N d'ORDRE : 03/2012-D/MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET
DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE
Faculté de Mathématiques

THÈSE

Présentée pour l'obtention du grade de Docteur
EN: MATHÉMATIQUES
Spécialité : Algèbre et Théorie des Nombres
Par

CHERCHEM AHMED

SUITES RÉCURRENTES LINÉAIRES SUR DES ANNEAUX NON COMMUTATIFS ET REPRÉSENTATIONS DES CODES QUASI-CYCLIQUES

Soutenue publiquement, le 13 Juin 2012, devant le jury composé de :

M. Farid BENCHERIF, Maître de Conférences/A à l'USTHB	Président
M. Thierry BERGER, Professeur à l'université de Limoges	Directeur de Thèse
M. André LEROY, Professeur à l'université d'Artois	Examinateur
M. Boualem BENSEBAA, Maître de Conférences/A à l'USTHB	Examinateur
M. Abdelkader Necer, Maître de Conférences à l'université de Limoges	Invité

Remerciements

J'exprime ma profonde gratitude à mon directeur de thèse Thierry Berger qui m'a fait l'honneur d'accepter de diriger ma thèse et pour son soutien sans faille durant toute sa préparation.

Je voudrais adresser mes sincères remerciements à Farid Bencherif qui me fait l'honneur de présider mon jury de thèse.

Je remercie vivement André Leroy qui a répondu favorablement à ma demande de participation au jury. J'apprécie particulièrement sa présence dans le jury en tant que spécialiste reconnu des anneaux non commutatifs.

Un grand merci également à Boualem Bensebaa qui a bien voulu accepter de faire partie de ce jury.

Je veux dire toute ma reconnaissance à Abdelkader Necer, qui a inspiré ce travail puis l'a accompagné et enrichi de nombreux apports. Je le remercie aussi d'avoir accepté de faire partie de mon jury.

Durant mes stages à l'université de Limoges, j'ai souvent été invité à partager la table des Necer. Je voudrais leur dire ici toute ma reconnaissance, tant j'ai toujours été accueilli comme un membre de la famille. Merci à Djahida et Manou et grosses bises à Yesmine et Wassim.

Je garde un fameux souvenir d'un terrible Algerie-Egypte que j'ai vu avec Fayçal et sa bande de copains qui ont véritablement explosé à la fin de la rencontre !

Je n'ai pas oublié Tito qui se faisait réprimander à chaque fois qu'il approchait son museau de moi.

Merci à Kader Beldi pour son immense gentillesse.

Merci à François Laubie qui m'a souvent accueilli dans son bureau et qui a su me mettre à l'aise avec générosité et simplicité.

Merci à Tarek Garici qui a travaillé avec moi avec enthousiasme. Je le remercie pour ses nombreuses contributions et je lui souhaite de soutenir sa thèse dans les meilleurs délais.

Merci à Larbi Benaissa et Noureddine Hannoun pour leur aide désintéressée dans la traduction de l'article publié dans *JAA*.

Ce projet n'aurait pu être concrétisé sans le dévouement de mon épouse Leila. Elle m'a d'abord poussé à m'inscrire puis m'a soutenu durant toutes ces années, me libérant souvent de nombreuses contraintes pour me permettre de me consacrer à mon travail de thèse. Merci encore pour les longues heures passées à chercher à comprendre pourquoi-ça-ne-veut-pas-compiler. Merci également à Aghis qui emplit notre maison de bonheur et d'enthousiasme. Je lui souhaite tout de même de se découvrir d'autres passions que le foot...

Merci aux participants du séminaire d'Arithmétique à l'USTHB qui ont écouté mes exposés avec patience et intérêt et qui ont nourri mes réflexions.

Merci à tous ceux qui ont tant donné à l'Université algérienne sans rien attendre en retour.

Table des matières

Introduction

Cette thèse est consacrée à l'étude des suites récurrentes linéaires sur des anneaux non commutatifs et à la construction de codes quasi-cycliques en utilisant des propriétés qui en découlent. Si les suites récurrentes linéaires sont bien connues dans le cas commutatif, elles le sont moins bien dans le cas général et leur étude dans le cas non commutatif est, à notre connaissance, très récente. Il en va de même de la construction de codes quasi-cycliques à partir de cette étude. Les premiers résultats datent en effet de 2010 (cf. [7]).

Dans le chapitre 1 de ce travail, nous commençons par des rappels de notions fondamentales de la théorie des codes linéaires. Les codes correcteurs d'erreurs ont pour objet l'étude de la transmission de l'information à travers un canal bruité. Ils constituent un bon outil pour corriger les erreurs lors de transmissions de données et sont ce titre indispensables dans plusieurs domaines comme en haute technologie, internet, téléphonie, aéronautique, secteur saptial, etc. C'est un théorème de probabilités, dû à Shannon, qui signe en 1948 la naissance de cette théorie qui fera par la suite appel à des domaines aussi variés que la combinatoire, l'algèbre linéaire, la géométrie algébrique, etc.
D'abord, nous introduisons les notions fondamentales de la théorie des codes linéaires tels que : matrice génératrice, matrice de contrôle, distance minimale, etc. Ensuite, nous nous intéressons aux codes cycliques. Ces codes possèdent une structure algébrique remarquable puisqu'ils peuvent être vus comme idéaux d'un anneau (quotient) de polynômes. De plus, les codes quasi-cycliques aux-

quels nous nous intéressons en sont la généralisation. Signalons que, outre la richesse de leur structure algébrique, les codes quasi-cycliques sont intéressants pour deux raisons fondamentales. En premier lieu, ce sont de *bons* codes, c'est-à-dire qu'ils ont les meilleures distances minimales [24]. En second lieu, ces codes sont utilisés en cryptographie dans le cryptosystème de McEliece. Dans cette thèse, nous nous intéressons à la structure algébrique de cette famille de codes. Depuis leur apparition vers la fin des années 60, il y a eu différentes représentations de ces codes. Nous présenterons la description de S. Ling et P. Solé qui utilisent le théorème des restes chinois puis la transformée de Fourier discrète.

Le chapitre 2 traite suites récurrentes linéaires sur des anneaux non commutatifs. Les suites récurrentes linéaires sont connues depuis fort longtemps, la plus célèbre étant sans doute la suite dite de Fibonacci dont on trouve la première trace dans le *Liber Abaci* dont la premire édition date de 1202 !

Depuis la fin du XIX^e siècle, ces suites ont été étudiées d'abord sur $\mathbb{Z}$, l'anneau des entiers rationnels, puis sur des corps commutatifs. On trouvera dans [16] une très bonne bibliographie et une longue liste d'applications intéressantes de ces objets (cryptologie, codes correcteurs d'erreurs, calcul rapide, arithmétique, etc.).

Pendant les années 1980, plusieurs auteurs ont travaillé sur des suites récurrentes linéaires sur des modules sur des anneaux commutatifs, voir [19] pour une bibliographie complète.

La notion de suite récurrente linéaire s'étend naturellement au cas de modules (à gauche) sur un anneau non nécessairement commutatif. Cette généralisation a trouvé des applications en théorie des codes correcteurs d'erreurs, en particulier dans la construction de codes quasi-cycliques auto-duaux [7], que l'on présentera dans le chapitre 3. Pour nous, l'objectif de départ était de généraliser des propriétés de suites récurrentes linéaires à valeurs dans un module sur un anneau commutatif au cas d'un anneau non nécessairement

commutatif. Mais il est apparu que dans le cas non commutatif, il y a perte de la stabilité de l'addition et de la multiplication par les scalaires usuelles. Plus précisément, soit A un anneau non commutatif et M un A-module. La somme de deux suites récurrentes linéaires à valeurs dans M et à coefficients dans A n'est pas toujours une suite récurrente linéaire sur A. Il en est de même de la multiplication d'une suite récurrente linéaire à valeurs dans M par les éléments de l'anneau A. Nous avons ainsi été amenés à poser la question suivante : sur quels types d'anneau conserve-t-on la strucure usuelle de $A[X]$ -module pour l'ensemble des suites récurrentes linéaires ? Nous donnons d'abord des conditions nécessaires pour que la somme de suites "géométriques " ainsi que la multiplication à gauche par les éléments de l'anneau soit une suite récurrente linéaire. Nous montrons que l'anneau de base, lorsqu'il est intègre, doit être nécessairement un anneau de Ore (voir aussi [10]).

Nous montrons ensuite que, dans le cas d'un anneau de matrices à coefficients dans un anneau commutatif, les suites récurrentes linéaires (de matrices ou de vecteurs) conservent la structure habituelle de $A[X]$-module. Ce qui permet la construction de codes quasi-cycliques auto-duaux citée précédemment. Nous abordons ensuite le cas où l'anneau de base A est un corps non commutatif. Nous montrons que dans ce cas également, l'ensemble des suites récurrentes linéaires à valeurs dans un A -module a une structure de $A[X]$-module. Nous nous intéressons plus particulièrement au cas où le corps est supposé de dimension finie sur son centre : grâce à un résultat de Jacobson [22], on donnera un algorithme de *dévissage* pour la détermination effective d'une relation de récurrence linéaire pour la somme de deux suites récurrentes linéaires.

La fin du chapitre est consacrée à la série génératrice d'une suite définie sur un corps non commutatif. Il est bien connu que la série génératrice d'une suite sur un corps commutatif est une une fraction rationnelle si, et seulement si, la suite est récurrente linéaire. Cette propriété a été démontrée, sous une forme appropriée, pour les suites récurrentes linéaires à valeurs dans un module sur

un anneau commutatif, voir [31], et pour les suites à coefficients matriciels, voir [5]. Nous étendons cette propriété au cas des corps non commutatifs.

Le chapitre 3 est consacré à des résultats récents concernant la représentation des codes quasi-cycliques en liaison avec les suites récurrentes linéaires. Dans [7], en considérant des suites récurrentes linéaires sur des anneaux de matrices à coefficients dans un corps fini, les auteurs parviennent à construire de nouveaux codes quasi-cycliques auto-duaux ayant les meilleures distances minimales connues pour les mêmes paramètres. Par la suite, dans [2], il est démontré que les codes quasi-cycliques peuvent être regardés comme analogues des codes cycliques : ce sont des idéaux engendrés par des polynômes générateurs à coefficients matriciels.

Si on désigne, comme d'habitude, par q une puissance d'un nombre premier, $\mathbb{F}_q$ le corps à q éléments et par ℓ et m des entiers naturels positifs, alors il y a une correspondance bijective entre les codes ℓ-quasi-cycliques de longueur $m\ell$ sur $\mathbb{F}_q$ et les idéaux de l'anneau des polynômes à coefficients matriciels $\mathbb{M}_\ell(\mathbb{F}_q)[X]/(X^m-1)$. Cette correspondance a permis de déduire que l'anneau $\mathbb{M}_\ell(\mathbb{F}_q)[X]/(X^m-1)$ est principal (idéaux principaux). Cette interprétation des codes quasi-cycliques a donné lieu à de nouvelles notions telles que les codes quasi-BCH. Elle a aussi pour résultat la construction de nouveaux codes ayant les meilleurs distances minimales tels que le code de paramètres $[189, 11, 125]_{\mathbb{F}_4}$ et 48 autres codes dérivés.

Chapitre 1

Codes linéaires, codes quasi-cycliques

1.1 Introduction

La théorie des codes correcteurs d'erreurs a pour objet l'étude de la transmission de l'information à travers un canal bruité. C'est un théorème de Probabilités, dû à Shannon, qui signe en 1948 la naissance de cette théorie qui fera par la suite appel à des domaines aussi variés que la Combinatoire, l'Algèbre Linéaire, la Géométrie algébrique, etc.

Dans ce chapitre, nous introduisons les notions fondamentales de la théorie des codes linéaires tels que : matrice génératrice, matrice de contrôle, distance minimale, etc. Ensuite, nous nous intéressons aux codes cycliques. Ces codes possédent une structure algébrique remarquable puisqu'ils peuvent être vus comme idéaux d'un quotient d'un anneau de polynômes. La dernière partie de ce chapitre est consacrée à la présentation des codes quasi-cycliques. Cette famille de codes, qui constitue une généralisation de la famille des codes cycliques, est intéressante puisqu'elle donne lieu à des codes ayant les meilleurs distances minimales. Depuis leur apparition vers la fin des années 60, il y a

eu différentes représentations des codes quasi-cycliques. Nous présenterons la description de S. Ling et P. Solé qui utilisent le Théorème Chinois puis la Transformée de Fourier discrète.

1.2 Généralités sur les codes linéaires

Dans tout le chapitre, q est une puissance d'un nombre premier p et $\mathbb{F}_q$ désigne le corps fini à q éléments.

Dans cette section, nous rappelons quelques notions fondamentales de la théorie des codes linéaires sur un corps fini.

Définition 1.1 *Soit n et k deux entiers positifs tels que $k \leq n$. Un* code linéaire sur $\mathbb{F}_q$ de longueur n et de dimension k *est un sous-espace vectoriel de dimension k de $\mathbb{F}_q^n$. Un élément du code est appelé* mot.

Soit $x, y \in \mathbb{F}_q^n$. Notons $x = (x_1, \cdots, x_n)$ et $y = (y_1, \cdots, y_n)$. La *distance de Hamming* entre x et y est définie par

$$d(x, y) = \#\{i \in \mathbb{N}, 1 \leq i \leq n : x_i \neq y_i\}.$$

Ceci définit une distance au sens usuel.

Définition 1.2 *La* distance minimale *d'un code linéaire $\mathcal{C}$ est l'entier d donné par :*

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

La distance minimale d'un code est un paramètre fondamental. Son importance découle du résultat suivant.

Proposition 1.1 *Soit $\mathcal{C}$ un code linéaire de distance minimale d. Si t est un entier tel que $d \geq 2t + 1$, alors le code $\mathcal{C}$ corrige jusqu'à t erreurs.*

Preuve : Soit x le mot envoyé et y le mot reçu. On suppose qu'il y a moins de t erreurs, i.e. $d(x,y) \leq t$. Alors x est le seul mot du code correspondant à y. En effet, si z est un mot du code $\mathcal{C}$, vérifiant $d(z,y) \leq t$, alors

$$d(x,z) \leq d(x,y) + d(y,z) \leq 2t \leq d-1 < d$$

d'où $x = z$.

□

Un code linéaire de longueur n et de dimension k est noté $[n,k]$ code. Si, de plus, sa distance minimale est d, on note $[n,k,d]$ code.

Pour $x \in \mathbb{F}_q^n$, le *poids* $w(x)$ de x est le nombre de coordonnées non nulles de x. Le *poids minimal* w d'un code $\mathcal{C}$ est alors défini par

$$w = \min\{w(x) : x \in \mathcal{C}, x \neq 0\}.$$

En fait, pour un code linéaire, la distance minimale du code coincide avec son poids minimal.

Pour n et k fixés, on obtient facilement la majoration suivante de la distance minimale d, appelée *borne de Singleton.*

Proposition 1.2 *Soit n, k et d des entiers positifs et soit $\mathcal{C}$ un $[n,k,d]$ code. Alors*

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

Preuve : Soit E l'ensemble de tous les vecteurs de $\mathbb{F}_q^n$ dont les $k-1$ dernières coordonnées sont nulles. C'est un $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension $n-k+1$. On a donc

$$\dim(\mathcal{C}) + \dim(E) = n + 1 > n.$$

Par suite, il existe $x \in \mathcal{C} \cap E, x \neq 0$, et on a clairement $w(x) \leq n - k + 1$.

On en déduit que $d \leq n - k + 1$.

□

Lorsque la borne de Singleton est atteinte, le code linéaire est dit *MDS.* (Maximum Distance Separable)

Définition 1.3 *Une matrice génératrice d'un* $[n, k]$ *code* $\mathcal{C}$ *est une matrice à* k *lignes et* n *colonnes dont les lignes forment une base de* $\mathcal{C}$ *sur* $\mathbb{F}_q$.

Une matrice génératrice G est dite de forme standard (ou systématique) si elle est de la forme :

$$G = (I_k \; P),$$

où I_k est la matrice identité d'ordre k et P une matrice à k lignes et $n - k$ colonnes.

Définition 1.4 *Pour* $x, y \in \mathbb{F}_q^n$, *notons* $x = (x_1, \cdots, x_n)$ *et* $y = (y_1, \cdots, y_n)$. *L'application*

$$\mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$$

$$(x, y) \mapsto < x, y >= \sum_{i=1}^{n} x_i y_i.$$

est appelée produit scalaire euclidien *sur* $\mathbb{F}_q^n$.

Définition 1.5 *Le* code dual $\mathcal{C}^\perp$ *d'un* $[n, k]$ *code* $\mathcal{C}$ *est le code linéaire défini par*

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

La dimension du code dual $\mathcal{C}^\perp$ d'un $[n, k]$ code $\mathcal{C}$ est égale à $n - k$. Si $\mathcal{C}^\perp = \mathcal{C}$, le code est dit *auto-dual.* Une matrice génératrice H du code dual $\mathcal{C}^\perp$ est appelée *matrice de contrôle* de $\mathcal{C}$. Le sens de cette définition apparaît à travers la caractérisation des mots du code qui est précisée dans la proposition qui suit.

Proposition 1.3 *Soit $\mathcal{C}$ un code linéaire de longueur n sur $\mathbb{F}_q$ et soit H sa matrice de contrôle. Alors*

$$\forall x \in \mathbb{F}_q^n, x \in \mathcal{C} \Longleftrightarrow H^t x = 0.$$

Autrement dit, le code $\mathcal{C}$ est le noyau de l'application définie par la matrice H.

Si $G = (I_k \ P)$ est une matrice génératrice standard d'un $[n, k]$ code $\mathcal{C}$, alors la matrice

$$H = \left(-{}^t P \ I_{n-k}\right)$$

est une matrice génératrice du code dual $\mathcal{C}^\perp$.

Notons encore qu'une matrice de contrôle d'un code linéaire a la propriété remarquable de permettre la détermination de la distance minimale du code, qui est égale au nombre minimum de ses colonnes linéairement dépendantes. Une matrice de contrôle peut aussi être utilisée pour le décodage. Soit $\mathcal{C}$ un $[n, k]$ code et H une matrice de contrôle de $\mathcal{C}$. Soit $x \in \mathbb{F}_q^n$. Le *syndrome de* x est par définition le vecteur $x^t H \in \mathbb{F}_q^{n-k}$. Soit $\mathcal{R}$ la relation d'équivalence définie sur $\mathbb{F}_q^n$ par

$$x \mathcal{R} y \Leftrightarrow x^t H = y^t H \Leftrightarrow x - y \in \mathcal{C}.$$

Soit x le message envoyé et soit $y = x + e$ le message reçu, où e est le vecteur erreur. Alors $y - e \in \mathcal{C}$, ce qui signifie que y et e ont le même syndrome. En utilisant le principe du maximum de vraisemblance, on corrigera y en choisissant dans sa classe un vecteur erreur de poids minimal : c'est le *coset leader*. Nous voyons là, en plus de l'utilisation des outils de l'Algèbre Linéaire, un autre intérêt de l'introduction de la structure d'espace vectoriel : pour un $[n, k]$ code, il y a q^k mots et q^n vecteurs qui peuvent être reçus. Pour retrouver le mot envoyé, il suffit de connaître les q^{n-k} coset leaders. En l'absence de structure, il faudrait chercher le vecteur erreur parmi les q^n

vecteurs possibles. D'autres avantages des structures algébriques apparaîtront lorsqu'on présentera les codes cycliques et les codes quasi-cycliques.

Exemple 1.1 *On veut envoyer le message* (x_1, x_2, x_3) *où* $x_i \in \mathbb{F}_2$. *On envoie* $x = (x_1, x_2, \cdots, x_6)$ *avec*

$$\begin{aligned} x_4 &= x_2 + x_3, \\ x_5 &= x_1 + x_3, \\ x_6 &= x_1 + x_2. \end{aligned}$$

Si x *est le message envoyé et* $y = x + e$ *est le message reçu, où* $e = (e_1, \ldots, e_6)$ *est le vecteur erreur, on aura :*

$$\begin{aligned} e_2 + e_3 + e_4 &= y_2 + y_3 + y_4 = s_1, \\ e_1 + e_3 + e_5 &= y_1 + y_3 + y_5 = s_2, \\ e_1 + e_2 + e_6 &= y_1 + y_2 + y_6 = s_3. \end{aligned}$$

On peut vérifier directement que si une seule erreur survient elle est ***détectée*** *et* ***corrigée.*** *Par exemple, si* $(s_1, s_2, s_3) = (1, 1, 0)$, *alors* $e = (0, 0, 1, 0, 0, 0)$ *est l'unique solution de poids* 1.
En fait, il s'agit ici d'un $[6, 3]$ *code* $\mathcal{C}$ *sur* $\mathbb{F}_2$ *de distance minimale* $d = 3$ *et de matrice génératrice standard*

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

On en déduit la matrice de contrôle

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

Le vecteur (s_1, s_2, s_3) *est le syndrome de* y.

Dans ce qui suit, nous allons rappeler quelques procédés qui permettent de construire de nouveaux codes à partir de codes donnés.

Définition 1.6 *Soit* $\mathcal{C}$ *un* $[n, k, d]$ *code. Le* code étendu $\widehat{\mathcal{C}}$ *de* $\mathcal{C}$ *est le code de longueur* $n+1$ *sur* $\mathbb{F}_q$ *formé des mots de la forme* $(c_1, \cdots, c_n, c_{n+1})$, *où* $(c_1, \cdots, c_n) \in \mathcal{C}$ *et* $c_{n+1} = -\sum_{i=1}^{n} c_i$.

Le code étendu $\widehat{\mathcal{C}}$ de $\mathcal{C}$ est de dimension k et de distance minimale d ou $d+1$. Inversement, on définit un *code tronqué d'un code* $\mathcal{C}$ en supprimant une ou plusieurs coordonnées de chaque mot de $\mathcal{C}$.

Pour $i \in \{1, 2\}$, soit $\mathcal{C}_i$ un $[n_i, k_i, d_i]$ code sur $\mathbb{F}_q$. Alors la *somme directe* de $\mathcal{C}_1$ et $\mathcal{C}_2$ est le $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]$ code donné par

$$\mathcal{C}_1 \oplus \mathcal{C}_2 = \{(\mathbf{c}_1, \mathbf{c}_2) : \mathbf{c}_1 \in \mathcal{C}_1, \mathbf{c}_2 \in C_2\}.$$

Si G_i et H_i désignent respectivement une matrice génératrice et une matrice de contrôle du code $\mathcal{C}_i$, alors les matrices

$$G = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix} \text{ et } H = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}$$

sont respectivement une matrice génératrice et une matrice de contrôle du code $\mathcal{C}_1 \oplus \mathcal{C}_2$.

Exemple 1.2 *Le* code binaire de Golay *est le code engendré par la matrice*

standard $G = (I_{12}\ A)$, *où*

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

C'est un $[23, 12, 7]$ code. Le code de Golay étendu est un $[24, 12, 8]$ code et une matrice génératrice de ce code peut être obtenue en rajoutant à G une colonne de sorte que la somme des coordonnées de chaque ligne soit nulle.

1.3 Codes cycliques

Le paramètre d est fondamental pour un code linéaire : si n et k sont fixés, un *bon* code est un code ayant la plus grande valeur possible d, c'est-à-dire la plus grande capacité de correction d'erreurs. Un autre paramètre important est l'existence d'un algorithme de décodage efficace, ce qui revient à déterminer le mot envoyé à partir du mot reçu en un temps raisonnable. Tenant compte de ces deux paramètres, la famille des codes cycliques fournit quantité de codes intéressants tels que les codes BCH, codes de Reed-Solomon, etc.

Définition 1.7 *Un code linéaire $\mathcal{C}$ de longueur n sur $\mathbb{F}_q$ est dit* cyclique *s'il*

vérifie

$$\forall\,(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}, (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

Autrement dit, tout mot de $\mathcal{C}$ est stable par décalage circulaire.

On a l'identification :

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n \longleftrightarrow c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x] / (x^n - 1).$$

On pourra donc parler de mot-code c comme mot-code $c(x)$ en utilisant cette identification. Remarquons que la multiplication par x correspond au décalage circulaire.

La proposition suivante est une caractérisation des codes cycliques.

Proposition 1.4 *Un $[n, k]$ code $\mathcal{C}$ sur $\mathbb{F}_q$ est cyclique si et seulement si $\mathcal{C}$ est un idéal de $\mathbb{F}_q[x] / (x^n - 1)$.*

L'anneau $\mathbb{F}_q[x] / (x^n - 1)$ étant principal, tout code cyclique $\mathcal{C}$ est engendré par un unique polynôme unitaire $g(x)$ de degré inférieur ou égal à $n - 1$.

Définition 1.8 *Le polynôme $g(x)$ est appelé* polynôme générateur *du code $\mathcal{C}$.*

Le polynôme générateur est un diviseur du polynôme $x^n - 1$. Supposons que $pgcd(n, q) = 1$, et soit $x^n - 1 = f_1(x) f_2(x) \cdots f_t(x)$ la décomposition en produit de polynômes irréductibles. Les polynômes $f_1(x), f_2(x), \cdots, f_t(x)$ sont distincts. On peut ainsi déterminer tous les codes cycliques de longueur n sur $\mathbb{F}_q$ qui sont au nombre de 2^t.

Soit $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$ le polynôme générateur d'un code cyclique $\mathcal{C}$ de longueur n. Les polynômes $g(x), xg(x), \cdots, x^{k-1} g(x)$ forment

une base de $\mathcal{C}$, par conséquent la matrice

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots & \cdots & \cdots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}$$

est une matrice génératrice du code cyclique $\mathcal{C}$. La matrice G est dite *circulante*.

Définition 1.9 *Soit $\mathcal{C}$ un code cyclique de polynôme générateur $g(x)$, et soit $h(x) = (x^n - 1)/g(x)$. Le polynôme $h(x)$ est appelé* polynôme de contrôle *du code $\mathcal{C}$.*

On a clairement :

$$\forall c(x) \in \mathbb{F}_q[x] / (x^n - 1), c(x) \in \mathcal{C} \Leftrightarrow h(x) c(x) = 0.$$

Théorème 1.1 *Soit $\mathcal{C}$ un $[n, k]$ code cyclique sur $\mathbb{F}_q$ de polynôme générateur $g(x)$ et soit $h(x)$ son polynôme de contrôle. Alors le polynôme*

$$g^{\perp}(x) = \frac{1}{h(0)} x^k h\left(\frac{1}{x}\right)$$

est un polynôme générateur pour le code dual $\mathcal{C}^{\perp}$ de $\mathcal{C}$.

Exemple 1.3 *Prenons $n = 7$ et $q = 2$. La factorisation du polynôme $x^7 - 1$ sur $\mathbb{F}_2$ donne*

$$x^7 - 1 = (x + 1)\left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right).$$

Nous obtenons tous les codes cycliques de longueur 7 sur $\mathbb{F}_2$ en faisant tous les produits des facteurs irréductibles de $x^7 - 1$. Il y en a 8 en tenant compte du

code nul. Considérons le code $\mathcal{C}$ engendré par le polynôme

$$g(x) = (x+1)\left(x^3+x+1\right) = x^4+x^3+x^2+1.$$

On en tire la matrice génératrice

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

D'autre part, le polynôme $h(x) = (x^7-1)/g(x) = x^3+x^2+1$ est un polynôme de contrôle du code $\mathcal{C}$, ce qui donne le polynôme

$$g^{\perp}(x) = x^3 h\left(\frac{1}{x}\right) = x^3+x+1$$

qui est un polynôme générateur du code dual $\mathcal{C}^{\perp}$. D'où la matrice de contrôle du code $\mathcal{C}$:

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

Parmi les codes cycliques, les codes BCH constituent l'une des familles les plus importantes. Ces codes ont été découverts par R.C. Bose et D.K. Ray-Chaudhuri (1960), et, indépendamment par A. Hocquenghem (1959). Une sous-famille importante des codes BCH a été découverte à la même période par Reed et Solomon. Les codes de Reed-Solomon sont utilisés pour la lecture des CD et DVD.

Définition 1.10 (codes BCH) *Soit n, δ et b des entiers positifs et soit α une racine primitive d'ordre n de l'unité. Un code cyclique de longueur n sur $\mathbb{F}_q$ est appelé* code BCH de distance prescrite δ *si son générateur $g(x)$ est le plus petit commun multiple des polynômes minimaux de $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$. Lorsque $n = q^m - 1$, où m est un entier positif, le code BCH est dit* primitif.

Le terme de distance prescrite est dû au résultat suivant.

Proposition 1.5 *La distance minimale d'un code BCH de distance prescrite δ est supérieure ou égale à δ.*

Exemple 1.4 *Soit $q = 2, m = 5$ et $n = 31$. Soit α un élément primitif de $\mathbb{F}_{32}$ et notons $m_i(x)$ le polynôme minimal de α^i, où i est un entier positif. On a*

$$\begin{aligned} m_1(x) &= (x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right)\left(x-\alpha^8\right)\left(x-\alpha^{16}\right), \\ m_3(x) &= \left(x-\alpha^3\right)\left(x-\alpha^6\right)\left(x-\alpha^{12}\right)\left(x-\alpha^{24}\right)\left(x-\alpha^{17}\right), \\ m_5(x) &= \left(x-\alpha^5\right)\left(x-\alpha^{10}\right)\left(x-\alpha^{20}\right)\left(x-\alpha^9\right)\left(x-\alpha^{18}\right), \\ m_7(x) &= \left(x-\alpha^7\right)\left(x-\alpha^{14}\right)\left(x-\alpha^{28}\right)\left(x-\alpha^{25}\right)\left(x-\alpha^{19}\right). \end{aligned}$$

Donc, en prenant

$$g(x) = m_1(x)\, m_3(x)\, m_5(x)\, m_7(x) = \operatorname{ppcm}\left(m_1(x), m_2(x), \cdots, m_{10}(x)\right),$$

on a $\delta = 11$, ce qui entraîne que $d \geq 11$.

Définition 1.11 (code de Reed-Solomon) *Avec les mêmes notations que la définition précédente, un* code de Reed-Solomon *est un code BCH primitif de longueur $n = q - 1$.*

Pour un code de Reed-Solomon, la racine primitive α de l'unité est d'ordre $q-1$, c'est donc un élément de $\mathbb{F}_q$. On en déduit que le polynôme générateur s'écrit sous la forme

$$g(x) = \left(x - \alpha^b\right)\left(x - \alpha^{b+1}\right)\cdots\left(x - \alpha^{b+\delta-2}\right).$$

Ainsi le degré de $g(x)$ est égal à $\delta - 1$ et la dimension du code est égale à $k = n - \delta + 1$. D'après la borne de Singleton, la distance minimale d du code vérifie

$$d \leq n - k + 1 = \delta.$$

Comme on a $d \geq \delta$ d'après la proposition précédente, alors $d = n - k + 1$. Un code de Reed-Solomon est donc MDS.

Il y a de nombreuses représentations des codes cycliques. Nous verrons par exemple en 3.3 comment utiliser les suites récurrentes linéaires dans ce but. Lorsque le générateur $g(x)$ d'un $[n, k]$ code cyclique $\mathcal{C}$ est un polynôme irréductible sur $\mathbb{F}_q$, on a

$$\mathcal{C} = \left\{c(x) \in \mathbb{F}_q[x] / (x^n - 1) : c(\alpha) = 0\right\},$$

où α est une racine de $g(x)$. Cette représentation permet la détermination de la distance minimale du code en utilisant les racines du polynôme $c(x)$.

Exemple 1.5 *Soit $g(x)$ un polynôme irréductible primitif de degré m sur $\mathbb{F}_2$ et soit $n = 2^m - 1$. Alors $g(x)$ est un diviseur de $x^n - 1$. Notons $\mathcal{C}$ le code cyclique de longueur n sur $\mathbb{F}_2$ engendré par le polynôme $g(x)$. Soit $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathcal{C} - \{0\}$ et soit α un élément primitif de $\mathbb{F}_{2^m}$. On a alors*

$$c(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0.$$

Le poids de $c(x)$ ne peut être égal à 1 puisque $\alpha^i \neq 0$. Il ne peut pas non plus

être égal à 2 *car cela entraînerait la relation* $\alpha^i + \alpha^j = 0, 0 \leq i < j \leq n-1$, *qui ne peut avoir lieu du fait que* α *est un élément primitif. Mais justement,* α *étant primitif, il existe* $i, 2 \leq i \leq n-1$, *tel que* $1 + \alpha = \alpha^i$. *Le polynôme* $1 + x + x^i$ *est donc un élément de* $\mathcal{C}$ *de poids* 3. *On en déduit que la distance minimale du code* $\mathcal{C}$ *est égale à* 3.

1.4 Codes quasi-cycliques

Les codes quasi-cycliques constituent une généralisations des codes cycliques. Cette famille de codes est connue pour fournir de bons codes, c'est-à-dire des codes ayant les meilleurs distances minimales [24]. L'autre intérêt de ces codes est leur utilisation en cryptographie dans le cryptosystème de McEliece.

Notons T l'opérateur appelé shift défini sur $\mathbb{F}_q^n$ par

$$T(a_1, a_2, ..., a_n) = (a_n, a_1, ..., a_{n-1})$$

Définition 1.12 *Un code linéaire* $\mathcal{C}$ *de longueur* n *sur* $\mathbb{F}_q$ *est dit quasi-cyclique d'indice* ℓ *(ou* ℓ*-quasi-cyclique) s'il vérifie :*

$$\forall c \in \mathcal{C}, T^\ell(c) \in \mathcal{C}.$$

Pour $\ell = 1$, on retrouve les codes cycliques.

Exemple 1.6 *Le code de longueur 6 sur* $\mathbb{F}_2$ *engendré par la matrice*

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

est un code quasi-cyclique d'indice 2.

Depuis leur apparition, plusieurs auteurs ont abordé la question de la structure des codes quasi-cycliques. En particulier, un code ℓ-quasi-cyclique peut être regardé comme R-sous-module de R^ℓ, où $R = \mathbb{F}[Y]/(Y^m - 1)$. On parlera de *représentation polynômiale* du code. C'est l'approche utilisée par Lally et Fitzpatrick dans [20], via les bases de Gröbner. C'est aussi l'approche de Ling et Solé qu'on présente dans la section qui suit. On verra au chapitre 3 une représentation très récente analogue à celle des codes cycliques.

1.5 La représentation de S. Ling et P. Solé

Dans une série d'articles ,[25],[26],[27],[28], S. Ling et P. Solé (et H. Niederreiter dans la dernière citation) décrivent la structure algébrique des codes quasi-cycliques. Cette description utilise d'abord le Théorème Chinois, ensuite la Transformée de Fourier discrète qui permet une description plus explicite.

Soient $\mathbb{F} = \mathbb{F}_q$ un corps fini à q éléments et soient m, ℓ et n des entiers positifs tels que $\text{pgcd}(m, q) = 1$ et $n = \ell m$. Posons $R = \mathbb{F}[Y]/(Y^m - 1)$.

L'anneau R se décompose en somme directe de corps de deux façons :

1. en utilisant le Théorème Chinois,
2. en utilisant DFT : Transformée de Fourier discrète.

Proposition 1.6 *Soit $\mathcal{C}$ un code quasi-cyclique de longueur n et d'indice ℓ tel que $n = m\ell$. Soit $c \in \mathcal{C}$,*

$$c = (c_{00}, c_{01}, \ldots, c_{0,\ell-1}, c_{10}, c_{11}, \ldots, c_{1,\ell-1}, \ldots, c_{m-1,0}, c_{m-1,1}, \ldots, c_{m-1,\ell-1}).$$

L'application

$$\begin{aligned} \Phi : \mathbb{F}^n &\longrightarrow R^\ell \\ c &\longrightarrow \left(\sum_{i=0}^{m-1} c_{ij}^i Y \right)_{0 \le j \le \ell-1} \end{aligned}$$

est bijective et linéaire et vérifie : $\Phi\left(T^{\ell}(c)\right) = x\Phi(c)$.

On en déduit que $\mathcal{C}$ est un code quasi-cyclique d'indice ℓ si, et seulement si, $\Phi(\mathcal{C})$ est un sous R-module de R^{ℓ}. Il existe donc une correspondance bijective entre les codes quasi-cycliques de longueur n sur $\mathbb{F}$ et d'indice ℓ et les codes R-linéaires de longueur ℓ.

On définit sur R l'application de conjugaison

$$R \to R$$

$$a(Y) = a_0 + a_1 Y + \cdots + a_{m-1}Y^{m-1} \to \overline{a(Y)} = a_0 + a_{m-1}Y + \cdots + a_1 Y^{m-1}.$$

Définition 1.13 *Soit* $x = (x_0, \cdots, x_{\ell-1}), y = (y_0, \cdots, y_{\ell-1}) \in R^{\ell}$. *Le* produit scalaire hermitien *de* x *par* y *est donné par*

$$< x, y >= \sum_{i=0}^{\ell-1} x_i \overline{y_i}.$$

Proposition 1.7 *Soit* m *et* ℓ *deux entiers positifs et soit* $\mathcal{C}$ *un code quasi-cyclique de longueur* $m\ell$ *et d'indice* ℓ *sur* $\mathbb{F}_q$. *On suppose que* $\text{pgcd}(m, q) = 1$. *Alors*

$$\Phi\left(\mathcal{C}^{\perp}\right) = \Phi(\mathcal{C})^{\perp},$$

où $\mathcal{C}^{\perp}$ *désigne le code dual de* $\mathcal{C}$ *relativement au produit scalaire euclidien et* $\Phi(\mathcal{C})^{\perp}$ *désigne le code dual de* $\Phi(\mathcal{C})$ *relativement au produit scalaire hermitien.*

1.5.1 Décomposition d'un code quasi-cyclique

Soit $Y^m - 1 = f_1 f_2 \cdots f_n$ la décomposition du polynôme $Y^m - 1$ dans $\mathbb{F}[Y]$ en produit de polynômes irréductibles. Puisque $pgcd(m, q) = 1$, alors le polynôme $Y^m - 1$ n'a que des racines simples, par suite les polynômes f_i sont tous distincts pour $1 \leq i \leq n$. Rappelons que le polynôme réciproque f^* de f

est défini par :

$$f^*(Y) = Y^{\deg(f)} f\left(\frac{1}{Y}\right)$$

On a :

$$(Y^m - 1)^* = (f_1 f_2 \cdots f_n)^* = f_1^* f_2^* \cdots f_n^*,$$

d'où

$$Y^m - 1 = -f_1^* f_2^* \cdots f_n^*.$$

L'unicité de la décomposition en produit de polynômes irreductibles, à une constante près, entraîne que dans la décomposition du polynôme $Y^m - 1$ apparaissent tous les f_i et tous les f_i^*. On peut alors écrire :

$$Y^m - 1 = \delta g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*,$$

où $\delta \in \mathbb{F} - \{0\}$, les g_i, $1 \leq i \leq s$, sont les f_j tels que f_j et f_j^* sont associés et les h_i, $1 \leq i \leq t$, sont les f_j tels que f_j et f_j^* ne sont pas associés. On obtient ainsi, d'après le Théorème Chinois, l'isomorphisme suivant :

$$R \simeq \left(\oplus_{i=1}^{s} \mathbb{F}[Y]/(g_i)\right) \oplus \left(\oplus_{j=1}^{t} \left(\mathbb{F}[Y]/(h_j) \oplus \mathbb{F}[Y]/\left(h_j^*\right)\right)\right). \tag{1.1}$$

Donc, tout code R-linéaire $\mathcal{C}$ de longueur ℓ peut être décomposé comme somme directe

$$\mathcal{C} = \left(\oplus_{i=1}^{s} \mathcal{C}_i\right) \oplus \left(\oplus_{j=1}^{t} \left(\mathcal{C}_j' \oplus \mathcal{C}_j''\right)\right),$$

où $\mathcal{C}_i$ (resp. $\mathcal{C}_j'$, resp. $\mathcal{C}_j''$) est un code linéaire de longueur ℓ sur G_i (resp. sur H_j, resp. sur H_j'').

Si $c(Y) \in \mathcal{C}$, on peut écrire :

$$c(Y) = \left(c_1(Y), \ldots, c_s(Y), c_1'(Y), c_1''(Y), \ldots, c_t'(Y), c_t''(Y)\right)$$

1.5.2 Formule de la Trace

On peut décrire de façon plus explicite l'isomorphisme (1.1) , via la transformée de Fourier discrète (DFT), appelée transformée de Mattson-Solomon dans le langage des codes cycliques.

Dans 1.1 le membre de droite contient des facteurs directs qui correspondent aux facteurs irréductibles de $Y^m - 1 \in \mathbb{F}[Y]$. Il existe une correspondance bijective entre ces facteurs et les classes cyclotomiques. Notons U_i $(1 \leq i \leq s)$ les classes correspondant aux g_i, V_j $(1 \leq j \leq t)$ les classes correspondant aux h_j et W_j $(1 \leq j \leq t)$ les classes correspondant aux h_j^*. Soit ζ une racine primitive d'ordre m de 1 (dans une extension convenable de $\mathbb{F}$) et soit $c = \sum_{g \in \mathbb{Z}/m\mathbb{Z}} c_g Y^g \in \mathbb{F}[Y]/(Y^m - 1)$. La *transformée de Fourier discrète* de c, notée $\hat{c}$, est définie par

$$\hat{c} = \sum_{h \in \mathbb{Z}/m\mathbb{Z}} \hat{c}_h Y^h,$$

où $\hat{c}_h = \sum_{g \in \mathbb{Z}/m\mathbb{Z}} c_g \zeta^{gh}$.

Théorème 1.2 *Soit ℓ et m deux entiers positifs. On suppose que* $\operatorname{pgcd}(m, q) = 1$. *Alors les codes quasi-cycliques de longueur $m\ell$ et d'indice ℓ sur $\mathbb{F} = \mathbb{F}_q$ sont donnés par la construction suivante. On écrit*

$$Y^m - 1 = \delta g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*$$

où $\delta \in \mathbb{F} - \{0\}$, les g_i, $1 \leq i \leq s$, sont les facteurs irreductibles qui sont associés à leurs réciproques, et les h_j, $1 \leq j \leq t$, sont les facteurs irréductibles dont les réciproques sont les h_j^*. On note $G_i = \mathbb{F}[Y]/(g_i)$, $H'_j = \mathbb{F}[Y]/(h_j)$ et $H''_j = \mathbb{F}[Y]/\left(h_j^*\right)$. Soit U_i (resp. V_j et W_j) la classe cyclotomique de $\mathbb{Z}/m\mathbb{Z}$ correspondant à G_i (resp. H'_j et H''_j) et fixons $u_i \in U_i$, $v_j \in V_j$ et $w_j \in W_j$. Pour chaque i, soit $\mathcal{C}_i$ un code de longueur ℓ sur G_i, et pour chaque j, soit $\mathcal{C}'_j$ un code de longueur ℓ sur H'_j et $\mathcal{C}''_j$ un code de longueur ℓ sur H''_j.

Pour $x_i \in \mathcal{C}_i$, $y'_j \in \mathcal{C}'_j$, $y''_j \in \mathcal{C}''_j$ et pour tout $0 \leq g \leq m-1$, soit

$$\begin{aligned} c_g\left((x_i),\left(y'_j\right),\left(y''_j\right)\right) &= \sum_{i=1}^{s} Tr_{G_i/\mathbb{F}}\left(x_i\zeta^{-gu_i}\right) + \\ &\quad \sum_{j=1}^{t} Tr_{H'_j/\mathbb{F}}\left(y'_j\zeta^{-gv_j}\right) + Tr_{H''_j/\mathbb{F}}\left(y''_j\zeta^{-gw_i}\right). \end{aligned}$$

Alors le code

$$\mathcal{C} = \left\{\left(c_0\left((x_i),\left(y'_j\right),\left(y''_j\right)\right),\cdots,c_{m-1}\left((x_i),\left(y'_j\right),\left(y''_j\right)\right) : x_i \in \mathcal{C}_i,\ y'_j \in \mathcal{C}'_j, y''_j \in \mathcal{C}''_j\right\}$$

est quasi-cyclique de longueur $m\ell$ et d'indice ℓ sur $\mathbb{F}$.
Réciproquement, tout code quasi-cyclique de longueur $m\ell$ et d'indice ℓ sur $\mathbb{F}$ est obtenu par cette construction.
De plus, $\mathcal{C}$ est auto-dual relativement au produit scalaire si, et seulement si, pour tout i, les $\mathcal{C}_i$ sont auto-duaux relativement au produit hermitien et $\mathcal{C}''_j = \left(\mathcal{C}'_j\right)^{\perp}$ pour tout j relativement au produit scalaire euclidien.

1.5.3 Exemples

Exemple 1.7 *Soit $m = 3$ et $q \equiv 2 \pmod 3$. On a $Y^3-1 = (Y-1)\left(Y^2+Y+1\right)$, alors*

$$\mathbb{F}_q[Y]/\left(Y^3-1\right) = \mathbb{F}_q \oplus \mathbb{F}_{q^2}.$$

L'isomorphisme donne une correspondance entre les codes quasi-cycliques de longueur 3ℓ sur $\mathbb{F}_q$ et d'indice ℓ et la paire $(\mathcal{C}_1, \mathcal{C}_2)$ où $\mathcal{C}_1$ est un code linéaire de longueur ℓ sur $\mathbb{F}_q$ et $\mathcal{C}_2$ est un code linéaire de longueur ℓ sur $\mathbb{F}_{q^2}$.
En utilisant DFT, on obtient :

$$\mathcal{C} = \left\{(x+2a-b\,|x-a+2b|\,x-a-b),\ x \in \mathcal{C}_1, a+\zeta b \in \mathcal{C}_2\right\},$$

où $\zeta^2+\zeta+1 = 0$.

En particulier, si $q = 2^t$ *où* t *est impair, on a pour tout entier* ℓ

$$\mathcal{C} = \{(x + b\,|x + a|\,x + a + b)\,,\ x \in \mathcal{C}_1, a + \zeta b \in \mathcal{C}_2\}\,.$$

La construction $(x + b\,|x + a|\,x + a + b)$ *appliquée aux deux codes linéaires de longueur* ℓ *sur* $\mathbb{F}_{2^t}$, t *impair, donne lieu à un code linéaire sur* $\mathbb{F}_{2^t}$ *de longueur* 3ℓ *qui est quasi-cyclique d'indice* ℓ.

On en déduit le résultat qui suit.

Corollaire 1.1 *Le code de Golay binaire étendu est quasi-cyclique d'indice* 8.

Exemple 1.8 *Soit* $m = 5$ *et* q *tel que le polynôme* $Y^4 + Y^3 + Y^2 + Y + 1$ *soit irréductible dans* $\mathbb{F}_q[Y]$. *Soit* $\zeta \in \mathbb{F}_{q^4}$ *tel que* $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$. *On note* Tr *l'application trace* $Tr_{\mathbb{F}_{q^4}/\mathbb{F}_q}$.
Alors si $\mathcal{C}_1$ *est un code de longueur* ℓ *sur* $\mathbb{F}_q$ *et* $\mathcal{C}_2$ *un code de longueur* ℓ *sur* $\mathbb{F}_{q^4}$, *le code*

$$\mathcal{C} = \left\{ \begin{array}{c} (x + Tr(y)\,|x + Tr(y\zeta^{-1})|\,x + Tr(y\zeta^{-2})\,|x + Tr(y\zeta^{-3})|\,x + Tr(y\zeta^{-4})\,, \\ x \in \mathcal{C}_1,\ y \in \mathcal{C}_2 \end{array} \right\}$$

est un code quasi-cyclique de longueur 5ℓ *sur* $\mathbb{F}_q$ *et d'indice* ℓ. *Tout code quasi-cyclique de longueur* 5ℓ *sur* $\mathbb{F}_q$ *et d'indice* ℓ *s'écrit de cette manière.*

Chapitre 2

Suites récurrentes linéaires sur des anneaux non commutatifs

2.1 Introduction

Les suites récurrentes linéaires sont connues depuis fort longtemps, la plus célèbre étant sans doute la suite de Fibonacci dont on trouve la première trace dans le *Liber Abaci* dont une deuxième édition date de 1228 !

Depuis la fin du XIX^{e} siècle, ces suites ont été étudiées d'abord sur $\mathbb{Z}$ puis sur des corps commutatifs. On trouvera dans [16] une très bonne bibliographie et une longue liste d'applications intéressantes de ces objets (cryptologie, codes correcteurs d'erreurs, calcul rapide, arithmétique, etc.).

Pendant les années 1980, plusieurs auteurs ont travaillé sur des suites récurrentes linéaires sur des modules sur des anneaux commutatifs, voir [19] pour une bibliographie complète.

La notion de suite récurrente linéaire s'étend naturellement au cas de modules (à gauche) sur un anneau non nécessairement commutatif. Cette généralisation a trouvé des applications en théorie des codes correcteurs d'erreurs, en particulier dans la construction de codes quasi-cycliques auto-duaux [7], que

l'on présentera dans le chapitre 3.

Généralement, dans le cas non commutatif, il y a perte de la stabilité de l'addition et de la multiplication par les scalaires usuelles. Plus précisément, soit A un anneau non commutatif et M un A-module. La somme de deux suites récurrentes linéaires à valeurs dans M et à coefficients dans A n'est pas toujours une suite récurrente linéaire sur A. Il en est de même de la multiplication d'une suite récurrente linéaire à valeurs dans M par les éléments de l'anneau A. En effet, contrairement au cas commutatif, le produit des polynômes caractéristiques de deux suites récurrentes linéaires n'est pas forcément un polynôme caractéristique pour la somme des suites.

L'objet de ce chapitre est la détermination de types d'anneaux sur lesquels la structure habituelle de A-module est conservée. Après quelques rappels et préliminaires, nous donnons, dans la section 4, des conditions nécessaires pour que la somme de suites "géométriques " ainsi que la multiplication (à gauche) par les éléments de l'anneau soit une suite récurrente linéaire. Nous établissons en particulier que l'anneau de base, lorsqu'il est intègre, doit être nécessairement un anneau de Ore.

Dans la section 5, nous montrons que, dans le cas d'un anneau de matrices à coefficients dans un anneau commutatif, les suites récurrentes linéaires (de matrices ou de vecteurs) conservent la structure habituelle de A-module. La preuve est analogue à celle déjà utilisée dans [32] pour étudier les systèmes récursifs. De la stabilité des opérations usuelles, nous déduisons, par exemple, que tout sous-anneau intègre d'un anneau de matrices à coefficients dans un anneau commutatif est un anneau de Ore.

Dans la section 6, nous abordons le cas où l'anneau de base A est un corps non commutatif. Nous montrons que dans ce cas également, l'ensemble des suites récurrentes linéaires à valeurs dans un A-module a une structure de A-module. Nous nous intéressons plus particulièrement au cas où le corps est supposé de dimension finie sur son centre : grâce à un résultat de Jacobson [22], on donnera un algorithme de *dévissage* pour la détermination d'une relation

de récurrence linéaire pour la somme de deux suites récurrentes linéaires.

Enfin, la section 7 est consacrée à la série génératrice d'une suite définie sur un corps non commutatif. Il est bien connu que la série génératrice d'une suite sur un corps commutatif est une une fraction rationnelle si, et seulement si, la suite est récurrente linéaire. Cette propriété a été démontrée, sous une forme appropriée, pour les suites récurrentes linéaires à valeurs dans un module sur un anneau commutatif, voir [31], et pour les suites à coefficients matriciels, voir [5]. Nous étendons cette propriété au cas des corps non commutatifs.

2.2 Aperçu sur la théorie des anneaux non commutatifs

Lorsqu'on évoque les anneaux non commutatifs, l'exemple qui vient à l'esprit et qui est souvent cité est l'exemple de l'anneau des matrices à coefficients sur un corps (ou un anneau) commutatif. En un certain sens, ce n'est pas le *bon* exemple. En effet, un tel anneau est une algèbre de dimension finie sur son centre, et n'est donc pas suffisamment non commutatif. Dans cette section, nous donnons un petit aperçu sur cette très belle et très riche théorie des anneaux non commutatifs. Nous insisterons en particulier sur les aspects liés à notre travail sur les suites récurrentes linéaires.

2.2.1 Rappels et exemples

Dans tout le texte les anneaux considérés sont des anneaux unitaires non nécessairement commutatifs. Rappelons que tout anneau ne possédant pas d'élément unité se plonge dans un anneau unitaire (voir *[12]*), ce qui justifie notre choix.

Soit A un anneau et soit a un élément non nul de A. On dira que a est un *diviseur de* 0 *à gauche* s'il existe un élément non nul b dans A tel que $ab = 0$. On définit de façon similaire un diviseur de 0 à droite. Un anneau $A \neq \{0\}$

est dit *intègre* s'il ne posséde pas de diviseur de 0 (à gauche ou à droite). Un élément a de l'anneau A est dit *inversible à droite* s'il existe b dans A tel que $ab = 1$. L'élément b est alors appelé *inverse de a à droite.* On définit là aussi de façon similaire l'inversibilité à droite. Si a admet un inverse à droite b et un inverse à gauche b', alors

$$b' = b'(ab) = (b'a)b = b.$$

Dans ce cas, on dira que a est *inversible* dans A, ou encore que a est une *unité de A,* et l'élément b, qui est unique, est appelé *l'inverse de A.* L'ensemble des éléments inversibles dans un anneau A forme un groupe multiplicatif noté $U(A)$. Un anneau $A \neq \{0\}$ tel que $A - \{0\} = U(A)$ est appelé *corps.* Notons que lorsque la multiplication n'est pas commutative, certains auteurs parlent de *corps gauche.* Dans toute la suite nous dirons simplement *corps non commutatif.*

Exemple 2.1 *Rappelons qu'une dérivation d définie sur un anneau A est un homomorphisme du groupe additif de A qui vérifie*

$$\forall a, b \in A, d(ab) = ad(b) + d(a)b.$$

Soit A un anneau, σ un endomorphisme de A et d une dérivation sur A. Soit X une indéterminée. L'anneau $A[X;\sigma;d]$ est l'anneau des polynômes sur A en l'indéterminée X avec la règle de multiplication

$$\forall a \in A, Xa = \sigma(a)X + d(a).$$

Si $\sigma = id$ et $d = 0$, on obtient l'anneau de polynômes $A[X]$.
Si $\sigma = id$, l'anneau est noté $A[X;d]$.
Si $d = 0$, l'anneau est noté $A[X;\sigma]$ et est appelé Twist de Hilbert. *Notons que*

la multiplication est donnée par

$$\left(\sum a_i X^i\right)\left(\sum b_j X^j\right) = \sum a_i \sigma^i\left(b_j\right) X^{i+j}.$$

Si k est un corps commutatif de caractéristique 0, $\sigma = id$ et $A = k[t]$, et si d est la différentiation relativement à t, l'anneau $A[X;d]$ obtenu est appelé algèbre de Weyl.

Exemple 2.2 *Soit k un anneau et $\{X_i : i \in I\}$ un système d'indéterminées indépendantes non commutatives sur k. On construit l'anneau noté*

$$A = k\langle X_i : i \in I\rangle$$

des polynômes en les indéterminées X_i, où les coefficients commutent avec les indéterminées mais $X_i X_j \neq X_j X_i, \forall i \neq j$.

Exemple 2.3 *Soit k un anneau et $\{X_i : i \in I\}$ un système d'indéterminées indépendantes. On suppose que les indéterminées commutent entre elles et avec les éléments de l'anneau k. Avec l'addition et la multiplication usuelles, on obtient* l'anneau des séries formelles

$$A = k\left[\left[X_i; i \in I\right]\right]$$

dont les éléments sont de la forme

$$f_0 + f_1 + f_2 + \cdots$$

où f_n est un polynôme homogène en les X_i de degré n. Un élément $f_0 + f_1 + f_2 + \cdots$ est inversible si, et seulement si, f_0 est inversible dans k. En effet, si on cherche $G = g_0 + g_1 + g_2 + \cdots$ tel que $FG = 1$, il suffit de résoudre les

équations

$$1 = f_0 g_0, 0 = f_0 g_1 + f_1 g_0, 0 = f_0 g_2 + f_1 g_1 + f_2 g_0, \cdots$$

Comme f_0 est inversible dans k, on trouve g_0, puis g_1, ensuite g_2, etc.

Exemple 2.4 *Soit k un anneau et X une indéterminée. Les éléments de l'anneau des* séries de Laurent $k((X))$ *sont de la forme*

$$F = \sum_{i \geq n_0} f_i X^i, n_0 \in \mathbb{Z}.$$

Une propriété remarquable est que si k est un corps, alors $k((X))$ l'est aussi. En effet, soit $F = \sum_{i \geq n_0} f_i X^i$ un élément de $k((X))$, où $n_0 \in \mathbb{Z}$ est tel que $f_{n_0} \neq 0$. En multipliant par X^{-n_0}, on obtient

$$F.X^{-n_0} = g_0 + g_1 X + g_2 X^2 + \cdots, \text{ avec } g_0 = f_{n_0} \neq 0.$$

Par suite, $F.X^{-n_0}$ est inversible dans $k[[X]]$. Comme X^{-n_0} est clairement inversible dans $k((X))$, alors il en est de même de F.

Exemple 2.5 *Soit k un corps commutatif et soit V le k-espace vectoriel engendré par la base dénombrable $\{e_i : i \in \mathbb{N}^*\}$. Notons $A = End_k(V)$ l'anneau des k-endomorphismes de V, où la multiplication est la composition des endomorphismes. Soit σ et τ les endomorphismes définis par*

$$\begin{aligned} \sigma(e_i) &= e_{i+1} \text{ pour } i \geq 1, \text{ et} \\ \tau(e_1) &= 0, \tau(e_i) = e_{i-1} \text{ pour } i \geq 2. \end{aligned}$$

Alors, $\sigma\tau = 1$ tandis que $\tau\sigma \neq 1$. Nous avons là un exemple d'élément inversible à droite qui n'est pas inversible à gauche. Un anneau dans lequel un élément est inversible à droite si, et seulement si, il est inversible à gauche est dit Dedekind-fini (ou von Neumann-fini).

Signalons quelques théorèmes de commutativité célèbres ; cela nous évitera de prendre des anneaux vérifiant certaines propriétés pour des anneaux quelconques lorsqu'ils sont implicitement commutatifs ! Par exemple, dans [31], les anneaux commutatifs sur lesquels toute suite récurrente linéaire est périodique sont étudiés. L'idée de généraliser les résultats aux anneaux non nécessairement commutatifs tourne court : les théorèmes qui suivent entraînent que de tels anneaux sont commutatifs.

Théorème 2.1 *Soit A un anneau de centre C. On suppose qu'il existe un entier $n \geq 2$ tel que*

$$\forall x \in A, x^n - x \in C.$$

Alors l'anneau A est commutatif.

Théorème 2.2 *Soit A un anneau vérifiant la propriété*

$$\forall x \in A, \exists n \geq 2 : x^n = x.$$

Alors A est commutatif.

Il est évident que, partant de ce dernier résultat, le théorème de Wedderburn *"Tout corps fini est commutatif"* devient un corollaire immédiat.

2.2.2 Anneaux de Ore

Historiquement, les anneaux de Ore sont liés à la question de l'existence d'un anneau des quotients (ou fractions) pour un anneau non commutatif. C'est le norvégien Oystein Ore qui donne, en 1931 [33], une condition nécessaire et suffisante pour l'existence d'un anneau des quotients pour un anneau intègre.

Définition 2.1 *Soit A un anneau. Un anneau Q est appelé* anneau des quotients à gauche *de l'anneau A s'il vérifie les conditions suivantes :*

1. $A \subset Q$,

2. *tout élément régulier b dans A possède un inverse b^{-1} dans Q,*
3. *tout élément de Q peut s'écrire sous la forme $b^{-1}a$, où a et b sont des éléments de A et b est régulier.*

On obtient assez naturellement une condition nécessaire pour l'existence d'un anneau des quotients. Soit Q un anneau des quotients à gauche de l'anneau A, et soit a et b des éléments de A. Si b est régulier, alors il possède un inverse b^{-1} dans Q, donc ab^{-1} se trouve dans Q. Par suite, il existe des éléments a' et b' dans A, b' régulier, tels que $ab^{-1} = b'^{-1}a'$, ou encore $b'a = a'b$. Cela conduit à la condition suivante, appelée *condition de Ore à gauche* :

$$\forall a, b \in A, b \text{ régulier}, \exists a', b' \in A,\ b' \text{ régulier, tel que } b'a = a'b.$$

Définition 2.2 *Un anneau est dit* de Ore à gauche *s'il vérifie la condition de Ore à gauche. On définit de façon similaire un anneau de Ore à droite.*

La condition nécessaire énoncée ci-dessus s'avère aussi suffisante.

Théorème 2.3 *Un anneau possède un anneau des quotients à gauche si, et seulement si, il vérifie la condition de Ore à gauche.*

Ce théorème a été démontré, dans le cas où l'anneau est supposé intègre, par Ore comme déjà mentionné. Le résultat a été ensuite démontré pour un anneau quelconque par Dubreil en 1946 [15], puis Asano qui en donne une autre preuve en 1949 [1].

Le cas intègre est particulièrement intéressant. On adopte la définition suivante.

Définition 2.3 *On appelle* domaine de Ore *à gauche tout anneau de Ore à gauche qui est intègre.*

La proposition suivante permet de caractériser les domaines de Ore.

Proposition 2.1 *Soit A un anneau intègre. Alors A est un domaine de Ore à gauche si, et seulement si,*

$$\forall a, b \in A - \{0\}, Aa \cap Ab \neq \{0\}.$$

Rappelons le résultat suivant bien connu sur les domaines de Ore, que l'on pourra trouver dans [23], et qui nous sera utile dans la section 5.

Théorème 2.4 *Si A est un domaine de Ore à gauche, alors il en est de même pour l'anneau $A[X;d]$.*

Ce théorème n'est plus valable si on enlève la condition d'intégrité. Dans [8], Cedo et Herbera donnent un exemple d'un anneau A qui est un anneau de Ore à gauche sans que l'anneau $A[X;d]$ le soit. On peut aussi se poser la question de savoir si un anneau de matrices à coefficients dans un anneau commutatif est un anneau de Ore. On apportera un élément de réponse dans la section 5 du présent chapitre.

2.2.3 Corps non commutatifs

Parmi les anneaux non commutatifs, les corps non commutatifs constituent l'oeuvre la plus accomplie. En effet, on peut non seulement y additionner, soustraire et multiplier les éléments, mais aussi les diviser. Il n'est donc pas étonnant de voir se développer une théorie de Galois pour les corps non commutatifs (voir [6]). Les résultats sont souvents surprenants quand on les compare au cas commutatif.

2.2.3.1 Un exemple célèbre de corps non commutatif : le corps des Quaternions (Hamilton, 1843)

L'histoire de la découverte du corps des quaternions est passionnante. Pendant des années, Sir William Rowan Hamilton cherchait sans succès un équivalent du corps des nombres complexes pour l'espace $\mathbb{R}^3$. On verra grâce au

théorème de Frobenius que cela est impossible. Il eut donc l'idée de rajouter une quatrième dimension. Le 16 octobre 1843, alors qu'il se promenait avec son épouse, il découvrit dans un éclair de génie les relations fondamentales $i^2 = j^2 = k^2 = ijk = -1$ qu'il grava sur une pierre du pont de Brougham à Dublin. C'était la naissance du premier corps non commutatif, le corps des quaternions noté $\mathbb{H}$ en l'honneur de Hamilton.

Soit l'espace vectoriel de dimension 4 sur $\mathbb{R}$ défini par

$$\mathbb{H} = \{a1 + bi + cj + dk : a, b, c, d \in \mathbb{R}\} = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k,$$

avec les régles de multiplication

$$i^2 = j^2 = k^2 = -1 \text{ et } ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

En étendant la multiplication à l'ensemble des éléments par linéarité et distributivité, on vérifie que $\mathbb{H}$ est un anneau non commutatif.

Soit $q = a + bi + cj + dk \in \mathbb{H}$ et notons $\overline{q} = a - bi - cj - dk$, on a alors

$q\overline{q} = \overline{q}q = a^2 + b^2 + c^2 + d^2$. Par suite, si $q \neq 0$, son inverse est donné par $q^{-1} = (a^2 + b^2 + c^2 + d^2)^{-1}\overline{q}$. Ainsi, $\mathbb{H}$ est un corps non commutatif.

Le corps des quaternions peut aussi être représenté par un ensemble de matrices carrées d'ordre 4 à coefficients dans $\mathbb{R}$ ou des matrices carrées d'ordre 2 à coefficients dans $\mathbb{C}$ en utilisant les identifications :

$$a + bi + cj + dk \in \mathbb{H} \leftrightarrow \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \in \mathbb{M}_4(\mathbb{R}),$$

$$a + bi + cj + dk \in \mathbb{H} \leftrightarrow \begin{pmatrix} a + bi & -c - di \\ c - di & a - bi \end{pmatrix} \in \mathbb{M}_2(\mathbb{C}).$$

Remarquons que le déterminant de ces matrices est égal à $a^2+b^2+c^2+d^2$. Notons enfin que cette construction reste valable si on remplace le corps de base $\mathbb{R}$ par un autre corps commutatif k à la seule condition que -1 ne soit pas somme de deux carrés dans k.

Le théorème de Frobenius qui suit montre que le seul équivalent de $\mathbb{C}$ en dimension supérieure à 2 est le corps des quaternions.

Définition 2.4 *Soit k un corps commutatif et soit A une algèbre sur k. Si A est un corps (non nécessairement commutatif), on dira que A est une* algèbre à division *sur k.*

Théorème 2.5 (Frobenius, 1877) *Si A est une algèbre à division de dimension finie sur $\mathbb{R}$, alors A est isomorphe à $\mathbb{R}, \mathbb{C}$, ou $\mathbb{H}$.*

On a essentiellement deux classes de corps non commutatifs :
1- Corps de dimension finie sur leur centre (algèbre centrale finie).
2- Corps de dimension infinie sur leur centre (algèbre centrale infinie).

2.2.3.2 Algèbre cyclique

Soit F un corps commutatif. Soit K/F une extension cyclique et σ un générateur de son groupe de Galois. Notons s l'ordre de σ et fixons $a \in F^*$. Posons

$$D = K.1 \oplus K.x \oplus \cdots \oplus K.x^{s-1}$$

avec la multiplication définie par

$$x^s = a \text{ et } xt = \sigma(t)\, x, \forall t \in K.$$

Alors D est une algèbre sur F de dimension s^2, appelée *algèbre cyclique.* En prenant $F = \mathbb{R}$, $K = \mathbb{C}$, $a = -1$ et σ le $\mathbb{R}$-automorphisme de $\mathbb{C}$ défini par $\sigma(i) = -i$, on retrouve le corps des quaternions réels.

2.2.3.3 Polynômes et racines

Dans cette partie, nous allons nous intéresser en particulier aux aspects "inhabituels" par rapport au cas commutatif.

Qu'est-ce qu'une racine d'un polynôme sur un corps (plus généralement un anneau) non commutatif ?

Rappelons que dans l'anneau $A[X]$ on a par construction $aX = Xa, \forall a \in A$. Si $f(X) = aX + b$, une racine r vérifie $f(r) = ar + b = 0$. On a aussi $f(X) = Xa + b$, mais si $ar \neq ra$ alors $ra + b \neq 0$. On devrait donc parler de *racine à droite*.

Remarquons que si $f(X) = (X - a)(X - b) = X^2 - (a + b)X + ab$ alors $f(a) = ab - ba \neq 0$ si $ab \neq ba$. Donc, si $f(X) = g(X)h(X)$, une racine de $g(X)$ n'est pas, en général, une racine de $f(X)$. Remarquons par contre que $f(b) = 0$. En fait, on a le résultat important suivant :

Proposition 2.2 *Soit $f(X) \in A[X]$ un polynôme non nul et soit $r \in A$. Alors r est une racine de $f(X)$ si, et seulement si, il existe $g(X) \in A[X]$ tel que $f(X) = g(X)(X - r)$.*

Preuve : Si $f(X) = \left(\sum_{i=0}^{n} c_i X^i\right)(X - r) = \sum_{i=0}^{n} c_i X^{i+1} - \sum_{i=0}^{n} c_i r X^i$,alors $f(r) = 0$. Réciproquement, supposons $f(r) = 0$. En divisant $f(X)$ par $X - r$ (c'est possible), on obtient $f(X) = g(X)(X - r) + s, s \in A$, donc $f(r) = 0 = 0 + s$, d'où $s = 0$.

□

Contrairement au cas commutatif, le nombre de racines d'un polynôme n'est pas majoré par le degré du polynôme. Par exemple, les quaternions i, j, et k sont racines du polynôme $X^2 + 1$.

En fait, la situation est bien plus *grave* : le polynôme $X^2 + 1$ possède une *infinité* de racines. Notons que du point de vue géométrique, l'ensemble des solutions de l'équation $X^2 + 1 = 0$ dans $\mathbb{H}$ est isomorphe à la sphère S^2.

Définition 2.5 *Soit D un corps non commutatif et soit $x \in D$. On appelle* conjugué de x *tout élément de la forme $\alpha x \alpha^{-1}$, où $\alpha \in D - \{0\}$. L'ensemble des conjugués de x est appelé* classe de conjugaison de x.

En multipliant $i^2 + 1$ par α à gauche et par α^{-1} à droite, on voit que tout conjugué $\alpha i \alpha^{-1} (\alpha \in \mathbb{H} - \{0\})$ de i est racine de $X^2 + 1$. Un théorème de Herstein permet de dire qu'il y a une infinité de tels conjugués.

Toutefois, le théorème qui suit permet de cerner la quantité de racines.

Théorème 2.6 (Gordon-Motzkin) *Soit $f(X) \in D[X]$ un polynôme de degré n. Alors les racines de $f(X)$ se trouvent dans au plus n classes de conjugaison. Si $f(X) = (X - a_1) ... (X - a_n)$, avec $a_1, ..., a_n \in D$, alors toute racine de $f(X)$ est conjuguée à l'un des a_i.*

La preuve se fait par récurrence. Pour $n = 1$, c'est clair. Pour $n \geq 2$, on écrit $f(X) = g(X)(X - c)$ et on utilise l'hypothèse de récurrence.

Comme il existe des polynômes ayant une infinité de racines, la question suivante est naturelle : peut-on trouver un polynôme non nul de $D[X]$ s'annulant en tout point de D ? La réponse est non.

Proposition 2.3 *Soit D un corps non commutatif et soit $f(X) \in D[X]$. Alors*

$$f(D) = 0 \Rightarrow f(X) = 0.$$

2.2.3.4 Cas des polynômes à coefficients dans le centre

Lorsque le polynôme est à coefficients dans le centre, tout conjugué d'une racine est aussi racine. En effet, soit F le centre d'un corps non commutatif D et soit $f(X) = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_1 X + a_0 \in F[X]$. Soit $\alpha \in D$ une racine de $f(X)$. On a alors

$$a_m \alpha^m + a_{m-1} \alpha^{m-1} + \cdots + a_1 \alpha + a_0 = 0$$

$$\Rightarrow e(a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0)e^{-1} = 0, \forall e \in D - \{0\}$$

$$\Rightarrow a_m \left(e\alpha e^{-1}\right)^m + a_{m-1}\left(e\alpha e^{-1}\right)^{m-1} + \cdots + a_1\left(e\alpha e^{-1}\right) + a_0 = 0.$$

On dira qu'une classe de conjugaison A est algébrique sur F si ses éléments sont algébriques sur F. Dans ce cas, les éléments de A ont le même polynôme minimal sur F : c'est *le polynôme minimal de* A. Les deux résultats qui suivent précisent le rôle de ce polynôme.

Théorème 2.7 *Soit D un corps non commutatif de centre F et soit $h(X) \in D[X]$. Notons A une classe de conjugaison algébrique sur F et $f(X)$ son polynôme minimal. Alors*

$$h(A) = 0 \Leftrightarrow h(X) \in D[X] f(X).$$

Théorème 2.8 (Dickson) *Soit D un corps non commutatif de centre F et soit a et b deux éléments de D algébriques sur F. Alors a et b sont conjugués dans D si, et seulement si, a et b ont le même polynôme minimal sur F.*

Le théorème suivant, dû à Wedderburn, est surprenant si on le compare au cas commutatif : si un polynôme irréductible à coefficients dans le centre d'un corps non commutatif D posséde une racine dans D, alors il se décompose entièrement dans $D[X]$. En d'autres termes, toute extension du centre est "normale".

Théorème 2.9 (Wedderburn) *Soit D un corps non commutatif de centre F et soit A une classe de conjugaison de D algébrique sur F, de polynôme*

minimal $f(X) \in F[X]$ *de degré* n. *Alors il existe* $a_1, \cdots, a_n \in A$ *tels que*

$$f(X) = (X - a_n) \cdots (X - a_1) \in D[X].$$

Corollaire 2.1 *Avec les notations du théorème précédent, si*

$$f(X) = X^n + d_1 X^{n-1} + \cdots + d_n \in F[X],$$

alors $-d_1$ *est égal à une somme d'éléments de* A *et* $(-1)^n d_n$ *est égal à un produit d'éléments de* A.

Théorème 2.10 (Gordon-Motzkin) *Soit* $g(X) \in D[X]$. *Soit* Γ *l'ensemble des racines de* $g(X)$ *dans* D *et* A *une classe de conjugaison dans* D. *Si* $\Gamma \cap A$ *a un cardinal supérieur ou égal à* 2, *alors* $\Gamma \cap A$ *est infini.*

Théorème 2.11 (Bray-Whaples) *Si* $c_1, ..., c_n$ *sont des éléments deux à deux non conjugués dans* D, *alors il existe un unique polynôme unitaire* $g(X) \in D[X]$, *de degré* n, *tel que* $g(c_1) = \cdots = g(c_n) = 0$. *De plus :*
(a) *Il n'y a pas d'autre racine de* $g(X)$ *dans* D.
(b) *Si* $h(X) \in D[X]$ *et* $h(c_i) = 0, \forall i, 1 \leq i \leq n$, *alors* $h(X) \in D[X].g(X)$.

2.3 Généralités sur les suites récurrentes linéaires

Dans cette section, on généralise quelques notions fondamentales sur les suites récurrentes linéaires au cas où l'anneau n'est plus supposé commutatif. On note $A[X]$ l'algèbre des polynômes à coefficients dans l'anneau A. La preuve du lemme qui suit, concernant la structure de $A[X]$-module associée à un endomorphisme, lorsque l'anneau est supposé commutatif, se trouve dans [4], page 105. Une simple vérification permet d'étendre ces résultats au cas d'un anneau quelconque.

Lemme 2.1 *Soit L un A-module et φ un endomorphisme de L. Pour tout $p \in A[X]$ et pour tout $x \in L$, on pose $p.x = p(\varphi)(x)$, alors*

i) pour tous polynômes p et q de $A[X]$, on a $pq(\varphi) = p(\varphi) \circ q(\varphi)$,

ii) la multiplication définie ci-dessus définit une structure de $A[X]$-module, et les sous $A[X]$- modules de L ne sont autres que les sous A- modules de L qui sont stables par φ.

Si M est un A-module, on note $S(M)$ l'ensemble des suites à valeurs dans M. L'ensemble $S(M)$, muni de l'addition et de la multiplication par un scalaire usuelles, est un A-module. Soit T l'endomorphisme de $S(M)$, appelé *shift*, défini par :

$$\forall u \in S(M), \forall n \in \mathbb{N}, T(u)(n) = u(n+1).$$

Grâce au lemme 2.1, en prenant $\varphi = T$, on voit qu'on obtient une structure de $A[X]$-module pour $S(M)$, où la multiplication est alors définie, pour $p(X) = a_0 + a_1X + \cdots + a_hX^h \in A[X]$ par :

$$\forall u \in S(M), \forall n \in \mathbb{N}, (p(X)u)(n) = a_0u(n) + a_1u(n+1) + \cdots + a_hu(n+h).$$

Définition 2.6 *Soit $u \in S(M)$. On dit que u est une* suite récurrente linéaire à valeurs dans M et à coefficients dans A *si l'annulateur de u dans $A[X]$ contient un polynôme unitaire (ou bien, ce qui revient au même, si l'annulateur contient un polynôme dont le coefficient dominant est inversible). Un tel polynôme est appelé* polynôme caractéristique de u. *Un polynôme caractéristique de degré minimal h est appelé* polynôme minimal *de u et h est appelé* longueur *de la suite u.*

L'ensemble des suites récurrentes linéaires à valeurs dans M et à coefficients dans A sera noté $SRL_A(M)$. Notons enfin que l'ensemble $SRL_A(M)$ est clairement stable par l'endomorphisme shift.

2.4 Suites récurrentes linéaires et domaines de Ore

On verra dans cette section que la somme de deux suites récurrentes linéaires n'est pas nécessairement une suite récurrente linéaire, et il en est de même de la multiplication d'une suite récurrente linéaire par un élément de l'anneau de base.

Proposition 2.4 *Soit A un anneau, et soient α et β deux éléments réguliers de A. On note $(u(n))_{n\in\mathbb{N}}$ et $(v(n))_{n\in\mathbb{N}}$ les suites récurrentes linéaires définies par : $u(n)=\alpha^n$ et $v(n)=\beta^n$. Alors*

1. *si la suite $(u(n)+v(n))_{n\in\mathbb{N}}$ est récurrente linéaire, alors $A\alpha\cap A\beta\neq\{0\}$,*
2. *si la suite $(\beta u(n))_{n\in\mathbb{N}}$ est récurrente linéaire, alors $A\alpha\cap A\beta\neq\{0\}$.*

Preuve : 1. Supposons que la suite $(u(n)+v(n))_{n\in\mathbb{N}}$ est récurrente linéaire, alors l'annulateur de $(u(n)+v(n))_{n\in\mathbb{N}}$ dans $A[X]$ contient un polynôme unitaire de la forme :

$$P(X)=X^h+a_{h-1}X^{h-1}+\cdots+a_0.$$

Remarquons que le cas $h=0$ entraîne que $\alpha=-\beta$, d'où $\alpha\in A\alpha\cap A\beta\neq\{0\}$. On supposera donc $h\geq 1$ et on aura

$$\forall n\in\mathbb{N},\ P(X)(u+v)(n)=0\Longleftrightarrow P(X)u(n)=-P(X)v(n).$$

En particulier, pour $n=1$, on obtient

$$P(X)u(1)=-P(X)v(1).$$

Notons k la valuation de $P(X)$, alors

$$\gamma = \sum_{i=k}^{h} a_i \alpha^{i+1} = -\sum_{i=k}^{h} a_i \beta^{i+1}.$$

Remarquons que $\gamma \in A\alpha \cap A\beta$. Donc si $\gamma \neq 0, A\alpha \cap A\beta \neq \{0\}$. Dans le cas contraire, on aura $k < h$ et

$$a_k = \left(-\sum_{i=k+1}^{h} a_i \alpha^{i-k-1} \right) \alpha = \left(-\sum_{i=k+1}^{h} a_i \beta^{i-k-1} \right) \beta.$$

On en déduit que $a_k \in A\alpha \cap A\beta$. Comme $a_k \neq 0$, on a le résultat énoncé.
2. Supposons que la suite $(\beta u(n))_{n\in\mathbb{N}}$ est récurrente linéaire, alors l'annulateur de $(\beta u(n))_{n\in\mathbb{N}}$ dans $A[X]$ contient un polynôme unitaire de la forme :

$$Q(X) = X^{\ell} + b_{\ell-1} X^{\ell-1} + \cdots + b_0.$$

Comme précédemment, on aura

$$\forall n \in \mathbb{N}, Q(X)(\beta u)(n) = 0 \iff \sum_{i=k}^{\ell} b_i \beta \alpha^{n+i} = 0.$$

Et, pour $n = 0$,

$$Q(X)(\beta u)(0) = 0.$$

Remarquons que, en notant k la valuation de $Q(X)$, on a nécessairement $k < \ell$, car sinon on obtiendrait

$$\beta \alpha^{\ell} = 0,$$

ce qui est impossible puisque α et β sont réguliers. On aura donc

$$\sum_{i=k}^{i=\ell} b_i \beta \alpha^{i-k} = 0,$$

d'où on tire

$$b_k \beta = \left(- \sum_{i=k+1}^{\ell} b_i \beta \alpha^{i-k-1} \right) \alpha.$$

Comme $b_k \beta \in A\alpha \cap A\beta$ et $b_k \beta \neq 0$, on en déduit le résultat.

□

Exemple 2.6 *Soit k un anneau quelconque et $A = k\langle x, y \rangle$ l'anneau aux indéterminées indépendantes x et y non commutatives. Notons u et v les suites récurrentes linéaires définies sur A par :*

$$u(n) = x^n \text{ et } v(n) = y^n, \text{ pour tout } n \in \mathbb{N}.$$

Comme $Ax \cap Ay = \{0\}$, alors, d'après la proposition précédente, la suite $u + v$ n'est pas récurrente linéaire.

Dans la suite, on écrira domaine de Ore pour désigner un domaine de Ore à gauche.

Remarque 2.1 *D'après la proposition, si A est un anneau intègre qui n'est pas un domaine de Ore, alors la somme de deux suites récurrentes linéaires sur A n'est pas nécessairement récurrente linéaire. De même, le produit d'une suite récurrente linéaire par un élément de l'anneau A n'est pas nécessairement une suite récurrente linéaire.*

2.5 Suites récurrentes linéaires sur un anneau de matrices

Soit A un anneau commutatif et $s \in \mathbb{N}^*$. Soit $\mathbb{M}$ l'anneau des matrices carrées d'ordre s à coefficients dans A. Dans cette section, nous montrons que $SRL_{\mathbb{M}}(\mathbb{M})$ est un $\mathbb{M}[X]$-module et nous en déduisons que tout sous-anneau intègre de $\mathbb{M}$ est un domaine de Ore.

Pour $U \in S(\mathbb{M})$, on pose $U = (u_{ij})_{1\leq i,j\leq s}$, où $u_{ij} \in S(A)$ pour $1 \leq i, j \leq s$.

Proposition 2.5 *Une suite $U = (u_{ij})_{1\leq i,j\leq s}$ d'éléments de $\mathbb{M}$ est récurrente linéaire sur $\mathbb{M}$ si, et seulement si, pour tout couple $(i,j) \in \{1,\cdots,s\} \times \{1,\cdots,s\}$, la suite u_{ij} est récurrente linéaire sur A.*

Preuve : Nous adaptons ici la méthode utilisée dans [32] pour l'étude des systèmes récursifs.Soit $U \in SRL(\mathbb{M})$, alors il existe des matrices $m_1, \cdots, m_h \in \mathbb{M}$ telles que :

$$\left(X^h + m_1 X^{h-1} + \cdots + m_h\right) U = 0.$$

Posons $C(X) = X^h + m_1 X^{h-1} + \cdots + m_h$, et regardons $C(X)$ comme matrice dont les coefficients sont des polynômes de $A[X]$. L'équation est équivalente à :

$$C(X)\, U = 0.$$

D'après le théorème de Cayley-Hamilton, la matrice $C(X)$ est racine de son polynôme caractéristique

$$P(Y) = Y^s + a_1(X)\, Y^{s-1} + \cdots + a_{s-1}(X)\, Y + a_s(X),$$

où $a_i(X) \in A[X]$ pour tout $i \in \{1,\cdots,s\}$. On a donc

$$P(C(X)) = 0 \text{ et } C(X)\, U = 0,$$

d'où

$$a_s(X)\,U = 0,$$

et, par conséquent,

$$a_s(X)\,u_{ij} = 0,\ \forall\ (i,j) \in \{1,\cdots,s\} \times \{1,\cdots,s\}.$$

Le polynôme $a_s(X)$ est égal, au signe près, au déterminant de $C(X)$.
La matrice $C(X)$ est de la forme

$$C(X) = \begin{pmatrix} X^h + c_{11}(X) & c_{12}(X) & \cdots & c_{1s}(X) \\ c_{21}(X) & X^h + c_{22}(X) & \cdots & c_{2s}(X) \\ \vdots & \vdots & \ddots & \vdots \\ c_{s1}(X) & c_{s2}(X) & & X^h + c_{ss}(X) \end{pmatrix},$$

où les $c_{ij}(X)$ sont des polynômes de degré strictement inférieur à h. Il s'ensuit que $\det(C(X))$ est un polynôme unitaire de degré sh.

On en conclut que, pour tout couple $(i,j) \in \{1,\cdots,s\} \times \{1,\cdots,s\}$, les suites u_{ij} sont récurrentes linéaires sur A.

Réciproquement, soit $U = (u_{ij})_{1\leq i,j\leq s} \in S(\mathbb{M})$ telle que, pour tout couple $(i,j) \in \{1,\cdots,s\} \times \{1,\cdots,s\}$, la suite u_{ij} est récurrente linéaire sur A.
Soit $P(X) = X^h + a_1X^{h-1} + a_2X^{h-2} + \cdots + a_h \in A[X]$ un annulateur commun à tous les u_{ij}. On a donc

$$\left(X^h + (a_1I_s)\,X^{h-1} + (a_2I_s)\,X^{h-2} + \cdots + (a_hI_s)\right)U = 0,$$

par suite $U \in SRL_{\mathbb{M}}(\mathbb{M})$.

□

Exemple 2.7 *Soient* $A = \mathbb{Z}$, $\mathbb{M} = \mathbb{M}_2(\mathbb{Z})$ *et*

$$U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$$

une suite récurrente linéaire d'éléments de $\mathbb{A}$ *vérifiant*

$$U(n+2) + \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} U(n+1) + \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} U(n) = 0.$$

Les premiers termes $U(0)$ *et* $U(1)$ *sont donnés. En utilisant notre formalisme, cette relation peut s'écrire*

$$\left(X^2 + \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \right) U = 0,$$

ou encore

$$C(X)\, U = 0$$

avec

$$C(X) = \begin{pmatrix} X^2 + X + 1 & 2X \\ 1 & X^2 + X + 2 \end{pmatrix}.$$

On a $\det(C(X)) = X^4 + 2X^3 + 4X^2 + X + 2$, *ce qui entraîne que les suites* u_{ij} *sont récurrentes linéaires sur* $\mathbb{Z}$ *et vérifient, pour* (i,j) *tel que* $1 \leq i, j \leq 2$ *la relation :*

$$u_{ij}(n+4) + 2u_{ij}(n+3) + 4u_{ij}(n+2) + u_{ij}(n+1) + 2u_{ij}(n) = 0, \forall n \in \mathbb{N}.$$

Proposition 2.6 *Soit* A *un anneau commutatif et soit* $s \in \mathbb{N}^*$. *Soit* $\mathbb{M}$ *l'anneau des matrices carrées d'ordre* s *à coefficients dans* A. *L'ensemble* $SRL_{\mathbb{M}}(\mathbb{M})$ *des suites récurrentes linéaires sur* $\mathbb{M}$ *est un sous-*$\mathbb{M}[X]$*-module de* $S(\mathbb{M})$.

Preuve : Soit $U = (u_{ij})_{1 \leq i,j \leq s} \in SRL_{\mathbb{M}}(\mathbb{M})$ et soit $m \in \mathbb{M}$. D'après la proposition 4.1 les suites u_{ij} sont récurrentes linéaires sur A. Comme les coefficients

de la matrice mU sont des combinaisons linéaires des u_{ij} sur l'anneau commutatif A, alors les coefficients de la matrice mU sont des suites récurrentes linéaires sur A. La proposition 4.1 entraîne que la suite mU est récurrente linéaire sur $\mathbb{M}$.
Soient maintenant U et V deux suites récurrentes linéaires sur $\mathbb{M}$, alors $U+V = (u_{ij} + v_{ij})_{1\leq i,j\leq s}$. Les coefficients de la matrice $U + V$ sont des suites récurrentes linéaires sur A en tant que sommes de deux suites récurrentes linéaires sur l'anneau commutatif A. Par suite, d'après la proposition 4.1, la suite $U+V$ est une suite récurrente linéaire sur $\mathbb{M}$.
Comme $SRL_{\mathbb{M}}(\mathbb{M})$ est stable par l'endomorphisme shift, on en déduit le résultat.

□

Corollaire 2.2 *Tout sous-anneau intègre de $\mathbb{M}$ est un domaine de Ore.*

Preuve : En effet, comme la somme de suites récurrentes linéaires sur un anneau de matrices est une suite récurrente linéaire, la remarque **2.1** donne le résultat voulu**.**

□

Remarque 2.2 .

1. *Soit A un anneau commutatif et $s, t \in \mathbb{N}^*$. Soit $\mathbb{M}$ l'anneau des matrices carrées d'ordre s à coefficients dans A.Si on prend $M = A^s$ ou $M = \mathbb{M}_{s,t}$ l'ensemble des matrices à s lignes et t colonnes et à coefficients dans A, on voit en utilisant la preuve de la Proposition 4.1, que $SRL_{\mathbb{M}}(M)$ est un $\mathbb{M}[X]$-module.*
2. *Soit M un $\mathbb{M}$-module à gauche. Sans rien changer dans la preuve de la Proposition 4.1, on peut montrer que l'ensemble $SRL_{\mathbb{M}}(M)$ des suites récurrentes linéaires à valeurs dans M et à coefficients dans $\mathbb{M}$ est stable pour l'addition et l'opérateur shift. Cependant, la stabilité n'est pas assurée pour la multiplication par les scalaires.*

2.6 Suites récurrentes linéaires sur un corps non commutatif

Dans cette section, on montrera que l'ensemble des suites récurrentes linéaires à coefficients sur un corps non commutatif D et à valeurs dans un D-module conserve la structure usuelle de $D[X]$-module. Lorsque le corps est de dimension finie sur son centre, on pourra déterminer effectivement une relation de récurrence linéaire pour la somme de deux suites récurrentes linéaires.

Proposition 2.7 *Soit D un corps et M un D-module. Alors l'ensemble $SRL_D(M)$ des suites récurrentes linéaires à valeurs dans M et à coefficients dans D est un sous-module du $D[X]$-module $S(M)$.*

Preuve : Soit D un corps et M un D-module. Soient $u, v \in SRL_D(M)$, de polynômes caractéristiques respectifs P et Q. D'après le théorème 2.4, $D[X]$ est un anneau de Ore, donc il existe deux polynômes R et S dans $D[X]$, tels que $RP = SQ$. Quitte à multiplier par un scalaire, on peut supposer que les polynômes R et S sont unitaires et on a

$$RP(u+v) = RPu + RPv = R(Pu) + S(Qv) = 0.$$

Il en découle que RP est un polynôme caractéristique pour la suite $u+v$, ce qui entraîne que $u+v \in SRL_D(M)$.

D'autre part, si $\alpha \in D$, $\alpha \neq 0$, on a

$$\alpha P \alpha^{-1}(\alpha u) = 0,$$

où le polynôme $\alpha P \alpha^{-1}$ est un polynôme unitaire. D'où $\alpha u \in SRL_D(M)$

Comme $SRL_D(M)$ est stable par l'endomorphisme shift, alors le lemme 2.1 permet de conclure.

□

Remarque 2.3 *Dans la preuve ci-dessus, on voit que si* $P(X) = X^h + a_{h-1}X^{h-1} + \cdots + a_0$ *est un polynôme caractéristique pour la suite récurrente* u*, alors, pour tout* $\alpha \in D$*,* $\alpha \neq 0$*, le polynôme*

$$Q(X) = X^h + \alpha a_{h-1}\alpha^{-1}X^{h-1} + \cdots + \alpha a_0\alpha^{-1}$$

est un polynôme caractéristique pour la suite αu*.*

Si on remplace le corps non commutatif D par un un domaine de Ore A, alors les polynômes R et S pourraient ne pas être unitaires (et ne pas avoir de coefficient dominant inversible), et, dans ce cas, l'ensemble $SRL_A(M)$ pourrait ne pas être un sous-module du $A[X]$-module $S(M)$. Cela nous conduit à la généralisation suivante de la définition d'un anneau de Fatou.

Définition 2.7 *Soit* A *un domaine de Ore à gauche de corps de fractions à gauche* Q*. On dira que* A *est un anneau de Fatou à gauche si on a :*

$$\forall u \in S(A), u \in SRL_Q(Q) \Rightarrow u \in SRL_A(A).$$

On obtient alors clairement le résultat suivant.

Proposition 2.8 *Si* A *est un anneau de Fatou, l'ensemble* $SRL_A(A)$ *des suites récurrentes linéaires sur* A *est un sous-module du* $A[X]$*-module* $S(A)$*.*

Rappelons maintenant le résultat suivant, dû à Jacobson, qui va nous permettre de construire le polynôme caractéristique de deux suites récurrentes linéaires lorsque le corps non commutatif est de dimension finie sur son centre.

Lemme 2.2 (Jacobson) *Soit* m *et* d *deux entiers naturels non nuls et soit* D *un corps de dimension* d *sur son centre* F*. Alors pour tout polynôme* $f(X) \in D[X]$*, de degré* m*, il existe un polynôme* $g(X) \in D[X]$*, non nul, de degré* $m(d-1)$*, et tel que* $f(X)g(X) = g(X)f(X) \in F[X]$*.*

Décrivons brièvement l'algorithme de détermination du polynôme g. Notons

$$f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0,$$

et

$$V = De_1 \oplus De_2 \oplus \cdots \oplus De_m,$$

où $\{e_1, \ldots, e_m\}$ est une base du D-module à gauche V. Soit φ l'endomorphisme de V défini par

$$\varphi(e_i) = e_{i+1} \text{ pour } 1 \leq i \leq m-1 \text{ et } \varphi(e_m) = -a_0e_1 - a_1e_2 - \cdots - a_{m-1}e_m.$$

alors $f(\varphi) = 0$. Regardons V comme espace vectoriel sur F ; φ est un F-endomorphisme. Notons h son polynôme caractéristique. Par division euclidienne de h par f, il existe deux polynômes g et r dans $D[X]$ tels que

$$h = gf + r, \deg r < m.$$

Posons $r(X) = r_{m-1}X^{m-1} + r_{m-2}X^{m-2} + \cdots + r_0$. Comme $r(\varphi) = 0$, on a $r(\varphi)(e_1) = r_0e_1 + \cdots + r_{m-1}e_m = 0$, d'où $r = 0$ et $h = gf$.

Proposition 2.9 *Soit d un entier naturel non nul. Soit D un corps non commutatif de dimension d sur son centre F. Soit M un D-module. Soient u et v deux éléments de $SRL_D(M)$ de polynômes minimaux f_1 et f_2 respectivement. On pose $s = \deg f_1$ et $t = \deg f_2$ et on suppose $s \leq t$. Notons g_1 le polynôme donné par le lemme de Jacobson et correspondant au polynôme f_1. Alors :*
1) le polynôme $f_1g_1f_2$ est un polynôme caractéristique de la suite $u + v$,
2) la suite récurrente $u + v$ est de longueur inférieure à $ds + t$.

Preuve : Soit u et v deux suites récurrentes linéaires à valeurs dans M et à coefficients dans D. Soit f_1 (resp. f_2) le polynôme minimal de u (resp. v).

D'après le lemme de Jacobson, il existe un polynôme g_1 dans $D[X]$ tel que $f_1 g_1 = g_1 f_1 \in F[X]$. On a alors

$$\begin{aligned} f_1 g_1 f_2.(u+v) &= (f_1 g_1) f_2.u + (f_1 g_1)(f_2.v) = f_2 (f_1 g_1).u \\ &= f_2 g_1 (f_1.u) = 0. \end{aligned}$$

D'après le lemme de Jacobson, le polynôme g_1 est de degré $s(d-1)$; on en déduit que le polynôme $f_1 g_1 f_2$, qui annule $u+v$, est de degré $ds+t$, d'où le résultat annoncé.

□

Exemple 2.8 *Soit F un corps commutatif tel que -1 ne soit pas somme de deux carrés et soit $\mathbb{H}$ un corps de quaternions de centre F. Rappelons que $\mathbb{H}$ est une algèbre sur F ayant pour base les éléments $1, i, j$ et k vérifiant :*

$$ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

Soient u et v les suites définies sur $\mathbb{H}$ par

$$\begin{aligned} u(0) &= 1 \text{ et } u(n+1) = (i+j)\,u(n),\ \forall\ n \in \mathbb{N}, \\ v(0) &= i,\ v(1) = j, \text{ et } v(n+2) = iv(n+1) + jv(n),\ \forall\ n \in \mathbb{N}, \end{aligned}$$

de polynômes minimaux respectifs $f_1(X) = X-(i+j)$ et $f_2(X) = X^2-iX-j$. On considère l'endomorphisme φ de $\mathbb{H}$ défini par : $\varphi(x) = (i+j)x$.
Comme

$$\begin{cases} \varphi(1) = i+j \\ \varphi(i) = (i+j)i = -1-k \\ \varphi(j) = (i+j)j = -1+k \\ \varphi(k) = (i+j)k = i-j, \end{cases}$$

la matrice associée à φ, considérée comme F-endomorphisme, relativement à

la base $(1, i, j, k)$ *est donnée par :*

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

Soit $h(X) = X^4 + 4X^2 + 4$ *le polynôme caractéristique de la matrice* A*, on a*

$$h(X) = \left(X^3 + (i+j)X^2 + 2X + 2(i+j)\right)(X - (i+j)).$$

Notons $w = u + v$*, alors* $f(X) = h(X) f_2(X)$ *est dans l'annulateur de* w*, ce qui donne une relation de récurrence linéaire pour la suite* w *de longueur* 6*. Dans cet exemple, on remarque que :*

$$h(X) = \left(X^2 + 2\right)^2 = (X + i + j)^2 (X - (i+j))^2,$$

par conséquent le polynôme $(X^2 + 2) f_2(X)$ *est dans l'annulateur de* w*, ce qui donne une relation de récurrence plus courte pour la suite* w*, de longueur* 4 :

$$w(n+4) = iw(n+3) + (j-2)w(n+2) + 2iw(n+1) + 2jw(n).$$

Exemple 2.9 *Soit encore* $\mathbb{H}$ *un corps de quaternions de centre* F *comme précedemment et* u *et* v *les suites définies sur* $\mathbb{H}$ *par les relations :*

$$u(0) = 1, u(1) = 0, \text{ et } \forall n \in \mathbb{N}, u(n+2) = iu(n+1) + u(n)$$

$$v(0) = v(1) = v(2) = 1, \text{ et } \forall n \in \mathbb{N}, v(n+3) = v(n+2) + jv(n),$$

de polynômes caractéristiques respectifs

$$f_1(X) = X^2 - iX - 1 \text{ et } f_2(X) = X^3 - X^2 - j.$$

Soit $V = \mathbb{H}e_1 \oplus \mathbb{H}e_2$ *le* $\mathbb{H}$*-module à gauche libre de base* $\{e_1, e_2\}$. *L'endomorphisme* φ *de* V *est alors donné par :*

$$\varphi(e_1) = e_2 \text{ et } \varphi(e_2) = e_1 + ie_2.$$

Désignons par $(u_1, \cdots, u_8)$ *la base canonique de l'espace vectoriel* F^8, *et remarquons que*

$$\forall a + bi + cj + dk \in \mathbb{H}, i(a + bi + cj + dk) = -b + ai - dj + ck.$$

Par "dévissage", on obtient :

$$\begin{aligned}
\varphi(u_i) &= u_{i+4} \text{ pour } 1 \leq i \leq 4, \\
\varphi(u_5) &= u_1 + u_6, \\
\varphi(u_6) &= u_2 - u_5, \\
\varphi(u_7) &= u_3 + u_8, \\
\varphi(u_8) &= u_4 - u_7.
\end{aligned}$$

D'où la matrice :

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

dont le polynôme caractéristique est

$$h(X) = X^8 - 2X^6 + 3X^4 - 2X^2 + 1.$$

La division de $h(X)$ *par* $f_1(X)$ *donne le polynôme*

$$g_1(X) = X^6 + iX^5 - 2X^4 - iX^3 + 2X^2 + iX - 1.$$

On en déduit que $f_1 g_1 f_2$ *est un polynôme caractéristique pour la suite* $u+v$.

2.7 Série génératrice

Il est bien connu que la série génératrice d'une suite sur un corps commutatif est une une fraction rationnelle si, et seulement si, la suite est récurrente linéaire. Cette propriété a été démontrée, sous une forme appropriée, pour les suites récurrentes linéaires à valeurs dans un module sur un anneau commutatif, voir [32], et pour les suites à coefficients matriciels, voir [5]. Nous étendons cette propriété au cas des corps non commutatifs.

Définition 2.8 *Soit* $u = (u(n))_{n\in\mathbb{N}}$ *une suite d'éléments d'un anneau quelconque. La série formelle associée à la suite* u *définie par* $G_u(X) = \sum_{n\geq 0} u(n) X^n$ *est appelée* série génératrice *de* u.

Soit D un corps non commutatif, alors l'anneau de polynômes $D[X]$ est un domaine de Ore à gauche qui admet un anneau des fractions à gauche. Tout élément de cet anneau des fractions s'écrit sous la forme $g^{-1}(X) f(X)$, où $f(X)$ et $g(X)$ sont des polynômes de $D[X]$ et $g(X) \neq 0$.

Proposition 2.10 *Soit D un corps non commutatif et soit u une suite d'éléments de D. Alors les propositions suivantes sont équivalentes*
1. $u \in SRL_D(D)$,
2. *La série génératrice de u est une fraction rationnelle à gauche de la forme $g^{-1}(X) f(X)$, où $f(X)$ et $g(X)$ sont des polynômes de $D[X]$ et $g(0) \neq 0$.*

Preuve : Soit $u \in SRL_D(D)$, de polynôme caractéristique $p(X) = X^h - a_1 X^{h-1} - \cdots - a_h \in D[X]$. Posons $g(X) = 1 - a_1 X - \cdots - a_h X^h$. Dans le produit $g(X) G_u(X)$, le coefficient de X^m est nul pour $m \geq h$ et on a alors

$$\begin{aligned} & g(X) G_u(X) \\ = \; & u(0) + (u(1) - a_1 u(0)) X + \cdots + (u(h-1) - a_1 u(h-2) - \cdots - a_{h-1} u(0)) X^{h-1} \\ = \; & f(X). \end{aligned}$$

On en déduit que $G_u(X) = g^{-1}(X) f(X)$, avec $g(0) \neq 0$.

Réciproquement, soit $u \in S(D)$ et supposons que la série génératrice de u est une fraction rationnelle à gauche de la forme $G_u(X) = g^{-1}(X) f(X)$, où $f(X) = a_0 + a_1 X + \cdots + a_h X^h, g(X) = b_0 + b_1 X + \cdots + b_k X^k$ et $b_0 \neq 0$. On a alors

$$\begin{aligned} & \left(b_0 + b_1 X + \cdots + b_k X^k\right) \left(u(0) + u(1) X + u(2) X^2 + \cdots\right) \\ = \; & b_0 u(0) + (b_0 u(1) + b_1 u(0)) X + \cdots + \left(b_0 u(h) + \cdots + b_k u(h-k) X^h\right). \end{aligned}$$

Par identification, on tire la relation de récurrence

$$\forall n \in \mathbb{N}, u(n+h+1) = -b_0^{-1} (b_1 u(n+h) + b_2 u(n+h-1) + \cdots + b_k u(n+h-k)),$$

et, par suite, $u \in SRL_D(D)$.

□

Chapitre 3

Application à la recherche de codes quasi-cycliques

3.1 Introduction

Ce chapitre est consacré à des résultats récents concernant la représentation des codes quasi-cycliques en liaison avec les suites récurrentes linéaires. Dans [7], en considérant des suites récurrentes linéaires sur des anneaux de matrices à coefficients dans un corps fini, les auteurs parviennent à construire de nouveaux codes quasi-cycliques auto-duaux ayant les meilleures distances minimales connues pour les mêmes paramètres. Cependant, cette approche ne recoupe pas l'ensemble de tous les codes quasi-cycliques. Par la suite, dans [2], il est démontré que les codes quasi-cycliques peuvent être regardés comme analogues des codes cycliques : ce sont des idéaux engendrés par des polynômes générateurs à coefficients matriciels. Et plus encore, il y a une correspondance bijective entre les codes ℓ-quasi-cycliques de longueur $m\ell$ et les idéaux de l'anneau des polynômes à coefficients matriciels $\mathbb{M}_\ell(\mathbb{F}_q)[X]/(X^m-1)$. Ceci a permis de déduire que l'anneau $\mathbb{M}_\ell(\mathbb{F}_q)[X]/(X^m-1)$ est principal. Cette interprétation des codes quasi-cycliques a donné lieu à de nouvelles notions

telles que les codes quasi-BCH. Elle a aussi pour résultat la construction de nouveaux codes ayant les meilleurs distances minimales tels que le code de paramètres $[189, 11, 125]_{\mathbb{F}_4}$ et 48 autres codes dérivés.

3.2 Codes quasi-cycliques et suites récurrentes linéaires sur un anneau de matrices (Cayrel-Chabot-Necer)

Le lien entre codes cycliques et suites récurrentes linéaires est bien connu, voir le théorème 3.3. Cette section est consacrée à la représentation des codes quasi-cycliques à partir de suites récurrentes linéaires à coefficients matriciels.

3.2.1 Suites récurrentes linéaires à coefficients matriciels

Dans cette partie, nous verrons qu'un code quasi-cyclique peut être obtenu comme ensemble de suites périodiques annulées par un polynôme matriciel réversible.

Soit l'anneau $\mathbb{A} = \mathbb{F}_q^\ell$ et soit $S(\mathbb{A})$ l'anneau des suites d'éléments de $\mathbb{A}$. On note $\mathbb{M}_\ell(\mathbb{F}_q)$ l'anneau des matrices carrées d'ordre ℓ à coefficients dans $\mathbb{F}_q$. Rappelons que l'opérateur shift , noté T est défini par

$$\forall u \in S(\mathbb{A}), Tu(n) = u(n+1), \forall n \in \mathbb{N}.$$

Notons $P(X) = \sum_{i=0}^{h} a_i X^i \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$. On munit $S(\mathbb{A})$ d'une structure de $\mathbb{M}_\ell(\mathbb{F}_q)[X]$-module à gauche en posant :

$$\begin{aligned} \mathbb{M}_\ell(\mathbb{F}_q)[X] \times S(\mathbb{A}) &\to S(\mathbb{A}) \\ (P(X), u) &\to P.u = \sum_{i=0}^{h} a_i T^i u. \end{aligned}$$

Définition 3.1 *Soit $u \in S(\mathbb{A})$.* L'annulateur *de u, noté $Ann(u)$, est défini par*

$$Ann(u) = \{P \in \mathbb{M}_\ell(\mathbb{F}_q)[X] : P.u = 0\}.$$

Une suite $u \in S(\mathbb{A})$ est dite récurrente linéaire à coefficients matriciels *si $Ann(u)$ contient un polynôme unitaire.*

Pour $P \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$, on pose

$$\Omega(P) = \{u \in S(\mathbb{A}) : P.u = 0\}.$$

Définition 3.2 *Un polynôme $P \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$ est dit* réversible *si son coefficient dominant et son coefficient constant sont des matrices inversibles.*

Si P est réversible, alors il existe $e \in \mathbb{N}^*$ tel que P divise $X^e - 1$. Plus précisément, il existe Q tel que $PQ = QP = X^e - 1$.

Proposition 3.1 *Soit $P \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$ un polynôme réversible. Alors*
1) Il existe un entier m tel que tout élément de $\Omega(P)$ est une suite périodique de période m.
2) L'ensemble $\mathcal{C}(P) = \{(u_0, ..., u_{m-1}) \in \mathbb{A}^m : u \in \Omega(P)\}$ est un code cyclique sur $\mathbb{F}_q$ et sur $\mathbb{M}_\ell(\mathbb{F}_q)$.
3) $\dim_{\mathbb{F}_q} \Omega(P) = \ell \deg(P)$.

En fait $\Omega(P)$ est un code ℓ-quasi-cyclique de longueur $m\ell$ sur $\mathbb{F}_q$.

3.2.2 Codes quasi-cycliques comme codes cycliques sur un anneau

Dans cette partie aussi, nous verrons qu'un code quasi-cyclique peut être obtenu comme partie de $\left(\mathbb{F}_q^\ell\right)^m$ annulée par un polynôme de l'anneau $\mathbb{M}_\ell\left(\mathbb{F}_q\right)[X]/(X^m-1)$.

Soit $\mathbb{A}=\mathbb{F}_q^\ell, n=\ell m$, et soit $\mathcal{C}$ un code de longueur n sur $\mathbb{F}_q$. L'application :

$$\Theta : \mathbb{F}_q^n \to \mathbb{A}^m$$

$$c=(c_0,c_1,...,c_{n-1}) \mapsto \Theta(c)=\left({}^t(c_0,...,c_{\ell-1}),{}^t(c_\ell,...,c_{2\ell-1}),...,{}^t\left(c_{(m-1)\ell},...,c_{m\ell-1}\right)\right)$$

est un isomorphisme de $\mathbb{F}_q$-espaces vectoriels, et on a

$\mathcal{C}$ est quasi-cyclique d'indice $\ell \Leftrightarrow \Theta(\mathcal{C})$ est cyclique sur $\mathbb{A}$.

Soient $P \in \mathbb{M}_\ell\left(\mathbb{F}_q\right)[X]/(X^m-1)$ et $x \in \left(\mathbb{F}_q^\ell\right)^m$. On définit comme précédemment le produit $P.x$ et on a là aussi une structure de $\mathbb{M}_\ell\left(\mathbb{F}_q\right)[X]/(X^m-1)$-module à gauche. On note encore

$$\Omega(P)=\{x \in \left(\mathbb{F}_q^\ell\right)^m : P.x=0\}.$$

C'est un $\mathbb{F}_q$-espace vectoriel. La proposition qui suit donne une description précise de $\Omega(P)$ à partir de la factorisation du polynôme X^m-1.

Proposition 3.2 *Soit P et Q deux polynômes de $\mathbb{M}_\ell\left(\mathbb{F}_q\right)[X]$ tels que $PQ=X^m-1$. Alors*

$$\Omega(P)=\{Qx : x \in \mathbb{A}^m\}=Q\mathbb{A}^m.$$

Preuve : Soit $y \in Q\mathbb{A}^m$ alors il existe $y_0 \in \mathbb{A}^m$ tel que $Py=PQy_0=(X^m-1)y_0$, d'où $y \in \Omega(P)$ et donc $Q\mathbb{A}^m \subset \Omega(P)$.
Soit maintenant l'application $\Phi_Q : \mathbb{A}^m \to \mathbb{A}^m$ définie par $\Phi_Q(y)=Qy$. C'est un morphisme de $\mathbb{F}_q$-espace vectoriel, et on a $\ker(\Phi_Q)=\Omega(Q)$ et $Im(\Phi_Q)=$

$Q\mathbb{A}^m$. On obtient alors

$$\begin{aligned}\dim\left(Q\mathbb{A}^m\right) &= \ell m - \dim\left(\Omega\left(Q\right)\right)\\ &= \ell m - \ell\deg\left(Q\right)\\ &= \ell m - \ell\left(m - \deg\left(P\right)\right)\\ &= \ell\deg\left(P\right) = \dim\left(\Omega\left(P\right)\right).\end{aligned}$$

D'où le résultat.

□

Corollaire 3.1 *Soit P et Q deux polynômes de $\mathbb{M}_\ell\left(\mathbb{F}_q\right)[X]$ tels que $PQ = X^m - 1$. Notons $Q\left(X\right) = q_0 + q_1X + \cdots + q_{\deg(Q)}X^{\deg(Q)}$. Alors une matrice génératrice de $\Omega\left(P\right)$ est donnée par :*

$$G_{\Omega(P)} = \begin{pmatrix} {}^tq_0 & {}^tq_1 & {}^tq_2 & \cdots & {}^tq_{\deg(Q)} & 0 & 0 & \cdots & 0\\ 0 & {}^tq_0 & {}^tq_1 & \cdots & {}^tq_{\deg(Q)-1} & {}^tq_{\deg(Q)} & 0 & \cdots & 0\\ \vdots & \ddots & & & \ddots & & & \ddots & \vdots\\ 0 & 0 & & & \cdots & 0 & {}^tq_0 & \cdots & {}^tq_{\deg(Q)}\end{pmatrix}.$$

Exemple 3.1 *On prend $m = 5$ et $\ell = 2$ dans $\mathbb{F}_4 = \mathbb{F}_2\left[\theta\right]$ où $\theta^2 + \theta + 1 = 0$.*

Soit

$$P\left(X\right) = X^2 + \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}X + \begin{pmatrix}0 & \theta\\ \theta^2 & 1\end{pmatrix},$$

et

$$Q\left(X\right) = X^3 + \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}X^2 + \begin{pmatrix}1 & \theta\\ \theta^2 & 1\end{pmatrix}X + \begin{pmatrix}1 & \theta\\ \theta^2 & 0\end{pmatrix}.$$

On a bien $PQ = X^5 - 1$, d'où une matrice génératrice

$$G_{\Omega(P)} = \begin{pmatrix} 1 & \theta^2 & 1 & \theta^2 & 1 & 0 & 1 & 0 & 0 & 0 \\ \theta & 0 & \theta & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \theta^2 & 1 & \theta^2 & 1 & 0 & 1 & 0 \\ 0 & 0 & \theta & 0 & \theta & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

3.2.3 Construction de codes quasi-cycliques auto-duaux

Cette sous-section est consacrée à la construction de codes quasi-cycliques auto-duaux.

Définition 3.3 *Si $\mathcal{R}$ est un anneau commutatif, le* produit scalaire euclidien *sur $\mathcal{R}^n$ est donné par*

$$\forall a = (a_1, \cdots, a_n) \in \mathcal{R}^n, \forall b = (b_1, \cdots, b_n) \in \mathcal{R}^n, < a, b >= \sum_{i=1}^{n} a_i b_i.$$

Un *code linéaire de longueur n sur un anneau commutatif $\mathcal{R}$* est un $\mathcal{R}$-sous-module de $\mathcal{R}^n$. Le *code dual euclidien* $\mathcal{C}^\perp$ d'un code linéaire $\mathcal{C}$ est défini par

$$\mathcal{C}^\perp = \{d \in \mathcal{R}^n : \forall c \in \mathcal{C}, \langle c, d \rangle = 0\}.$$

Lorsque $\mathcal{C}^\perp = \mathcal{C}$, le code est dit *auto-dual*.

Par analogie avec le cas des codes cycliques, on obtient le résultat suivant concernant le code dual $\Omega(P)^\perp$.

Théorème 3.1 *Soient P et Q deux polynômes réversibles tels que $PQ = X^m - 1$. Alors*

$$\Omega(P)^{\perp} = \Omega\left({}^{t}Q^{*}\right).$$

En conséquence, pour la recherche des codes quasi-cycliques auto-duaux, on posera $m = 2m'$ et on recherchera des polynômes P de degré m' à coefficients matriciels vérifiant l'équation $X^m - 1 = P.{}^{t}P^{*}$.

On peut aussi chercher de tels polynômes en imposant la condition $P = {}^{t}P^{*}$, ce qui réduit le nombre d'inconnues de moitié dans les équations à résoudre. Il s'avère que cette condition n'est pas contraignante et donne les meilleurs codes (plus grandes distances minimales).

Table de codes auto-duaux euclidiens

n	meilleure borne connue	meilleure distance trouvée	nombre de codes
8	4	**4**	2
12	6	4	2
16	6	**6**	3
20	8	7	2
24	8-10	**8**	9
28	9-11	**9**	2
32	10-12	**10**	8
36	10-14	**10**	22
40	12-16	**12**	8
56	15-21	**15**	2
60	16-23	**16**	1

Dans la colonne qui donne la meilleure borne connue, la notation *a*-*b* signifie que a est la meilleure distance connue et b est la borne supérieure théorique.

Exemple

L'un des $[8, 4, 4]$ codes binaires est obtenu à partir du polynôme

$$P(X) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X^2 + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

dont une matrice génératrice est

$$G_{\Omega(P)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

3.3 Les codes quasi-cycliques comme analogues des codes cycliques (Barbier-Chabot-Quintin)

Dans cette section, nous verrons que les codes quasi-cycliques sont des analogues des codes cycliques : Il existe une correspondance bijective entre l'ensemble des codes ℓ-quasi-cycliques de longueur $m\ell$ sur $\mathbb{F}_q$ et l'ensemble des idéaux de l'anneau $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$.

3.3.1 Pliage et dépliage d'un code

On définit dans ce qui suit deux applications qui permettent de relier les codes quasi-cycliques aux codes cycliques.

Soit ℓ un entier positif, alors il existe un polynôme irréductible $P(X) \in \mathbb{F}_q[X]$, de degré ℓ, et $\alpha \in \mathbb{F}_{q^\ell}$ une racine de $P(X)$ tel que

$$\mathbb{F}_{q^\ell} = \mathbb{F}_q[\alpha] \simeq \mathbb{F}_q[X]/(P(X)).$$

On définit le *pliage* de $a \in \mathbb{F}_q^\ell$ par l'application

$$\begin{array}{rcl} \phi & : & \mathbb{F}_q^{\ell} \to \mathbb{F}_q[\alpha] \\ (a_1, a_2, \cdots, a_\ell) & \mapsto & a_1 + a_2\alpha + \cdots + a_\ell\alpha^{\ell-1}. \end{array}$$

L'application réciproque

$$\begin{array}{rcl} \phi^{-1} & : & \mathbb{F}_q[\alpha] \to \mathbb{F}_q^{\ell} \\ a_1 + a_2 + \cdots + a_\ell & \mapsto & (a_1, a_2, \cdots, a_\ell) \end{array}$$

définit le *dépliage* de $a \in \mathbb{F}_q[\alpha]$.

Remarquons que ces applications sont $\mathbb{F}_q$-linéaires. On étend ces définitions aux codes. On appellera $\mathbb{F}_q$-code de longueur m sur $\mathbb{F}_{q^\ell}$ toute partie de $\left(\mathbb{F}_{q^\ell}\right)^m$ stable par addition et par multiplication par un élément de $\mathbb{F}_q$.

Définition 3.4 (code plié) *Soit $\mathcal{C}$ un $\mathbb{F}_q$-code de longueur m sur $\mathbb{F}_{q^\ell}$. On définit le* pliage *du code $\mathcal{C}$ par*

$$\phi(\mathcal{C}) = \{(\phi(c_1), \cdots, \phi(c_m)) : c = (c_1, \cdots, c_m) \in \mathcal{C}\}.$$

Définition 3.5 (code déplié) *Soit $\mathcal{C}$ un $\mathbb{F}_q$-code dans $\left(\mathbb{F}_{q^\ell}\right)^m$. On définit le* dépliage *du code $\mathcal{C}$ par*

$$\phi^{-1}(\mathcal{C}) = \left\{\left(\phi^{-1}(c_1), \cdots, \phi^{-1}(c_m)\right) : c = (c_1, \cdots, c_m) \in \mathcal{C}\right\}.$$

Soit i, j et n des entiers tels que $1 \leq i \leq j \leq n$. On note $pr_{i,j}$ la projection définie par

$$\begin{array}{rcl} pr_{i,j} & : & \mathbb{F}_q^n \to \mathbb{F}_q^{j-i+1} \\ (x_1, \cdots, x_n) & \mapsto & (x_i, x_{i+1}, \cdots, x_j). \end{array}$$

Lemme 3.1 *Soit $\mathcal{C}$ un code ℓ-quasi-cyclique de longueur $m\ell$ sur $\mathbb{F}_q$ et soit $r = \dim pr_{1,\ell}(\mathcal{C})$. Alors pour toute matrice génératrice G de $\mathcal{C}$, et pour tout entier $i, 0 \leq i \leq m-1$, le rang des colonnes $i\ell+1, i\ell+2, \cdots, (i+1)\ell$ de G est égal à r.*

Définition 3.6 (rang-bloc) *Avec les notations précédentes, l'entier r défini dans le lemme précédent est appelé* rang-bloc *de $\mathcal{C}$.*

Remarque 3.1 *Le code plié d'un code ℓ-quasi-cyclique de longueur $m\ell$ sur $\mathbb{F}_q$ est un $\mathbb{F}_q$-code cyclique de longueur m sur $\mathbb{F}_{q^\ell}$. Le code déplié d'un code cyclique de longueur m sur $\mathbb{F}_{q^\ell}$ est un code ℓ-quasi-cyclique de longueur $m\ell$ sur $\mathbb{F}_q$.*

3.3.2 Construction d'un code quasi-cyclique à partir d'un idéal principal

Cette sous-section est consacrée à la construction d'un code quasi-cyclique à partir d'un idéal de l'anneau $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$.

Soit $\mathcal{I}$ un idéal de $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$. Pour $i = 1, \cdots, \ell$, considérons les applications $\mathbb{F}_q$-linéaires suivantes :

$$\begin{aligned} L_i &: M_\ell(\mathbb{F}_q)[X]/(X^m-1) \to \mathbb{F}_q^{m\ell} \\ Q(X) &= \sum_{j=0}^{m-1} Q_j X^j \mapsto L_i(Q(X)) = (L_i(Q_0), \cdots, L_i(Q_{m-1})), \end{aligned}$$

où $L_i(Q_j)$ désigne la $i^{ème}$ ligne de la matrice Q_j.

Définition 3.7 (code associé à un idéal) *Soit $\mathcal{I}$ un idéal de $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$. On définit le code $\mathcal{C}_\mathcal{I}$ associé à $\mathcal{I}$ par*

$$\mathcal{C}_\mathcal{I} = \sum_{i=1}^{\ell} L_i(\mathcal{I}),$$

le $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{F}_q^{\ell m}$ engendré par les vecteurs de $L_1(\mathcal{I}), \cdots, L_\ell(\mathcal{I})$.

Proposition 3.3 *Avec les notations précédentes, on a*

$$\mathcal{C}_{\mathcal{I}} = L_1(\mathcal{I}).$$

Remarque 3.2 *On a les propriétés suivantes*
1) L'idéal $\mathcal{I}$ est un $\mathbb{F}_q$-espace vectoriel, donc $\mathcal{C}_{\mathcal{I}}$ l'est aussi.
2) La multiplication par X dans $\mathcal{I}$ correspond au ℓ-shift dans $\mathcal{C}_{\mathcal{I}}$.
3) La multiplication par une matrice dans $\mathcal{I}$ correspond à des combinaisons linéaires de mots dans $\mathcal{C}_{\mathcal{I}}$.

Corollaire 3.2 *Soit $\mathcal{I}$ un idéal de $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$. Alors il existe des polynômes $P_1(X), \cdots, P_r(X)$ tels que $\mathcal{I} = \langle P_1(X), \cdots, P_r(X)\rangle$ et $\mathcal{C}_{\mathcal{I}}$ est engendré par l'ensemble*

$$\left\{L_k\left(X^i P_j(X)\right) : i = 0, \cdots, m-1,\ j = 1, \cdots, r,\ k = 1, \cdots, \ell\right\}$$

en tant qu'espace vectoriel sur $\mathbb{F}_q$. De plus, $\mathcal{C}_{\mathcal{I}}$ est un code ℓ-quasi-cyclique de longueur $m\ell$ sur $\mathbb{F}_q$.

Exemple 3.2 *Soit $\mathbb{F}_4 = \mathbb{F}_2[\omega]$ et $\mathcal{I} = \langle P(X), Q(X)\rangle \subset M_3(\mathbb{F}_4)[X]/(X^5-1)$ avec*

$$P(X) = \begin{pmatrix} \omega & 0 & 1 \\ \omega & \omega & 0 \\ \omega^2 & \omega^2 & 0 \end{pmatrix} X^4 + \begin{pmatrix} \omega & \omega^2 & \omega^2 \\ 0 & \omega & 1 \\ \omega^2 & 0 & \omega \end{pmatrix} X^3 + \begin{pmatrix} 0 & \omega^2 & \omega \\ \omega & \omega^2 & \omega^2 \\ 0 & 1 & \omega^2 \end{pmatrix} X^2 + \begin{pmatrix} 1 & 0 & \omega^2 \\ 0 & \omega & 1 \\ 0 & \omega & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 0 & \omega^2 \\ 0 & 1 & \omega^2 \\ 0 & 0 & 0 \end{pmatrix}$$

et

$$Q(X) = \begin{pmatrix} \omega & 0 & 1 \\ \omega & \omega & 0 \\ \omega^2 & \omega^2 & 0 \end{pmatrix} X^4 + \begin{pmatrix} 0 & 1 & \omega^2 \\ 0 & 1 & \omega^2 \\ 0 & \omega & 1 \end{pmatrix} X^3 + \begin{pmatrix} \omega & \omega^2 & \omega^2 \\ 1 & \omega & \omega \\ \omega & \omega^2 & \omega^2 \end{pmatrix} X^2 +$$

$$\begin{pmatrix} 1 & \omega^2 & 1 \\ 0 & \omega^2 & \omega \\ 0 & 1 & \omega^2 \end{pmatrix} X + \begin{pmatrix} 1 & 1 & 0 \\ \omega & \omega^2 & \omega^2 \\ \omega^2 & 1 & 1 \end{pmatrix}.$$

Ici $\ell = 3, m = 5, r = 2$ *et* $\mathcal{C}_{\mathcal{I}}$ *est un code* 3*-quasi-cyclique de longueur* 15 *sur* $\mathbb{F}_4$*, engendré par les* 30 *vecteurs*

$$\begin{aligned}
\left(\omega, 0, 1, \omega, \omega^2, \omega^2, 0, \omega^2, \omega, 1, 0, \omega^2, 1, 0, \omega^2\right) &= L_1\left(P\left(X\right)\right), \\
\left(\omega, \omega, 0, 0, \omega, 1, \omega, \omega^2, \omega^2, 0, \omega, 1, 0, 1, \omega^2\right) &= L_2\left(P\left(X\right)\right), \\
\left(\omega^2, \omega^2, 0, \omega^2, 0, \omega, 0, 1, \omega^2, 0, \omega, 1, 0, 0, 0\right) &= L_3\left(P\left(X\right)\right), \\
\left(\omega, \omega^2, \omega^2, 0, \omega^2, \omega, 1, 0, \omega^2, 1, 0, \omega^2, \omega, 0, 1\right) &= L_1\left(XP\left(X\right)\right), \\
\left(0, \omega, 1, \omega, \omega^2, \omega^2, 0, \omega, 1, 0, 1, \omega^2, \omega, \omega, 0\right) &= L_2\left(XP\left(X\right)\right), \\
\left(\omega^2, 0, \omega, 0, 1, \omega^2, 0, \omega, 1, 0, 0, 0, \omega^2, \omega^2, 0\right) &= L_3\left(XP\left(X\right)\right), \\
\left(0, \omega^2, \omega, 1, 0, \omega^2, 1, 0, \omega^2, \omega, 0, 1, \omega, \omega^2, \omega^2\right) &= L_1\left(X^2P\left(X\right)\right), \\
&\ldots
\end{aligned}$$

3.3.3 Construction d'un idéal principal à partir d'un code quasi-cyclique

Dans cette sous-section, $\mathcal{C}$ désigne un code ℓ-quasi-cyclique de longueur $m\ell$ sur $\mathbb{F}_q$. Un idéal de l'anneau $M_\ell\left(\mathbb{F}_q\right)[X] / \left(X^m - 1\right)$ est construit à partir d'un tel code, ensuite la correspondance bijective entre codes quasi-cycliques et idéaux est établie.

Définition 3.8 *On appelle* premier indice *d'un vecteur non nul* $(x_1, \cdots, x_{m\ell})$ *le plus petit entier* $i, 0 \leq i \leq m-1$*, tel que* $\left(x_{i\ell+1}, \cdots, x_{(i+1)\ell}\right) \neq 0$*. On le note* $\mathcal{F}\left(x_1, \cdots, x_{m\ell}\right)$.

Soit l'application

$$\begin{array}{rcl} p & : & \mathbb{F}_q^{m\ell} \to \mathbb{F}_q^{\ell} \\ (x_1, \cdots, x_{m\ell}) & \mapsto & \left(x_{i\ell+1}, \cdots, x_{(i+1)\ell}\right), \end{array}$$

où $i = \mathcal{F}(x_1, \cdots, x_{m\ell})$ et $p(0) = 0$.

L'algorithme qui suit permet d'obtenir une base formée de r vecteurs de $\mathcal{C}$, où r désigne le rang-bloc de $\mathcal{C}$, et de certains de leurs shifts.

Algorithme 3.1 *Calcul d'une base avec le rang-bloc*

Calculer une matrice génératrice G' de $\mathcal{C}$ sous forme échelonnée suivant les lignes et noter $g_1, \cdots, g_k$ ses lignes.

1 : $F, G \leftarrow \emptyset$.
2 : ***for*** $j = m - 1 \to 0$ ***do***
3 : $B = \{g_i : \mathcal{F}(g_i) = j\}$.
4 : $B'' \leftarrow \emptyset$.
5 : ***for*** *chaque élément* $x \in B$ ***do***
6 : ***if*** $p(F) \cup p(B'') \cup \{p(x)\}$ *sont libres* ***then***
7 : $B'' \leftarrow B'' \cup \{x\}$.
8 : ***end if***
9 : ***end for***
10 : $B \leftarrow B \backslash B''$
11 : *Prendre un sous-ensemble* F' *de* F *tel que* $\#F' = \#B'$.
12 : $F_T \leftarrow \left\{T^{(j-\mathcal{F}(x))\ell}(x) : x \in F'\right\}$.
13 : $G \leftarrow G \cup B'' \cup F_T$.
14 : $F \leftarrow F \cup B''$.
15 : ***end for***
16 : ***return*** F, G.

Corollaire 3.3 *Avec les notations précédentes, il existe des vecteurs $g_1, \cdots, g_r$ de $\mathcal{C}$, linéairement indépendants, tels que $g_1, \cdots, g_r, T^{\ell}(g_1), \cdots, T^{\ell}(g_r), \cdots, T^{(m-1)\ell}(g_1), \cdots, T^{(m-1)\ell}(g_r)$ engendrent $\mathcal{C}$.*

Corollaire 3.4 *Avec les notations précédentes, on note $g_{i,j}$ la $j^{ème}$coordonnée de g_i. Soit*

$$G_i = \begin{pmatrix} g_{1,i\ell+1} & \cdots & g_{1,(i+1)\ell} \\ \vdots & & \vdots \\ g_{r,i\ell+1} & \cdots & g_{r,(i+1)\ell} \\ & 0 & \end{pmatrix} \in M_\ell(\mathbb{F}_q)$$

et

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

où ν est le plus petit entier tel que $G_i \neq 0$. Alors

$$\mathcal{C} = \mathcal{C}_{\langle g(x) \rangle}.$$

Définition 3.9 (Générateur) *Soit $\mathcal{C}$ un code ℓ-quasi-cyclique de longueur $m\ell$ sur $\mathbb{F}_q$. Soit $g_1, \cdots, g_r$ des éléments de $\mathcal{C}$ tels que $g_1, \cdots, g_r, T^\ell(g_1), \cdots, T^\ell(g_r), \cdots, T^{(m-1)\ell}(g_1), \cdots, T^{(m-1)\ell}(g_r)$ engendrent $\mathcal{C}$. Le polynôme $g(X) \in M_\ell(\mathbb{F}_q)[X]$ du corollaire 3.4 est appelé* générateur *de $\mathcal{C}$.*

Théorème 3.2 *Il existe une correspondance bijective entre l'ensemble des codes ℓ-quasi-cycliques de longueur $m\ell$ sur $\mathbb{F}_q$ et l'ensemble des idéaux de $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$. De plus, l'anneau $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$ est principal.*

Preuve : Soit $\mathcal{I}$ un idéal de $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$, $\mathcal{C}_\mathcal{I}$ le code ℓ-quasi-cyclique associé à $\mathcal{I}$ et $g(X)$ le générateur de $\mathcal{C}_\mathcal{I}$. Soit $P(X) \in \mathcal{I}$. Par définition de $g(X)$, il existe $c_{jk}^{(i)} \in \mathbb{F}_q$ tel que

$$L_k(P(X)) = \sum_{i=0}^{m-1} \sum_{j=1}^{r} c_{jk}^{(i)} T^{i\ell}(g_j)$$

pour $k = 1, \cdots, \ell$. D'où

$$P(X) = \left[\sum_{i=0}^{m-1} \begin{pmatrix} c_{11}^{(i)} & \cdots & c_{\ell 1}^{(i)} \\ \vdots & & \vdots \\ c_{1\ell}^{(i)} & \cdots & c_{\ell\ell}^{(i)} \end{pmatrix} X^i \right] g(X).$$

On en déduit que $\mathcal{I} \subset \langle g(X) \rangle$.
Réciproquement, soit $P_1(X), \cdots, P_n(X)$ des générateurs de $\mathcal{I}$. Par définition de $g(X)$, il existe $b_i^{(j)} \in \mathbb{F}_q$ tel que

$$L_j(g(X)) = \sum_{i=1}^{n} b_i^{(j)} L_j(P_i(X)).$$

On a alors

$$g(X) = \sum_{i=1}^{n} \begin{pmatrix} b_1^{(i)} & b_2^{(i)} & \cdots & b_\ell^{(i)} \\ b_1^{(i)} & b_2^{(i)} & \cdots & b_\ell^{(i)} \\ \vdots & \vdots & & \vdots \\ b_1^{(i)} & b_2^{(i)} & \cdots & b_\ell^{(i)} \end{pmatrix} P_i(X),$$

d'où $g(X) \in \mathcal{I}$.

Le corollaire 3.4entraîne alors que les applications $\mathcal{C} \mapsto \langle g(X) \rangle$ et $\mathcal{C} \mapsto \mathcal{C}_{\mathcal{I}}$ sont inverses l'une de l'autre, ce qui permet de conclure.

□

Exemple 3.3 *On reprend l'exemple 3.2 avec* $\mathcal{I} = \langle P(X), Q(X) \rangle \subset M_3(\mathbb{F}_4)[X] / (X^5 - 1)$.

La matrice génératrice échelonnée suivant les lignes du code $\mathcal{C}_{\mathcal{I}}$ est donnée par

$$G = \begin{pmatrix} 1 & 0 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega & \omega & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & \omega & \omega & 0 & 1 & 0 & \omega^2 \\ 0 & 0 & 0 & 1 & 0 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega & \omega & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega^2 & \omega & \omega & 0 & 1 & \omega & \omega & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & \omega^2 & 0 & \omega & 0 & \omega^2 & \omega \end{pmatrix}.$$

D'après l'Algorithme 3.1, $(g_4, g_5, T^{-3}(g_4), T^{-3}(g_5), T^{-6}(g_5))$ est une base de $\mathcal{C}_{\mathcal{I}}$. De plus, le polynôme

$$g(X) = \begin{pmatrix} 0 & 1 & \omega^2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & \omega^2 & \omega \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} X + \begin{pmatrix} \omega & 0 & 1 \\ \omega^2 & 0 & \omega \\ 0 & 0 & 0 \end{pmatrix} X^2 + \begin{pmatrix} \omega & \omega & 0 \\ 0 & \omega^2 & \omega \\ 0 & 0 & 0 \end{pmatrix} X^3$$

est un générateur de $\mathcal{C}_{\mathcal{I}}$ et $\mathcal{I} = \langle P(X), Q(X) \rangle = \langle g(X) \rangle$.

3.3.4 Propriétés des générateurs

Par analogie avec le cas cyclique, le résultat qui suit précise le lien entre le polynôme générateur d'un code quasi-cyclique et le polynôme générateur de son code dual.

Proposition 3.4 *Soit $\mathcal{C}$ un code ℓ-quasi-cyclique de longueur $m\ell$ sur $\mathbb{F}_q$. Soit $P(X)$ un générateur de $\mathcal{C}$ et $Q(X)$ un générateur du code dual $\mathcal{C}^{\perp}$. Notons $Q^*(X)$ le polynôme réciproque de $Q(X)$ et ${}^tQ(X)$ le polynôme dont les coefficients sont les transposés des coefficients de $Q(X)$. Alors il existe $U(X) \in M_\ell(\mathbb{F}_q)[X]$ tel que*

$$P(X)\left({}^tQ^*(X)\right) = U(X)(X^m - 1).$$

3.3.5 Codes Quasi-BCH

Les codes quasi-cycliques étant vus comme analogues des codes cycliques, il est naturel de chercher des définitions équivalentes et des applications pour les codes cycliques classiques tels que les codes BCH.

Définition 3.10 (racine primitive de l'unité) *Soit ℓ, m et e des entiers positifs et soit q une puissance d'un nombre premier. Une matrice $A \in M_\ell(\mathbb{F}_{q^e})$ est appelée* racine primitive $m^{ème}$ *de l'unité si on a*

- $A^m = I_\ell$,
- $A^i \neq I_\ell$ si $i < m$,
- $\det(A^i - A^j) \neq 0$ si $i \neq j, 1 \leq i, j \leq m$.

Proposition 3.5 *Soit q une puissance d'un nombre premier et soit e, ℓ et m des entiers positifs tels que $q^{e\ell} \equiv 1 \mod m$. Alors il existe une racine primitive $m^{ème}$ de l'unité dans $M_\ell(\mathbb{F}_{q^e})$.*

Définition 3.11 (distance minimale de bloc) *Soit $\mathcal{C}$ un code de longueur $m\ell$ sur $\mathbb{F}_q$. La* distance minimale de ℓ-bloc *de $\mathcal{C}$ est par définition la distance minimale du code plié de $\mathcal{C}$.*

Définition 3.12 (code quasi-BCH à gauche) ***Définition 3.13*** *Soit A une racine primitive $m^{ème}$ de l'unité dans $M_\ell(\mathbb{F}_{q^e})$ et soit δ un entier positif tel que $\delta \leq m$. On appelle code ℓ-quasi-BCH à gauche de longueur $m\ell$ sur $\mathbb{F}_q$ défini par A et de distance désignée δ l'ensemble noté $Q\text{-}BCH_q(m, \ell, \delta, A)$ donné par*

$$Q\text{-}BCH_q(m, \ell, \delta, A) = \left\{ (c_0, \cdots, c_{m-1}) \in \left(\mathbb{F}_q^\ell\right)^m : \sum_{j=0}^{m-1} A^{ij} c_j = 0, \forall i, 1 \leq i \leq \delta - 1 \right\}.$$

Proposition 3.6 *Avec les mêmes notations, la dimension du code $Q\text{-}BCH_q(m, \ell, \delta, A)$ est supérieure ou égale à $(m - e(\delta - 1))\ell$ et sa distance minimale de ℓ-bloc est supérieure ou égale à δ.*

Exemple 3.4 *Considérons les codes* 3*-quasi-BCH définis par des racines primitives d'ordre* 21 *de l'unité dans* $M_3(\mathbb{F}_{2^2})$, *de longueur* 63 *sur* $\mathbb{F}_2$ *et de distance minimale désignée* 6. *En d'autres termes, avec les notations précédentes, on a* $q = 2, m = 21, \ell = 3, e = 2$ *et* $\delta = 6$. *On trouve* 22 *codes non équivalents représentés dans le tableau suivant*

Nombre de codes	*Paramètres*
2	$[63, 33, 6]_{\mathbb{F}_2}$
18	$[63, 33, 7]_{\mathbb{F}_2}$
2	$[63, 36, 6]_{\mathbb{F}_2}$

Exemple 3.5 *Soit* $q = 5, m = 7, \ell = 3, e = 2$ *et* $\delta = 3$. *Soit* $\omega \in \mathbb{F}_{5^2}$ *une racine primitive de l'unité d'ordre* $24 = 5^2 - 1$ *et soit*

$$A = \begin{pmatrix} \omega^9 & \omega^4 & \omega^{22} \\ \omega^{11} & \omega^{11} & \omega^{15} \\ \omega^2 & \omega^{19} & 1 \end{pmatrix} \in M_3(\mathbb{F}_{5^2}).$$

Alors le code 3*-quasi-BCH de longueur* 21 *sur* $\mathbb{F}_5$ *défini par* A,*de distance minimale désignée* 3 *a pour paramètres* $[21, 9, 7]_{\mathbb{F}_5}$. *Il s'agit en fait du code* $\mathcal{C}_{\langle g(X)\rangle}$ *avec*

$$g(X) = \begin{pmatrix} 1 & 4 & 3 \\ 3 & 3 & 4 \\ 1 & 1 & 4 \end{pmatrix} X^4 + \begin{pmatrix} 4 & 4 & 0 \\ 4 & 0 & 0 \\ 4 & 0 & 4 \end{pmatrix} X^3 + \begin{pmatrix} 3 & 0 & 4 \\ 0 & 3 & 4 \\ 0 & 0 & 0 \end{pmatrix} X^2 + \begin{pmatrix} 2 & 3 & 2 \\ 4 & 4 & 4 \\ 3 & 1 & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{F}_5)[X].$$

Remarquons qu'on a ${}^t g(A) = {}^t g(A^2) = 0$, *et ceci est vrai pour tous les codes quasi-BCH jusqu'à la puissance* $A^{\delta-1}$.

3.4 Représentation des codes cycliques par des suites récurrentes linéaires

La relation entre les suites récurrentes linéaires et les codes cycliques est soulignée dans dans plusieurs ouvrages, voir par exemple [29]. Dans cette section, nous donnons une description explicite de la représentation d'un code cyclique par des suites récurrentes linéaires. Pour démontrer ce résultat, nous utilisons le théorème 1.1, qui donne un polynôme générateur du code dual d'un code cyclique.

Théorème 3.3 *Soit $\mathcal{C}$ un $[n,k]$-code cyclique sur $\mathbb{F}_q$ de polynôme générateur $g(x)$ et soit $h(x)$ son polynôme de contrôle. Notons $h(x) = \sum_{i=0}^{k} h_i x^i$ et posons*

$$\forall i \in \mathbb{N}, 0 \leq i \leq k, b_i = \frac{h_i}{h(0)}.$$

Alors le code $\mathcal{C}$ peut être représenté comme suit : $\mathcal{C}$ est l'ensemble des n-uplets $(c_0, c_1, \cdots, c_{n-1}) \in \mathbb{F}_q^n$, où $c_0, c_1, \cdots, c_{n-1}$ sont les n premiers termes d'une suite récurrente linéaire d'éléments de $\mathbb{F}_q$, périodique de période n, définie par la donnée de k premiers termes arbitraires $c_0, c_1, \cdots, c_{k-1}$ et la relation de récurrence

$$c_\ell + \sum_{i=1}^{k} b_i c_{\ell-i} = 0, \forall \ell \geq k.$$

Preuve : Notons $h(x) = \sum_{i=0}^{k} h_i x^i$. Le calcul des coefficients b_i du polynôme $g^\perp(x) = \frac{1}{h(0)} x^k h\left(\frac{1}{x}\right)$ donne :

$$\forall i \in \mathbb{N}, 0 \leq i \leq k, b_i = \frac{h_i}{h(0)}.$$

En particulier, on a $b_0 = 1$. D'après le théorème 1.1, les polynômes $g^{\perp}(x), xg^{\perp}(x), \cdots, x^{n-k-1}g^{\perp}(x)$ forment une base du code dual $\mathcal{C}^{\perp}$, d'où la matrice génératrice

$$H = \begin{pmatrix} b_k & b_{k-1} & \cdots & b_1 & 1 & 0 & \cdots & 0 \\ 0 & b_k & \cdots & b_2 & b_1 & 1 & \cdots & 0 \\ \vdots & & \ddots & & & & \ddots & \vdots \\ 0 & \cdots & 0 & b_k & b_{k-1} & \cdots & b_1 & 1 \end{pmatrix}.$$

Comme H est une matrice génératrice du code dual $\mathcal{C}^{\perp}$, alors c'est une matrice de contrôle du code $\mathcal{C}$ et on a donc

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

d'où les relations

$$c_\ell + \sum_{i=1}^{k} b_i c_{\ell-i} = 0, \forall \ell \in \mathbb{N}, k \leq \ell \leq n-1.$$

Comme la suite est périodique de période n, on obtient le résultat voulu.

□

3.5 Conclusions et perspectives

Nous avons montré que si A est un corps non commutatif, ou un anneau de matrices à coefficients dans un anneau commutatif, l'ensemble des suites récurrentes linéaires sur A conserve la structure usuelle de $A[X]$-module bien connue dans le cas où A est commutatif. Lorsque l'anneau A est un intègre mais n'est pas un anneau de Ore, cette structure est perdue. Entre ces deux intervalles, on a généralisé au cas non commutatif la notion d'anneau de Fatou, dans lequel la structure de module est conservée. Mais il reste des zones d'ombre et on ne trouve pas d'exemple d'anneau de Fatou non « trivial ».

Nous avons exposé différentes approches pour décrire la structure des codes quasi-cycliques. Nous avons souligné en particulier le lien avec les suites récurrentes linéaires sur des matrices à coefficients dans un corps fini.

Pour la suite de notre travail, nous nous fixons les perspectives suivantes :

1. généralisation de propriétés connues des suites récurrentes linéaires au cas non commutatif,
2. étude des propriétés de l'anneau des matrices à coefficients dans un anneau commutatif,
3. étude de la factorisation du polynôme $X^n - 1 \in M_\ell(\mathbb{F}_q)[X]$,
4. construction de nouvelles classes de codes quasi-cycliques correspondant aux différentes classes de codes cycliques, à l'exemple des codes quasi-BCH,
5. examen du lien entre suites récurrentes linéaires et codes quasi-cycliques (emboîtement, décimation).

Bibliographie

[1] K. Asano. Uber die Quotientenbildung von Schiefringen. *J. Math. Soc. Japan 1(1949) 73-78.*

[2] M. Barbier, C. Chabot, Quintin, On Quasi-Cyclic Codes as a Generalization of Cyclic Codes, *arXiv : 1108.3754 (19 août 2011).*

[3] B. Benzaghou. Anneaux de Fatou, *Séminaire Delange-Pisot-Poitou, tome 10, n°*1, 1968-1969.

[4] Bourbaki, Eléments de Mathématiques, Vol. AIII, (Hermann, 1970).

[5] M. Camus, Suites récurrentes linéaires à coefficients matriciels, *Mémoire de DEA, Université de Limoges, (2004).*

[6] H. Cartan, Théorie de Galois pour les corps non commutatifs, *Annales Scientifiques de l'E.N.S.* ,64(1947), 59-77.

[7] P.-L. Cayrel, C. Chabot, A. Necer, Quasi-cyclic codes over rings of matrices, *Finite Fields Appl., 16, Issue 2, (2010), 100-115.*

[8] F. Cedo and D. Herbera, The Ore condition for polynomial and power series rings, *Comm. Algebra 23 (1995), 5131-5159.*

[9] J.-L. Chabert. Anneaux de "polynômes à valeurs entières" et anneaux de Fatou, *Bulletin de la S.M.F. tome 99,* 273-283, 1971.

[10] A. Cherchem, T. Garici, A. Necer, Linear recurring sequences over non-commutative rings, *Journal of Algebra and its Applications, Vol. 12, Issue 2 (2012).*

[11] J. Conan, G Séguin. Structural Properties and Enumeration of Quasi-Cyclic Codes. *AAECC 4. (1993) 25-39.*

[12] P. M. Cohn. (1995). Skew fields, Cambridge University Press.

[13] S. Couteaud. Différentes approches des codes quasi-cycliques, *Mémoire de Master, Université de Limoges, (2006).*

[14] S. C. Coutinho, J. C. McConnell. The Quest for Quotient Rings. *The American mathematical monthly,* vol. 110, N°4, (Apr 2003), pp.298-313.

[15] P. Dubreil. *Algèbre,* vol. 1, Gauthier-Villars, Paris, 1946.

[16] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward. (2003).Recurrence Sequences, American Mathematical Society.

[17] W. Cary Huffman and Vera Pless, Fundamentals of Error Correcting Codes, Cambridge.

[18] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2", *IEEE Trans. Inform. Theory, vol. IT-20, p.679, 1974.*

[19] A. S. Kuzmin, V. L. Kurakin, and A. A. Nechaev, Linear recurrences over rings and modules, *J. Math. Sci.*, 76 (6), 2793–2915, 1995.

[20] K. Lally, P. Fitzpatrick, Algebraic Structure of Quasi-Cyclic Codes, *Discr. Appl. Math, vol. 111, 157-175, 2005.*

[21] T. Y. Lam. (1991). A First course in Noncommutative Rings, Springer-Verlag.

[22] T. Y. Lam. (1995). Exercices in Classical Ring Theory, Springer-Verlag.

[23] T. Y. Lam. (1999). Lectures on Modules and Rings, Graduate Texts in Mathematics, Springer-Verlag.

[24] S. Ling, P. Solé. Good self-dual quasi-cyclic codes exist. *Information Theory, IEEE Transactions on, 49(4) : 1052-1053, april 2003.*

[25] S. Ling and P. Solé, On the Algebraic Structure of Quasi-cyclic Codes I : Finite Fields, *IEEE Transactions on Information Theory, Vol. 47 (2001), 2751-2760.*

[26] S. Ling and P. Solé, On the Algebraic Structure of Quasi-cyclic Codes II : Chain Rings, *Des. Codes and Crypto., Vol. 30 (2003), 113-130.*

[27] S. Ling and P. Solé, On the Algebraic Structure of Quasi-cyclic Codes III : Generator Theory*, IEEE Transactions on Information Theory, Vol. 51 (2005), 2692-2700.*

[28] S. Ling, H.Niederreiter and P. Solé, On the Algebraic Structure of Quasi-cyclic Codes IV : Repeated Roots, *Des. Codes and Crypto., Vol 38 (2006), 337-361.*

[29] J. H. van Lint. (1999). Introduction to Coding Theory, Graduate Texts in Mathematics, Springer-Verlag.

[30] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland, Amesterdam (1977).

[31] A. Necer. (1998) Suites récurrentes linéaires et séries formelles en plusieurs variables. *Thèse. Univ de Limoges.*

[32] A. Necer, Systèmes récursifs et algèbre de Hadamard de suites récurrentes linéaires sur des anneaux commutatifs, *Comm. Algebra,* **27**-12 (1999) : 6175–6189.

[33] O. Ore, Linear Equations in noncommutative fields, *Ann. Math.* 32 (1931) 463-477.

[34] G. E. Séguin and G. Drolet, The Trace Description of Irreducible Quasi-Cyclic Codes, *IEEE Transactions on Information Theory, Vol. 36 (1990), 1463-1466.*