathbb{F}(\mathcal{X})$, est appelé corps de fonctions rationnelles ou tout simplement corps de fonction de $\mathcal{X}$. Les éléments de $\mathbb{F}(\mathcal{X})$ sont appelés fonctions rationnelles sur $\mathcal{X}$.

Soient f un élément sur $\mathcal{X}$ et $P \in \mathcal{X}$. On dit que f est défini au point P si pour chaque $a, b \in \Gamma(\mathcal{X})$, $f = a/b$, et $b(P) \neq 0$. On a $\mathbb{F} \subseteq \mathbb{F}(\mathcal{X})$. La dimension de $\mathcal{X}$ est le degré de transcendance de $\mathbb{F}(\mathcal{X})/\mathbb{F}$.

2.1.16 Définition. Une courbe affine algébrique $\mathcal{X}$ est une variété affine de dimension 1.

2.1.17 Exemple. Si $\mathcal{X}$ est la parabole d'équation $y^2 = x$ sur le plan affine sur $\mathbb{F}$, alors $\mathbb{F}(\mathcal{X})$ est une extension algébrique de $\mathbb{F}(x)$ de degré 2 du corps $\mathbb{F}(\mathcal{X})$ par un élément y. L'anneau de coordonnées $\mathbb{F}[\mathcal{X}]$ consiste de tous les expressions de la forme $A + By$, où A et B sont dans $\mathbb{F}[\mathcal{X}]$ et y satisfait $y^2 = x$.

2.1.18 Définition. Pour un point $P \in \mathcal{X}$, soit

$$O_P(\mathcal{X}) = \{f \in \mathbb{F}(\mathcal{X})/f = g/h \quad \text{avec g, h} \in \mathbb{F}[X_1, \ldots, X_n]/I \quad \text{et} \quad h(P) \neq 0\}$$

C'est un anneau local avec corps quotient $\mathbb{F}(\mathcal{X})$. Il est un sous anneau de $\mathbb{F}(\mathcal{X})$ contenant $\Gamma(\mathcal{X})$, c'est-à-dire $\mathbb{F} \subset \Gamma(\mathcal{X}) \subset O_P(\mathcal{X}) \subset \mathbb{F}(\mathcal{X})$.

Son unique idéal maximal est

$$M_P(\mathcal{X}) = \{f \in \mathbb{F}(\mathcal{X})/f = g/h \quad \text{avec} \quad g, h \in \mathbb{F}[X_1, \ldots, X_n]/I, \quad h(P) \neq 0 \quad \text{et} \quad g(P) = 0\}$$

$O_P(\mathcal{X})$ est appelé l'anneau local de $\mathcal{X}$ et P. Pour $f = g/h \in O_P(\mathcal{X})$ avec $h(P) \neq 0$, la valeur de f en P est défini par

$$f(P) = g(P)/h(P).$$

2.1.19 Définition. L'ensemble des points $P \in \mathcal{X}$ où une fonction rationnelle f n'est pas définie en P est appelé *ensemble de pôles* de f.

2.1.20 Proposition. *(1) L'ensemble de pôles d'une fonction rationnelle sur $\mathcal{X}$ est un sous-ensemble algébrique de X.*

(2) $\Gamma(\mathcal{X}) = \bigcap_{P \in \mathcal{X}} O_P(\mathcal{X})$.

Preuve. On suppose que $\mathcal{X} \subset \mathbb{A}^n$. Soit $G \in \mathbb{F}[X_1, \ldots, X_n]$, on note par $\overline{G}$ le résidu de G dans $\Gamma(\mathcal{X})$. Soient $f \in \mathbb{F}(\mathcal{X})$ et $J_f = \{G \in \mathbb{F}[X_1, \ldots, X_n]/\overline{G} \in \Gamma(\mathcal{X}).\}$ J_f est un idéal dans $\mathbb{F}[X_1, \ldots, X_n]$ contenant $I(\mathcal{X})$, et les points de $\mathcal{X}(J_f)$ sont exactement ses points où f n'est pas définie. Ce qui prouve (1). Si $f \in \bigcap_{P \in \mathcal{X}} O_P(\mathcal{X})$ et $\mathcal{X}(J_f) = \varnothing$, alors $1 \in J_f$, c'est-à-dire $\overline{1} f = f \in \Gamma(\mathcal{X})$. D'où (2). □

2.2 Variétés projectives

2.2.21 Définition. Sur l'ensemble $\mathbb{A}^{n+1}\backslash\{0,\ldots,0\}$, on définit la relation d'équivalence notée par $\sim$ suivante.

$(a_0,\ldots,a_n) \sim (b_0,\ldots,b_n)$ ssi il existe $0 \neq \lambda \in \mathbb{F}$ tel que $b_i = \lambda a_i$, pour $0 \leq i \leq n$.

La classe d'équivalence de $(a_0,\ldots,a_n)$ relative à $\sim$ est notée par $(a_0 : \ldots : a_n)$

L'espace projectif de dimension n noté $\mathbb{P}^n = \mathbb{P}^n(\mathbb{F})$ est l'ensemble de toutes les classes d'équivalence, c'est-à-dire,

$$\mathbb{P}^n = \{(a_0 : \ldots : a_n)/a_i \in \mathbb{F}, \text{non tous nuls.}\}$$

Pour $n = 1$, $\mathbb{P}^1$ est appelé *ligne projective* et pour $n = 2$, $\mathbb{P}^2$ est appelé *plan projectif.* Un élément $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$ est appelé *point* et $a_0,\ldots,a_n$ sont appelés *coordonnés homogènes* de P.

Un *monôme* de degré d est un polynôme $G \in \mathbb{F}[X_1,\ldots,X_n]$ de la forme

$$G = a\prod_{i=0}^{n} X_i^{d_i} \text{ avec } 0 \neq a \in \mathbb{F} \text{ et } \sum_{i=1}^{n} d_i = d.$$

Un polynôme F est un *polynôme homogène* si la somme de monômes est de même degré. Un idéal $I \subseteq \mathbb{F}[X_1,\ldots,X_n]$ engendré par des polynômes homogènes est appelé *idéal homogène.*

2.2.22 Définition. Soit $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$ et $F \in \mathbb{F}[X_1,\ldots,X_n]$ un polynôme homogène. $F(P) = 0$ si $F(a_0,\ldots,a_n) = 0$.

2.2.23 Remarque. Comme $F(\lambda a_0,\ldots,\lambda a_n) = \lambda^d F(a_0,\ldots,a_n)$, où $d = degF$, on a

$$F(a_0,\ldots,a_n) = 0 \Leftrightarrow F(\lambda a_0,\ldots,\lambda a_n) = 0.$$

Un sous-ensemble $V \in \mathbb{P}^n$ est un *ensemble algébrique projectif* s'il existe un ensemble de polynômes homogènes $M \subseteq \mathbb{F}[X_1,\ldots,X_n]$ tel que

$$V = \{P \in \mathbb{P}^n/F(P) = 0 \quad \text{pour tour} \quad F \in M\}$$

L'idéal $I(V) \subseteq \mathbb{F}[X_1,\ldots,X_n]$ tel que

$I(V) = \{M \subseteq \mathbb{F}[X_1,\ldots,X_n]/F$ ensemble des polynômes homogènes et F(P) = 0 pour tout P $\in V\}$.

est appelé idéal de V. C'est un idéal homogène.

2.2.24 Définition. Un ensemble algébrique projectif $V \in \mathbb{P}^n$ est irréductible si on ne peut pas écrire sous la forme $V = V_1 \cup V_2$ où V_1 et V_2 sont des sous-ensembles algébriques projectifs propres de V.

Un ensemble algébrique projectif $V \in \mathbb{P}^n$ est irréductible si est seulement si $I(V)$ est un idéal premier homogène dans $\mathbb{F}[X_1,\ldots,X_n]$

2.2.25 Définition. Une *variété projective* est un ensemble projectif irréductible.

Soit $\varnothing \neq V \subset \mathbb{P}^n$ une variété projective, on définit son anneau de coordonnée homogène par $\mathbb{F}[X_1, \ldots, X_n]/I(V)$. C'est un domaine intègre contenant $\mathbb{F}$. Un élément $f \in \mathbb{F}[X_1, \ldots, X_n]/I(V)$ est appelé une *forme* de degré d si $f = F + I(V)$ pour un certain polynôme homogène $F \in \mathbb{F}[X_1, \ldots, X_n]$ de degré d.

2.2.26 Définition. Soient V une affine ou une variété projective et P un point de V. On dit qu'une fonction rationnelle ϕ est régulière au point P si $\phi = f/g$, où f et g sont respectivement des polynômes homogènes de même degré, tel que $f(P) \neq 0$.

2.2.27 Définition. Le *corps de fonction* de V est défini par

$$\mathbb{F}(V) = \{\frac{g}{h} | g, h \in \mathbb{F}[X_1, \ldots, X_n]/I(V) \text{sont ds formes de même degré et } h \neq 0.\}$$

$\mathbb{F}(V)$ est un sous-corps du corps de quotient de $\mathbb{F}[X_1, \ldots, X_n]/I(V)$.
La dimension de V est le degré de transcendance de $\mathbb{F}(V)$ sur $\mathbb{F}$

Soit $P = (a_0 : \ldots : a_n) \in V$ et $f \in \mathbb{F}(V)$. On écrit $f = g/h$ où $g = G + I(V), h = H + I(V) \in \Gamma_h(V)$ et G et H sont des polynômes homogènes de degré d.

Comme

$$\frac{G(\lambda a_0, \ldots, \lambda a_n)}{H(\lambda a_0, \ldots, \lambda a_n)} = \frac{\lambda^d G(a_0 \ldots, a_n)}{\lambda^d H(a_0 \ldots, a_n)} = \frac{G(a_0 \ldots, a_n)}{H(a_0 \ldots, a_n)}$$

On peut poser $f(P) = G(a_0 \ldots, a_n)/H(a_0 \ldots, a_n) \in \mathbb{F}$ si $H(P) \neq 0$. Alors on dit que f est définie en P et on écrit $f(P)$ la valeur de f en P.

2.2.28 Définition. L'anneau local O_P (souvent noté par $O_P(V)$) pour le point P sur une variété V est l'ensemble de fonctions rationnelles qui sont régulières au point P, c'est-à-dire

$$O_P(V) = \{f \in \mathbb{F} \quad \text{est définie en P}\} \subseteq \mathbb{F}(V)$$

avec idéal maximal

$$M_P(V) = \{f \in O_P(V)/f(P) = 0\}.$$

2.2.29 Exemple. On considère la variété V défini par $XZ - Y^2 = 0$ sur $\mathbb{A}^2$ de coordonnées $(x : y : z)$. C'est le parabole de l'exemple précédent, avec un point à l'infini $Q(1 : 0 : 0)$. La fonction x/y est égale à y/z pour la courbe, ainsi elle est régulière au point $P = (0 : 0 : 1)$. La fonction $(2xy + z^2)(y^2 + z^2)$ est régulière au point P. En remplaçant y^2 par xz, on voit que la fonction est égale à $(2x + z)(x + z)$, et est donc régulière au point Q.

2.3 Courbes algébriques.

2.3.30 Définition. On appelle courbe algébrique projective (affine) $\mathcal{X}$, une variété projective (ou affine) de dimension 1. Cela signifie que le corps de fonctions rationnelles $\mathbb{F}(\mathcal{X})$ sur $\mathcal{X}$ est un corps de fonction algébrique d'une variable.

2.3.31 Définition. Un point $P \in \mathcal{X}$ est dit non singulier (ou simple) si l'anneau local $O_P(\mathcal{X})$ est un anneau de valuation discrète (c'est-à-dire $O_P(\mathcal{X})$ est un domaine d'idéaux principaux avec un seul idéal maximal $\neq \{0\}$.) Il existe un nombre fini seulement de point singulier sur une courbe. Une courbe $\mathcal{X}$ est appelé *singulière (ou simple)* si tout point $P \in \mathcal{X}$ est non singulier.

2.3.32 Définition. Une courbe affine plane est une courbe affine $\mathcal{X} \subseteq \mathbb{A}^2$. Son idéal $I(\mathcal{X}) \subseteq \mathbb{F}[X_0, X_1]$ est engendré par un polynôme irréductible $G \in \mathbb{F}[X_0, X_1]$ (qui est unique à un facteur constant près). Inversement, étant donné un polynôme irréductible $G \in \mathbb{F}[X_0, X_1]$, l'ensemble

$$\mathcal{X} = \{P \in \mathbb{A}^2 / G(P) = 0\}$$

est une courbe affine plane et G engendre l'idéal correspondant $I(\mathcal{X})$.

2.3.33 Définition. On considère une courbe définit par $F(X, Y) = 0$ dans $\mathbb{A}^2$. Un point $P = (a, b)$ de ce courbe est dit simple ou non singulier si est seulement si $F_X(P) \neq 0$ ou $F_Y(P) \neq 0$ ou tous les deux, où F_X et F_Y sont les dérivées partielles de $F(X, Y)$ par rapport à X et Y. Dans ce cas, l'équation de la tangente à la courbe au point P est définit par

$$F_X(P)(X - a) + F_Y(P)(Y - b) = 0.$$

Une courbe est dit non singulière, régulière si tous les points sont non singuliers. Une courbe plane projective est définie de la même façon comme suit. Soient $F(X, Y, Z) = 0$ une courbe plane projective et P un point appartenant à cette courbe. Si au moins une des dérivées F_X, F_Y ou F_Z n'est pas nulle en P, alors P est appelé point simple ou point singulier de la courbe. L'équation de la tangente au point P est

$$F_X(a, b, c)X + F_Y(a, b, c)Y + F_Z(a, b, c)Z = 0$$

2.3.34 Définition. L'idéal d'une courbe projective plane $V \subseteq \mathbb{A}^2$ est engendrée par un polynôme homogène $H \in \mathbb{F}[X_0, X_1, X_2]$. Un point $P \in V$ est non singulier ssi $H_{X_i}(P) \neq 0$ pour au moins un $i \in \{0, 1, 2\}$.

2.3.35 Exemple. La *courbe de Fermat* F_m est une courbe projective plane définie par

$$X_0^m + X_1^m + X_2^m = 0. \tag{2.3}$$

Les dérivées partielles de $X_0^m + X_1^m + X_2^m$ par rapport à X_0, X_1 et X_2 sont données respectivement par mX_0^{m-1}, mX_1^{m-1} et mX_2^{m-1}.

2.4 Courbe hermitienne.

2.4.36 Définition. Soit $H = \mathbb{F}_{q^2}(x, y)$ un corps de fonction défini sur $\mathbb{F}_{q^2}$ par

$$u^{q+1} + v^{q+1} = 1. \tag{2.4}$$

H est appelé corps de fonction hermitienne sur $\mathbb{F}_{q^2}$. Son équation homogène est de la forme

$$u^{q+1} + v^{q+1} + w^{q+1} = 0 \tag{2.5}$$

c'est la courbe de Fermat F_m sur $\mathbb{F}_{q^2}$ définie par (2.3) avec $m = q + 1$.

Maintenant, on va construire une autre formulation de cette équation homogène. Soit $u \in \mathbb{F}_{q^2}$. Puisque $\mathbb{F}_{q^2}$ est une extension quadratique de $\mathbb{F}_q$ donc $\overline{u} = u^q$ est le conjugué de u. Par conséquent l'équation (2.5) est équivante à

$$u\overline{u} + v\overline{v} + w\overline{w} = 0 \tag{2.6}$$

Ainsi, elle a $q+1$ points à l'infini. On va donner une transformation telle que la nouvelle équation de la courbe hermitienne a cette propriété.

Soit b un élément de $\mathbb{F}_{q^2}$ tel que $b^{q+1} = -1$. Il y a exactement $q+1$ de ces derniers. Et si on considère le point $P = (1 : b : 0)$. Alors P est un point de la courbe hermitienne. L'équation de la tangente au point P est $u + b^q v = 0$. En multipliant par b, l'équation devient $v = bu$ et en substituant $v = bu$ dans l'équation homogène de la courbe précédente, elle devient $w^{p+1} = 0$. Ainsi P est le seul point d'interséction de la courbe hermitiènne et de la tangente à P. De nouvelles coordonnées homogènes sont choisies tels que cette droite tangente devient la droite à l'infinie. On va poser $x_1 = w$, $y_1 = u$ et $z_1 = bu - v$. Donc la courbe a pour équation homogène

$$x_1^{q+1} = b^q y_1^{q+1} z_1 + b y_1^q z_1 - z_1^{q+1} \tag{2.7}$$

dans les coordonnées x_1, y_1 et z_1. On choisit un élément $a \in \mathbb{F}_{q^2}$ tel que $a^q + a = -1$. Il y a q valeurs de a. Maintenant, on pose $x = x_1$,$y = by_1 + az_1$ et $z = z_1$. L'équation homogène de la courbe devient alors

$$x^{q+1} = y^q z + y z^q. \tag{2.8}$$

On obtient la définition suivante.

2.4.37 Définition. L'équation affine de la courbe Hermitiènne, notée par $\mathcal{X}$, sur F_{q^2} est définie par

$$x^{q+1} = y^q + y. \tag{2.9}$$

Le genre g de ce courbe hermitienne est donné par $g = q(q-1)/2$. Cette courbe est maximale c'est-à-dire le nombre des points rationnels atteint la borne de Hasse-Weil. Elle possède alors q^3 points rationnels $P_1, \ldots, P_{q^3}$ sur $\mathbb{F}_{q^2}$ et un point rationnel à l'infini P_∞. cf.[Sti89, VI.4.4].

Chapitre 3

Principe du décodage

3.1 Codes pour les courbes algébriques.

Soit $\mathcal{X}$ une courbe projective non singulière de genre g sur $\mathbb{F}_q$, où $\mathbb{F}_q$ est un corps fini à q éléments. Soit $D = P_1 + ... + P_n$, où $P_1, ..., P_n$ sont des points rationnels de $\mathcal{X}$. Soit $G = m.Q$ un autre diviseur tel que $Q \neq P_i$ pour $1 \leq i \leq n$ et

$$2g - 2 < deg(G) < n. \tag{3.1}$$

On rappelle que $\mathcal{L}(G)$ est l'espace vectoriel défini par $\mathcal{L}(G) := \{f \in \mathbb{F}(\mathcal{X}) : (f) + G \geq 0\} \bigcup \{0\}$ où $\mathbb{F}(\mathcal{X})$ est le corps de fonctions rationnelles de $\mathcal{X}$.

3.1.1 Définition. Le code linéaire $C(D, G)$ de longueur n sur $\mathbb{F}_q$ est l'image de l'application linéaire $\alpha : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$ définie par

$$\alpha(f) := (f(P_1), f(P_2), \ldots, f(P_n))$$

3.1.2 Théorème. *Le code $C(D, G)$ est de dimension $k = deg(G) - g + 1$ et sa distance minimale $d \geq n - deg(G)$.*

Preuve.

(i) Si f appartient au noyau de α, alors $f \in \mathcal{L}(G - D)$ et puisque $2g - 2 < deg(G) < n$ alors $G - D < 0$, donc $\mathcal{L}(G - D) = \{0\}$, ce qui implique $f = 0$. D'après l'inéquation $2g - 2 < deg(G)$, on a $l(D) = deg(G) - g + 1$. D'où le résultat.

(ii) Si le poids de $\alpha(f)$ est d alors il existe $n - d$ points P_i, c'est-à-dire $P_{i_1}, P_{i_2}, \ldots, P_{i_{n-d}}$ tel que $f(P_i) = 0$. Par conséquant $f \in \mathcal{L}(G - E)$ où $E = P_{i_1} + P_{i_2} + \cdots + P_{i_{n-d}}$. Ainsi $deg(G) - n - d \geq 0$.

□

On considère maintenant une autre classe du code géométrique algébrique appelé "code géométrique de Gopppa," noté par $C_\Omega(D, G)$, où D et G sont des diviseurs définis précédemment.

3.1.3 Définition. Le code linéaire $C_\Omega(D, G)$ de longueur n sur F_q est l'image de l'application linéaire $\alpha^* = \Omega(D - G) \longrightarrow F_q^n$ définie par

$$\alpha^*(w) = (Res_{P_1}(w), Res_{P_2}(w), ..., Res_{P_n}(w))$$

où $Res_{P_i}(w)$ est le résidu de w au point i, pour $1 \leq i \leq n$.

3.1.4 Théorème. *Le code $C_\Omega(D,G)$ est de dimension $k^* = n - deg(G) + g - 1$ et sa distance minimale est $d^* \geq deg(G) - 2g + 2$.*

Preuve. La preuve résulte du théorème précédent et ses assertions sont les conséquence du théorème de Riemann-Roch.(Pour plus d'information sur le théorème Riemann-Roch, voir Annexe.)
□

3.1.5 Théorème. *Les codes $C(D,G)$ et $C_\Omega(D,G)$ sont des codes duaux.*

Preuve. D'après le théorème (3.1.2) et le théorème (3.1.4), on sait que $k + k^* = n$. Ainsi, il suffit de prendre un mot pour chaque code et montrer que le produit scalaire de ces deux mots est nul. Soient $f \in \mathcal{L}(G)$ et $\mu \in \Omega(G - D)$. Par les définitions (3.1.1) et (3.1.3) le différentiel $f\mu$ n'a aucun pôle à l'exception des pôles d'ordre 1 sur les points $P_1, P_2, \ldots, P_n$. Donc le résidu de $f\mu$ est égal à $f(P_i)Res_{P_i}(\mu)$. Donc, on sait que la somme des résidus de $f\mu$ est égale à zéro (cf Annexe théorème (4.5.28)). Par suite, on a

$$0 = \sum_{i=1}^{n} f(P_i)Res_{P_i}(\mu) =< \alpha(f), \alpha^*(\mu) > .$$

□

3.2 Procédure de décodage

Soit $\mathcal{X}$ une courbe projective non singulière de genre g sur $\mathbb{F}_q$, où $\mathbb{F}_q$ est un corps fini à q éléments. Soit D le diviseur $P_1 + ... + P_n$, où $P_1, ..., P_n$ sont des points rationnels de $\mathcal{X}$. Soit $G = m.Q$ tel que $Q \neq P_i$ pour $1 \leq i \leq n$

Les paramètres du code sont

$$d^* = m - 2g + 2$$

$$k = m - g + 1$$

$$t = [(d^* - 1)/2] = [(m + 2)/2] - g$$

et on suppose que $t > 0$ ou $m > 2g$.

Pour commencer cette section, on rappelle que un entier o_i est un non gap pour Q si $\mathcal{L}(o_iQ) \neq \mathcal{L}((o_i - 1)Q)$, alors il existe une fonction ϕ_{o_i} d'ordre o_i au point Q. (Pour plus d'information, voir l'annexe). Ces non gaps satisfont le lemme suivant.

3.2.6 Lemme. $i_0 = 0$,

$$0 < i_1 < i_2 < \cdots < i_{g-1} < 2g$$

$$i_j = g + j \text{ pour } j = g, g + 1, \ldots, m - g$$

Preuve. (cf. Annexe)

Soient $f_1, f_2, \ldots, f_{m-g+1}$ avec $f_i = \phi_{o_i}$ pour $i = 1, 2, \ldots, m - g + 1$, la base de l'espace vectoriel $\mathcal{L}(G)$. Soient $u = (u_1, u_2, \ldots, u_n)$ un mot reçu, $e = (e_1, e_2, \ldots, e_n)$ un vecteur erroné et soit $c = (c_1, c_2, \ldots, c_n)$ le mot de code tel que $u = c + e = (u_1 + e_1, \ldots, u_n + e_n)$. Alors, on va définir les syndromes comme suit :

3.2.7 Définition. Muni du produit scalaire usuel, pour $i = 1, 2, \ldots, n$, les syndromes s_i sont définis par

$$s_i =< u, \alpha^* \phi_i >= \sum_{j=1}^{n} u_j \phi_i(P_j) \tag{3.2}$$

Evidemment, on a $s_i = \sum_{\mu=1}^{\nu} e_{k_\nu} \phi_i(P_{k_\mu})$ où ν est le nombre des erreurs. En effet,

$$\begin{aligned} s_i &= \sum_{j=1}^{n} u_j \phi_i(P_j) \\ &= \sum_{j=1}^{n} (c_j + e_j) \phi_i(P_j) \\ &= \sum_{j=1}^{n} c_j \phi_i(P_j) + \sum_{j=1}^{n} e_j \phi_i(P_j) \\ &= \sum_{\mu=1}^{\nu} e_{k_\mu} \phi_i(P_{k_\mu}) \end{aligned}$$

Maintenant, on va définir les syndromes à deux dimensionnels.
Les syndromes à deux dimensionnels sont définis par

$$S_{i,j} = \sum_{\mu=1}^{\nu} e_{k_\mu} \phi_{o_{i-1}} \phi_{o_{j-1}}(P_{k_\mu}) \tag{3.3}$$

On sait que si $o_{i-1} + o_{j-1} = o_p \leq m$, alors $\phi_{o_{i-1}} \phi_{o_{j-1}} \in \mathcal{L}(o_p Q) \subseteq \mathcal{L}(G) = \mathcal{L}(mQ)$.
En effet, $v_Q(\phi_{o_p}) = o_p \geq -o_p$ car $o_p \geq 0$. Comme $o_p \leq m$ alors $-o_p Q \geq -mQ$. Par conséquent $\mathcal{L}(o_p Q) \subseteq \mathcal{L}(mQ)$. De même, puisque $v_Q(\phi_{o_{i-1}}.\phi_{o_{j-1}}) = o_{i-1} + o_{j-1} \geq -(o_{i-1} + o_{j-1}) = -o_p$, donc $\phi_{o_{i-1}}.\phi_{o_{j-1}} \in L(o_p Q)$

On va démontrer que $S_{i,j}$ est une combinaison linéaire de $s_{o_1}, s_{o_2}, \ldots, s_{o_p}$ et le coefficient de s_{o_p} est non nul. Soient $\mathcal{L}(G) =< \phi_0, \phi_1, \ldots, \phi_{m-g} >$ et $\mathcal{L}(o_p Q) =< \phi_{o_0}, \phi_{o_1}, \ldots, \phi_{o_p} >$. On obtient $\dim \mathcal{L}(G) = m - g + 1$ et $\dim \mathcal{L}(o_p Q) = p + 1$.
Soit $\phi_{o_{i-1}}.\phi_{o_{j-1}} = \sum_{l=0}^{p} \lambda_{o_l} \phi_{o_l}$, tel que $\lambda_{o_0} = \lambda_{o_1} = \cdots = \lambda_{o_{p-1}} = 0$, On a

$$\begin{aligned} S_{i,j} &= \sum_{\mu=1}^{\nu} e_{k_\nu} (\sum_{l=0}^{o_p} \lambda_{o_l} \phi_{o_l})(P_{k_\mu}) \\ &= \sum_{\mu=1}^{\nu} \sum_{l=0}^{p} \lambda_{o_l} e_{k_\nu} \phi_{o_l}(P_{k_\mu}) \\ &= \sum_{l=0}^{p} \lambda_{o_l} \sum_{\mu=1}^{\nu} e_{k_\nu} \phi_{o_l}(P_{k_\mu}) \\ &= \sum_{l=0}^{p} \lambda_{o_l} s_{o_l} = \lambda_p s_{o_p} \end{aligned}$$

Par conséquent $S_{i,j}$ est une combinaison linéaire de $s_{o_1}, s_{o_2}, \ldots, s_{o_p}$.

Donc, d'une part tous les $S_{i,j}$ sont connus pour $o_{i-1} + o_{j-1} = o_p \leq m$..

D'autre part, $S_{i,j}$ peut ne pas être égal à $s_{o_{i-1}+o_{j-1}}$, car il se peut que $\phi_{o_i} \phi_{o_j} \neq \phi_{o_i+o_j}$. Mais il y a une relation linéaire entre eux, c'est-à-dire, $S_{i,j}$ peut être déterminé par s_k pour $0 \leq k \leq o_{i-1} + o_{j-1}$.

Dans ce cas, on dit que $s_{o_{i-1}+o_{j-1}}$ et $S_{i,j}$ sont *consistants* et $S_{i,j}$ est le *terme consistant* de $s_{o_{i-1}+o_{j-1}}$. Comme notation, on utilise $s'_{o_{i-1}+o_{j-1}}$ pour exprimer les termes consistants de $s_{o_{i-1}+o_{j-1}}$. Dans le prochain chapitre, on aura un exemple. Ci-après, "la valeur de $s_{o_{i-1}+o_{j-1}}$" signifie "la valeur de $s_{o_{i-1}+o_{j-1}}$ et les valeurs possibles de ses termes consistants" ; "le nombre de $s_{o_{i-1}+o_{j-1}}$ dans la matrice S^*" signifie " son nombre possible et les nombres possibles de ses termes consistants dans S^*" ; " substituer @ de $s_{o_{i-1}+o_{j-1}}$" signifie " substituer @ de lui et ses termes consistants possibles " ; "le nombre de $s_{o_{i-1}+o_{j-1}}$ avec la même valeur " signifie " sa valeur possible et les valeurs de ses termes consistants possibles" ; et ainsi de suite.

On construit une matrice $S = (S_{i,j})_{(m-g+1)\times(m-g+1)}$, telle que :

$$S = \begin{bmatrix} S_{1,1} & S_{1,2} & S_{1,3} & \dots & S_{1,m-g} & S_{1,m-g+1} \\ S_{2,1} & S_{2,2} & S_{2,3} & \dots & S_{2,m-g} & S_{2,m-g+1} \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ S_{2,m-g} & S_{m-g,2} & S_{m-g,3} & \dots & S_{m-g,m-g} & S_{m-g,m-g+1} \\ S_{2,m-g+1} & S_{m-g+1,2} & S_{m-g+1,3} & \dots & S_{m-g+1,m-g} & S_{m-g+1,m-g+1} \end{bmatrix}$$

En supposant que les valeurs de $S_{i,j}$ dans S sont tous connus, on a le théorème suivant.

3.2.8 Théorème. *Si la colonne j de S est une combinaison linéaire partielle de ses colonnes précédentes avec les $[(m+1)/2]$ premières composantes et si a_i sont les coefficients pour $1 \leq i \leq j-1$, alors la colonne j est linéairement dépendante avec ses colonnes précédentes et les points rationnels erronés sont les racines de*

$$f_j - \sum_{i=1}^{j-1} a_i . f_i = 0 \tag{3.4}$$

Preuve : cf.[SVL90]Théorème 1.

Malheureusement, les valeurs de $s_{m+1}, \dots, s_{m+g}$ sont inconnues, c'est-à-dire les valeurs de $S_{i,j}$ pour $o_{i-1} + o_{j-1} = m+1, m+2, \dots, m+g$ sont inconnues, de la matrice S,(3.4) peut ne pas être trouvé. Ainsi, la clé du problème dans le décodage des codes géométriques algébriques est de *trouver les valeurs réelles de* s_i pour $i = m+1, m+2, \dots, m+g$ et l'équation (3.4) précédente. On peut résoudre ces problémes en utilisant le MFIA développé dans le chapitre 1. Afin de trouver les valeurs de s_i pour $i = m+1, m+2, \dots, m+g$, notre procédure de décodage est de les chercher successivement, c'est-à-dire, on cherche en premier temps s_{m+1}, puis s_{m+2} et ainsi de suite jusqu'à trouver s_{m+g}.

Dans la suite, on décrit comment trouver s_{m+w} si on connait s_i pour $i = 0, o_1, o_2, \dots, m, \dots, m+w-1$, où $1 \leq w \leq g$.

On suppose que $s_{m+1}, \dots, s_{m+w-1}$ sont trouvés et s_{m+w} est toujours inconnu, où $1 \leq w \leq g$. Maintenant, on veut trouver la valeur de s_{m+w}. Soit S^* une deuxième écriture de S, où $S_{i,j}(o_{i-1} + o_{j-1} = p)$ est remplacé par s_p pour $p \leq m+w-1$, et $S_{u,v}(o_{u-1} + o_{v-1} = m+w)$, est remplacé par @ c'est-à-dire, $s_{m+w} =$ @ et on remplace $S_{k,h}(o_{k-1} + o_{h-1} > m+w)$, par #, c'est-à-dire, $s_q =$ # pour

$q > m + w$. Évidement, S^* répond aux exigences de S' dans le chapitre précédent. On utilisera le MFIA pour trouver la valeur de @, c'est-à-dire, la valeur de s_{m+w}.

Avant de décrire comment trouver la valeur de s_{m+w}, on calcule premièrement, le nombre de @, c'est-à-dire, le nombre de s_{m+w} dans S^*.
On a besoin du lemme suivant :

3.2.9 Lemme. *Si A_w le nombre des nongaps dans $[1, w-1]$ pour $1 \leq w \leq g$, alors*

$$A_w \leq [(m-1)/2]. \tag{3.5}$$

Preuve. Pour $w = 1$ c'est évident. Pour $2 \leq w \leq g$, on considère deux cas :

Cas 1) Si w est un gap, alors on considère deux sous-cas :

- **a)** w est impair. Si $s \in [1, w-1]$, alors $w - s \in [1, w-1]$ et $s \neq w - s, s$ et $w - s$ ne sont pas les deux nongaps. Ainsi, (3.5) est vraie.
- **b)** w est pair. $w/2 \in [1, w-1]$ peut ne pas être un nongap. Si $s \in [1, w-1]$ et $s \neq w/2$ alors $w-s \in [1, w-1]$, $s \neq w-s, s$ et $w-s$ sont les deux des nongaps. Ainsi, $A_w \leq [(m-2)/2]$ et (3.5) est vraie.

Cas 2) si w est un nongap, alors d'après lemme (3.2.6) et comme $w/2 \in [1, w-1]$, on peut supposer que $w, w+1, \ldots, w+p-1$ sont des nongaps et $w+p$ est un gap, où $1 \leq p < g$. Et d'après la preuve précédente, on a $A_{w+p} \leq [(w+p-1)/2]$. D'autre part, $A_{w+p} = A_w + p$, on a $A_w + p \leq [(w+p-1)/2]$ et (3.5) est vraie.

□

Le nombre de @ est donné par le théorème suivant

3.2.10 Théorème. *Le nombre de @ dans S^* est au moins $m-2g$, c'est-à-dire, au moins d^*-2.*

Preuve. Pour chaque $1 \leq j \leq m-g+1$, de (3.2) il existe un @ dans la colonne j, si est seulement si

$$m + w - o_{j-1} \in \{o_0, o_1, \ldots, o_{m-g}\}. \tag{3.6}$$

D'une manière équivalente, il n'existe aucun @ à la colonne j, si est seulement si

$$m + w - o_{j-1} \notin \{o_0, o_1, \ldots, o_{m-g}\}. \tag{3.7}$$

On va calculer le nombre de j, qui satisfait (3.7). On considère les deux cas suivants :

- **a)** Si $m + w - o_{j-1} > m$, c'est-à-dire, $o_{j-1} < w$, alors (3.7) est satisfait. D'après le lemme (3.2.9), le nombre de chaque j est $1 + A_w$ ($j = 1$ satisfait cette condition).
- **b)** Si $m + w - o_{j-1} \leq m$, c'est-à-dire,$o_{j-1} \geq w$, alors le nombre de $m + w - o_{j-1}$ étant gaps is B_w, qui le nombre de gaps dans $[w, 2g-1]$.

De cette discussion, le nombre de colonnes, dans lesquelles il y a aucun @, est $1 + A_w + B_w$. Puisque le nombre de non gaps dans $[1, w-1]$ est A_w, le nombre de gaps dans $[1, w-1]$ est $w-1-A_w$. Du lemme (3.2.6), on a

$$w - 1 - A_w + B_w = g \tag{3.8}$$

puisqu'il y a exactement g gaps. Donc, du lemme , on a

$$w - 1 - A_w + B_w = 1 + A_w + g - w + 1 + A_w \leq g + 1,$$

à savoir, le nombre de @ est au moins $(m - g + 1) - (g + 1) = m - 2g$. □

Maintenant on va expliquer comment utiliser le MFIA pour trouver la valeur de s_{m+w}, on introduit quelques résulats intéressants comme suit et on laissera leur preuve au lecteur.

3.2.11 Lemme. *Si (A) il existe une valeur unique de @ telle que la colonne j de S^* est une combinaison linéaire partielle de ses colonnes précédentes avec les i premières composantes et (B) la colonne j de S est linéairement dépendante avec ses colonnes précédentes, alors la valeur unique doit être égale à s_{m+w}.*

Réciproquement, du lemme (1.1.2) et du lemme (3.2.11), on a

3.2.12 Lemme. *Si (A) est vraie et si (C) la valeur unique n'est pas égale à s_{m+w}, alors la colonne j de S est linéairement indépendante des colonnes précédentes, et lorsqu'on applique le FIA à S, il existe un $\times$ dans (i, j).*

Par construction, si (A) est vraie, alors la valeur unique est appelée une *valeur candidate pour* s_{m+w}, ou simplement, *candidat.* Donc, afin de déterminer s_{m+w}, notre premier objectif est de trouver tous les candidats. Dans le chapitre 4, on développera le MFIA pour trouver tous les candidats. S'il existe un " $\times$ " sur (i, j), on dit que ce " $\times$ " affecte @ au point qui se trouve à la ligne i et à la colonne j. Lorsque le MFIA est appliqué à S^*, on peut voir les propriétés suivantes :

a) S'il existe " $\times$ " dans la colonne j, alors la colonne j de S est linéairement indépendante avec ses colonnes précédentes.

b) Si @ est dans (i, j), alors il peut être déterminé uniquement par la combinaison linéaire partielle de ses colonnes précédentes avec ses i premiers composantes, si est seulement si aucun " $\times$ " lui affecte.

c) Un " $\times$" dans $(1, 1)$ n'en affecte pas @. Un " $\times$" sur la première ligne et non pas sur la première colonne affecte tout au plus un @. Un " $\times$ " ni sur la première ligne ni sur la première colonne n'affecte tout au plus deux @.

D'après le lemme (3.2.6) et de (3.2) et (3.3) on a $S_{1,j} = s_{o_{j-1}}$ et $S_{i,1} = s_{o_{i-1}}$. Ainsi la matrice $S = (S_{i,j})_{(m-g+1)\times(m-g+1)}$ précédente peut être décomposée en produit de trois matrices comme suit

$$S = X^T.Y.X,$$

où

$$X = \begin{bmatrix} 1 & \phi_{o_1}(P_{k_1}) & \phi_{o_2}(P_{k_1}) & \dots & \phi_{o_{m-g-1}}(P_{k_1}) & \phi_{o_{m-g}}(P_{k_1}) \\ 1 & \phi_{o_1}(P_{k_2}) & \phi_{o_2}(P_{k_2}) & \dots & \phi_{o_{m-g-1}}(P_{k_2}) & \phi_{o_{m-g}}(P_{k_2}) \\ 1 & \vdots & \vdots & \dots & \vdots & \vdots \\ 1 & \phi_{o_1}(P_{k_\nu}) & \phi_{o_2}(P_{k_\nu}) & \dots & \phi_{o_{m-g-1}}(P_{k_\nu}) & \phi_{o_{m-g}}(P_{k_\nu}) \end{bmatrix}$$

et

$$Y = \begin{bmatrix} e_{i_1} & 0 & \dots & 0 \\ 0 & e_{i_2} & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & e_{i_\nu} \end{bmatrix}$$

Maintenant on a le théorème suivant :

3.2.13 Théorème. *En appliquant le MFIA à la matrice S^*, il existe au moins un @, qui peut être déterminé uniquement par une combinaison linéaire partielle, à savoir, il existe au moins une valeur candidate pour s_{m+w} calculée par l'étape 3b).*

Preuve. On pose $t = [(d^* - 1)/2]$. Si $v \leq t$, il y a au plus v colonnes linéairement indépendantes dans X aussi bien que dans S. On suppose qu'il y a μ " $\times$ " dans la matrice de discrépance D après avoir appliqué le MFIA à S^*. D'après la propriété a), on obtient $\mu \leq v \leq t$. On considère les trois cas suivant :

1) S'il existe un " $\times$ " à (1,1), alors il n'en affecte pas @, et les autre $\mu - 1$" $\times$ " affectent au plus $2(\mu - 1)$ @ d'après c). Donc les $2\mu - 2$ @ sont au plus affectés.
2) Si un " $\times$ " dans la première colonne n'est pas sur la première ligne, alors il affecte au plus un @ d'après propriété 3). Mais, il doit y avoir un autre " $\times$ " dans la première ligne ; ce " $\times$ " affecte tout au plus un @, aussi (si le vecteur reçu possède v erreurs pour $\mu \leq v \leq t$, alors tous les syndromes sont nuls et il doit avoir respectivement un " $\times$ " à la première ligne et à la première colonne. Donc les autres $\mu - 2$ " $\times$ " peuvent affecter au plus $2\mu - 2$. Par conséquent, au total plus $2\mu - 2$ de @ sont affectés.
3) Si $\mu = 1$,d'après la discussion dans 2) cet " $\times$ " doit être à $(1, 1)$. Donc, il n'y aucun @ affecté d'après c), c'est-à-dire $2\mu - 2$ (dans ce cas $2\mu - 2 = 0$) @ sont affectés.

D'après le théorème précédent, le nombre de @ est au moins $d^* - 2$, au moins $d^* - 2 - (2\mu - 2) \geq 1$ de @ n'est pas affecté et il est un candidat d'après la propriété b). □

D'une manière générale, après avoir appliqué le MFIA à S^*, il y a souvent plus d'un candidat et eux peuvent être pas tout corrects. Heureusement, s_{m+w} peut être facilement déterminé à partir de tous les candidats par le théorème suivant.

3.2.14 Théorème. *Après avoir appliqué le MFIA à S^*, le nombre de candidats corrects est plus nombreux que celui des candidats incorrects.*

Preuve. On suppose que il existe μ " $\times$ " dans la matrice de discrépance D après avoir appliqué le MFIA à S^*. D'après la preuve du théorème précédent, on peut obtenir au moins $d^* - 2 - (2\mu - 2)$ candidats. Si le candidat est égal à s_{m+w}, il est appelé un candidat correct, sinon il est appelé un candidat incorrect. Maintenant, on va calculer le nombre de candidats incorrects.

De la propriété b), les colonnes de S, qui correspondent à celles de S^* contenant " $\times$ ", sont linéairement indépendants avec ses colonnes précédentes. Le nombre de ce colonne est μ. Si on suppose que le rang de S est inférieur ou égal à v). Donc le nombre total des colonnes linéairement indépendant de S est inférieur ou égal à v, et d'après lemme (3.2.12), le nombre des candidats incorrects est au plus $v - \mu$. Par conséquent, au moins $d^* - 2 - (2\mu - 2) - (v - \mu) = d^* - v - \mu$ candidats sont corrects, et le nombre des candidats corrects est plus grand que le nombre des candidats incorrects, c'est-à-dire $d^* - v - \mu > v - \mu$. La preuve est terminée. □

Une fois s_{m+w} est trouvé, S^* est modifiée : en substituant la valeur correcte de s_{m+w} à @ et en substituant @ à s_{m+w+1}. Par suite le nombre de s_{m+w+1}, est supérieur ou égal à $d^* - 2$, c'est-à-dire le nouveau @. Si (3.4) n'est pas trouvé, alors par la même raison et de la même manièère, s_{m+w+1} peut être calculé. Cependant, il est facile de voir que l'application du MFIA à la nouvelle matrice S^* est équivalente à la modification da la matrice de discrépance D comme suit : on substitue la valeur de s_{m+w} à tous les @ qui n'étant pas des candidats et on élimine la discrépance à ce point si c'est possible, c'est-à-dire il n'existe aucun " $\times$ " sur sa colonne et il existe un " $\times$ " sur sa ligne ; on remplace @ qui étant le candidat correct par 0 et par " $\times$" le @ qui étant le candidat incorrect (par le lemme (3.2.11) et le lemme (3.2.12) : et on place @ sur (i, j),sur lequel s_{m+w+1} était. La complexité de modification de la matrice de discrépance D est $O((m-g+1)^2)$. Donc, la construction de S^* dans notre étude du décodage possède $O((m - g + 1)^2 n)$ de complexité. La complexité de l'algorithme pour déterminer la valeur de s_{m+1} est $O((m - g + 1)^3)$. Pour trouver $s_{m+2}, s_{m+3}, \ldots, s_{m+g}$, au plus $g - 1$ modifications de D sont exigés (pour quelques d'erreur, (3.4) peut être tôt trouvés,) qui a $O((g - 1)(m - g + 1)^2)$. Par conséquent, pour trouver tous les s_i pour $i = m + 1, m + 2, \ldots, m + g$, et (3.4), la complexité est $O((m - g + 1)^2 n)$.
Notre procédure de décodage peut être décrite comme suit :

1) On calcule les syndromes s_i à partir du vecteur reçu pour $i = o_0, o_1, \ldots, o_{m-g+1}$
2) On détermine s_i pour $i = m + 1, m + 2, \ldots, m + g$ et (3.4).
3) On cherche les racines de (3.4) parmi les points rationnels.
4) On résoud le système d'équations linéaires et on détecte les places des erreurs et les erreurs en même temps.

Chapitre 4

Décodage d'un code hermitien

4.1 Construction du code

Dans cette section, on va illustrer cette procédure de décodage à l'aide d'un exemple. Pour cela, on considère la courbe plane suivante définie par

$$f(X,Y,Z) = X^5 + Y^4Z + YZ^4 = 0 \tag{4.1}$$

sur $\mathbb{F}_{2^4} \cong \mathbb{F}_2[\alpha]/ < X^5 + Y^4Z + YZ^4 >$. Ce courbe est de la forme $X^{r+1} + Y^rZ + YZ^r = 0$ avec $r = 4$. C'est l'équation d'une courbe hérmitienne. Ainsi, elle a un point à l'infini $Q = (0 : 1 : 0)$ et possède r^3 points rationnels sur $\mathbb{F}_{2^4}$, c'est-à-dire, possède 64 points (Voir [Sti98]). $x = X/Z$ a un pôle d'ordre 4 et $y = Y/Z$ a un pôle d'ordre 5. La courbe est de genre $g = 1/2(q-1)(q-2) = 6$ avec $q = 5$.

Maintenant, on construit le code de longueur $n = 64$ et soient $D = P_1 + P_2 + \cdots + P_{64}$ et $G = 23Q$.

Le code linéaire $C_\Omega(D,G)$ de longueur 64 sur $\mathbb{F}_{2^4}$ est l'image l'application

$$\alpha* : \Omega(G-D) \longrightarrow \mathbb{F}_{2^4}^{64}$$

définie par

$$\alpha^*(w) = (Res_{P_1}(w), Res_{P_2}(w), ..., Res_{P_n}(w))$$

D'après le théorème de Riemann-Roch, la distance désignée minimale d^* est égale à $deg(G) - 2g+2 = 23-2\times6+2 = 13$ et la capacité du correcteur d'erreurs est $t = (d*-1)/2 = (13-1)/2 = 6$. La dimension du code est $k = deg(G) - g + 1 = 23 - 6 + 1 = 18$. Soient $f_1, f_2, \ldots, f_{18}$ la base de l'espace vectoriel $L(G)$. Alors la matrice de contrôle pour le code $C_\Omega(D,G)$ est donnée par

$$H = \begin{bmatrix} f_1(P_1) & f_1(P_2) & \ldots & f_1(P_{64}) \\ f_2(P_1) & f_2(P_2) & \ldots & f_2(P_{64}) \\ \ldots & \ldots & \ldots & \ldots \\ f_{18}(P_1) & f_{18}(P_2) & \ldots & f_{18}(P_{64}) \end{bmatrix} \tag{4.2}$$

D'après [Sti98], les éléments $x^\alpha y^\beta$ forment une base de $L(G)$ pour les courbes hérmitiennes avec $0 \le \alpha, 0 \le \beta \le 4$ et $4\alpha + 5\beta \le 23$. On a

$$
\begin{array}{lll}
f_1 = 1 & ; & f_2 = x\,; \\
f_3 = y & ; & f_4 = x^2\,; \\
f_5 = xy & ; & f_6 = y^2\,; \\
f_7 = x^3 & ; & f_8 = x^2y\,; \\
f_9 = xy^2 & ; & f_{10} = y^3\,; \\
f_{11} = x^4 & ; & f_{12} = x^3y\,; \\
f_{13} = x^2y^2 & ; & f_{14} = xy^3\,; \\
f_{15} = y^4 & ; & f_{16} = x^4y\,; \\
f_{17} = x^3y^2 & ; & f_{18} = x^2y^3\,;
\end{array}
\tag{4.3}
$$

Les ordres des fonctions f_i pour $i = 1, \ldots, 18$ sont donnés par $\rho(x^\alpha y^\beta) = 4\alpha + 5\beta$[HJL98]. Donc les f_i ont pour ordres respectifs :

$$0; 4; 5; 8; 9; 10; 12; 13; 14; 15; 16; 17; 18; 19; 20; 21; 22; 23$$

Par convenance, soient $\phi_0 = f_1, \phi_4 = f_2, \phi_5 = f_3, \phi_8 = f_4, \phi_9 = f_5, \phi_{10} = f_6, \phi_{12} = f_7, \phi_{13} = f_8, \phi_{14} = f_9, \phi_{15} = f_{10}, \phi_{16} = f_{11}, \phi_{17} = f_{12}, \phi_{18} = f_{13}, \phi_{19} = f_{14}, \phi_{20} = f_{15}, \phi_{21} = f_{16}, \phi_{22} = f_{17}$ et $\phi_{23} = f_{18}$

Ainsi,

$$ord_Q(\phi_i) = -i \quad \text{pour} \quad i = 0, 4, 5, 8, 9, 10, 12, 13, \ldots, 23$$

Pour chaque i, on peut y avoir d'autres fonctions ϕ tel que $ord_Q(\phi) = -i$. Mais elles sont des combinaisons linéaires de $\phi_0, \phi_1, \phi_2, \ldots, \phi_i$.

Par exemple, $ord_Q(x^5) = -20$. En divisant l'équation $X^5 + Y^4Z + YZ^4 = 0$, par Z^5, on obtient

$$\frac{X^5}{Z^5} + \frac{Y^4}{Z^4} + \frac{Y}{Z} = 0$$

et en posant $x = X/Z$ et $y = Y/Z$, on a

$$x^5 = y^4 + y$$

par suite,

$$x^6 = y^4x + yx,$$

et ainsi de suite.

Soient $\phi_{20} = y^4, \phi'_{20} = x^5, \phi_{24} = xy^4$ et $\phi'_{24} = x^6$ et ainsi de suite. Donc d'après les équations précédentes, on a

$$\phi'_{20} = \phi_{20} + \phi_5, \quad \phi'_{24} = \phi'_{24} + \phi_9. \tag{4.4}$$

4.2 Calcul des syndrômes

Soient $u = (u_1, u_2, \ldots, u_{64})$ un mot reçu, $e = (e_1, e_2, \ldots, e_{64})$ un vecteur erroné et $c = (c_1, c_2, \ldots, c_{64})$ le mot de code. Ainsi, on a $u = e + c$. Alors on définit les syndrômes

$$\begin{aligned} s_i &= < u, \alpha^* \phi_i > \\ &= \sum_{j=1}^{64} u_j \phi_i(P_j), \quad \text{pour} \quad \imath = 0, 4, 5, 8, 9, 10, 12, 13, \ldots, 23 \\ &= \sum_{j=1}^{64} (c_j + e_j)\phi_i(P_j) \\ &= \sum_{j=1}^{64} c_j \phi_i(P_j) + \sum_{j=1}^{64} e_j \phi_i(P_j), \quad \text{or} \quad \sum_{j=1}^{64} c_j \phi_i(P_j) = 0 \end{aligned}$$

Donc

$$s_i = \sum_{j=1}^{64} e_j \phi_i(P_j), \tag{4.5}$$

De même

$s'_i = < u, \alpha^* \phi'_i > = \sum_{j=1}^{64} u_j \phi'_i(P_j)$, pour $\imath = 20$. on a

$$s'_i = \sum_{j=1}^{64} e_j \phi'_i(P_j). \tag{4.6}$$

$s_i = \sum_{j=1}^{64} e_j \phi_i(P_j)$ et $s'_i = \sum_{j=1}^{64} e_j \phi'_i(P_j)$ pour $i \geq 24$, où ϕ_i et ϕ'_i sont de même ordres $-i$ avec Q. Il est certain que s_i et s'_i sont inconnus pour $i \geq 24$. Puisque $\phi'_{20} = \phi_{20} + \phi_5$ et $\phi'_{24} = \phi'_{24} + \phi_9$, et d'après la définition de s'_i, on a

$$s'_{20} = s_{20} + s_5 \quad \text{et} \quad s'_{24} = s_{24} + s_9. \tag{4.7}$$

En effet,

$$s'_{20} = \sum_{j=1}^{64} e_j \phi'_{20}(P_j) = \sum_{j=1}^{64} e_j (\phi_{20} + \phi_5)(P_j) = \sum_{j=1}^{64} e_j \phi_{20}(P_j) + \sum_{j=1}^{64} e_j \phi_5(P_j) = s_{20} + s_5$$

et

$$s'_{24} = \sum_{j=1}^{64} e_j \phi'_{24}(P_j) = \sum_{j=1}^{64} e_j (\phi_{24} + \phi_9)(P_j) = \sum_{j=1}^{64} e_j \phi_{24}(P_j) + \sum_{j=1}^{64} e_j \phi_9(P_j = s_{24} + s_9.$$

On suppose qu'il existe μ e_{k_μ} erreurs au point $P_{k_\mu} = (X_{k_\mu} : Y_{k_\mu} : Z_{k_\mu})$ pour $\mu = 1, 2, \ldots, \nu$ où $\nu \leq 6$. On considère le vecteur reçu

$$u = (\alpha^{12}, \alpha^4, \alpha^7, \alpha^8, \alpha^9, \alpha^9, 0, \ldots, 0, 0, 0, 0, \ldots, 0, 0, 0, 0, 0),$$

c'est-à-dire $u_1 = \alpha^{12}, u_2 = \alpha^4, u_3 = \alpha^7, u_4 = \alpha^8, u_5 = \alpha^9, u_7 = \alpha^9$, et les autres composantes sont 0.

Soient

$$P_1 = (1 : 1 : \alpha), P_2 = (1 : 1 : \alpha^2), P_3 = (1 : 1 : \alpha^4), P_4 = (1 : 1 : \alpha^8), P_5 = (0 : 0 : 1), P_6 = (1 : \alpha : 1).$$

Puisqu'on travaille sur le corps fini $\mathbb{F}_{2^4}$. Il faut déterminer avant tout les éléments de ce corps. Soit $P(1:1:\alpha)$ un point de la courbe définie par (4.1) dans le corps fini $\mathbb{F}_{2^4}$. On a

$\alpha^4 + \alpha + 1 = 0$, c'est-à-dire $\alpha^4 = \alpha + 1$.
$\alpha^5 = \alpha + \alpha^2$
$\alpha^6 = \alpha^2 + \alpha^3$
$\alpha^7 = \alpha^3 + \alpha^4 = 1 + \alpha + \alpha^3$
$\alpha^8 = \alpha^4 + \alpha^5 = 1 + \alpha^2$
$\alpha^9 = \alpha^5 + \alpha^6 = \alpha + \alpha^3$
$\alpha^{10} = \alpha^2 + \alpha^4 = 1 + \alpha + \alpha^2$
$\alpha^{11} = \alpha + \alpha^2 + \alpha^3$
$\alpha^{12} = \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha + \alpha^2 + \alpha^3$
$\alpha^{13} = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha^2 + \alpha^3$
$\alpha^{14} = \alpha + \alpha^3 + \alpha^4$
$\alpha^{15} = \alpha + \alpha^4 = 1$
$\alpha^{16} = \alpha$.

$$\text{Donc,} \quad \mathbb{F}_{[2^4]} := \mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{12}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}.$$

Maintenant, on va calculer les syndrômes s_i pour $i = 0, 4, 5, 8, 9, 10, 12, 13, \ldots, 23$. De (4.3) et (4.5), on a $s_i = \sum_{j=1}^{6} u_j \phi_i(P_j)$ où P_j sont les points cités ci-dessus et u_j les composantes du vecteur u.

Pour $i = 0$, $s_0 = \sum_{j=1}^{6} u_j \phi_0(P_j) = \sum_{j=1}^{6} u_j 1(P_j) = u_1 + u_2 + u_3 + u_4 + u_5 + u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^9 + \alpha^9 = \alpha$.

Pour $i = 4$, $s_4 = \sum_{j=1}{}_{j} \phi_4(P_j) = \sum_{j=1}^{6} u_j x(P_j) = u_1 + u_2 + u_3 + u_4 + u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^9 = \alpha^3$.

Pour $i = 5$, $s_4 = \sum_{j=1}{}_{j} \phi_5(P_j) = \sum_{j=1}^{6} u_j xy(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{10} = 1 + \alpha^2 = \alpha^8$.

Pour $i = 8$, $s_4 = \sum_{j=1}{}_{j} \phi_8(P_j) = \sum_{j=1}^{6} u_j x^2(P_j) = u_1 + u_2 + u_3 + u_4 + u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^9 = \alpha^3$.

Pour $i = 9$, $s_4 = \sum_{j=1}{}_{j} \phi_9(P_j) = \sum_{j=1}^{6} u_j xy(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{10} = 1 + \alpha^2 = \alpha^8$.

Pour $i = 10$, $s_4 = \sum_{j=1}{}_{j} \phi_{10}(P_j) = \sum_{j=1}^{6} u_j y^2(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha^2 u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{11} = \alpha^6$.

Pour $i = 12$, $s_4 = \sum_{j=1}{}_{j} \phi_{12}(P_j) = \sum_{j=1}^{6} u_j x^3(P_j) = u_1 + u_2 + u_3 + u_4 + u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^9 = \alpha^3$.

Pour $i = 13, s_4 = \sum_{j=1}^{6} {}_j\phi_{13}(P_j) = \sum_{j=1}^{6} u_j x^2 y(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{10} = 1 + \alpha^2 = \alpha^8$.

Pour $i = 14, s_4 = \sum_{j=1}^{6} {}_j\phi_{14}(P_j) = \sum_{j=1}^{6} u_j x y^2(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha^2 u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{11} = \alpha^6$.

Pour $i = 15, s_4 = \sum_{j=1}^{6} {}_j\phi_{15}(P_j) = \sum_{j=1}^{6} u_j y^3(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha^3 u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{12} = \alpha^{13}$.

Pour $i = 16, s_4 = \sum_{j=1}^{6} {}_j\phi_{16}(P_j) = \sum_{j=1}^{6} u_j x^4(P_j) = u_1 + u_2 + u_3 + u_4 + u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^9 = \alpha^3$.

Pour $i = 17, s_4 = \sum_{j=1}^{6} {}_j\phi_{17}(P_j) = \sum_{j=1}^{6} u_j x^3 y(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{10} = 1 + \alpha^2 = \alpha^8$.

Pour $i = 18, s_4 = \sum_{j=1}^{6} {}_j\phi_{18}(P_j) = \sum_{j=1}^{6} u_j x^2 y^2(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha^2 u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{11} = \alpha^6$.

Pour $i = 19, s_4 = \sum_{j=1}^{6} {}_j\phi_{19}(P_j) = \sum_{j=1}^{6} u_j x y^3(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha^3 u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{12} = \alpha^{13}$.

Pour $i = 20, s_4 = \sum_{j=1}^{6} {}_j\phi_{20}(P_j) = \sum_{j=1}^{6} u_j y^4(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha^4 u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{13} = \alpha^{12}$.

Pour $i = 21, s_4 = \sum_{j=1}^{6} {}_j\phi_{21}(P_j) = \sum_{j=1}^{6} u_j x^4 y(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{10} = 1 + \alpha^2 = \alpha^8$.

Pour $i = 22, s_4 = \sum_{j=1}^{6} {}_j\phi_{22}(P_j) = \sum_{j=1}^{6} u_j x^3 y^2(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha^2 u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{11} = \alpha^6$.

Pour $i = 19, s_4 = \sum_{j=1}^{6} {}_j\phi_{19}(P_j) = \sum_{j=1}^{6} u_j x^2 y^3(P_j) = u_1 + u_2 + u_3 + u_4 + \alpha^3 u_6 = \alpha^{12} + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{12} = \alpha^{13}$.

Et $s'_{20} = \sum_{j=1}^{6} {}_j(\phi_{20} + \phi_5)(P_j) = \sum_{j=1}^{6} u_j(y^4 + y)(P_j) = s_{20} + s_5 = \alpha^8 + \alpha^{12} = \alpha^{9.}$

D'où

$$
\begin{array}{llll}
s_0 = \alpha & s_4 = \alpha^3 & s_5 = \alpha^8 & s^8 = \alpha_3 \\
s_9 = \alpha^8 & s_{10} = \alpha^6 & s_{12} = \alpha^3 & s_{13} = \alpha^8 \\
s_{14} = \alpha^6 & s_{15} = \alpha^{13} & s_{16} = \alpha^3 & s_{17} = \alpha^8 \\
s_{18} = \alpha^6 & s_{19} = \alpha^{13} & s_{20} = \alpha^{12} & s_{21} = \alpha^8 \\
s_{22} = \alpha^5 & s_{23} = \alpha^{10} & s'_{20} = \alpha^9. &
\end{array}
$$

Maintenant, on va chercher s_{24} et s'_{24}. Pour cela, on considère la matrice S' suivante où @ exprime

s_{24} ou s'_{24} et # exprime les autres syndrômes inconnus. $S' =$

$$\begin{bmatrix}
s_0 & s_4 & s_5 & s_8 & s_9 & s_{10} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} & s_{17} & s_{18} & s_{19} & s_{20} & s_{21} & s_{22} & s_{23} \\
s_4 & s_8 & s_9 & s_{12} & s_{13} & s_{14} & s_{16} & s_{17} & s_{18} & s_{19} & s'_{20} & s_{21} & s_{22} & s_{23} & @ & \# & \# & \# \\
s_5 & s_9 & s_{10} & s_{13} & s_{14} & s_{15} & s_{17} & s_{18} & s_{19} & s_{20} & s_{21} & s_{22} & s_{23} & @ & \# & \# & \# & \# \\
s_8 & s_{12} & s_{13} & s_{16} & s_{17} & s_{18} & s'_{20} & s_{21} & s_{22} & s_{23} & @ & \# & \# & \# & \# & \# & \# & \# \\
s_9 & s_{13} & s_{14} & s_{17} & s_{18} & s_{19} & s_{21} & s_{22} & s_{23} & @ & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{10} & s_{14} & s_{15} & s_{18} & s_{19} & s_{20} & s_{22} & s_{23} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{12} & s_{16} & s_{17} & s'_{20} & s_{21} & s_{22} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{13} & s_{17} & s_{18} & s_{21} & s_{22} & s_{23} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{14} & s_{18} & s_{19} & s_{22} & s_{23} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{15} & s_{19} & s_{20} & s_{23} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{16} & s'_{20} & s_{21} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{17} & s_{21} & s_{22} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{18} & s_{22} & s_{23} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{19} & s_{23} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{20} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{21} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{22} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
s_{23} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \#
\end{bmatrix}$$

En remplaçant s_i par ses valeurs, la matrice S' devient comme suit

$$\begin{bmatrix}
\alpha & \alpha^3 & \alpha^8 & \alpha^3 & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^8 & \alpha^6 & \alpha^{13} & \alpha^3 & \alpha^8 & \alpha^6 & \alpha^{13} & \alpha^{12} & \alpha^8 & \alpha^6 & \alpha^{13} \\
\alpha^3 & \alpha^3 & \alpha^8 & \alpha^3 & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^8 & \alpha^6 & \alpha^{13} & \alpha^9 & \alpha^8 & \alpha^6 & \alpha^{13} & @ & \# & \# & \# \\
\alpha^8 & \alpha^8 & \alpha^6 & \alpha^8 & \alpha^6 & \alpha^{13} & \alpha^8 & \alpha^6 & \alpha^{13} & \alpha^{12} & \alpha^8 & \alpha^6 & \alpha^{13} & @ & \# & \# & \# & \# \\
\alpha^3 & \alpha^3 & \alpha^8 & \alpha^3 & \alpha^8 & \alpha^6 & \alpha^9 & \alpha^8 & \alpha^6 & \alpha^{13} & @ & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \alpha^8 & \alpha^6 & \alpha^8 & \alpha^6 & \alpha^{13} & \alpha^8 & \alpha^6 & \alpha^{13} & @ & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \alpha^6 & \alpha^{13} & \alpha^6 & \alpha^{13} & \alpha^{12} & \alpha^6 & \alpha^{13} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^3 & \alpha^3 & \alpha^8 & \alpha^9 & \alpha^8 & \alpha^6 & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \alpha^8 & \alpha^6 & \alpha^8 & \alpha^6 & \alpha^{13} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \alpha^6 & \alpha^{13} & \alpha^6 & \alpha^{13} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{13} & \alpha^{13} & \alpha^{12} & \alpha^{13} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^3 & \alpha^9 & \alpha^8 & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \alpha^8 & \alpha^6 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \alpha^6 & \alpha^{13} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{13} & \alpha^{13} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{12} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{13} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \#
\end{bmatrix}$$

calcul de s_{24} et s'_{24} :

On applique alors la MFIA à S' pour trouver les valeurs possibles de s_{24} et s'_{24}. On note par $@_j$ la candidate sur la colonne j et $\times_j$ la discrépence $\times$ non nulle sur la colonne j.

On examine successivement les éléments de chaque colonne de la matrice, en commençant par la première. Soient

$$s^{(r)}(x) = 1 + s_{r,1}x + s_{r,2}x^2 + ... + s_{r,N}x^N$$

$$\text{et} \quad C^{(i-1,j)}(x) = c_0^{(i-1,j)} + c_1^{(i-1,j)}x + c_2^{(i-1,j)}x^2 + ... + c_{j-1}^{(i-1,j)}.$$

Pour $j = 1$ (première colonne)et $r = 1$ (première ligne), on a $C^{(0,1)}(x) = 1$, et $d_{1,1} = [C^{(0,1)}(x)s^{(1)}(x)]_1 = [1 \times (1+\alpha x)]_1 = \alpha \neq 0$. Et comme il n'y a pas de $d_{1,u}$ pour $u < 1$, on stocke $C^{(1)}(x) := C^{(0,1)}(x) = 1$ dans C et $d_{1,1} = \alpha$ dans le Tableau D.

Pour $j = 2$ (deuxième colonne) et $r = 1$, on a $C^{(0,2)}(x) := C^{(1)}(x) = 1$, et $d_{1,2} = [C^{(0,1)}(x)s^{(2)}(x)]_2 = [1 \times (1 + \alpha x + \alpha^3 x^2)]_2 = \alpha^3 \neq 0$. Comme $d_{1,1} = \alpha \neq 0$, on a

$$C^{(2)}(x) = C^{(2)}(x) - \frac{d_{1,2}}{d_{1,1}}C^(1)(x)x^{3-1} = 1 - \frac{\alpha^3}{\alpha}x = 1 + \alpha^2 x$$

En suite, on passe à la ligne suivante, c'est-à-dire pour $r = 2$. On a $d_{2,2} = [C^{(2)}(x)s^{(2)}(x)]_2 = [(1 + \alpha_2)x \times (1 + \alpha^3 x + \alpha^3 x^2)]_2 = \alpha^{11} \neq 0$. Et comme il n'y a pas de $d_{2,u}$ pour $1 \leq u < 2$, on stocke $C^{(2)}(x)$ dans C et $d_{2,2} = \times_2 = 1$ dans le Tableau D et passe à la troisième colonne.

Pour $j = 3$ et $r = 1$, on a $C^{(0,3)}(x) := C^{(2)}(x) = 1 + \alpha^2 x$ et $d_{1,3} = [C^{(3)}(x)s^{(1)}(x)]_3 = [(1+\alpha)x \times (1+\alpha x+\alpha^2 x^2+\alpha^8 x^3)]_3 = \alpha^4 \neq 0$. Comme $d_{1,1} = \alpha \neq 0$, alors $C^{(3)}(x) := C^{(3)}(x) - \frac{d_{1,3}}{d_{1,1}}C^(1)(x)x^{3-1} = 1 + \alpha x + \alpha^3 x^2$. Puis on se déplace à ligne suivante.

Pour $r = 2$, on a $d_{2,3} = [C^{(3)}(x)s^{(2)}(x)]_3 = \alpha^{12} \neq 0$. Comme $d_{2,2} = \alpha^{11} \neq 0$,

$$C^{(3)}(x) := C^{(3)}(x) - \frac{d_{2,3}}{d_{2,2}}C^(2)(x)x^{3-2} = 1 + \alpha^5 x$$

.

Pour $r = 3$, on a $d_{3,3} = [C^{(3)}(x)s^{(3)}(x)]_3 = [(1+\alpha^5 x) \times (1+\alpha^8 x+\alpha^3 x^2+\alpha^8 x^3)] = 1 \neq 0$. Comme il n'y a pas de $d_{3,u} \neq 0$, pour $1 \leq u < 3$, alors on stocke $C^{(3)}(x) = 1 + \alpha^5 x$ dans C et $d_{3,3} = 1$ dans le Tableau D et passe à la troisième colonne.

Pour $j = 4$, et $r = 1$ (première ligne), on a $C^{(4)}(x) := C^{(3)}(x) = 1+\alpha^5 x$, et $d_{1,4} = [C^{(4)}(x)s^{(1)}(x)]_4 = \alpha^8 \neq 0$. Comme $d_{1,1} = \alpha \neq 0$, alors $C^{(4)}(x) := C^{(4)}(x) - \frac{d_{1,4}}{d_{1,1}}C^{(1)}(x)x^{4-1} = 1 + \alpha^5 x + \alpha^7 x^3$.

Pour $r = 2$ (deuxième ligne), $d_{2,4} = [C^{(4)}(x)s^{(2)}(x)]_4 = \alpha \neq 0$. Comme $d_{2,2} = \alpha^{11} \neq 0$, alors $C^{(4)}(x) := C^{(4)}(x) - \frac{d_{2,4}}{d_{2,2}}C^{(2)}(x)x^{4-2} = 1 + \alpha x + \alpha^5 x^2$.

Pour $r = 3$ (troisième ligne), $d_{3,4} = [C^{(4)}(x)s^{(3)}(x)]_4 = \alpha^5 \neq 0$. Comme $d_{3,3} = 1 \neq 0$, alors $C^{(4)}(x) := C^{(4)}(x) - \frac{d_{3,4}}{d_{3,3}}C^{(3)}(x)x^{4-3} = 1 + x^2$.

Pour $r = 4, 5, 6$, on a $d_{4,4} = d_{5,4} = d_{6,4}$ et $C^{(4)}(x) = 1 + x^2$. Mais $d_{7,4} = [C^{(4)}(x)s^{(7)}(x)]_4 = [(1 + x^2) \times (1 + \alpha^3 x + \alpha^3 x^2 + \alpha^8 x^3 + \alpha^9 x^4)]_4 = \alpha$ Et comme il n'existe pas un $d_{7,u}(1 \leq u < 4)$, alors on passe à la colonne suivante.

Pour $j = 5$, on prend $C^{(5)}(x) := C^{(4)}(x) = 1 + x^2$ et on a

$$d_{1,5} = d_{2,5} = d_{3,5} = d_{4,5} = d_{5,5} = d_{6,5} = d_{7,5} = d_{8,5} = d_{9,5} = 0$$

Comme $s_{10,5} = @$ et il n'existe aucun $s_{10,u}$ pour $1 \leq u < 5$, alors on peut calculer @. On a

$$@ := @_5 = -\sum_{h=1}^{4} c_h^{(5)}.s_{10,5-h} = c_1^{(5)}.s_{10,4} + c_2^{(5)}.s_{10,3} + c_3^{(5)}.s_{10,2} + c_4^{(5)}.s_{10,1} = 1 + \alpha + \alpha^2 + \alpha^3 = \alpha^{12}.$$

On stocke la valeur de @ dans E et $C^{(5)}(x)$ dans F. On passe à la colonne suivante.

Pour $j = 6$ (sixième colonne), et $r = 1$, on a $C^{(6)}(x) := C^{(5)}(x) = 1+x^2$ et $d_{1,6} = [C^{(6)}(x)s^{(1)}(x)]_6 = \alpha^2 \neq 0$. Comme $d_{1,1} = \alpha \neq 0$, alors $C^6(x) := C^{(6)}(x) - \frac{d_{1,6}}{d_{1,1}} C^{(1)}(x)x^5 = 1 + x^2 + \alpha^5$.

Pour $r = 2$, $d_{2,6} = [C^{(6)}(x)s^{(2)}(x)]_6 = \alpha^{10} \neq 0$. Comme $d_{2,2} = \alpha^{11} \neq 0$, alors

$$C^{(6)}(x) := C^{(6)}(x) - \frac{d_{2,6}}{d_{2,2}} C^{(2)}(x)x^4 = 1 + x^2 + \alpha^{14}x^4.$$

Pour $r = 3$, $d_{3,6} = [C^{(6)}(x)s^{(3)}(x)]_6 = \alpha^4 \neq 0$. Comme $d_{3,3} = 1 \neq 0$, alors

$$C^{(6)}(x) := C^{(6)}(x) - \frac{d_{3,6}}{d_{3,3}} C^{(3)}(x)x^3 = 1 + x^2 + \alpha^4x^3 + \alpha^4x^4.$$

Pour $r = 4, 5, 6, 7$, on a $d_{4,6} = d_{5,6} = d_{6,6} = 0$. et $d_{7,6} = \alpha$ Comme $d_{7,4} = \alpha \neq 0$, alors $C^{(6)}(x) := C^{(6)}(x) - \frac{d_{7,6}}{d_{7,4}} C^{(4)}(x)x^2 = 1 + \alpha^4x^3 + \alpha x^4$

Pour $r = 8, d_{8,6} = 0$ et puisque $s_{9,6} = @$ et il n'existe aucun $s_{9,u}$ pour $1 \leq u < 6$, alors on peut calculer @. On a

$$@ := @_6 = -\sum_{h=1}^{5} c_h^{(6)}.s_{9,5-h} = c_1^{(6)}.s_{9,5} + c_2^{(6)}.s_{9,4} + c_3^{(6)}.s_{9,3} + c_4^{(6)}.s_{9,2} + c_5^{(6)}.s_{9,1} = 1 + \alpha + \alpha^2 + \alpha^3 = \alpha^{12}.$$

On stocke la valeur de @ dans E et $C^{(6)}(x)$ dans F. On passe à la colonne suivante.

Pour $j = 7$ (septième colonne), et $r = 1$, on a $C^{(7)}(x) := C^{(6)}(x) = 1 + \alpha^4x^3 + \alpha x^4$ et $d_{1,7} = [C^{(7)}(x)s^{(1)}(x)]_7 = \alpha^{14} \neq 0$. Comme $d_{1,1} = \alpha \neq 0$, $C^7(x) := C^{(7)}(x) - \frac{d_{1,7}}{d_{1,1}} C^{(1)}(x)x^6 = 1 + \alpha^4x^3 + \alpha x^4 + \alpha^{13}x^6$.

Pour $r = 2$, on a $d_{2,7} = [C^{(7)}(x)s^{(2)}(x)]_7 = \alpha^7 \neq 0$. Comme $d_{2,2} = \alpha^{11} \neq 0$, alors

$$C^{(7)}(x) := C^{(7)}(x) - \frac{d_{2,7}}{d_{2,2}} C^{(2)}(x)x^5 = 1 + \alpha^4x^3 + \alpha x^4 + \alpha^{11}x^5.$$

Pour $r = 3$, $d_{3,7} = [C^{(7)}(x)s^{(3)}(x)]_7 = \alpha \neq 0$. Comme $d_{3,3} = 1 \neq 0$, alors

$$C^{(7)}(x) := C^{(7)}(x) - \frac{d_{3,7}}{d_{3,3}} C^{(3)}(x)x^4 = 1 + \alpha^4x^3 + \alpha x^5.$$

Pour $r = 4$, on a $d_{4,7} = [C^{(7)}(x)s^{(4)}(x)]_7 = \alpha$. Puisqu'il n'y a pas de $d_{4,u}$ pour $1 \leq u < 7$, alors on passe à la colonne suivante.

Pour $j = 8$ (huitième colonne), et $r = 1$, on a $C^{(8)}(x) := C^{(7)}(x) = 1 + \alpha^4x^3 + \alpha x^5$ et pour $r = 1, 2, 3, 4, 5, 6$, on a $d_{1,8} = \cdots = d_{6,8} = 0$ Comme $s_{7,8} = \#$,on passe à la colonne suivante.

Pour $j = 9$ (neuvième colonne), et $r = 1$, on a $C^{(9)}(x) := 1+\alpha^4x^3+\alpha x^5$ et $d_{1,9} = [C^{(9)}(x)s^{(1)}(x)]_9 = \alpha_3 \neq 0$. Comme $d_{1,1} = \alpha \neq 0$,

$$C^9(x) := C^{(9)}(x) - \frac{d_{1,9}}{d_{1,1}}C^{(1)}(x)x^8 = 1 + \alpha^4x^3 + \alpha x^5 + \alpha^2x^8$$

Pour $r = 2$, on a $d_{2,9} = [C^{(9)}(x)s^{(2)}(x)]_9 = \alpha^{11} \neq 0$. Comme $d_{2,2} = \alpha^{11} \neq 0$, alors $C^{(9)}(x) := C^{(9)}(x) - \frac{d_{2,9}}{d_{2,2}}C^{(2)}(x)x^7 = 1 + \alpha^4x^3 + \alpha x^5 + x^7$

Pour $r = 3$, $d_{3,9} = [C^{(9)}(x)s^{(3)}(x)]_9 = \alpha^5 \neq 0$. Comme $d_{3,3} = 1 \neq 0$, alors $C^{(9)}(x) := C^{(9)}(x) - \frac{d_{3,9}}{d_{3,3}}C^{(3)}(x)x^6$

Pour $r = 4, 5$, on a $d_{4,9} = d_{5,9} = 0$ Comme $s_{6,9} = @$ et il n'y a pas du $s_{6,u}$ pour $1 \leq u < 9$, alors on peut calculer @. On a

$$@ := @_9 = -\sum_{h=1}^{8} c_h^{(9)}.s_{6,9-h} = 1 + \alpha + \alpha^2 + \alpha^3 = \alpha^{12}.$$

On stocke la valeur de @ dans E et $C^{(9)}(x)$ dans F,on passe à la colonne suivante.

Pour $j = 10$ (dixième colonne), et $r = 1$, on a $C^{(10)}(x) := C^{(9)}(x) = 1+\alpha^4x^3+\alpha x^5+\alpha^5x^6+\alpha^5x^7$ et $d_{1,10} = [C^{(10)}(x)s^{(1)}(x)]_{10} = \alpha^2 \neq 0$. Comme $d_{1,1} = \alpha \neq 0$,

$$C^{10}(x) := C^{(10)}(x) - \frac{d_{1,10}}{d_{1,1}}C^{(1)}(x)x^9 = 1 + \alpha^4x^3 + \alpha x^5 + \alpha^5x^6 + \alpha^5x^7 + \alpha^9.$$

Pour $r = 2$, on a $d_{2,10} = [C^{(10)}(x)s^{(2)}(x)]_{10} = \alpha^{10} \neq 0$. Comme $d_{2,2} = \alpha^{11} \neq 0$, alors

$$C^{(10)}(x) := C^{(10)}(x) - \frac{d_{2,10}}{d_{2,2}}C^{(2)}(x)x^8 = 1 + \alpha^4x^3 + \alpha x^5 + \alpha^5x^6 + \alpha^5x^7 + \alpha^{14}x^8.$$

Pour $r = 3$, $d_{3,10} = [C^{(10)}(x)s^{(3)}(x)]_{10} = \alpha^4 \neq 0$. Comme $d_{3,3} = 1 \neq 0$, alors

$$C^{(10)}(x) := C^{(10)}(x) - \frac{d_{3,10}}{d_{3,3}}C^{(3)}(x)x^7 = 1 + \alpha^4x^3 + \alpha x^5 + \alpha^5x^6 + \alpha^8x^7 + \alpha^4x^8.$$

Pour $r = 4$, on a $d_{4,10} = [C^{(10)}(x)s^{(4)}(x)]_{10} = \alpha^5$ Puisque $d_{4,7} = \alpha \neq 0$, alors $d_{2,2} = \alpha^{11} \neq 0$, alors

$$C^{(10)}(x) := C^{(10)}(x) - \frac{d_{4,10}}{d_{4,7}}C^{(7)}(x)x^3 = 1 + \alpha x^5 + \alpha^4x^6 + \alpha^8x^7 + \alpha^8x^8$$

et on a $d_{4,10} = 0$. Comme $s_{5,9} = @$ et il n'y a pas du $s_{5,u}$ pour $1 \leq u < 10$, alors on peut calculer @.

$$@ := @_{10} = -\sum_{h=1}^{9} c_h^{(10)}.s_{5,10-h} = 1 + \alpha + \alpha^2 + \alpha^3 = \alpha^{12}.$$

Puisqu'il n'y a plus des candidates sur les dernières autres colonnes, alors on peut arrêter là notre calcul.

On obtient les valeurs de toutes les candidates : $@_5 = @_6 = @_9 = @_{10} = \alpha^{12}$. Donc d'après le théorème[(3.2. 13)], $s_{24} = @_5 = @_6 = @_9 = @_{10} = \alpha^{12}$ sont correctes.

La matrice de discrépence est comme suit où $\times_1 = \alpha, \times_2 = \alpha^{12}, \times_3 = 1, \times_4 = \times_7 = \alpha$

$$\left[\begin{array}{ccccccccccccccccc}
\times_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha^3 & \times_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & @ & \# & \# & \# \\
\alpha^8 & \alpha^8 & \times_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & @ & \# & \# & \# & \# \\
\alpha^3 & \alpha^3 & \alpha^8 & 0 & 0 & 0 & \times_7 & 0 & 0 & 0 & @ & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \alpha^8 & \alpha^6 & 0 & 0 & 0 & \alpha^8 & 0 & 0 & @_{10} & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \alpha^6 & \alpha^{13} & 0 & 0 & 0 & \alpha^6 & 0 & @_9 & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^3 & \alpha^3 & \alpha^8 & \times_4 & 0 & 0 & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \alpha^8 & \alpha^6 & \alpha^8 & 0 & 0 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \alpha^6 & \alpha^{13} & \alpha^6 & 0 & @_6 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{13} & \alpha^{13} & \alpha^{12} & \alpha^{13} & @_5 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^3 & \alpha^9 & \alpha^8 & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \alpha^8 & \alpha^6 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \alpha^6 & \alpha^{13} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{13} & \alpha^{13} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{12} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{13} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \#
\end{array}\right]$$

calcul de s_{25} :

On fait une modification de la matrice S' comme suit. On substitue les @ non candidates par α^{12} et on élimine les discrépences à ces endroits si c'est possible. Et les candidates correctes sont ramplacées par α^{12}, les discrépences à ces endroits sont 0. On cherche maintenant les valeurs de s_{25} et s'_{25} en utilisant le MFIA, c'est-à-dire, on calcule les valeurs de toutes les candidates s_{25} et on élimine les discrépences sur l'endroit où s_{24} se trouve. Après avoir modifié la matrice de discrépence, on obtient la nouvelle matrice ci-dessous où $\times_1 = \alpha, \times_2 = \alpha^{12}, \times_3 = 1, \times_4 = \times_7 = \alpha$ et $@_5 = @_{11} = \alpha^8$ et $@_6 = @_{10} = \alpha^7$.

$$\begin{bmatrix}
\times_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha^3 & \times_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & @ & \# & \# \\
\alpha^8 & \alpha^8 & \times_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & @ & \# & \# & \# \\
\alpha^3 & \alpha^3 & \alpha^8 & 0 & 0 & 0 & \times_7 & 0 & 0 & 0 & 0 & @ & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \alpha^8 & \alpha^6 & 0 & 0 & 0 & \alpha^8 & 0 & 0 & 0 & @_{11} & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \alpha^6 & \alpha^{13} & 0 & 0 & 0 & \alpha^6 & 0 & 0 & @_{10} & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^3 & \alpha^3 & \alpha^8 & \times_4 & 0 & 0 & \alpha^{12} & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \alpha^8 & \alpha^6 & \alpha^8 & 0 & 0 & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \alpha^6 & \alpha^{13} & \alpha^6 & 0 & 0 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{13} & \alpha^{13} & \alpha^{12} & \alpha^{13} & 0 & @_6 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^3 & \alpha^9 & \alpha^8 & \alpha^{12} & @_5 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & \alpha^8 & \alpha^6 & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \alpha^6 & \alpha^{13} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{13} & \alpha^{13} & \alpha^{12} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{12} & \alpha^{12} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^8 & @ & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^6 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\
\alpha^{13} & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# & \#
\end{bmatrix}$$

En faisant la même démarche comme précédemment, on peut trouver $s_{26}, s_{27}, s_{28}, s_{29}$. On obtient $s_{26} = \alpha^6, s_{27} = \alpha^{13}, s_{28} = \alpha^{12}$ et $s_{29} = \alpha^8$. On voit que la colonne 8 est une combinaison linéaire partielle de ses colonnes précédentes. Les coefficients de dépendance sont donnés par les coefficients du polynôme suivant.

$$C^{(8)}(x) = 1 + \alpha^4 x^3 + \alpha x^5. \tag{4.8}$$

Ainsi, on a trouvé une solution de l'équation (3.4) du théorème (3.2.8). 0n a

$$f_8 = \alpha^4 f_3 + \alpha f_5 \tag{4.9}$$

où f_i sont les éléments de la base de $\mathcal{L}(G)$. On obtient alors

$$x^2 y + \alpha^4 y + \alpha xy = 0 \tag{4.10}$$

Cette équation possède six racines communes. Ces points sont

$$P_1 = (1:1:\alpha), P_2 = (1:1:\alpha^2), P_3 = (1:1:\alpha^4), P_4 = (1:1:\alpha^8), P_5 = (0:0:1), P_6 = (1:\alpha:1).$$

En effet, si $x = y = 1$, l'équation (4.1) implique $1 + z + z^4 = 0$. c'est-à-dire $z = \alpha$. On a de même

$1 + \alpha^2 + (\alpha^2)^4 = (1 + \alpha + \alpha^4)^2 = 0$;

$1 + \alpha^6 + (\alpha^6)^4 = (1 + \alpha + \alpha^4)^6 = 0$;

$1 + \alpha^8 + (\alpha^8)^4 = (1 + \alpha + \alpha^4)^8 = 0$. On a alors $z = \alpha, \alpha^2, \alpha^4, \alpha^8$, pour $x = y = 1$

Puisque le système (4.9) possède six racines, alors c'est sûre qu'il y a une erreur sur chacun de ces points. Ces erreurs sont déterminées comme suit.

Soit $c = (c_1, c_2, \ldots, c_{64}) \in C_\Omega(D, G)$ un vrai code, c'est-à-dire, $H.c^T = 0$ où H est la matrice de contrôle définie dans (4.2). On a

$$\begin{pmatrix} f_1(P_1) & f_1(P_2) & \dots & f_1(P_{64}) \\ f_2(P_1) & f_2(P_2) & \dots & f_2(P_{64}) \\ \dots & \dots & \dots & \dots \\ f_{18}(P_1) & f_{18}(P_2) & \dots & f_{18}(P_{64}) \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \dots \\ c_{64} \end{pmatrix} = 0$$

Soient $u = (u_1, u_2, \dots, u_{64})$ comme mot reçu tel que $u = e + c$ avec $e = (e_1, e_2, \dots, e_{64})$ et c le mot du code.

On a alors

$$H.u^T = H(c+e)^T = H.c^T + H.e^T = H.e^T. \tag{4.11}$$

Puisque $u = (\alpha^{12}, \alpha^4, \alpha^7, \alpha^8, \alpha^9, \alpha^9, 0, 0, \dots, 0)$, et comme $H.u^T = H.e^T$ d'après (4.11), alors on a un système réduit de six équations avec six inconnues e_1, e_2, e_3, e_4, e_5, et e_6. En resolvant ce système, on a $e_1 = \alpha^{12}, e_2 = \alpha^4, e_3 = \alpha^7, e_4 = \alpha^8, e_5 = \alpha^9$ et $e_6 = \alpha^9$.

Ainsi, on a six erreurs et elles se trouvent sur les points P_1, P_2, P_3, P_4, P_5 et P_6 et les valeurs des erreurs en ces points sont $e_1 = \alpha^{12}, e_2 = \alpha^4, e_3 = \alpha^7, e_4 = \alpha^8, e_5 = \alpha^9$ et $e_6 = \alpha^9$.

Conclusion

Dans ce mémoire, nous avons présenté une très simple procédure de décodage des codes algébriqués $C_\Omega(D, G)$ avec $G = mQ$ pour les courbes hérmitiennes, qui peut corriger jusqu' aux $[(d^* - 1)/2]$ erreurs. Cette procédure de décodage a été décrite comme suit. Nous avons calculé d'abord les syndromes s_i à partir du vecteur reçu pour $i = o_0, o_1, \ldots, o_{m-g+1}$. Puis nous avons déterminé les autres s_i pour $i = m+1, m+2, \ldots, m+g$ et nous avons établi un système d'équations. Enfin nous avons cherché les racines de ce système parmi les points rationnels et avons résolu le système d'équations linéaires et détecté les endroits des erreurs et les erreurs en même temps.

Annexe

4.3 Paramètre local

Dans cette section, on considère l'anneau local $\mathcal{O}_P$ défini dans le chapitre 2. On veut savoir que l'idéal maximal $\mathcal{M}_P$ de l'anneau $\mathcal{O}_P$ est un idéal principal, c'est-à-dire, engendré par un seul élément. Soit $\mathcal{X}$ une courbe non singulière dans $\mathbb{A}^2$ définie par l'équation $F = 0$ et soit $P = (a, b)$ un point de $\mathcal{X}$. L'idéal maximal $\mathcal{M}_P$ est engendré par $x - a$ et $y - b$. Maintenant

$$F_X(P)(x - a) + F_Y(P)(y - b) \equiv \mathcal{M}_P^2.$$

Ainsi le $\mathbb{F}$-espace vectoriel $\mathcal{M}_P/\mathcal{M}_P^2$ est de dimension 1 et par conséquent $\mathcal{M}_P$ a un seul générateur.

4.3.1 Définition. Soit t l'élément générateur de $\mathcal{M}_P$. Il s'en suit que chaque élément z de $\mathcal{O}_P$ peut s'écrire d'une seule manière comme $z = ut^m$, où u est un élément unité et $m \in \mathbb{N}$. La fonction t est appelée *paramètre local* ou encore *paramètre uniformisante* pour P. Si $m > 0$ alors P un zéro de z de multicité m. On écrit $m = ord_P(z) = v_P(z)$. Par convention $v_P(0) = \infty$ On prolonge alors l'ordre de fonction v_P à $\mathbb{F}(\mathcal{X})$ en définissant $v_P(f/g) := v_P(f) - v_P(g)$. Si $v_P(z) = -m < 0$, alors on dit que z a un pôle d'ordre m pour P.

4.3.2 Exemple. Soit $\mathcal{X}$ le cercle dans $\mathbb{A}^2$ d'équation $x^2 + y^2 = 1$ et soit $P = (1, 0)$. Soit $z = z(x, y) = 1 - x$. Cette fonction est 0 au point P, ainsi elle est dans $\mathcal{M}_P$. On suppose que z est d'odre 2. En effet, y est le paramètre local pour P puisque l'équation $y = 0$ intersecte $\mathcal{X}$ avec multiplicité 1 pour P. En outre, de $\mathcal{X}$ on a $1 - x = y^2(1 + x)$ et la fonction $(1 + x)^{-1}$ est une unité $\mathcal{O}_P$. On peut faire pareillement tout dans $\mathbb{P}^2$. Donc $\mathcal{X}$ est donné par $x^2 + y^2 - z^2 = 0$ et $P = (1, 0, 1)$. Soient $(z - x)/z$ dans $\mathcal{O}_P$ et aussi un élément de $\mathcal{M}_P$. $t = y/z$ est le paramètre local pour P. On a $(z - x)/z = t^2.(z/(z + x))$, où le deuxième facteur du deuxième membre est une unité dans $\mathcal{O}_P$. Ainsi $v_P(z - x)/z = 2$.

4.3.3 Définition. Une valuation discrète est une application : $\mathcal{O}_P \longrightarrow \mathcal{N}_0 \bigcup \{\infty\}$ telle que

(i) $v_p(f) = \infty$ si est seulement si $f = 0$
(ii) $v_p(a) = 0$ pour tout $\neq a \in \mathcal{O}_P$.
(iii) $v_p(fg) = v_p(f) + v_p(g)$
(iv) Il existe $z \in \mathcal{O}_P$ tel que $v_p(z) = 1$
(v) $v_p(f + g) \geq min\{v_p(f), v_p(g)\}$

4.3.4 Théorème. *L'application v_p satisfait les propriétés suivantes :*

1. $v_p(\lambda f) = v_p(f)$ *pour tout* $0 \neq \lambda \in \mathcal{F}$
2. $v_p(f + g) = min\{v_p(f), v_p(g)\}$ *si* $v_p(f) \neq v_p(g)$.

Preuve. Par (ii) et (iv), on a $v_p(\lambda f) = v_p(f)$ pour $0 \neq \lambda \in \mathcal{F}$. En particulier, on a $v_p(-f) = v_p(f)$. Comme $v_p(f) \neq v_p(g)$, on peut supposer que $v_p(f) < v_p(g)$. Supposons que $v_p(f+g) \neq min\{v_p(f), v_p(g)\}$ alors $v_p(f+g) > v_p(f)$ de (v) et on obtient $v_p(f) = v_p((f+g)-g) \geq min\{v_p(f+g), v_p(g)\} \geq v_p(f)$. Contradiction. □

4.3.5 Définition. Soit $\mathcal{X}$ une courbe définie sur $\mathbb{F}_q$, c'est-à-dire, les équations sont à coefficients dans $\mathbb{F}_q$. Les points sur $\mathcal{X}$ des coordonnées dans $\mathbb{F}_q$ sont appelés *points rationnels.*

4.4 Diviseurs

Dans cette section, $\mathcal{X}$ représente une courbe projective non-singulière irréductible sur un corps algébriquement clos $\mathbb{F}$.

4.4.6 Définition. Un diviseur est une somme de la forme $D = \sum_{P \in \mathcal{X}} n_p P$, avec $n_p \in \mathbb{Z}$ et n_p sont presque tous nuls pour un nombre fini de points P. Le support d'un diviseur D, noté par $suppD$, est l'ensemble des points de $\mathcal{X}$ avec des coefficients non nuls :

$$suppD := \{P \in \mathcal{X} / n_P \neq 0\}.$$

Le groupe de diviseur de $\mathcal{X}$ (noté additivement) engendré par les points de $\mathcal{X}$ est appelé *groupe de diviseur* de $\mathcal{X}$, noté par $Div\mathcal{X}$.

4.4.7 Définition. On dit qu'un diviseur D est effectif (ou positif) si tous les coefficients n_P sont positifs et on note $D \geq 0$. Le degré $\deg D$ d'un diviseur D est la somme de ses coefficients : $\deg D = \sum n_P$.

4.4.8 Proposition. *Soient $D = \sum_{P \in X} n_p P$ et $D' = \sum_{P \in X} {n'}_p P$ deux diviseurs de la courbe, la somme de D et D' est définit par*

$$D + D' = \sum_{P \in X} (n_p + {n'}_p) P$$

4.4.9 Définition. Soit $v_P = ord_P$ la valuation descrète des fonctions sur $\mathcal{X}$. Soit $0 \neq z \in \mathbb{F}(\mathcal{X})$. On définit le diviseur de z par $div(z) = \sum_{P \in \mathcal{X}} ord_p(z)P$. On définit le diviseur des zéros de z par $(z)_0 = \sum_{ord_p(z)<0} ord_p(z)P$ et le diviseur des pôles de z par

$$(z)_\infty = \sum_{ord_p(z)>0} ord_p(z)P.$$

Alors le diviseur principal de z est donné par $(z) = (z)_0 + (z)_\infty$ On note que $(zz') = (z) + (z')$ et $(z)^{-1} = -(z)$.

4.4.10 Proposition. *Soit $z \in \mathbb{F}(\mathcal{X})$ une fonction rationnelle. Le degré du diviseur $divz$ est zéro. Une fonction rationnelle possède le même nombre de zéros de pôles*

Preuve. Soit C une courbe plane de degré n. Soit $z = g/h, g, h$ sont des formes de même degré dans $\Gamma_h(C)$; on dit que g et h sont des formes résiduelles G et G de degré m dans $\mathbb{F}[X, Y, Z]$. Ainsi $divz = divG - divH$, et puisque $divG$ et $divH$ ont le même degré mn. Alors $divz = 0$. □

4.4.11 Corollaire. *Soit* $0 \neq z \in \mathbb{F}(\mathcal{X})$. *LASSE* $(i) \quad div(z) \geq 0$ *;* $(ii) \quad z \in \mathbb{F}$; $(iii) \quad div(z) = 0$.

Preuve. Si $div(z) \geq 0, z \in \mathcal{O}_P(\mathcal{X})$ pour tout $P \in \mathcal{X}$. Si $z(P_0) = \lambda_0$ pour chaque P_0, alors $div(z-\lambda_0) \geq 0$ et $deg(div(z-\lambda_0)) > 0$. Contradiction,à moins que $z-\lambda_0 = 0$, c'est-à-dire, $z \in \mathbb{F}$. □

4.4.12 Corollaire. *Soient* $0 \neq z$ *et* $0 \neq z' \in \mathbb{F}(\mathcal{X})$. *Alors* $div(z) = div(z')$ *si est seulement si* $z' = \lambda z$ *pout chaque* $\lambda \in \mathbb{F}$.

4.4.13 Définition. Deux diviseurs D et D' sont dit linéairement équivalents si $D' = D + div(z)$ pour chaque $z \in \mathbb{F}(\mathcal{X})$, dans ce cas on écrit $D' \equiv D$.

4.4.14 Proposition. *(1) La releation* $\equiv$ *est une relation d'équivalence.*

(2) $D \equiv 0$ *si est seulement si* $D = div(z), z \in \mathbb{F}(\mathcal{X})$.

(3) Si $D \equiv D'$, *alors* $deg(D) = deg(D')$.

(4) Si $D \equiv D'$ *et* $D_1 \equiv D'_1$, *alors* $D + D_1 \equiv D' + D'_1$.

(5) Soit C *une courbe plane. Alors* $D \equiv D'$ *si est seulement si il existe deux courbes* G *et* G' *de même degré tels que* $D + div(G) = D' + div(G')$

Preuve. (1) et (4) sont laissées aux lecteurs. Pour (5), il suffit d' écrire $z = G/G'$, ainsi $div(Z) = div(G) - div(G')$ dans ce cas. □

4.4.15 Définition. Soit D un diviseur d'une courbe $\mathcal{X}$. On définit l'ensemble $\mathcal{L}(D)$ sur $\mathbb{F}(\mathcal{X})^*$ par

$$\mathcal{L}(D) := \{f \in \mathbb{F}(\mathcal{X})^* : (f) + D > 0\} \cup \{0\}.$$

On note par $l(D)$ la dimension de l'espace vectoriel $\mathcal{L}(D)$

4.4.16 Remarque. Soit D un diviseur de $\mathcal{X}$. Alors

(a) $(f) \in \mathcal{L}(D) \Longleftrightarrow v_p(f) \geq -v_p(D)$ pout tout point P sur $\mathcal{X}$.

(b) $\mathcal{L}(D) \neq \{0\}$ si est seulement si il existe un diviseur $D' \equiv D$ tel que $D' \geq 0$.

4.4.17 Lemme. *Soit* D *un diviseur de* $\mathcal{X}$. *Alors*

(a) $\mathcal{L}(D)$ *est un espace vectoriel sur* $\mathbb{F}$.

(b) Si D' *est un diviseur tel que* $D' \equiv D$ *alors* $\mathcal{L}(D') \cong \mathcal{L}(D)$ *(isomorphe en tant qu'espace vectoriel.)*

(c) Si $D < D'$, *alors* $\mathcal{L}(D) \subset \mathcal{L}(D')$ *et* $dim_{\mathbb{F}}(\mathcal{L}(D')/\mathcal{L}(D)) \leq deg(D' - D.)$

(d) $\mathcal{L}(0) = \mathbb{F}$ *;* $\mathcal{L}(D) = 0$ *si* $deg(D) < 0$.

(e) $\mathcal{L}(D)$ *est de dimension finie pour tout* D. *Si* $deg(D) \geq 0$, *alors* $l(D) \leq deg(D) + 1$.

Preuve. (a) Soient f et $g \in \mathcal{L}(D)$ et $a \in \mathbb{F}$. Pour tout $P \in \mathcal{X}$, on a $v_p(f, g) \geq min\{v_p(f), v_p(g)\} \geq -v_p(D)$, donc $f + g \in \mathcal{L}(D)$. Puisque $v_p(af) = v_p(a) + v_p(f) = v_p(f) \geq -v_p(D)$, alors $af \in \mathcal{L}(D)$. D'où $\mathcal{L}(D)$ est un espace vectoriel.

(b) Par hypothèse, $D = D' + (f)$ avec $0 \neq f \in \mathbb{F}(\mathcal{X})$. On considère l'application

$$\psi : \begin{cases} \mathcal{L}(D) \longrightarrow \mathbb{F}(\mathcal{X}), \\ x \longmapsto xf \end{cases}$$

C'est une application $\mathbb{F}-$linéaire dont l'image est contenue dans $\mathcal{L}(D')$. De la même manière

$$\psi' : \begin{cases} \mathcal{L}(D') \longrightarrow \mathbb{F}(\mathcal{X}), \\ x \longmapsto xf^{-1} \end{cases}$$

est $\mathbb{F}-$linéaire de $\mathcal{L}(D)$ vers $\mathcal{L}(D')$. Ces applications sont inversibles entre eux, ainsi ψ est un isomorphisme entre $\mathcal{L}(D)$ et $\mathcal{L}(D')$.

(*c*) $D' = D + P_1 + \cdots + P_s$ et $\mathcal{L}(D) \subset \mathcal{L}(D + P_1) \subset \cdots \subset \mathcal{L}(D + P_1 + \cdots + P_s)$, ainsi il suffit de montrer que $dim(\mathcal{L}(D + P)\mathcal{L}(D)) \leq 1$. En effet soit t un paramètre local de $\mathcal{O}_P(\mathcal{X})$, et $r = n_p$ le coefficient de P dans D. On définit l'application $\varphi : \mathcal{L}(D + P) \longrightarrow \mathbb{F}$ par $\varphi(f) = (t^{r+1}f)(P)$; ainsi $ord_P(f) \geq -r - 1$, elle est bien définit. φ est une application linéaire et $Ker(\varphi) = \mathcal{L}(D)$, ainsi φ induit une application linéaire bi-univoque $\overline{\varphi} : \mathcal{L}(D + P)/\mathcal{L}(D) \longrightarrow \mathbb{F}$ ce qui donne le résultat.

(*d*) On a $(f) = 0$ pour $0 \neq f \in \mathbb{F}$, par conséquent $\mathbb{F} \subseteq \mathcal{L}(0)$. Inversement, si $0 \neq f \in \mathcal{L}(0)$ alors $(f) \geq 0$. C'est-à-dire (f) n'a pas de pôles, ainsi $f \in \mathbb{F}$. Supposons qu'il existe un élément $0 \neq f \in \mathcal{L}(D)$. Alors $(f) \geq -D > 0$, ce qui implique que f a au moins un zéro mais n'a pas de pôle, c'est impossible.

(e) Si $deg(D) = n \geq 0$, choisissons $P \in \mathcal{X}$ et posons $D' = D - (n + 1)P$. Alors $\mathcal{L}(D') = 0$, et par (c), $dim_{\mathbb{F}}(\mathcal{L}(D)/\mathcal{L}(D')) \leq deg(D' - D) = n + 1$ □

4.4.18 Définition. Soient D un diviseur de $\mathcal{X}$ et $\mathbb{F}(\mathcal{X})$ le corps de fonctions sur $\mathbb{F}$. On appelle dimension de D, le nombre $dim(D) := dim\mathcal{L}(D)$ et le genre g de $\mathbb{F}(\mathcal{X})$ est définit par

$$g := \{\deg(D) - dim(D) + 1/D \in Div(\mathcal{X}).\}$$

Le genre g de $\mathbb{F}(\mathcal{X})$ est un entier positif. En effet, si on remplace $D = 0$ dans la définition de g, on a $deg(0) - dim(0) + 1 = 0$, donc $g \geq 0$.

4.4.19 Théorème (Théorème de Riemann)**.** *Soit $\mathbb{F}(\mathcal{X})$ un corps de fonction de genre g.*

(a) Pour tout diviseur D de $\mathcal{X}$, on a

$$dim(D) \geq deg(D) + 1 - g.$$

(b) Il existe un entier N tel que pour tous diviseurs D de degré¿N,

$$dim(D) = deg(D) + 1 - g.$$

Preuve. (*a*) C'est juste la définition de g.

(*b*) on choisit un diviseur D_0 avec $g = deg(D_0) - dim(D_0) + 1$ et on pose $N := deg(D_0) + 1$. Si $deg(D) \geq N$ alors

$$dim(D - D_0) \geq deg(D - D_0) + 1 - g \geq N - deg(D_0) + 1 - g \geq 1.$$

Ainsi il existe un élément $0 \neq f \in \mathcal{L}(D - D_0)$. Considérons le diviseur $D' := D + (f)$ qui est $\geq D_0$. On a $deg(A) - dim(D) = deg(D') - dim(D')$ (d'après le lemme précédent) $\geq deg(D_0) - dim(D_0) = g - 1$. Donc $dim(D) \leq deg(D) + 1 - g$. □

4.5 Différentiel sur une courbe

Soit $\mathcal{X}$ une courbe irréductible non-singulière sur le corps de fonction $\mathbb{F}(\mathcal{X})$.

4.5.20 Définition. soit $\mathcal{V}$ un espace vectoriel sur $\mathbb{F}(\mathcal{X})$. Une application $\mathbb{F}-$linéaire $D : \mathbb{F}(\mathcal{X}) \longrightarrow \mathcal{V}$ est appelée une dérivation s'il satisfait la règle du produit

$$D(fg) = fD(g) + gD(f).$$

4.5.21 Définition. On note par $Der(\mathcal{X}, \mathcal{V})$ l'ensemble de toutes la dérivation $D : \mathbb{F}(\mathcal{X}) \longrightarrow \mathcal{V}$. Et si $\mathcal{V} = \mathbb{F}(\mathcal{X})$, $Der(\mathcal{X}, \mathcal{V})$ sera notée par $Der(\mathcal{V})$.

Si $D_1, D_2 \in Der(\mathcal{X}, \mathcal{V})$, on définit la somme de D_1 et de D_2 par $(D_1 + D_2)(f) = D_1(f) + D_2(f)$. Le produit de $D \in Der(\mathcal{X}, \mathcal{V})$, est définit par $(fD)(g) = fD(g)$ avec $f \in \mathcal{X}$. Ainsi $D \in Der(\mathcal{X}, \mathcal{V})$ est un espace vectoriel sur $\mathbb{F}(\mathcal{X})$.

4.5.22 Définition. Une forme rationnelle différentielle sur $\mathcal{X}$ est une application $\mathbb{F}$-linéaire de $Der(\mathcal{V})$ vers $\mathbb{F}(\mathcal{X})$. On note par $\Omega(\mathcal{X})$ l'ensemble de les toutes formes rationnelles différentielles.

Donc $\Omega(\mathcal{X})$ devient aussi un espace vectoriel sur $\mathbb{F}(\mathcal{X})$. Soit l'application $d : \mathbb{F}(\mathcal{X}) \longrightarrow \Omega(\mathcal{X})$. Pour $f \in \mathbb{F}(\mathcal{X}$, le différentiel $df : Der(\mathcal{X} \longrightarrow \mathbb{F}(\mathcal{X})$ est définit par $df(D) = D(f)$ pour tout $D \in Der(\mathcal{X})$. Donc d est une dérivation.

Pour chaque point P avec paramètre local t_P, une différentielle w peut représenter d'une seule manière comme $w = f_P dt_P$, où f_P est une fonction rationnelle. Cela donne une sens à la définition suivante.

4.5.23 Définition. Le diviseur (w) d'une différentielle w est définit par

$$(w) = \sum_{P \in \mathcal{X}} v_P(w)P.$$

où $w = f_P dt_P$ est une représentation locale de w et v_P est la valuation sur O_P.

On note par $W = (w)$. Alors W est appelé diviseur canonique.
Si w' est une autre différentielle non nulle dans $\Omega(\mathcal{X})$, alors $w' = fw$ pour chaque fonction rationnelle f. Ainsi $(w') = (f) + (w)$ et $(w') \equiv (w)$. Inversement si $W' = W$, c'est-à-dire $W' = (f) + W$, alors $W' = (fw)$. Ainsi les diviseurs canoniques forment une classe d'évalence sous l'équivalence linéaire.

4.5.24 Définition. Soit $\mathcal{X}$ courbe projective non-singulière sur $\mathbb{F}$. On définit par $g := l(W)$ le genre de $\mathcal{X}$, où $l(W)$ est la dimension de $\mathcal{L}(W)$.

4.5.25 Exemple. On considère une différentielle dx sur une ligne projective. Alors dx est regulière à tous points $P_a = (a : 1)$, ainsi $x - a$ est un paramètre local dans P_a et $dx = d(x - a)$. Soit $Q = (1 : 0)$ un point à l'infini. Alors $t = 1/x$ est un paramètre local dans Q et $dx = -t^{-2}dt$. Ainsi $v_Q(dx) = -2$. Par conséquent $(dx) = -2Q$ et $l(-2Q) = 0$. D'où la ligne projective est de genre zéro.

Maintenant, on a le théoreème suivant qu'on laisse au lecteur sa démonstration.

4.5.26 Théorème. *Si $\mathcal{X}$ est une courbe projective non singulière de degré m dans $\mathbb{P}^2$, alors*

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

4.5.27 Définition. Soit P un point de $\mathcal{X}$, avec un paramètre local t. Chaque élément $f \in \mathbb{F}(\mathcal{X})$ peut s'écrire d'une manière unique comme $f = \sum_{i=m}^{\infty} a_i t^i$ avec $a_i \in \mathbb{F}$ pour chaque entier m. Pour chaque différentiel w de $\mathcal{X}$, on écrit $w = fdt$. On définit $res_P(w) := a_1$

4.5.28 Théorème. *Si ω est une différentielle sur courbe projective non singulière $\mathcal{X}$, alors*

$$\sum_{P\mathcal{X}} Res_P(\omega) = 0.$$

4.5.29 Théorème (Théorème de Riemann Roch)**.** *. Soit D un diviseur sur une courbe projective non singulière de genre g. Alors pour chaque diviseur canonique W*

$$l(D) - l(W - D) = deg(D) - g + 1.$$

4.5.30 Corollaire. *Pour un diviseur canonique W, on a $deg(W) = 2g - 2$ et $l(W) = g$*

Preuve. Pour $D = 0$, d'après le théorème de Riemann-Roch, on a $1 = l(0) = deg(0) - g + 1 + l(W - 0)$. D'où $l(W) = g$.

On pose $D = W$, on a $g = l(W) = deg(W) - g + 1 + l(W - W) = deg(W) - g + 2$. D'où $de(W) = 2g - 2$. □

4.5.31 Théorème. *Si D est le diviseur de $\mathcal{X}$ de degré $\geq 2g - 1$ alors*

$$l(D) = degD + 1 - g$$

Preuve.

On a $l(D) = degD + 1 - g + l(W - D)$, où W est un diviseur canonique. Comme $degD \geq 2g - 1$ et $degW = 2g - 2$,d'après le théorème de Riemann Roch, alors $deg(W - D) < 0$. Par conséquent $l(W - D) = 0$. Ainsi $l(D) = degD + 1 - g$. □

Dans la section suivante, on va donner quelques propriétés des pôles de nombres dont elles sont l'une des conséquences du théorème de Riemann-Roch. On aura besoin de cette section pour la résolution de notre problème.

4.6 Pôle de nombres

4.6.32 Proposition. *Soit $\mathbb{F}(\mathcal{X})$ un corps de fonction algébrique de genre $g > 0$ où $\mathbb{F}$ est un corps fini et soit P un point de $\mathcal{X}$. Alors, pour tout $n > 2g$, il existe un élément $x \in \mathcal{X}$ avec diviseur de pôle $(x)_\infty = nP$.*

Preuve. D'après le théorème précédent, on sait que $dim((n-1)P) = (n-1)degP + 1 - g$ et $dim((n)P) = n.degP + 1 - g$. Donc $\mathcal{L}((n-1)P) \subsetneqq \mathcal{L}(nP)$. Il existe un élément $x \in \mathcal{L}(nP)/\mathcal{L}((n-1)P)$ qui a un diviseur de pôle nP. □

4.6.33 Définition. Soit Q un point de $\mathcal{X}$. Un entier n est appelé pôle de nombres de Q, si est seulement si, il existe un élément $\phi_n \in \mathcal{X}$ tel que $(\phi_n)_\infty = nQ$.

4.6.34 Définition. Si $l(nQ) = l((n-1)Q)$, alors n est appelé un (Weierstrass) gap de Q, où $l(nQ)$ est la dimension l'espace vectoriel $\mathcal{L}(Q)$

4.6.35 Définition. Un entier positif qui n'est pas gap est appelé un nongap de Q. On l'appelle aussi pôle de nombres.

L'ensemble $PN(Q) = \{o_i \geq 0 / o_i : \text{pôle de nombres de Q}\}$ est un sous semi-groupe d'un semi-groupe de $\mathbb{N}$. C'est-à-dire, si $o_i, o_j \in PN(Q)$ alors $o_i + o_j \in PN(Q)$. Et on a $(\phi_{o_i+o_j})_\infty = (o_i + o_j)Q$. Il se peut que $\phi_{o_i}\phi_{o_j} \neq \phi_{o_i+o_j}$.

4.6.36 Proposition. *Soit $Q \in \mathbb{P}_F$. $o_i \geq 0$ est un pôle de nombres de Q si est seulement si $l(o_iQ) \neq l(o_i - 1)Q)$.*

Preuve. C'est juste la définition. □

4.6.37 Théorème. *On suppose que $\mathbb{F}(\mathcal{X})$ un corps de fonction algébrique de genre $g > 0$ où $\mathbb{F}$ est un corps fini et P est une place de degré un. Alors il y a exactement g gaps $i_1 < i_2 < \cdots < i_g$ de P. On a*

$$i_1 = 1 \text{ et } i_g \leq 2g - 1$$

Preuve. Tout le gap de P est $\leq 2g-1$ d'après la proposition précédente. En effet si n est nongap de P alors $n \geq 2g$, donc tout le gap de P est $\leq 2g - 1$. Il est clair que 0 est nongap. On a vu que i est le gap de P $\Leftrightarrow l((i-1)P) = l(iP)$.

Maintenant, on considère la suite d'espace vectoriel

$$K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \cdots \subseteq (2g-1)P. \tag{4.12}$$

où $dim\mathcal{L}(0) = 1$ et $dim((2g-1)P) = (2g-1).degP + 1 - g = (2g-1) + 1 - g = 1$ par le théorème précédent. Puisque

$$dim\mathcal{L}(iP) - dim\mathcal{L}((i-1)P) \leq \mathcal{L}deg(iP) - deg((i-1)P) = i - (i-1) = 1$$

alors

$$dim\mathcal{L}(iP) \leq dim((i-1)P) + 1$$

pour tout i. Ainsi, on a exactement $g-1$ nombres de $1 \leq i \leq 2g-1$ dans (7) avec $\mathcal{L}((i-1)P) \subsetneqq \mathcal{L}(iP)$. Donc les g restants ne sont pas des pôles de nombres de P.

Finalement, il faut montrer que 1 ne soit pas un pôle de nombre. Supposons que 1 n'est pas gap. Comme les pôles de nombres forment une semi-groupe additive, tout $n \in \mathbb{N}$ est nongap, il n'existe du tout aucun gaps. C'est une contradiction car $g > 0$. □

4.6.38 Lemme. *Les nongaps satisfont $i_0 = 0$,*

$$0 < i_1 < i_2 < \cdots < i_{g-1} < 2g$$

$$i_j = g + j \text{ pour } j = g, g+1, \ldots, m-g$$

Preuve. La preuve résulte du théorème précédent. □

Bibliographie

[FeT91] G.L.Feng and K. K. Tzeng, "A Generalization of the Berlekamp-Massey Algorithm for Multisequence Shift-Register Synthesis with Applications to Decoding Cyclic Codes,"*IEEE Trans. on Inform. Theory, vol. 37, pp.1274-1287, Sept 1991*

[Har86] S.Harari "New Codes from algebraic curves of genus 2" presented at the IEEE Int. Symp. Inform. Theory, Ann Arbor, Ml, Oct. 1986.

[HJL98] Tom Høholdt, Jacobus H, J.H. van Lint and Ruud Pellikaan, "Algebraic geometry codes," *in the Handbook of Coding Theory*, vol I, pp. 871-961,(V.S. Pless, W.C. Human and R.A. Brualdi Eds.), Elsevier, Amsterdam 1998. Corrected version, September 20, 2011.

[JLE92] J. Justesen, K. J. Larsen, H. Elbrdnd Jensen, and T. Hdholdt, "Fast Decoding of Codes from Algebraic Plane Curves," IEEE Trans. Inform. Theory, vol 38, pp. 111-119, Jan. 1992.

[KTV84] G.L.Katsman, M.A.Tsfasman, S.G. Vlãdut, and T.Zink,"*Modular curves, and codes with construction,"*, *IEEE Trans. on Inform. Theory,*,vol. IT-30,pp. 353-355, Mar.1984

[LFK94] Gui-Liang, Feng and Kenneth "Codes up to Actual Minimum Distance" IEEE Trans. Inform. Theory, vol 40, No.5, September. 1994.

[Lin88] J.H. van Lint, "Algebraic geometry codes," *in Coding Theory and Design Theory,* vol.20(IMA Volumes in Mathematics and Its Applications). New York : Springer, 1988, pp. 137-162.

[Pel89] R. Pellikaan, "On a decoding algorithm for codes on maximal curves," IEEE Trans. Inform. Theory, vol. 35, pp. 1228-1232, Nov. 1989.

[Sti98] H. Stichtenoth, "Algebraic function Felds and codes", Universitext, Springer, Berlin 1993.

[SVl90] A.N. Skorobogatov and S.G. Vlăduţ, "On the decoding of algebraicgeometric-codes," IEEE Trans. Inform. Theory, vol. 36, pp. 1051-1060, Nov. 1990.

[TaM01] Dr. Jhon Tate, D.B.Mcreynolds, "Algebraic Geometry, Spring 2001.

[TVZ82] .A.Tsfasman, S.G. Vlădut, and T.Zink,"*Modular curves, Shimura curves and Coppa codes, better than Varshamove-Gilbert bound,"*, *Math. Nahcr.*,vol. 104,pp. 13-28, 1982

Impétrant : RAKOTONINDRINA Zo Tsaratany

E-mail : zotsaratany@gmail.com

Tél : (+261)332522520

Titre : ALGORITHME ITERATIF FONDAMENTAL MODIFIE ET DECODAGE DES CODES HERMITIENS

Résumé : Ce mémoire consiste à présenter une procédure de décodage des codes algébriques pour une courbe hermitienne en faisant une simple modification d'un algorithme d'itération, à savoir l'algorithme itératif fondamental. Nous avons vu que cette procédure peut décoder un code hermitien de longueur n jusqu'à $[d^* - 1]/2$ erreurs.

Mots clés : Courbes algébriques, Codes algébriques, Décodage.

Abstract : This report consists in presenting an decoding procedure of the algebraic codes for the hermitian curve by making a simple modification of an algorithm of iteration, namely the fundamental iterative algorithm. We saw that this procedure can decode a hermitian code with length n, until $[d^* - 1]/2$ errors.

KeyWords : Algebraic curves, Algebraic codes, Decoding.

Encadreur : Mr ANDRIATAHINY Harinaivo
Maître de conférences
Mention : Mathématiques et Informatique
Sciences et technologies
Université d'Antananarivo
E-mail : aharinaivo@yahoo.fr