UNIVERSITE CHEIKH ANTA DIOP

FACULTE DES SCIENCES ET TECHNIQUES

ECOLE DOCTORALE MATHEMATIQUES INFORMATIQUE

Thèse de Doctorat Unique ès Sciences Mathématiques

Pour obtenir le grade de docteur délivré par

L'Ecole Doctorale de Mathématiques et informatique

Mention : Mathématiques et Modélisation

Option : Codage, Cryptographie, Algèbre et Application

Année : 2011-2012 N° ordre :

Suites Multiplexées et Applications en Cryptographie

Présentée par **Chérif Bachir DEME**

Le 05 Mai 2012

Devant le jury composée de :

Président :

Mamadou SANGHARE, Professeur, UCAD

Rapporteurs :

Maurice MIGNOTTE, Professeur, Univ. Strasbourg(France)

Rochdi ADELLATIF, Professeur, Univ. Hassa II-Mouhammedia(Casalanca)

Examinateurs:

Djiby SOW, Maître de conférences, UCAD

Cheikh Thiécoumba GUEYE, Maître de conférences, UCAD

Sidy Demba Touré, Maître de conférences, UCAD

Directeur:

Oumar DIANKHA, Maître de conférences, UCAD

UNIVERSITE CHEIKH ANTA DIOP

FACULTE DES SCIENCES ET TECHNIQUES

ECOLE DOCTORALE MATHEMATIQUES INFORMATIQUE

Thèse de Doctorat Unique ès Sciences Mathématiques

Pour obtenir le grade de docteur délivré par

L'Ecole Doctorale de Mathématiques et informatique

Mention : Mathématiques et Modélisation

Option : Codage, Cryptographie, Algèbre et Application

Année : 2011-2012 N° ordre :

Suites Multiplexées et Applications en Cryptographie

Présentée par **Chérif Bachir DEME**

Le 05 Mai 2012

Devant le jury composée de :

Président :

Mamadou SANGHARE, Professeur, UCAD

Rapporteurs :

Maurice MIGNOTTE, Professeur, Univ. Strasbourg(France)

Rochdi ADELLATIF, Professeur, Univ. Hassa II-Mouhammedia(Casalanca)

Examinateurs:

Djiby SOW, Maître de conférences, UCAD

Cheikh Thiécoumba GUEYE, Maître de conférences, UCAD

Sidy Demba Touré, Maître de conférences, UCAD

Directeur:

Oumar DIANKHA, Maître de conférences, UCAD

Table des matières

Dédicaces

Après avoir rendu grâce à Dieu le Tout Puissant et son prophète Mouhamed (PSL).

À mes parents EL Hadji Malick et Sokhna SARR qui n'ont menagé aucun effort pour ma réussite à qui je souhaite une santé de fer et longue vie afin qu'ils puisse assister à la réussite de leurs enfants.

À toute ma famille, je veux parler de Amadou, Ali, Ousmane, Ibou, Marième, Moussa, Mouhameth Abdel Rahmane, Ndeye Sophie Malick, Fatou Bintou, Fatou Bintou Fall, Fatou Kiné, Koro, Rama, Aminata, Awa et Aïssatou Bobo.

À mes tantes Khady SY, Mariama DIAO, Koro, Bousso et Awa.

À mes cousins, cousines et amis, Awa DIOP, Modou Diop, Moudo Diouf, Thierno DIALLO, Papa Ailoune SARR, Mayé THIOR, Malick FALL, Ndeye GUEYE, Baye Sonar DIOUF, Bébé, Moustapha et Ndeye Rokhya SARR, Omar COLY, Baye Saloum CISSE, Ibrahima SECK, Mamadou WADE, Mouhameth DIALLO...

Remerciements

En premier lieu, je tiens à remercier mon directeur de thèse **Docteur Oumar DIANKHA** sans qui cette thèse n'aurait jamais pu voir le jour. Je le remercie pour son encadrement, sa disponibilité, ses conseils, sa clairvoyance et pour sa générosité aussi bien dans le travail que dans la vie de tous les jours.

Je remercie le **Professeur Mamadou SANGHARE**, Directeur de l'École Doctorale Mathématiques Informatique(EDMI), Directeur du laboratoire LACGAA pour ses idées novatrices, notamment pour avoir été l'instigateur des disciplines comme la Théorie de Codes et la Cryptologie au Sénégal et dans la sous région. Veuillez trouver ici Professeur l'expression de toute mon estime pour votre grand esprit scientifique et pour avoir présidé mon jury. Merci encore pour la connaissance transmise depuis la MP1 en 2003 et que vous continuez à nous transmettre. Je suis honoré Professeur.

Merci au **Professeur Maurice MIGNOTTE** de l'université de Starsbourg habitué à lire mes écrits d'avoir accepter de rapporter ma thèse et pour ses remarques pertinentes du point de vue forme qui ont contribué surtout à l'amélioration de l'anglais de mes articles et de ce document.

Je remercie le **Professeur Rochdi ABDELLATIF** du Département de Mathématiques et Informatique de la Faculté des Sciences Ben M'Sik (Casablanca) de l'Université Hassan II-Mohammedia en sa qualité de rapporteur de ma thèse

et de l'honneur qu'il me fait par sa présence comme membre du jury.

Mes remerciements au **Docteur Djiby SOW** d'avoir accepté de faire parti du jury. Vous êtes un chercheur débordant d'idées et prêt à les partager avec qui voudra. Je vous remercie pour vos conseils et pour la connaissance transmise.

Mes remerciements vont également au **Docteur Cheikh Thiécoumba GUEYE** d'avoir accepté d'être dans le jury. Vous êtes un chercheur débordant d'idées et prêt à les partager avec qui voudra. je vous remercie de votre aimabilité et pour la connaissance transmise depuis la Licence de Mathématique.

Je tiens à remercier le **Docteur Sidy Demba TOURE** d'avoir accepté d'être dans le jury, pour son aimabilité et son sens de l'humour.

Je tiens à remercier le **Professeur Hamidou DATHE** Chef du département de Mathématiques et Informatique pour son aimabilité.

Je remercie les **Docteurs Mamadou BARRY, Abdoulaye MBAYE, Mme MBAYE Leila, Ismaïla** et tous les membres du LACGAA pour leur compréhension et leur aimabilité.

Je remercie mes promotionnaires et collègues Demba SOW, El Hadji Mamadou MBOUP, Jean Pierre TOUPANE, M SENE, M. PAYE, Mamadou Moustapha SARR, Dr Abdoul Aziz CISS, Dr Amadou TALL, Dr Regis BABANIMANA, Dr Raoul, Mame Demba CISSE, Allasane DIOUF, Albert DIOMPY, Alfouseyni, Yousseph, Ghouraissou CAMARA, Abdoul aziz DIAW, Seydina Oumar NDIAYE et tous ceux j'ai oublié de citer.

Enfin, je remercie Mme Bousso et M SECK de l'ESSA, et les étudiants. Je

remercie aussi les étudiants du master 1, du master 2 TDSI et MAGA, M MASSALY, Mlle TOUNKARA, Mme NDIAYE et Mme MBAYE.

Résumé

Dans cette thèse nous avons étudié les suites multiplexées. Nées pour remédier aux attaques sur les suites récurrentes linéaires, les suites multiplexées ne sont pas eux non plus à l'abri de nouvelles attaques.

Nous élaborons des méthodes qui permettent de borner et minorerr les complxités des suites de longueurs maximales constituant une suite multiplexée à l'aide de la classification décrite dans [17], puis de déterminer leur complexités k et m suivant que p$gcd(m,k) = m$ ou p$gcd(m,k) = k$.

Introduction

Les suites récurrentes linéaires (SRL ou LRS(Linear recurrent sequence en anglais)), nées en 1202 avec l'exemple donné par Fibonacci de la suite $1, 1, 2, 3, 5, 8, 13, \ldots$ sont des composantes majeures dans les systèmes de communication modernes. Elles sont faciles à appliquer et leurs propriétés mathématiques sont assez bien comprises. Leurs applications comprennent entre autre la construction de générateurs pseudo-aléatoires fréquemment utilisés dans les systèmes de radar, la synchronisation des données, les systèmes de positionnement global (GPS), la théorie du codage et de Code Division Multiple-Access systèmes de communication (CDMA).

Une des principales applications des suites récurrentes linéaires est la cryptographie où elles sont plus particulièrement utilisés pour la génération de clés dans un chiffrement par flot.

Les suites récurrentes linéaires peuvent être produites et implémentées dans les différents domaines cités à l'aide des LFSRs(Linear Feedback Shift Register). Les suites possèdent de bonnes répartitions pseudo-aléatoires, des propriétés périodiques et de bonnes propriétés statistiques.

Malgré toutes ces propriétés, les suites récurrentes linéaires ne sont pas suffisamment complexes et ne fournissent habituellement pas assez de sécurité par eux-mêmes.

Elles possèdent des faiblesses qui font qu'on peut retrouver leur polynôme minimal, leur complexité et leur reconstitution entière avec l'algorithme de Berlekamp-Massey que nous allons détailler ici.

Pour surmonter l'algorithme de Berlekamp-Massey, des techniques sont mises en place pour contourner la linéarité des suites récurrentes linéaires, en utilisant

- Une fonction de combinaison non linéaire qui combine plusieurs suites récurrentes.
- La sortie d'une ou de plusieurs suites récurrentes linéaires pour contrôler l'horloge d'une ou de plusieurs suites récurrentes linéaires.

Ces dernières techniques ont aussi fait l'objet d'autres attaques parmi lesquelles l'attaque par corrélation qui porte sur la corrélation de la suite récurrente linéaire. Pour palier à ces faiblesses et attaques, plusieurs autres types de suites non linéaires basées elles mêmes sur les suites récurrentes linéaires ont aussi vu le jour, parmi elles, les suites multiplexées qui ont fait l'objet de nos deux premiers articles. Une suite multiplexée est une suite construite à partir de deux suites récurrentes linéaires de périodes maximales ou m-sequences.

Pour qu'une suite puisse être utilisée dans les domaines tels que la cryptographie, nous avons besoin qu'elle ait des propriétés cryptographiques nécessaires c'est-à-dire :

- d'une période très grande
- d'une grande complexité linéaire
- de bonnes propriétés statistiques.

Ces suites et leurs propriétés sont développées dans [20, 21]. Elles constituent de très bonnes candidates pour être considérées comme des générateurs aléatoires afin que nous puissions les utiliser dans un chiffrement par flot. Mais cela ne les mettent pas tout à fait, à l'abri d'attaques.

Dans cette thèse, nous avons élaboré des méthodes pour essayer de les attaquer. Ces méthodes ont permis une classification de ces suites multiplexées et d'élaborer un lien entre cette classification et le polynôme minimal.

Ce document est structuré en trois chapitres :

Chapitre 1 : dans ce chapitre, nous faisons des rappels sur les suites récurrentes linéaires sur un corps fini et sur leur applications en cryptographie, plus précisément dans un chiffrement par flot ou chiffrement par flux.

Chapitre 2 : Ici, nous faisons une classification des suites multiplexées, qui a fait l'objet de notre première publication. Cette classification a pour but de regrouper

ces suites en classe afin de pouvoir mettre en place des méthodes pour les attaquer lorsqu'elles sont utilisées comme générateurs de clés dans un chiffrement par flot.

Chapitre 3 : Dans ce chapitre, nous faisons un rapprochement entre la classification et le polynôme minimal d'une suite multiplexée. Ce rapprochement est aussi mise en place pour trouver des méthodes pour déterminer les complexités des suites récurrentes linéaires de périodes maximales constituant une suite multiplexée.

Chapitre 1

Suites Récurrentes Linéaires et applications en cryptographie

1.1 Suites récurrentes linéaires sur un corps fini

Ce chapitre contient essentiellement des rappels de résultats, de notations sur les corps finis et les suites récurrentes linéaires dont nous ferons usage dans cette thèse.

1.2 Rappels sur les corps finis

1.2.1 Corps finis et extensions

Définition 1.2.1. *Un corps fini est un corps contenant un nombre fini d'éléments.*

Remarque 1.2.2. *Les corps finis sont appelés corps de Galois.*

Exemple 1.2.3. **(1)** $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ *et* $(\mathbb{C}, +, .)$ *sont des corps qui ne sont pas finis.*

(2) $(\mathbb{Z}_5, +, .)$ *et* $(\mathbb{Z}_2, +, .)$ *sont des corps finis.*

Le corps $\mathbb{Z}_2$ ne contient que deux éléments 0 et 1 et nous avons les tables d'opérations suivantes :

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

Les éléments 0 et 1 sont appelés éléments binaires.

Définition 1.2.4. *Soit $p > 1$ un nombre premier. On note $\mathbb{F}_p$ le corps fini à p éléments $\mathbb{Z}/p\mathbb{Z}$.*

Remarque 1.2.5. *Les notations suivantes sont les mêmes : il s'agit de $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}_p$.*

Pour tout q puissance d'un nombre premier p, il existe un corps fini de cardinal q.

Proposition 1.2.6. *[19] Tout anneau intègre ayant un nombre fini $n \geq 2$ d'éléments est un corps.*

Théorème 1.2.7. *[19]*

1. *Soient $q = p^n$ et $q' = p^m$ où $n,\ m \geq 1$ et p est un nombre premier.*

   On a : $\mathbb{F}_q \subset \mathbb{F}_{q'} \iff n$ divise m.

2. *Soit $\mathbb{F}$ un corps fini de cardinal $q > 1$. Alors*

   i) *$q = p^m$, où p est un nombre premier et m un entier positif.*

   ii) *$\mathbb{F}$ est unique (à un isomorphisme de corps près).*

Théorème 1.2.8. *[3] Pour tout corps fini $\mathbb{F}_q$, le groupe multiplicatif, noté $\mathbb{F}_q^*$, est cyclique.*

Définition 1.2.9. *Si $\mathbb{F}_q$ est un corps fini et s'il existe un entier positif non nul minimal n tel que $n\beta = 0$ pour tout $\beta \in \mathbb{F}_q$, alors un tel entier est appelé caractéristique de $\mathbb{F}_q$ et $\mathbb{F}_q$ est dit de caractéristique n.*

Théorème 1.2.10. *Soit $\mathbb{F}_q$ un corps fini. Alors la caractéristique de $\mathbb{F}_q$ est premier.*

Démonstration. Le cardinal de $\mathbb{F}_q$ est égal à q. $\mathbb{F}_q$ contient l'élément unité 1, et puisque $\mathbb{F}_q$ est fini les éléments $1,\ 1+1=2,\ 1+1+1=3,\ldots$ ne sont pas tous distincts. De plus, le plus petit entier p tel que

$$p \cdot 1 = \underbrace{1+1+1+\cdots+1}_{p(fois)} = 0,$$

doit être un nombre premier (car $(r \cdot s) \cdot 1 = 0 \Rightarrow (r \cdot 1)(s \cdot 1) = 0 \Rightarrow\ r \cdot 1 = 0$ *ou* $s = 0$). □

Théorème 1.2.11. *[3] Tout corps fini est de caractéristique un nombre premier p et possède p^m éléments où $m \in \mathbb{N}^*$.*

Proposition 1.2.12. ***(Théorème Wedderburm)*** *Tout anneau intégre fini est un corps commutatif.*

Définition 1.2.13. *Un générateur de $\mathbb{F}_q^*$ est appelé élément primitif de $\mathbb{F}_q$. Un polynôme ayant un élément primitif comme racine est appelé polynôme primitif.*

Corollaire 1.2.14. *[3] Tout corps fini contient un élément primitif.*

Lemme 1.2.15. *Dans un corps fini de caractéristique p, on a*

$$(x+y)^p = x^p + y^p$$

Démonstration. Nous avons expression binomiale suivante :

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k$$

où

$$\binom{p}{0} = \binom{p}{p} = 1.$$

Si $1 \leq k \leq p-1$, alors $pgcd(k!, p) = 1$. Donc

$$\binom{p}{k} = \frac{p(p-1)(p-2)\ldots(p-k+1)}{k!} = p\frac{(p-1)(p-2)\ldots(p-k+1)}{k!} \equiv 0\ (mod\ p).$$

□

Par induction, nous avons le corollaire suivant :

Corollaire 1.2.16. *Dans tout corps fini de caratéristique p, on a*

$$(x+y)^{p^n} = x^{p^n} + y^{p^n} \quad pour \quad tout \quad n > 1$$

Définition 1.2.17. ***Extension d'un corps*** *Soit $\mathbb{L}$ un corps. On dit que $\mathbb{K}$ est une extension de $\mathbb{L}$ si et seulement si $\mathbb{L}$ est un sous-corps de $\mathbb{K}$.*

Exemple 1.2.18. *Le corps de cardinal $q = p^m$, noté $\mathbb{F}_q$ est une extension de degré m du corps premier $\mathbb{F}_p$.*

1. *$\mathbb{C}$ est une extension de $\mathbb{R}$ et de $\mathbb{Q}$.*
2. *$\mathbb{R}$ est une extension de $\mathbb{Q}(\sqrt{2})$.*
3. *$\mathbb{Q}(\sqrt{2})$ est une extension de $\mathbb{Q}$.*

Proposition 1.2.19. *Soit $\mathbb{K}$ une extension de $\mathbb{L}$. Alors $\mathbb{K}$ est un espace vectoriel sur $\mathbb{L}$.*

Proposition 1.2.20. *Pour tout entier $m > 1$, $\mathbb{F}_{q^m}$ est une extension de degré m de $\mathbb{F}_q$.*

Définition 1.2.21. *On note $[\mathbb{K} : \mathbb{L}]$ la dimension de l'espace vectoriel $\mathbb{K}$ sur $\mathbb{L}$. Cet entier s'appelle le degré de l'extension de k sur L.*

Exemple 1.2.22.

1. *Le corps des nombres complexes $\mathbb{C}$ est une extension de $\mathbb{R}$ de degré $[\mathbb{C} : \mathbb{R}] = 2$.*
2. *Le corps $\mathbb{R}$ est une extension de $\mathbb{Q}$ de degré infini : $[\mathbb{R} : \mathbb{Q}] = \infty$.*
3. *$\mathbb{F}_q$, où $q = p^n$ est une extension de $\mathbb{F}_q$ de degré n.*

Définition 1.2.23. *Soit $\mathbb{L}$ un corps.*

Une extension $\mathbb{K}$ de $\mathbb{L}$ est un ***corps de rupture*** *pour le polynôme $f(x) \in \mathbb{L}[X]$ sur $\mathbb{L}$ si et seulement si, $\mathbb{K}$ contient une racine de f.*

Exemple 1.2.24. *$\mathbb{R}$ est un corps de rupture pour $X^3 - 2$ sur $\mathbb{Q}$.*

Théorème 1.2.25. *Si $f(X)$ est un polynôme irréductible dans $\mathbb{K}[X]$, alors f possède un corps de rupture sur $\mathbb{K}$.*

Corollaire 1.2.26. *Tout polynôme $f(X) \in \mathbb{K}[X]$ possède un corps de rupture sur $\mathbb{K}$.*

Démonstration. En effet, tout polynôme $f \in \mathbb{K}[X]$ se décompose en produit de polynômes irréductibles. □

Définition 1.2.27. *Une extension $\mathbb{K}$ de $\mathbb{L}$ est un* ***corps de décomposition****(ou* ***corps scindé****) pour $f \in \mathbb{L}[X]$ sur $\mathbb{L}$ si et seulement si, f peut être scindé dans $\mathbb{K}[X]$ c'est-à-dire il peut être décomposé en produit de polynômes linéaires dans $\mathbb{K}[X]$. Autrement dit si toutes les racines de f dans une clôture algébrique de $\mathbb{L}$ contenant $\mathbb{K}$ sont dans $\mathbb{K}$.*

Exemple 1.2.28.

1. *Le corps $\mathbb{C}$ est un corps de décomposition sur $\mathbb{R}$ pour le polynôme $P(X) = X^2 + 1 = (X - i)(X + i)$.*
2. *Le corps $\mathbb{Q}$ est un corps de décomposition sur $\mathbb{Q}$ pour le polynôme $Q(X) = X^2 - 1 = (X - 1)(X + 1)$.*

Théorème 1.2.29. *Tout polynôme $f \in \mathbb{K}[X]$ possède un corps de décomposition sur $\mathbb{K}$.*

Définition 1.2.30. *Un corps de décomposition minimal sur $\mathbb{K}$ est appelé un* ***corps des racines*** *pour f sur $\mathbb{K}$.*

Exemple 1.2.31.

1. *$\mathbb{C}$ est un corps des racines sur $\mathbb{R}$ pour le polynôme $X^2 + 1$.*
2. *$\mathbb{Q}(\sqrt{2})$ est un corps de décomposition sur $\mathbb{Q}$ pour le polynôme $X^2 - 2$.*

1.3 Suites récurrentes linéaires et propriétés

Définition 1.3.1. *Une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{F}_q$ est dite récurrente linéaire homogène (ou homogeneous linear feedback shift register sequence ou LFSR sequence*

en anglais) si elle satisfait, pour tout $n \geq 0$, une relation de récurrence linéaire homogène (à coefficients constants) de la forme

$$x_{n+k} = a_{k-1}x_{n+k-1} + a_{k-2}x_{n+k-2} + \cdots + a_1x_{n+1} + a_0x_n \tag{1.1}$$

avec $a_0,\ a_1,\ a_2,\ \ldots,\ a_{k-1} \in \mathbb{F}_q$.

L'entier k est appelé degré ou ordre de la relation 1.1 et l'état initial ou conditions initiales de cette dernière est $(x_0,\ x_1,\ x_2,\ x_{k-2},\ x_{k-1})$.

La relation de récurrence linéaire est notée parfois

$$x_{n+k} - a_{k-1}x_{n+k-1} - a_{k-2}x_{n+k-2} - \cdots - a_1x_{n+1} - a_0x_n = 0$$

Remarque 1.3.2. *Les termes* ***équation de récurrence linéaire*** *et* ***solution*** *sont aussi employés pour désigner* ***la relation de récurrence*** *et* ***une suite*** *la satisfaisant.*

Exemple 1.3.3. ***Suite de Fibonacci.*** *Posons* $q = 2$, *alors nous travaillons dans* $\mathbb{F}_2 = \{0, 1\}$.

Soit la relation de récurrence linéaire

$$x_{n+2} = x_{n+1} + x_n \ \forall\ n \geq 0.$$

et comme conditions initiales $x_0 = 1,\ x_1 = 0$, *on trouve la suite bien connue*

$$(x_n)_{n\in\mathbb{N}} = 1,\ 0,\ 1,\ 1,\ 0,\ 1,\ 1,\ 0,\ 1,\ 1,\ 0, \ldots.$$

Définition 1.3.4. *Une suite* $(x_n)_{n\in\mathbb{N}} \in \mathbb{F}_q$ *est dite récurrente linéaire non homogène (ou nonhomogeneous linear feedback shift register sequence en anglais) si elle satisfait, pour tout* $n \geq 0$, *une relation de récurrence linéaire non homogène (à coefficients constants) de la forme*

$$x_{n+k} = a_{k-1}x_{n+k-1} + a_{k-2}x_{n+k-2} + \cdots + a_1x_{n+1} + a_0x_n + b \tag{1.2}$$

avec $a_0,\ a_1,\ a_2,\ \ldots,\ a_{k-1},\ b \in \mathbb{F}_q$ *et* $b \neq 0$.

l'entier k est appelé le degré ou ordre de la relation 1.2 et l'état initial ou conditions initiales de cette dernière est $(x_0,\ x_1,\ x_2,\ x_{k-2},\ x_{k-1})$.

La relation de récurrence homogène qui lui est associée est simplement

$$x_{n+k} = a_{k-1}x_{n+k-1} + a_{k-2}x_{n+k-2} + \cdots + a_1x_{n+1} + a_0x_n$$

Exemple 1.3.5. *Posons $q = 2$, alors $\mathbb{F}_2 = \{0, 1\}$. Soit la relation de récurrrence linéaire d'ordre 4 suivante :*

$$x_{n+4} = x_{n+3} + x_{n+1} + x_n + 1,$$

avec $x_0 = 1,\ x_1 = 1,\ x_2 = 0,\ x_3 = 1$ comme conditions initiales.

Les termes de la suite sont

$$|\,1\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,1\,|\,1\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,1\,|\,1\,1\ \ldots$$

Remarque 1.3.6. *La suite nulle $(0)_{n\in\mathbb{N}}$ est solution de toute équation linéaire récurrente homogène et ne l'est pour aucune équation linéaire récurrente non homogène.*

Dans la suite, nous allons nous concentrer principalement sur les suites récurrentes linéaires homogènes. De plus, toute suite récurrente linéaire homogène sera dite suite récurrente linéaire tout simplement.

1.3.1 Suites récurrentes linéaires et déterminants de Hankel

Définition 1.3.7. *Soit $x_0, x_1, x_2, \ldots$ une suite d'éléments de $\mathbb{F}_q$. Pour les entiers $n \geq 0$ et $r \geq 1$, on pose*

$$D_n^{(r+1)} = \begin{vmatrix} x_n & x_{n+1} & \cdots & x_{n+r} \\ x_{n+1} & x_{n+2} & \cdots & x_{n+r+1} \\ \vdots & \vdots & & \vdots \\ x_{n+r} & x_{n+r+1} & \cdots & x_{n+2r} \end{vmatrix}$$

et ces déterminants sont appelés déterminants de Hankel.

Exemple 1.3.8. *Considérons l'exemple 1.3.3 avec les conditions initiales suivantes* $x_0 = 1,\ x_1 = 1$. *La suite devient :*

$$|1\,1\,0|1\,1\,0|1\,1\,0|1\,1\,0|1\,1\,0|1\,1\,0|1\,1\,0|1\,1\,0|1\,1\,0|\ \ldots$$

Calculons maintenant les déterminants de ***Hankel*** *suivant les valeurs de* n *et de* r *:*

$$D_0^2 = det\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = -1, \quad D_0^3 = det\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = -2, \quad D_0^4 = det\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} = 0$$

Ceci montre qu'à priori, la suite en question peut satisfaire une relation de récurrence d'ordre 3, *mais aucune relation de récurrence d'ordre inférieur.*

Lemme 1.3.9. *[20] Soit* $x_0, x_1, x_2, \ldots$ *une suite d'éléments de* $\mathbb{F}_q$, *et soient les entiers* $n \geq 0$ *et* $r \geq 1$. *Si* $D_n^{(r)} = D_n^{(r+1)} = 0$, *alors* $D_{n+1}^{(r)} = 0$.

Théorème 1.3.10. *[20] La suite* $x_0, x_1, x_2, \ldots$ *d'éléments de* $\mathbb{F}_q$ *est une suite récurrente linéaire si et seulement si, il existe un entier positif* r *tel que* $D_n^{(r)} = 0$ *pour tout nombre fini de* $n \geq 0$.

Théorème 1.3.11. *[20] La suite* $x_0, x_1, x_2, \ldots$ *d'éléments de* $\mathbb{F}_q$ *est une suite récurrente linéaire, de polynôme minimal de degré* k *si et seulement si* $D_n^{(r)} = 0$ *pour tout* $r \geq k+1$ *et* $k+1$ *est le plus petit entier pour lequel ces conditions sont remplies.*

1.3.2 Matrice associée d'une suite récurrente linéaire

Dans cette partie, nous déterminons et étudions ce qu'est une matrice associée à une suite récurrente linéaire.

Remarque 1.3.12. *La* ***matrice associée*** *est encore appelée* ***matrice compagnon*** *et même pardois* ***matrice de trasition.***

Définition 1.3.13. *À l'équation (1.1), on associe la matrice carré d'ordre k définie par*

$$M = \begin{pmatrix} a_{k-1} & a_{k-2} & \dots & \dots & a_0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

Si $k = 1$, alors $M = (a_0)$. De plus, si $k > 1$ et $(x_n)_{n\in\mathbb{N}}$ est solution de l'équation (1.1), alors

$$\begin{pmatrix} x_{n+k} \\ x_{n+k-1} \\ \vdots \\ x_{n+1} \end{pmatrix} = M \begin{pmatrix} x_{n+k-1} \\ x_{n+k-2} \\ \vdots \\ x_n \end{pmatrix}$$

et en particulier, pour tout $n \geq 0$

$$\begin{pmatrix} x_{n+k-1} \\ x_{n+k-2} \\ \vdots \\ x_n \end{pmatrix} = M^n \begin{pmatrix} x_{k-1} \\ x_{k-2} \\ \vdots \\ x_0 \end{pmatrix}$$

Exemple 1.3.14. *Soit x_0, x_1, x_2, ... une suite récurrente linéaire sur $\mathbb{F}_2$ satisfaisant la relation de récurrence $x_{n+5} = x_{n+4} + x_{n+2} + x_{n+1} + x_n$. Nous avons $a_4 = 1$, $a_3 = 0$, $a_2 = 1$, $a_1 = 1$, $a_0 = 1$. Alors la matrice M associée à la relation de récurrence est une matrice 5×5 définie par :*

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

Remarque 1.3.15. *Soit $x_0, x_1, x_2, \dots$ une suite récurrente linéaire sur $\mathbb{F}_q$ satisfaisant à la relation*

$$x_{n+k} = a_{k-1}x_{n+k-1} + a_{k-2}x_{n+k-2} + \cdots + a_0 x_n \text{ pour } n \geq 0$$

où les a_i, $1 \leq i \leq k-1$ *appartiennent à* $\mathbb{F}_q$.

Posons

$$X_n = \begin{pmatrix} x_{n+k-1} \\ x_{n+k-2} \\ \vdots \\ x_n \end{pmatrix}.$$

Alors à cette suite on associe la matrice M *d'ordre* $k \times k$ *sur* $\mathbb{F}_q$ *définie par :*

$$M = \begin{pmatrix} a_{k-1} & a_{k-2} & \cdots & \cdots & a_0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

Et de plus, nous avons $X_{n+1} = MX_n$ *pour* $n \geq 0$ *et donc*

$$X_n = M^{\,n} X_0 \quad \textit{avec} \quad X_0 = \begin{pmatrix} x_{k-1} \\ x_{k-2} \\ \vdots \\ x_0 \end{pmatrix}$$

Une conséquence de la définition d'une matrice associée d'une suite récurrente linéaire :

Proposition 1.3.16. *Soit* $x_0, x_1, x_2, \ldots$ *une suite récurrente linéaire d'ordre* k *sur* $\mathbb{F}_q$ *satisfaisant à la relation (1.1) avec* $a_0 \neq 0$, *alors l'ordre de la suite* $x_0, x_1, x_2, \ldots$ *divise l'ordre de la matrice qui lui est associée.*

Démonstration. Comme $det(\mathsf{M}) = (-1)^{k-1}a_0 \neq 0$, alors si r l'ordre de la matrice M associée à la suite $x_0, x_1, x_2, \ldots$ est fini, alors

$$X_{n+r} = \mathsf{M}^{\,n+r} X_0 = \mathsf{M}^{\,n} X_0 \times \mathsf{M}^{\,r} = \mathsf{M}^{\,n} X_0 \times \mathsf{I} = \mathsf{M}^n X_0 = X_n.$$

Donc r est une période de $x_0, x_1, x_2, \ldots$. Il résulte du Lemme 1.3.22 (définie dans la section qui suit) que l'ordre de la suite divise r. □

En plus de ces quelques définitions, nous alllons donner quelques propriétés des suites récurrentes linéaires. Pour ce faire, nous commençons par dire ce qu'est une suite ultimement périodique et périodique.

1.3.3 Périodicité d'une suite récurrente linéaire

Définition 1.3.17. *Soit $x_0, x_1, \ldots$ une suite d'éléments de $\mathbb{F}_q$. S'il existe des entiers r et n_0 avec $r \geq 1$, tels que $x_{n+r} = x_n$ pour tout $n \geq n_0$ alors la suite $x_0, x_1, \ldots$ est dite ultimement périodique.*

Exemple 1.3.18. *Soit $x_0,\ x_1,\ x_2,\ \ldots$ une suite récurrente linéaire sur $\mathbb{F}_2$ satisfaisant la relation de récurrence $x_{n+4} = x_{n+2} + x_{n+1}$ avec comme état initial ($x_3 = 1,\ x_2 = 0,\ x_1 = 1,\ x_0 = 1$).*

Alors les termes sont :

$$1\,|\,1\,0\,1\,1\,1\,0\,0\,|\,1\,0\,1\,1\,1\,0\,0\,|\,1\,0\,1\,1\,1\,0\,0\,|\,1\,0\,1\,1\,1\,0\,0\,|\ldots$$

Là, nous voyons bien que cette suite est périodique à partir du rang 1 et de période 7.

De ce fait, nous pouvons dire que pour tout $n \geq n_0 = 1$ la suite $x_{n+4} = x_{n+2} + x_{n+1}$ est périodique.

Donc ultimement périodique et les termes dans cette période sont

$$1\,0\,1\,1\,1\,0\,0$$

Remarque 1.3.19. *La plus petite parmi toutes les périodes possibles de la suite ultimement périodique est appelée la période de la suite.*

Définition 1.3.20. *Une suite $x_0, x_1, \ldots$ d'éléments de $\mathbb{F}_q$ est dite périodique s'il existe un entier r tel que $x_{n+r} = x_n$ pour tout $n = 0, 1, \ldots$ et r est appelé période de la suite.*

Exemple 1.3.21. *Soit* $x_0,\ x_1,\ x_2,\ \ldots$ *une suite récurrente linéaire de relation de récurrence* $x_{n+5} = x_{n+1} + x_n$ *et son état initial est* $x_4 = 1,\ x_3 = 0,\ x_2 = 1,\ x_1 = 1,\ x_0 = 1$.

Alors les termes de la suite sont :

$$|1\,1\,1\,0\,1\,0\,0\,|\,1\,1\,1\,0\,1\,0\,0\,|\,1\,1\,1\,0\,1\,0\,0\,|\,1\,1\,1\,0\,1\,0\,0\,|\ldots$$

La suite est bien périodique pour tout $n \geq 0$ *et de période 7. Les termes de la période sont*

$$1\,1\,1\,0\,1\,0\,0$$

Lemme 1.3.22. *Toute période d'une suite ultimement périodique est divisible par la période de la suite.*

Démonstration. Soit t une période d'une suite ultimement périodique $x_0, x_1, x_2, \ldots$ et t_1 la période de cette suite, alors on a $x_{n+t} = x_n$ pour tout $n \geq n_0$ et $x_{n+t_1} = x_n$ pour tout $n \geq n_1$.

Supposons que t_1 ne divise pas t, alors il existe des entiers q et r tels que $t = qt_1 + r$ avec $0 \leq r < t_1$. Ce qui implique que (pour n assez grand)

$$x_{n+t} = x_n = x_{n+qt_1+r} = x_{n+(q-1)t_1+r} = \cdots = x_{n+r},$$

Par conséquent r est une période de la suite $x_0, x_1, x_2, \ldots$. Ce qui est une contradiction avec la définition de t_1. Donc $r = 0$ et t_1 divise t. □

Lemme 1.3.23. *[20] La suite* $x_0, x_1, x_2, \ldots$ *est périodique si et seulement si il existe un entier* $r > 0$ *tel que* $x_{n+r} = x_n$ *pour tout* $n = 0, 1, \ldots$

Théorème 1.3.24. *[20] Si* $x_0, x_1, x_2, \ldots$ *est une suite récurrente linéaire dans un corps fini satisfaisant à la relation (1.1), et si le coefficient* a_0 *est non nul, alors la suite* $x_0, x_1, x_2, \ldots$ *est périodique.*

La valeur maximale de la période d'une suite satisfaisant à la relation de récurrence 1.1 d'ordre k dans $\mathbb{F}_q$, peut être déterminée par une **suite de réponse impulsionnelle**.

Pour cela, nous allons d'abord définir ce qu'est une suite de réponse impulsionnelle avant de montrer ce qu'elle est capable de faire.

Définition 1.3.25. *La **suite de réponse impulsionnelle (ou impulse response sequence en anglais)** correspondant à une suite récurrente linéaire d'ordre k satisfaisant à la relation 1.1 est la suite $d_0,\ d_1,\ d_2,\ \ldots$ déterminée uniquement par ses valeurs initiales*

$$d_0 = d_1 = d_2 = \cdots = d_{k-2} = 0, \quad d_{k-1} = 1 \quad (d_0 = 1 \quad si \quad k = 1)$$

et satisfaisant à la relation de récurrence

$$d_{n+k} = a_{k-1}d_{k-1} + a_{k-2}d_{k-2} + \cdots + a_0 d_n \quad pour \quad n = 0,\ 1,\ 2,\ \ldots.$$

L'exemple suivant va montrer comment la suite de réponse impulsionnelle permet de calculer la valeur maximale de la période d'une suite récurrente linéaire.

Exemple 1.3.26. *Considérons la $s_0,\ s_1,\ s_2,\ \ldots$ satisfaisant à la relation de récurrence dans $\mathbb{F}_2$*

$$s_{n+5} = s_{n+1} + s_n, \quad n = 0,\ 1,\ 2,\ \ldots$$

Puisque l'ordre $k = 5$ de cette suite, alors l'état initial de la suite de réponse impulsionnelle est $d_0 = d_1 = d_2 = d_3 = 0$ et $d_4 = 1$. Les termes de cette suite sont

$$|\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,|\,0\,0\,0\,0\,1\ \ldots$$

et sa période est 21 qui correspond à la valeur maximale de la période de la suite $s_0,\ s_1,\ s_2,\ \ldots$.

Lemme 1.3.27. *[20] Soit d_0, d_1, d_2, d_2, ... une suite de réponse impulsionnelle satisfaisant à la relation de la définition 1.3.25, et soit M la matrice à la définition 1.3.13. Alors les deux vecteurs d_m et d_n sont identiques si et seulement si $M^m = M^n$.*

Théorème 1.3.28. *[20] La période d'une suite récurrente linéaire dans $\mathbb{F}_q$ divise la période de la suite d'impulsion résponse.*

1.4 Polynôme caractéristique, polynôme minimal et fonction génératrice d'une suite récurrente linéaire

1.4.1 Polynômes

Définition 1.4.1. *Soit $\mathbb{K}$ un corps commutatif.*

On appelle polynôme sur $\mathbb{K}$, toute suite

$$(a_0, a_1, \ldots, a_n, \ldots) \text{ où les } a_i \in \mathbb{K},\ i = 0, 1, 2, \ldots$$

dans laquelle on a un nombre fini d'éléments non nuls.

Exemple 1.4.2. *1. Dans $\mathbb{Z}/3\mathbb{Z}$, $(1, 0, 2, 0, 0, \ldots)$ est un polynôme.*

2. Dans $\mathbb{Z}/9\mathbb{Z}$, $(0, 0, 0, 5, 8, 4, 3, 0, 0, \ldots)$ est un polynôme.

Définition 1.4.3. *Si $P = (a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ et n le plus grand indice tel que $a_n \neq 0$, alors n est appelé* ***degré*** *du polynôme et on le note le plus souvent $deg(P)$.*

Exemple 1.4.4. $P = (1, 0, -2, 0, 3, 0, \ldots) \implies deg(P) = 4.$

Remarque 1.4.5. *Si $P = (0, 0, 0, \dots)$, alors son degré est égal à $-\infty$.*

De plus, un polynôme P non nul est noté :

$$P(X) = (a_0, a_1, \dots, a_n, \dots) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in \mathbb{K}[X]$$

où $\mathbb{K}$ est un corps.

Exemple 1.4.6. *1. $P(x) = 1 + 2x + x^2 \in \mathbb{F}_3[x]$ et son monôme de plus haut degré est x^2.*

2. $Q(x) = 2 + 5x + x^2 + x^3 \in \mathbb{F}_8[x]$ et son monôme de plus haut degré est x^3.

Définition 1.4.7. *Soit f un polynôme de $\mathbb{F}_q[X]$. Son ordre est noté $ord(f)$ et est le plus petit entier t tel que*

$$X^t \equiv 1 \ mod \ f(x).$$

Exemple 1.4.8. *Soit $f(x) = x^2 + x + 1$ définie sur $\mathbb{F}_2$. Dans cet exemple, nous allons déterminer l'ordre de f à l'aide du tableau suivant :*

$f(x)$	t	x^t	$x^t \ mod \ f(x)$
$x^2 + x + 1$	0	1	–
	1	x	–
	2	x^2	$x + 1$
	3	x^3	1

Alors $x^3 \equiv 1 \ mod \ f(x)$. Donc $ord(f) = 3$.

1.4.2 Polynômes irréductibles et primitifs

Définition 1.4.9. *Soit P un polynôme appartenant à $\mathbb{K}[X]$. P est dit irréductible ou premier dans $\mathbb{K}[X]$, si P est tel que $deg(P) > 0$ et $P = QR$, alors Q ou R est une*

constante.

Un polynôme de degré positif qui n'est pas irréductible est dit réductible. La réductibilité dépendent du corps de base.

Exemple 1.4.10. *1. Tous les polynômes de degré 1 sont irréductibles.*

2. Dans $\mathbb{R}[X]$, tout polynôme de degré 2 et de discriminant négatif est irréductible et son corps de base est $\mathbb{R}$.

3. Le polynôme $f(x) = x^2 - 2$ est irréductible sur $\mathbb{Q}[X]$ car

$$f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}) \quad et \quad \sqrt{2} \notin \mathbb{Q}$$

et son corps de base est $\mathbb{Q}$.

Théorème 1.4.11. *[20] Si f est un polynôme irréductible de degré m sur $\mathbb{F}_q[X]$, alors f possède une racine α dans $\mathbb{F}_{q^m}$.*

Cependant toutes les racines de f sont simples et données par les éléments distincts $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^m-1}$ de $\mathbb{F}_{q^m}$.

Corollaire 1.4.12. *Soit f un polynôme irréductible de degré m dans $\mathbb{F}_q[X]$, alors le corps scindé de f sur $\mathbb{F}_q$ est $\mathbb{F}_{q^m}$.*

Démonstration. D'après le théorème 1.4.11, f est scindé sur $\mathbb{F}_{q^m}$. Donc

$$\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^m-1}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$$

où α est une racine de f. □

Théorème 1.4.13. *[20] Soit $f \in \mathbb{F}_q[X]$ un polynôme irréductible de degré m sur $\mathbb{F}_q$ et $f(0) \neq 0$. Alors l'ordre de f est égal à l'ordre d'une racine de f dans le groupe multiplicatif $\mathbb{F}_{q^m}^*$.*

Corollaire 1.4.14. *Si $f \in \mathbb{F}_q^*[x]$ un polynôme irrédutible de degré m, alors l'ordre de f divise $q^m - 1$.*

Démonstration. Si $f(x) = cx$, $c \in \mathbb{F}_{q^m}^*$, alors l'ordre de f est égal à 1. donc le résultat est trivial. Dans le cas contraire, le résultat vient du thérème 1.4.13 et du fait que l'ordre de $\mathbb{F}_{q^m}^*$ égal à $q^m - 1$. □

Définition 1.4.15. *Un polynôme irréductible f, de degré m sur $\mathbb{F}_q[X]$ est primitif s'il est d'ordre $q^m - 1$.*

Exemple 1.4.16. *Soit $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$, un polynôme irréductible sur $\mathbb{F}_2$, de degré 3. Alors $ord(f) = 7 = 2^3 - 1$. Donc f est un polyôme primitif.*

Remarque 1.4.17. *Un polynôme primitif de degré m sur $\mathbb{F}_q$, peut être considéré comme un polynôme unitaire, irréductible sur $\mathbb{F}_q[X]$ ayant une racine $\alpha \in \mathbb{F}_{q^m}$ et qui génère le groupe multiplicatif $\mathbb{F}_{q^m}^*$.*

Revenons maintenant à la définition et aux propriétés d'un polynôme caractéristique d'une suite récurrente linéaire.

1.4.3 Polynôme caractéristique

Définition 1.4.18. *Soit $s_0, s_1, s_2, \ldots$ une suite récurrente linéaire d'ordre k satisfaisant à la relation de récurrence*

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_1 s_{n+1} + a_0 s_n \quad pour \quad n = 0, 1, \ldots$$

où $a_j \in \mathbb{F}_q$ pour $0 \leq j \leq k-1$.

Le polynôme

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_0 \in \mathbb{F}_q[x]$$

est appelé polynôme caractéristique de la suite récurrente linéaire $s_0, s_1, s_2, \ldots$. *On rencontrera aussi le polynôme réciproque de cette suite récurrente linéaire défini par*

$$f^*(x) = x^k.f(1/x) = 1 - a_{k-1}x - a_{k-2}x^2 - \cdots - a_0x^k \in \mathbb{F}_q[x].$$

Exemple 1.4.19. *Soit* s_0, s_1, s_2, ... *une suite satisfaisant à la relation de récurrence* $s_{n+5} = s_{n+1} + s_n$ *d'ordre* 5 *sur* $\mathbb{F}_2$. *Le polynôme caractéristique* f *de cette suite est donné par*

$$f(x) = x^5 - x - 1 = x^5 + x + 1$$

et son polynôme réciproque est

$$f^*(x) = x^5 f(1/x) = x^5(\frac{1}{x^5} + \frac{1}{x} + 1) = 1 + x^4 + x^5$$

Remarque 1.4.20. *On peut aussi déterminer le polynôme caractéristique d'une suite récurrente linéaire à l'aide de sa matrice compagnon :*

$$f(x) = det\Big(M - xI \Big)$$

et son polynôme réciproque est

$$f^*(x) = x^k f(1/x) = x^k det\Big(M - \tfrac{1}{x}I \Big).$$

Le polynôme caractéristique d'une suite récurrente linéaire et son polyôme réciproque ont même degré.

Proposition 1.4.21. *[20] Soit* s_0, s_1, s_2, ... *une suite récurrente linéaire d'ordre* k *sur* F_2.

La suite s_0, s_1, s_2, ... *a pour polynôme caractéristique* $f(x)$ *si et seulement si son développement en série formelle*

$$S(x) = \sum_{n\geq 0} s_n x^n \quad s'écrit \quad S(x) = \frac{g(x)}{f(x)}$$

où $g(x) \in F_2[x]$ est un polynôme dont $\deg(g) < \deg(f)$ et est entièrement déterminé par l'état initial de cette suite définie par :

$$g(x) = \sum_{i=}^{k-1} x^i \sum_{j=0}^{i} a_{i-j} s_j,$$

Lemme 1.4.22. *[20] Soit*

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_0 \in \mathbb{F}_q[x]$$

avec $k \geq 1$ et $a_0 \neq 0$, le polynôme caractéristique de la suite $s_0,\ s_1,\ s_3,\ \ldots$.

Alors l'ordre de $f(x)$ est égal à l'ordre de la matrice associée M de la suite dans $GL(k, \mathbb{F}_q)$.

Théorème 1.4.23. *[20] Soit $s_0, s_1, s_2, \ldots$ une suite récurrente linéaire de polynôme caractéristique $f(x)$ sur $\mathbb{F}_q$.*

Si les racines $\alpha_1, \ldots, \alpha_k$ de $f(x)$ sont distinctes, alors

$$s_n = \sum_{j=1}^{k} \beta_j \alpha_j^n \quad pour \quad n = 0, 1, \ldots$$

où $\beta_1, \ldots, \beta_k$ sont des éléments uniquement déterminés par l'état initial de cette suite et appartiennent au corps scindé de $f(x)$ sur $\mathbb{F}_q$.

Théorème 1.4.24. *[20] Soit $s_0, s_1, s_2, \ldots$ une suite récurrente linéaire périodique d'ordre k sur $\mathbb{F}_q$, de période r et de polynôme caractéristique $f(x) \in \mathbb{F}_q[x]$.*

Alors

$$f(x)s(x) = (1 - x^r)h(x)$$

avec

$$s(x) = s_0 x^{r-1} + s_1 x^{r-2} + \cdots + s_{r-2}x + s_{r-1} \in \mathbb{F}_q[x]$$

et

$$h(x) = \sum_{j=0}^{k-1} \sum_{i=0}^{k-1-j} a_{i+j+1} s_i x^j \in \mathbb{F}_q[x]$$

où $a_k = -1$

Définition 1.4.25. *Soit* $f(X)$ *un polynôme irréductible de* $\mathbb{F}_q[X]$*, de degré* m*. Il est dit primitif si l'une de ses racines engendre le sous groupe multiplicatif* $\mathbb{F}_{q^m}^*$.

Exemple 1.4.26. *Soit* $f(x) = x^3 + x + 1$ *un polynôme irréductible de* $\mathbb{F}_2[x]$*, et soit* α *tel que* $f(\alpha) = 0$*. Montrons que* $f(x)$ *est un polynôme primitif. Pour ce faire, énumérons les puissances de* α *:*

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

Donc le polynôme $f(x) = x^3 + x + 1$ *est primitif et* 7 *est l'ordre de* α*.*

1.4.4 Fonction génératrice d'une suite récurrente linéaire

Dans cette section, nous allons définir une fonction génératrice d'une suite récurrente linéaire. Dans [20], nous avons la définition suivante :

Définition 1.4.27. *Soit* $s_0, s_1, \ldots,$ *une suite d'éléments de* $\mathbb{F}_q$ *à laquelle on associe*

sa fonction génératrice, notée

$$G(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n + \cdots = \sum_{n=0}^{\infty} s_n x^n$$

où x est l'indéterminée, $G(x)$ est appelé la fonction génératrice associée à la suite $s_0, s_1, \ldots$.

Exemple 1.4.28. *Soit la suite $s_0,\ s_1,\ s_2,\ \ldots$ satisfaisant à la relation de récurrence $s_{n+2} = s_{n+1} + s_n$ d'ordre 2 et d'état initial $s_1 = 0,\ s_0 = 1$.*

Les termes de cette suite sont

$$|\,1\,0\,1\,|\,1\,0\,1\,|\,1\,0\,1\,|\,1\,0\,1\,|\,\ldots.$$

et sa fonction génératrice est alors

$$G(x) = 1 + x^2 + x^3 + x^5 + x^6 + x^8 + x^9 + \ldots$$

Théorème 1.4.29. *[20] Soient $s_0, s_1, \ldots$ une suite récurrente linéaire d'ordre k, de polynôme caractéristique $f(x)$ sur $\mathbb{F}_q$, $f^*(x) \in \mathbb{F}_q[x]$ son polynôme réciproque et $G(x) \in \mathbb{F}_q[x]$ sa fonction génératrice.*

Alors

$$G(x) = \frac{g(x)}{f^*(x)}$$

avec

$$g(x) = \sum_{j=0}^{k-1} \sum_{i=0}^{j} a_{i+k-j} s_i x^i \in \mathbb{F}_q$$

où $a_k = -1$.

Inversement, si $g(x)$ est un polynôme de $deg(g(x)) < k$ sur $\mathbb{F}_q$ et si $f^*(x) \in \mathbb{F}_q[x]$, alors la série formelle de $G(x) \in \mathbb{F}_q[x]$ définit la fonction génératrice d'une suite récurrente linéaire d'ordre k dans $\mathbb{F}_q$ satisfaisant à la relation de récurrence (1.1).

1.4.5 Polynôme minimal d'une suite récurrente linéaire

Définition 1.4.30. *Soit $s_0, s_1, s_2, \ldots$ une suite récurrente linéaire sur $\mathbb{F}_q$. Le polynôme minimal de la suite $s_0, s_1, s_2, \ldots$ est son polynôme caractéristique de plus petit degré.*

Définition 1.4.31. *Soit $s_0, s_1, s_2, \ldots$ une suite récurrente linéaire sur $\mathbb{F}_q$. Alors, tout polynôme $g(x) \in F_q[x]$ est un polynôme caractéristique de cette suite si et seulement si il existe un unique polynôme unitaire $h(x) \in \mathbb{F}_q[x]$, de degré $deg(h(x)) \geq 1$ tel que $h(x)$ divise $g(x)$.*

Le polynôme $h(x)$ est appelé dans ce cas polynôme minimal et son degré est appelé ***complexité linéaire*** *ou* ***équivalence linéaire*** *de $s_0, s_1, s_2, \ldots$.*

Énumérons quelques propriétés sur des polynômes minimaux.

Propriétés 1. *Soit $s_0, s_1, s_2, \ldots$ d'ordre k sur $\mathbb{F}_p$ et de polynôme minimal $m(x)$.*

Alors

1. *$m(x)$ est irréuctible*
2. *pour tout polynôme caractéristique $f(x) \in \mathbb{F}_p[x]$ de cette suite, $m(x)$ divise $f(x)$.*
3. *$m(x)$ divise $(x^{p^k} - x)$.*
4. *$deg(m(x)) \leq k$.*

Démonstration. pour les preuves des propriétés citées ci-dessus il faut se référer à [3]. □

Exemple 1.4.32. *Soit $x_0, x_1, \ldots$ une suite récurrente linéaire sur $\mathbb{F}_2$ satisfaisant à la relation*

$$x_{n+4} = x_{n+3} + x_{n+1} + x_n, \ n = 0, 1, \ldots$$

et d'état initial $(1,1,0,1)$.

Alors le polynôme caractéristique $f(x)$ *est*

$$f(x) = x^4 - x^3 - x - 1 = x^4 + x^3 + x + 1 \in \mathbb{F}_2[x].$$

Déterminons maintenant le polynôme minimal $m(x)$ *de la suite* $x_0,\ x_1,\ \ldots$.

On a :

$$\begin{aligned} f(x) &= x^4 + x^3 + x + 1 \\ &= (x+1)(x^3+1) \\ &= (x+1)^2(x^2+x+1) \end{aligned}$$

Donc, d'après les propriétés 1, le polynôme minimal est $m(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$.

Remarque 1.4.33. *On peut aussi vérifier que* $m(x) = x^2 + x + 1$ *en utilisant les déterminants de* ***Hankel*** *ou bien comparer les termes des suites récurrentes linéaires données par les polynômes*

$$f(x) = x^4 + x^3 + x + 1 \quad et \quad m(x) = x^2 + x + 1.$$

On aboutira toujours au même résultat.

Définition 1.4.34. *Soit* $\alpha \in \mathbb{F}_{2^n}$. *Alors les éléments* $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$ *sont appelés éléments conjugués de* α.

Théorème 1.4.35. *[20] Soit* $s_0, s_1, \ldots$ *une suite récurrente linéaire dans* $\mathbb{F}_q$. *Alors*

1) *un polynôme unitaire* $f(x) \in \mathbb{F}_q[x]$ *de degré positif est dit polynôme caractéristique de* $s_0, s_1, \ldots$ *si et seulement si il existe un unique polynôme unitaire* $m(x) \in \mathbb{F}_q[x]$ *tel que* $m(x)$ *divise* $f(x)$.

2) *si de plus la suite de de polynôme minimal* $m(x) \in \mathbb{F}_q[x]$. *Alors,*

i) *la période de la suite* $s_0, s_1, \ldots$ *est égale à* $ord(m(x))$.

ii) *le polynôme minimal* $m_1(x)$ *de la suite décalée* $s_b, s_{b+1}, \ldots$ *divise le polynôme minimal* $m(x)$ *de la suite originale. Si* $s_0, s_1, \ldots$ *est périodique, alors* $m_1(x) = m(x)$.

Théorème 1.4.36. *[20] Soient* $f(x) \in \mathbb{F}_q$ *un polynôme unitaire irréductible sur* $\mathbb{F}_q$, *et* $s_0, s_1, \ldots$ *une suite récurrente linéaire dans* $\mathbb{F}_q$ *dont tous les termes ne sont pas égaux à* 0. *Si* $f(x)$ *est le polynôme caractéristique de cette suite, alors son polynôme minimal est égal à* $f(x)$.

1.4.6 Les suites à période maximale ou m-séquences

Définition 1.4.37. *Une suite récurrente linéaire dans* $\mathbb{F}_q$, *de polynôme caractéristique primitif et d'état initial non nul est dite suite de période maximale (ou m-séquence) dans* $\mathbb{F}_q$.

Théorème 1.4.38. *[21, 20] Toute suite de période maximale sur* $\mathbb{F}_q$ *est périodique, de période* $q^k - 1$.

Théorème 1.4.39. *[20]Soit* $s_0,\ s_1,\ s_2,\ \ldots$ *une m-séquence d'état initial non nul, de polynôme caractéristique* $f(x)$ *satisfaisant à* $f(0) \neq 0$. *Alors* $s_0,\ s_1,\ s_2,\ \ldots$ *est périodique et sa période est égale à l'ordre de* $f(x)$.

Remarque 1.4.40. *Puisque le polynôme caractéristique d'une suite de période maximale est son polynôme minimal, alors son degré ou l'ordre de la suite est égale à sa complexité linéaire.*

1.4.7 Corrélation d'une suite récurrente linéaire

Définition 1.4.41. ***Corrélation périodique.*** *Soient les suites récurrentes linéaires $(x_n)_{n\geq 0}$ et $(y_n)_n$ et τ un entier. On appelle corrélation périodique des deux suites $(x_n)_{n\geq 0}$ et $(y_n)_{n\geq 0}$, la suite $\theta_{x,y}(\tau)$ de longueur k décalée de τ définie par*

$$\theta_{x,y}(\tau) = \sum_{n=0}^{k-1} (-1)^{x_{n+\tau}-y_n} \text{ pour tout } n \geq 0.$$

et τ est la valeur de décalage entre les deux suites.

Définition 1.4.42. ***Corrélation apériodique.*** *Soient les suites récurrentes linéaires $(x_n)_{n\geq 0}$ et $(y_n)_n$ et τ un entier. On appelle corrélation apériodique des deux suites $(x_n)_{n\geq 0}$ et $(y_n)_n$, la suite $C_{x,y}(\tau)$ de longueur k décalée de τ définie par*

$$C_{x,y}(\tau) = \sum_{n=0}^{k-\tau-1} (-1)^{x_{n+\tau}-y_n} \text{ pour tout } n \geq 0$$

et τ est la valeur de décalage entre les deux suites.

Remarque 1.4.43. *Si $x_n = y_n$, la corrélation de $(x_n)_{n\geq 0}$ est dite autocorrélation de $(x_n)_{n\geq 0}$ décalée de τ et est égale à*

$$\theta_x(\tau) = \sum_{n=0}^{k-1} (-1)^{x_{n+\tau}-x_n} \text{ pour tout } n \geq 0.$$

et sa corrélation apériodique est

$$C_x(\tau) = \sum_{n=0}^{k-\tau-1} (-1)^{x_{n+\tau}-x_n} \text{ pour tout } n \geq 0.$$

Si $(x_n)_{n\geq 0}$ est une m-séquence de longueur n, alors l'autocorrélation est

$$\theta_x(\tau) = \begin{cases} 2^n - 1 & si\ \tau \equiv 0\ (\ mod\ 2^n - 1)\,; \\ -1 & si\ \tau \not\equiv 0\ (\ mod\ 2^n - 1). \end{cases}$$

pour tout $n \geq 0$ dans $\mathbb{F}_2$.

1.5 Application d'une suite récurrente linéaire à la cryptographie

Cette section porte sur des rappels sur la cryptologie et l'utilisation des suites récurrentes linéaires en cryptologie. Mais pour être plus précis nous allons surtout mettre l'accent sur le chiffrement par flot dans lequel on utilise ces suites.

1.5.1 Qu'est-ce que la cryptologie ?

Définition 1.5.1. *La **cryptologie** est la science des messages secrets. Longtemps restreinte aux usages diplomatiques et militaires, elle est maintenant une discipline scientifique à part entière, dont l'objet est l'étude des méthodes permettant d'assurer les services d'**intégrité**, d'**authenticité** et de **confidentialité** dans les systèmes d'information et de communication.*

*De plus, elle se partage en deux sous-disciplines, également importantes : la **cryptographie** et la **cryptanalyse**.*

Définition 1.5.2. *La **cryptographie** est l'art de rendre inintelligible, de crypter, de coder, un message pour ceux qui ne sont pas habilités à en prendre connaissance.*

Définition 1.5.3. *La **cryptanalyse** est l'art pour une personne non habilitée, de décrypter, de décoder, de déchiffrer, un message. C'est donc l'ensemble des procédés d'attaque d'un système cryptographique.*

1.6 Cryptographie

Si le but traditionnel de la cryptographie est d'élaborer des méthodes permettant de transmettre des données de manière confidentielle, la cryptographie moderne

s'attaque en fait plus généralement aux problèmes de sécurité des communications.

Pour cela, on utilise un certain nombre de mécanismes basés sur des algorithmes cryptographiques. Nous allons voir dans ce chapitre quelles sont les techniques que la cryptographie fournit pour réaliser ces mécanismes.

Il existe deux grandes familles d'algorithmes cryptographiques à base de clés : les algorithmes à clé secrète ou algorithmes symétriques, et les algorithmes à clé publique ou algorithmes asymétriques.

1.6.1 Chiffrement symétrique ou à clé secrète

Dans la cryptographie conventionnelle, les clés de chiffrement et de déchiffrement sont identiques : c'est la clé secrète, qui doit être connue des tiers communiquants et d'eux seuls. Le procédé de chiffrement est dit symétrique.

Les algorithmes symétriques sont de deux types :

- les algorithmes de chiffrement en continu ou par flot, qui agissent sur le texte en clair un bit à la fois, en particulier ceux basés sur des registres à décalage ;
- les algorithmes de chiffrement par blocs, qui opèrent sur le texte en clair par groupes de bits appelés blocs.

1.6.2 Chiffrement par blocs

Un chiffrement par blocs est un des types de chiffrement à clé secrète. Dans un tel procédé, le message est découpé en blocs de taille fixe et chiffré bloc par bloc.

Exemple 1.6.1. *Notons que les chiffrements suivants sont des chiffrements par blocs :*

- *chiffrements par transposition,*
- *chiffrements par substitution. Dans le cas de la substitution simple les blocs sont réduits à une lettre*

Remarque 1.6.2. *Les algorithmes de chiffrement par blocs peuvent être utilisés suivant différents modes, dont les deux principaux sont : le mode ECB (Electronic Code-Book) et le mode CBC (Cipher Block Chaining) que nous n'allons pas détailler dans cette thèse.*

1.6.3 Chiffrement en continu

Contrairement aux algorithmes de chiffrement par blocs, les algorithmes de chiffrement en continu (Stream Cipher), opèrent sur chaque unité de chiffrement du clair (chiffrement d'un bit/caractère à la fois, chiffrement bit à bit ou caractère par caractère). Ils sont généralement plus rapides que ceux par blocs, en hardware, et ont des circuits moins complexes. De plus, lorsque la taille mémoire est limitée ou lorsque les bits du message doivent être chiffrés dès réception, leur utilisation s'impose. En outre, ils sont adaptés à des contextes dans lesquels les erreurs de transmission sont fréquentes.

Dans tout algorithme de chiffrement par flot, un flot de clés est génèré et combiné avec le message. Ces deux opérations ne sont pas forcément indépendantes : lorsqu'elles le sont, on dit que ce chiffrement est **synchrone** et dans le cas contraire, on dit qu'il est **asynchrone**.

- Le chiffrement en continu repose sur un générateur de clefs qui engendre un flux de bits (Key Stream) c'est à dire, une suite ou séquence de clés (ou flot de clés)
- $K = (k_1 k_2 \dots k_i \dots k_n)$ c'est à dire, qui, combinée (par Ou exclusif) aux bits du clair $X = (x_1 x_2 \dots x_i \dots x_n)$ fournit le crypto $Y = (y_1 y_2 \dots y_i \dots y_n)$.

Les équations de chiffrement et de déchiffrement d'un chiffrement en continu sont conçues comme suit :

$$\begin{aligned} \textbf{Chiffrement :} \quad y_i &= E_{k_i}(x_i) = x_i \bigoplus k_i \\ \textbf{Déchiffrement :} \quad x_i &= D_{k_i}(y_i) = y_i \bigoplus k_i. \end{aligned}$$

Nous allons étudier plus précisément les méthodes de génération d'un flot de clés à partir de registres à décalage. Leur utilisation dans un algorithme de chiffrement par flot synchrone étant en général réalisée en combinant de manière simple chaque bit de la sortie du générateur de clés avec chaque bit du clair (message à chiffrer) pour obtenir le message chiffré. Pour ce faire, nous allons d'abord définir ce qu'est un registre à décalage.

Définition 1.6.3. *Un registre à décalage de longueur n est constitué de n cases mémoire ou bascules numérotées de 0 à $n-1$, chacune pouvant contenir un bit, et ayant une entrée et une sortie, et d'une horloge contrôlant le mouvement des données. À chaque coup d'horloge,*

- *un bit de rétroaction s est calculé par combinaison des bits des cases de 0 à $n-1$,*
- *le contenu de la case 0 sort du registre pour former la séquence de sortie,*
- *le contenu de la case i passe dans la case $(i-1)$, $1 \leq i \leq n-1$,*
- *la case $n-1$ est remplie avec le bit s.*

Lorsque la combinaison est un simple "xor" de certaines des cases du registre, on parle de rétroaction linéaire.

Pour fonctionner, un registre doit être au préalable rempli avec une suite de n bits $[s_{n-1}, \ldots, s_1, s_0]$, appelée état initial du registre. Il est à noter que les n premiers bits de la suite produite par le registre sont $s_0, s_1, \ldots, s_{n-1}$.

Les LFSRs sont les registres les plus utilisés pour la génération d'un flot de clés. Par leur simplicité d'implémentation et par le bon choix des paramètres, ils produisent des suites dites suites récurrentes linéaires ayant des propriétés intéressantes comme nous allons le voir dans suite de notre thèse.

Définition 1.6.4. *Un LFSR(Linear Feedback Shift Register en anglais) ou registre à décalage à rétroaction linéaire binaire de longueur n est composé d'un registre à*

décalage contenant une suite de n bits $(s_i,\ s_{i+1},\ \ldots,\ s_{i+n-1})$ *et d'une fonction de rétroaction linéaire, et les bits* $(s_0,\ s_1, \ldots,\ s_{n-1})$ *qui déterminent entièrement la suite produite constituent l'état initial du registre.*

Le fonctionnement d'un LFSR binaire de longueur n est le suivant :

à chaque top d'horloge, le bit de "gauche" si constitue la sortie du registre, et les autres sont décalés vers la gauche ; le nouveau bit s_{i+n} placé dans la cellule de "droite" du registre est donné par une fonction linéaire :

$$s_{i+n} = a_1 s_{i+n-1} + \cdots + a_{n-1} s_1 + a_n s_i \text{ pour tout } i \geq 0. \tag{1.3}$$

appelée fonction de rétroaction ou fonction de réinjection ou fonction de rebouclage, où les coefficients a_i sont binaires.

Définition 1.6.5. *Soit un LFSR dont la fonction de rétroaction est donnée par la relation 1.3. Son polynôme de rétroaction f est le polynôme de $\mathbb{F}_2[x]$*

$$f(x) = 1 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n,\ a_i \in \mathbb{F}_2,\ 1 \leq i \leq n.$$

Proposition 1.6.6. *Toute suite binaire à récurrence linéaire homogène d'ordre n est ultimement périodique, et sa plus petite période T est inférieure ou égale à $2^n - 1$. De plus, si le coefficient a_n est non nul, alors la suite est périodique.*

De plus, si le polynôme de rétroaction d'un LFSR est primitif irréductible et le coefficient dominant non nul, alors la suite produite par ce LFSR est une suite de longueur maximale et de période $2^n - 1$. De telles suites sont dites des m-séquences.

Nous reviendrons plus en détails, dans le chapitre suivant, sur les suites dites récurrentes linéaires produites par les LFSRs.

1.6.4 Complexité linéaire d'un LFSR

Proposition 1.6.7. *La suite $(s_i)_{i\geq 0}$ est produite par un LFSR dont le polynôme de rétroaction*

$$f(x) = 1 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n,\ a_i \in \mathbb{F}_2,\ 1 \leq i \leq n.$$

si et seulement si son développement en série formelle $s(x) = \sum_{k=0}^{\infty} s_k x^k$ s'écrit

$$s(x) = \frac{g(x)}{f(x)}$$

où g est un polynôme de $\mathbb{F}_2[X]$ tel que $\deg(g) < \deg(f)$. En outre, le polynôme g est entièrement déterminé par l'état initial du registre :

$$g(x) = \sum_{i=0}^{n-1} x^i \sum_{j=0}^{i} a_{i-j} s_j$$

Afin d'obtenir une forme canonique de la série génératrice de $(s_n)_{n\geq 0}$, on définit le polynôme de rétroaction minimal du registre : c'est un diviseur de $f(x)$, qui de plus est le polynôme de plus bas degré parmi les polynômes de rétroaction de tous les LFSRs possibles qui génèrent la suite $(s_n)_{n\geq 0}$.

Définition 1.6.8. *Soit $(s_i)_{i\geq 0}$ une suite binaire à rétroaction linéaire d'ordre n dont l'état initial est non nul. Son polynôme de rétroaction minimal est l'unique polynôme unitaire f_0 de $\mathbb{F}_2[x]$ tel qu'il existe $g_0 \in \mathbb{F}_2[X]$, avec $\deg(g_0) < \deg(f_0)$ et $pgcd(g_0, f_0) = 1$, vérifiant*

$$s(x) = \frac{g_0(x)}{f_0(x)}.$$

La complexité linéaire du LFSR produisant la suite $(s_i)_{i\geq 0}$, notée $\Lambda(s)$, est alors égale au degré de f_0.

En clair, la complexité linéaire d'un LFSR produisant une suite $(s_i)_{i\geq 0}$ est la longueur du plus petit LFSR permettant d'engendrer $(s_i)_{n\geq 0}$.

Définition 1.6.9. *La complexité linéaire d'une suite infinie s de bits, notée $\Lambda(s)$, est :*

- $\Lambda(s) = 0$ *si* $s_i = 0$ *pour tout* i ;
- $\Lambda(s) = \infty$ *si aucun registre à décalage à rétroaction linéaire ne produit* s ;
- $\Lambda(s) = n$ *si le plus petit registre à décalage à rétroaction linéaire produisant* s *a une longueur* n.

1.6.5 Générateurs de flots de clés basés sur des LFSR

Bien que les propriétés de la suite produite dans le cas où le polynôme de rétroaction est primitif soient intéressantes, un LFSR ne peut être utilisé directement pour produire un flot de clés : ces propriétés sont seulement nécessaires. En effet, ce type de générateur est prédictible dans le sens où si on en connaît une sous-suite suffisamment longue, on peut retrouver le polynôme de rétroaction du registre et donc, génèrer le reste de la suite.

Plus précisément, si on note s la suite génèrée par un LFSR de taille n et si on connaît une sous-suite $(s_k, s_{k+1}, \ldots, s_{k+n-1})$ avec $k \geq 0$ de taille $i \geq 2n$, alors la résolution du système de n équations à n inconnues $a_1, \ldots, a_n$ sur $\mathbb{F}_2$ suivant :

$$\begin{pmatrix} s_k & s_{k+1} & \cdots & s_{k+n-1} \\ s_{k+1} & s_{k+2} & \cdots & s_{k+n} \\ \vdots & \vdots & \cdots & \vdots \\ s_{k+n-1} & s_{k+n} & \cdots & s_{k+2n-2} \end{pmatrix} \begin{pmatrix} a_n \\ a_{n-1} \\ \vdots \\ a_1 \end{pmatrix} = \begin{pmatrix} s_{k+n} \\ s_{k+n+1} \\ \vdots \\ s_{k+2n-1} \end{pmatrix}$$

permet de retrouver le polynôme de rétroaction $f(x) = 1 + \sum_{i=1}^{n} a_i x^i$ du LFSR. En effet, on peut montrer que si s a été génèrée par un polynôme irréductible de $\mathbb{F}_2[x]$, alors ce système admet une solution unique dans $\mathbb{F}_2^n$. Bien sûr, même si on dispose d'une sous-suite $(s_k, s_{k+1}, \ldots, s_{k+i-1})$, on ne connaît pas n. On peut alors construire un système d'équations linéaires de taille plus grande que nécessaire, dont la résolution

fournit une solution, les colonnes de ce système n'étant pas indépendantes. Mais, le point important est que le LFSR est totalement connu dès lors que n est suffisamment grand.

La simplicité en implantation des LFSR demeure un atout évident. Leur vulnérabilité aux attaques à clair connu étant dûe à leur linéarité, l'idée pour pouvoir néanmoins les utilser est de les "détruire". Trois méthodes sont employées :

- utiliser plusieurs LFSR dont les sorties sont combinées à l'aide d'une fonction non-linéaire f. La sortie de f constitue alors le flot de clés.
- utiliser plusieurs LFSR dont l'un sert à choisir la sortie du LFSR qui sera utilisée à un instant donné.
- utiliser un seul LFSR : le flot de clés étant obtenu par combinaison du contenu de ses cases mémoire par une fonction non-linéaire.

1.6.6 Cryptage avec un LFSR

Pour crypter à l'aide d'un LFSR on commence par transformer le message, m, en une suite binaire (par exemple à l'aide des codes ASCII des symboles), c'est à dire en une suite, $(m_i)_{i\in\mathbb{N}}$, d'éléments de $\mathbb{F}_2$ puis on XORise la suite obtenue avec la suite récurrente linéaire fournie par le LFSR, $(x_i)_{i\in\mathbb{N}}$ pour obtenir le message codé, $(c_i)_{i\in\mathbb{N}}$ sous forme d'une suite d'éléments de $\mathbb{F}_2$:

$$\begin{array}{ccccccc} m_0 & m_1 & m_2 & \dots & m_i & \dots \\ \oplus & \oplus & \oplus & \dots & \oplus & \dots \\ x_0 & x_1 & x_2 & \dots & x_i & \dots \\ \hline c_0 & c_1 & c_2 & \dots & c_i & \dots \end{array}$$

Le décodage est symétrique c'est à dire que l'on XORise le message chiffré (supposé être une suite binaire) avec la suite récurrente linéaire fournie par le LFSR. L'exemple suivant on donne un exemple académique de cryptage et décryptage à l'aide d'un LFSR.

Exemple 1.6.10. *On considère le LFSR sur* $\mathbb{F}_2$*, défini par la relation de récurrence*

$$u_{n+4} = u_{n+1} + u_n$$

et de conditions initiales $(k_0, k_1, k_2, k_3) = (1, 0, 0, 0) \in \mathbb{F}_2^4$*. Pour tout choix de conditions initiales la période de la suite récurrente linéaire* $(u_n)_{n\in\mathbb{N}}$ *est majorée par* 15.

On code par XORisation à l'aide du LFSR précédent avec les conditions initiales $(k_0, k_1, k_2, k_3) = (1, 0, 0, 0)$*. Chaque lettre de l'alphabet est codée par le quintuplet* $(a_0, a_1, a_2, a_3, a_4)$ *tel que* $a_0 + 2a_1 + 4a_2 + 8a_3 + 16a_4$ *soit le rang de la lettre dans l'alphabet ordinaire compté entre* 1 *et* 26*, le quintuplet* $(0, 0, 0, 0, 0)$ *correspond à l'espace entre deux mots (exemples : A la première lettre de l'alphabet est codée (1, 0, 0, 0, 0), M la treizième lettre de l'alphabet est codée* $(1, 0, 1, 1, 0)$*, T la vingtième lettre de l'alphabet est codée* $(0, 0, 1, 0, 1)$*. Le début de la suite* $n \to u_n$ *est*

$$\begin{aligned}
u_0 &= 1,\\
u_1 &= 0,\\
u_2 &= 0,\\
u_3 &= 0,\\
u_4 &= u_0 + u_1 = 1,\\
u_5 &= u_1 + u_2 = 0,\\
u_6 &= u_2 + u_3 = 0,\\
\ldots &= \ldots
\end{aligned}$$

Donc si on veut coder TA on le tranforme par le codage précédent en $(0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$

on XORise cette suite fini avec la suite $(u_0, ..., u_9)$ *et il vient*

$$\begin{array}{cccccccccccc} & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus \\ & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ \hline = & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ = & EM & & & & & & & & & \end{array}$$

1.6.7 Algorithme de Berlekamp-Massey

L'algorithme de Berlekamp-Massey est un algorithme très important en informatique et a de nombreuses applications. Il est introduit en 1968 par E. Berlekamp comme algorithme de décodage pour des codes BCH. En 1969, J.M Massey montra que l'on pouvait se servir de l'algorithme pour calculer la complexité linéaire d'une suite. Dans [20], l'algorithme de Berlekamp-Massey est décrit comme suit :

Soit $s_0, s_1, \ldots$ une suite d'éléments de $\mathbb{F}_q$ avec $G(x) = \sum_{n=0}^{\infty} s_n x^n$. Pour $j = 0, 1, \ldots$, nous définissons les polynômes $g_j(x)$ et $h_j(x)$ sur $\mathbb{F}_q$, les entiers m_j, et b_j de $\mathbb{F}_q$ comme suit. Initialement, nous établissons

$$g_0(x) = 1,\ h_0(x) = x \text{ et } m_0 = 0.$$

Alors nous procédons récursivement par le fait que b_j soit le coefficient de x^j dans $g_j(x)G(x)$ et établissons :

$$g_{j+1}(x) = g_j(x) - b_j h_j(x),$$

$$h_{j+1}(x) = \begin{cases} b_j^{-1} x g_j(x), & si \quad b_j \neq 0 \quad et \quad m_j \geq 0, \\ x h_j(x), & \text{sinon.} \end{cases}$$

$$m_{j+1} = \begin{cases} -m_j, & si \quad b_j \neq 0 \quad et \quad m_j \geq 0, \\ m_j + 1, & \text{sinon.} \end{cases}$$

Si la suite $s_0, s_1, \ldots$ est une suite récurrente linéaire dont le polynôme minimal de degré k, alors le polynôme $g_{2k}(x)$ est égale à son polynôme minimal réciproque. Donc

le polynôme minimal $m(x)$ de cette suite est donné par

$$m(x) = x^k g_{2k}(1/x).$$

Si le polynôme de cette suite est de degré inférieur ou égale à k, alors nous posons l'entier $r = \lfloor k + \frac{1}{2} - \frac{1}{2}m_{2k} \rfloor$ tel que le polynôme minimal

$$m(x) = x^r g_{2k}(1/x).$$

Dans les deux cas la détermination du polynôme minimal $m(x)$ dépends des $2k$ termes $s_0, s_1, \ldots, s_{2k-1}$ de cette suite.

Exemple 1.6.11. *Dans [20], nous avons l'exemple suivant qui nous montre le fonctionnement l'algorithme de Berlekamp-Massey. Ici, il consiste à trouver une suite récurrente linéaire avec un petit ordre dans* $\mathbb{F}_2$ *dont les* 8 *premiers termes sont* 1, 1, 0, 0, 1, 0, 1, 1.

La fonction génératrice $G_7(x)$ *de la suite est donnée par les premiers termes de la suite et*

$$G_7(x) = 1 + x + x^4 + x^6 + x^7 \in \mathbb{F}_2[x].$$

Nous utilisons l'algorithme de Berlekamp-Massey décrit ci-dessus pour déterminer la suite. Le calcul est résumé par le tableau suivant :

j	$g_j(x)$	$h_j(x)$	m_j	b_j
0	1	x	0	1
1	$1+x$	x	0	0
2	$1+x$	x^2	1	1
3	$1+x+x^2$	$x+x^2$	-1	1
4	1	x^2+x^3	0	1
5	$1+x^2+x^3$	x	0	0
6	$1+x^2+x^3$	x^2	1	0
7	$1+x^2+x^3$	x^3	2	0
8	$1+x^2+x^3$		3	

Alors $r = \lfloor 4 + \frac{1}{2} - \frac{1}{2}m_8 \rfloor = 3$, *et le polynôme trouvé est* $m(x) = x^3 + x + 1$. *Par conséquent les termes de l'état initial de la suite récurrent linéoire* $s_0, s_1, \ldots$ *satisfont à la relation de récurrence* $s_{n+3} = s_{n+1} + s_n$ *for* $n = 0, 1, \ldots$

Pour contourner l'algorithme de Berlekamp-Massey et pour éviter les attaques à clair en cryptographie, et continuer à utiliser les bonnes propriétés des suites récurrentes linéaires, plusieurs suites non linéaires basées sur ces dernières ont vu le jour. Parmi lesquelles les suites multiplexées.

1.7 Suites Multiplexées

Définition 1.7.1. *[20, 21]Une suite multiplexée* $u_0,\ u_1,\ u_2,\ \ldots$ *dans* $\mathbb{F}_p$ *est construite comme suit :*

(i) *Soient* $s_0,\ s_1,\ s_2,\ \ldots$ *d'ordre* k *et* $t_0,\ t_1,\ t_2,\ \ldots$ *d'ordre* m *deux suites de périodes maximales dans* $\mathbb{F}_p$.

(ii) *Soit h un entier compris $1 \leq h \leq k$ tel que $p^h \leq m$ si $h < k$ et $p^h - 1 \leq m$ si $h = k$.*

(iii) *Soient les entiers $j_1, j_2, ..., j_h$ avec $0 \leq j_1 < j_2 < .... < j_h \leq k-1$. Pour $n = 0, 1, ...$ considérons le h-uplets $(s_{n+j_1}, s_{n+j_2}, ..., s_{n+j_h})$ éléments de $\mathbb{F}_p$ et interprétons le comme la réprésentation digitale en base p de l'entier $b_n \in I_h$ où*

$$I_h = \{0, 1, ..., p^h - 1\} \text{ si } h < k,$$

$$I_h = \{1, 2, ..., p^h - 1\} \text{ si } h = k.$$

(iv) *Soit φ une fonction injective définie de I_h dans $\{0, 1, ..., m-1\}$.*

(v) *Avec les choix de $h, j_1, j_2, ..., j_h$ et φ nous établissons*

$$U_n = t_{n+\varphi(b_n)}$$

Exemple 1.7.2. *Soit $p = 2$, et soient s_0, s_1, s_2, ... et t_0, t_1, t_2, ... deux suites de périodes maximales de $\mathbb{F}_2$ avec*

$$s_{n+3} = s_{n+1} + s_n \quad pour \quad n = 0, 1, \ldots$$

$$t_{n+4} = t_{n+3} + t_n \quad pour \quad n = 0, 1, \ldots$$

et (1, 0, 0) et (1, 0, 0, 0), leur états initiaux respectifs. La première suite a pour période 7 et les termes dans la période sont

1 0 0 1 0 1 1.

La seconde suite a pour période 15 et les termes dans la période sont

1 0 0 0 1 1 1 1 0 1 0 1 1 0 0.

Maintenant, nous choisissons $h = 2$, $j_1 = 0$, $j_2 = 1$, *et une fonction injective* φ *définie de* $\{0, 1, 2, 3\}$ *sur lui même par*

$$\varphi(0) = 1,\ \varphi(1) = 2,\ \varphi(2) = 3,\ \varphi(3) = 0$$

La suite d'entiers $b_0, b_1, \ldots$ *dans la Definition 1.7.1 (iii) a pour période 7 et les termes dans la période sont*

$$2\ 0\ 1\ 2\ 1\ 3\ 3$$

Par conséquent, les premiers termes de la suite multiplexée $u_0,\ u_1,\ u_2, \cdots$ *sont*

$$0\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0 \cdots$$

Théorème 1.7.3. *[20] La suite multiplexée* $u_0, u_1, \ldots$ *est périodique et sa période divise* $\text{ppcm}(p^k - 1, p^m - 1)$.

Démonstration. Soit $r = \text{ppcm}(p^k - 1, p^m - 1)$.

Puisque r est un multiple de $p^k - 1$ période de la suite $s_0,\ s_1,\ s_2,\ \ldots$, nous avons

$$(s_{n+j_1},\ \ldots,\ s_{n+j_h}) = (s_{n+r+j_1},\ \ldots,\ s_{n+r+j_h})$$

et de plus $b_{n+r} = b_n$ pour tout $n \geq 0$.

Puisque r est un multiple de $p^m - 1$ période de la suite $t_0,\ t_1,\ t_2,\ \ldots$, nous avons

$$u_{n+r} = t_{n+r+\varphi(b_{n+r})} = t_{n+r+\varphi(b_n)} = t_{n+\varphi(b_n)} = u_n \quad \textit{pour} \quad \textit{tout} \quad n \geq 0$$

Le reste vient des Lemme 1.3.22 et Lemme 1.3.23. □

Proposition 1.7.4. *[20] Si* ν *désigne la suite multiplexée* $u_0, u_1, \ldots$ *et* ξ *désigne la suite* $t_0, t_1, \ldots$ *dans la Definition 1.7.1(i), alors*

$$\nu_d^{(i)} = \xi_d^{j(i)} \qquad i = 0, 1, \ldots$$

où $d = p^k - 1$ *et* $j(i) = i + \varphi(b_i)$.

Démonstration. Les termes de $\nu_d^{(i)}$ sont les éléments u_{nd+i}, $n = 0,\ 1,\ 2,\ \ldots$.

Puisque $d = p^k - 1$ est la période de la suite $s_0,\ s_1,\ s_2,\ \ldots$, nous avons $b_{nd+i} = b_i$ par la construction. Donc

$$u_{nd+i} = t_{nd+i+\varphi(b_{nd+i})} = t_{nd+i+\varphi(b_i)} \qquad n \geq 0.$$

d'où le résultat. □

Proposition 1.7.5. *[20] Pour tous les entiers $a \geq 2$, $k \geq 1$, et $m \geq 1$ nous avons*

$$pgcd(a^k - 1, a^m - 1) = a^{pgcd(k,m)} - 1.$$

Démonstration. Si $b = pgcd(k, m)$, alors il est clair que $a^b - 1$ divise

$c = pgcd(a^k - 1, a^m - 1)$.

Posons $k = dm + e$ avec les entiers $d \geq 0$ et $0 \leq e < m$ alors

$$a^k - 1 = (a^{dm} - 1)a^e + (a^e - 1),$$

de plus c divise $a^e - 1$.

En continuant ce processus par analogie avec l'algorithme d'Euclide pour k et m, nous trouvons que c divise $a^e - 1$. Donc $c = a^b - 1$. □

Théorème 1.7.6. *Si $pgcd(k, m) = 1$, alors la période de la suite multiplexée $u_0, u_1, \ldots$ est un multiple de $\frac{p^m-1}{p-1}$.*

Démonstration. se référer à [20], pages :351 – 352. □

1.7.1 Polynôme Minimal

Soient u une suite multiplexée, s et t des suites de périodes maximales, d'ordres respectifs k et m, et de polyômes caractéristiques respectifs $f(x)$ et $g(x)$ constituant u.

Soient $\mathbb{F}_{2^k}$ et $\mathbb{F}_{2^m}$, les corps scindés de $f(x)$ et $g(x)$. Alors les factorisations de $f(x)$ et $g(x)$ dans leurs corps scindés respectifs sont :

$$f(x) = \prod_{i=0}^{k-1}(x + \alpha^{2^i}) \quad et \quad g(x) = \prod_{j=0}^{m-1}(x + \beta^{2^j}).$$

où α et β sont des éléments primitifs dans leur corps respectifs.

Pour donner le polynôme minimal d'une suite multiplexée, nous avons besoin de l'oprérateur § défini par :

$$(f\S g)(x) \;=\; \prod_{i=0}^{k-1}\prod_{j=0}^{m-1}(x + \alpha^{2^i}\beta^{2^j})$$

et du polynôme suivant :

Définition 1.7.7. *Pour $1 \leq \delta \leq k$, on définie le polynôme de degré $\sum_{i=1}^{\delta}\binom{k}{i}$ sur $\mathbb{F}_2$ par*

$$F_\delta(x) = \prod_{1\leq i\leq 2^m-1, 1\leq w(i)\leq \delta}(x + \alpha^i).$$

où $w(i)$ est le poids de i.

Définition 1.7.8. ***Poids de Hamming.*** *Soit n un entier non-négatif. On appelle poids de Hamming de n, le nombre de 1 dans l'expression binaire de n et on le note $w(n)$.*

Exemple 1.7.9.

1. *Pour $n = 13$, l'écriture binaire de n est 1 1 0 1. Donc le poids $w(n)$ de n est égal au nombre de 1, c'est-à-dire $w(n) = 3$.*
2. *Pour $n = 20$, l'écriture binaire de n est 1 0 1 0 0. Donc le poids $w(n)$ de n est égal au nombre de 1, c'est-à-dire $w(n) = 2$.*

Remarque 1.7.10. *Dans [21], il est dit que le polynôme minimal d'une suite multiplexée est très proche de $f(x)$ polynôme minimal de la suite s.*

Finalement le polynôme minimal d'une suite multiplexée est donné par le thérème suivant :

Théorème 1.7.11. *[21] Soit $H(x)$ le polynôme minimal d'une suite multiplexée u constituée par les suites de périodes maximales s et t dont les polynômes minimaux respectifs sont $f(x)$ et $g(x)$ de degrés k et m.*

(i) *Si $h = 1$, alors $H(x) = ((f\S g) \cdot g)(x)$ de degré $m \cdot (1 + k)$.*

(ii) *Si $2 \leq h < k$ et les h boîtes s_0, s_{τ_1}, $\ldots$ $s_{\tau_{h-1}}$ sont équidistantes, alors*

$$H(x) = ((F_h \S g).g)(x) \text{ de degré } m \cdot \sum_{i=0}^{h} \binom{k}{i}.$$

(iii) *Si $h = k$, alors $H(x) = (F_k \S g)(x)$ de degré $m \cdot (2^k - 1)$.*

Chapitre 2

Classification des Suites Multiplexées

Dans ce chapitre, nous allons donner une classification des suites multiplexées. La classification de ces dernières est faite dans le but de les regrouper par classe à partir du choix de h de la définition 1.7.1.

De ce fait, nous procédons en expliquant d'abord comment la classification va se faire. Dans la définittion 1.7.1 d'une suite multiplexée, nous avons vu, une fois les deux suites de périodes $2^k - 1$ et $2^m - 1$ avec k et m leur ordres respectifs données, le reste de la définition est déterminé par le choix de h. Et nous définissons la classification comme suit : pour chaque couple (m, k), nous associons un et un seul h tel que $1 \leq h \leq k$, vérifiant l'une seule de ces conditions

$$\begin{cases} p^h \leq m & \text{si h} < \text{k}; \\ p^h - 1 \leq m & \text{si h} = \text{k}. \end{cases}$$

2.1 Principe de la classification

La classification des suites multiplexées s'est faite en considérant les couples (m, k) (où k et m sont les ordres des suites constituant une suite multiplexée) et à chaque

couple (m,k) on associe l'entier h. Ainsi on obtient une fonction non injective

$$\begin{aligned} \lambda_h : \mathbb{N}^* \times \mathbb{N}^* &\to \{1,2,\ldots,k\} \\ (m,k) &\mapsto h. \end{aligned}$$

qui permet de calculer le h correspondant à chaque couple (m,k).

De ce fait, on appelle classe d'une suite multiplexée constituée par deux suites récurrentes linéaires de périodes maximales d'ordres respectifs m et k, l'ensemble des couples (m,k) ayant le même h. En guise de définition, nous avons

Définition 2.1.1. *Soient u une suite multiplexée constituée par les suites s et t d'ordres respectifs k et m, de périodes maximales respectives 2^k-1 et 2^m-1, et h, $1 \leq h \leq k$ un entier tel que*

$$\begin{cases} 2^h \leq m & si\ h < k; \\ 2^h - 1 \leq m & si\ h = k. \end{cases}$$

On appelle classe de u l'ensemble des couples (m,k) ayant le même h et on le note $C^{(h)}$.

Exemple 2.1.2. *Soit*

$$\begin{aligned} \lambda_h : \{1,2,3,\ldots,15,16\} \times \{1,2,3,\ldots,15,16\} &\longrightarrow \{1,2,3,\ldots,15,16\} \\ (m,k) &\longmapsto \lambda_h(m,k) = h. \end{aligned}$$

Ce qui donne le tableau suivant :

m/k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
5	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
6	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
7	1	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2
8	1	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
9	1	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
10	1	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
11	1	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
12	1	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
13	1	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
14	1	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
15	1	2	3	4	3	3	3	3	3	3	3	3	3	3	3	3
16	1	2	3	4	4	4	4	4	4	4	4	4	4	4	4	4

2.2 Détermination des classes

Dans l'exemple 2.1.2, nous considérons que k et m variant de 1 à 16, et à chaque couple (m, k), il est associé l'entier h, $1 \leq h \leq 16$.

Remarque 2.2.1. *La classe $C^{(0)}$ n'existe pas car h ne prend pas la valeur 0 d'après la définition 1.7.1. Alors l'ensemble $\{(m,k),\ m = 1 \quad et \quad 2 \leq k \leq 16\}$ dont le $h = 0$ est exclu du fait du choix de h.*

Avant de commencer l'énumération des classes, nous allons d'abord définir les notions de **sous-ensembles intermédiaires** et de **sous-ensembles extrêmes**.

Tout sous-ensemble de la classe $C^{(h)}$ compris entre le premier et le dernier est appelé **sous-ensemble intermédiaire**.

Le premier et le dernier sous-ensembles de la classe $C^{(h)}$ sont appelés **sous-ensembles extrêmes**. Et dans la classification ils correspondent aux sous-ensembles respectifs

$$\{(m,k),\ k=h \quad et \quad m \geq 2^h - 1\}$$

et

$$\{(m,k), k \geq h+1 \quad et \quad m = 2^{h+1} - 1\} \setminus \{(2^{h+1} - 1, h+1)\}$$

Curieux comme ensembles, d'où viennent ils ? La réponse c'est qu'ils vont apparaître lors de la construction de nos classes.

Remarque 2.2.2. *Le nombre de sous-ensembles intermédiares disjoints dépend de la valeur de h. Plus la valeur de h est grande plus le nombre de sous-ensembles intermédiaires est important.*

Pour construire une classe $C^{(h)}$, nous nous référons au tableau précédent dans l'exemple 2.1.2.

Pour $h = 1$, nous obtenons la classe $C^{(1)}$ et cette dernière est constituée par les sous-ensembles suivants :

$$\begin{aligned}
&\{(m,k), k = 1 \quad et \quad m \geq 1\},\\
&\{(m,k),\ k \geq 2 \quad et \quad m = 2\},\\
&\{(m,k), k \geq 2 \quad et \quad m = 3\} \setminus \{(3,2)\}
\end{aligned}$$

Donc nous avons

$$C^{(1)} = \{(m,k), k = 1 \quad et \quad m \geq 1\} \bigcup \{(m,k), 2 \leq m \leq 3 \quad et \quad k \geq 2\} \setminus \{(3,2)\}$$

Cette classe possède $f_1 = 2^1 - 1 = 1$ sous-ensemble intermédiaire et a $\Delta_1 = 2^1 + 1 = 3$ sous-ensembles disjoints au total.

Notre seconde classe $C^{(2)}$ est constituée par

$$\begin{aligned}
&\{(m,k), k = 2 \quad et \quad m \geq 3\},\\
&\{(m,k), k \geq 3 \quad et \quad m = 4\},\\
&\{(m,k), k \geq 3 \quad et \quad m = 5\},\\
&\{(m,k), k \geq 3 \quad et \quad m = 6\},\\
&\{(m,k), k \geq 3 \quad et \quad m = 7\} \setminus \{(7,3)\}
\end{aligned}$$

Donc nous avons

$$C^{(2)} = \{(m,k), k = 2 \quad et \quad m \geq 3\} \bigcup \{(m,k), 4 \leq m \leq 7 \quad et \quad k \geq 3\} \setminus \{(7,3)\}.$$

La classe $C^{(2)}$ possède $f_2 = 2^2 - 1 = 3$ sous-ensembles intermédiaires disjoints et $\Delta_2 = 2^2 + 1 = 5$ sous-ensembles disjoints au total.

Ensuite la classe $C^{(3)}$ possède

$$\begin{aligned}
&\{(m,k), k=3 \quad et \quad m \geq 7\},\\
&\{(m,k), k \geq 4 \quad et \quad m=8\},\\
&\{(m,k), k \geq 4 \quad et \quad m=9\},\\
&\{(m,k), k \geq 4 \quad et \quad m=10\},\\
&\{(m,k), k \geq 4 \quad et \quad m=11\},\\
&\{(m,k), k \geq 4 \quad et \quad m=12\},\\
&\{(m,k), k \geq 4 \quad et \quad m=13\},\\
&\{(m,k), k \geq 4 \quad et \quad m=14\},\\
&\{(m,k), k \geq 4 \quad et \quad m=15\} \setminus \{(15,4)\}
\end{aligned}$$

ou bien

$$C^{(3)} = \{(m,k), k=3 \quad et \quad m \geq 7\} \bigcup \{(m,k), 8 \leq m \leq 15 \quad et \quad k \geq 4\} \setminus \{(15,4)\}$$

qui possède $f_3 = 2^3 - 1 = 7$ sous-ensembles intermédiaires disjoints et $\Delta_3 = 2^3 + 1 = 9$ sous-ensembles disjoints au total.

Et enfin nous en arrivons à la classe $C^{(h)}$. Cette dernière possède les sous-ensembles disjoints suivants

$$\begin{aligned}
&\{(m,k), k=h \quad et \quad m \geq 2^h - 1\},\\
&\{(m,k), k \geq h+1 \quad et \quad m=2^h\},\\
&\{(m,k), k \geq h+1 \quad et \quad m=2^h+1\},\\
&\qquad \ldots \qquad \ldots \qquad \ldots\\
&\{(m,k), k \geq h+1 \quad et \quad m=2^{h+1}-2\},\\
&\{(m,k), k \geq h+1 \quad et \quad m=2^{h+1}-1\} \setminus \{(2^{h+1}-1, h+1)\}
\end{aligned}$$

ou bien

$$C^{(h)} = \{(m,k), k=h \, et \, m \geq 2^h - 1\} \bigcup \{(m,k), 2^h \leq m \leq 2^{h+1} - 1 \, et \, k \geq h+1\} \setminus \{(2^{h+1}-1, h+1)\}.$$

qui possède $f_h = 2^h - 1$ sous-ensembles intermédiaires disjoints et $\Delta_h = 2^h + 1$ sous-ensembles disjoints au total.

Nous allons maintenant donner la définition d'une classe $C^{(h)}$ de la manière suivante :

Définition 2.2.3. *Soit $u_0, u_1, \ldots$ une suite multiplexée constituée de deux suites récurrentes linéaires de périodes maximales $2^k - 1$ et $2^m - 1$ respectives, d'ordres respectifs k et m.*

La classe d'une suite multiplexée u qui est l'ensemble des couples (m, k) associé à l'entier $h > 0$(ayant le même h) est notée

$$C^{(h)} = \{(m,k), k = h \text{ et } m \geq 2^h - 1\} \bigcup \{(m,k), 2^h \leq m \leq 2^{h+1} - 1 \text{ et } k \geq h+1\} \backslash \{(2^{h+1}-1, h+1)\}$$

ayant $\Delta_h = 2^h + 1$ sous-ensembles disjoints et $f_h = 2^h - 1$ sous-ensembles intermédiaires disjoints.

Lemme 2.2.4. *Soit u une suite multiplexée de classe $C^{(h)}$ dans $\mathbb{F}_2$. Alors les propriétés suivantes sont équivalentes :*

1) $\Delta_h = 2^h + 1$

2) $\Delta_h = \Delta_{h-1} + 2^{h-1}$ pour $h \geq 2$

Démonstration. 1) $\Longrightarrow$ 2)
Supposons que $\Delta_h = 2^h + 1$ et montrons que $\Delta_h = \Delta_{h-1} + 2^{h-1}$:
Nous aons

$$\begin{aligned} \Delta_h &= 2^h + 1 - 2^{h-1} + 2^{h-1} \\ &= 2 \times 2^{h-1} + 1 - 2^{h-1} + 2^{h-1} \\ &= 2^{h-1} + 1 + 2^{h-1} \end{aligned}$$

donc

$$\Delta_h = \Delta_{h-1} + 2^{h-1}$$

2). $\Longrightarrow$ 1).
Supposons que $\Delta_h = \Delta_{h-1} + 2^{h-1}$ et montrons que $\Delta_h = 2^h + 1$:
Nous avons $\Delta_h - \Delta_{h-1} = 2^{h-1}$ d'après 2). Pour $h = 1$, $\Delta_1 = 3$,

$$\begin{aligned} \Delta_2 - \Delta_1 &= 2^1 \\ \Delta_3 - \Delta_2 &= 2^2 \\ \ldots \quad \ldots &= \quad \ldots \\ \Delta_{h-1} - \Delta_{h-2} &= 2^{h-2} \\ \Delta_h - \Delta_{h-1} &= 2^{h-1}. \end{aligned}$$

Après sommation de toutes les lignes, nous obtenons :

$$\begin{aligned}\Delta_h &= \Delta_1 - 2^1 + 2^h \\ &= 3 - 2^1 + 2^h \\ &= 2^h + 1.\end{aligned}$$

D'où le résultat.

□

Lemme 2.2.5. *Soit u une suite multiplexée de classe $C^{(h)}$ dans $\mathbb{F}_2$. Alors les propriétés suivantes sont équivalentes :*

1) $f_h = 2^h - 1$

2) $f_h = f_{h-1} + 2^{h-1}$ *pour* $h \geq 2$

Démonstration. 1) $\Longrightarrow$ 2)

$$\begin{aligned}f_h &= 2^h - 1 - 2^{h-1} + 2^{h-1} \\ &= 2^{h-1} - 1 + 2^{h-1} \\ &= f_{h-1} + 2^{h-1}.\end{aligned}$$

D'où le résultat.
2) $\Longrightarrow$ 1)
$f_1 = 1$ et d'après 2), nous avons :

$$\begin{aligned}f_2 - f_1 &= 2^1 \\ f_3 - f_2 &= 2^2 \\ \ldots \quad \ldots &= \quad \ldots \\ f_{h-1} - f_{h-2} &= 2^{h-2} \\ f_h - f_{h-1} &= 2^{h-1}.\end{aligned}$$

Après sommation, on obtient :

$$\begin{aligned}f_h &= f_1 - 2 + 2^h \\ &= 1 - 2 + 2^h \\ &= 2^h - 1.\end{aligned}$$

D'où le résultat.

□

Corollaire 2.2.6. *Soit u une suite multiplexée de classe $C^{(h)}$ dans $\mathbb{F}_2$. Alors*

$$f_h(u) = \Delta_h(u) - 2$$

Démonstration. Se referer aux Lemme 2.2.4 et Lemme 2.2.5. □

Théorème 2.2.7. *Soit $u_0, u_1, \ldots$ une suite multiplexée dans $\mathbb{F}_2$.Alors, il existe un entier $h > 0$ tel que $C^{(h)}$ soit la classe de u et $C^{(h)}$ a $\Delta_h = 2^h + 1$ sous-ensembles au total et $f_h = 2^h - 1$ sous-ensembles intermédiaires.*

Démonstration. Soit u une suite multiplexée dans $\mathbb{F}_2$.
D'après la définition 1.7.1 :

(i) ils existent deux suites récurrentes linéaires u and v, d'ordres respectifs k_0 et m_0,de périodes maximales respectives $2^{k_0} - 1$ et $2^{m_0} - 1$.

(ii) il existe un entier h, $1 \leq h \leq k_0$, vérifiant

$$\begin{cases} 2^h \leq m_0 & \text{si h} < k_0\,; \\ 2^h - 1 \leq m_0 & \text{si h} = k_0. \end{cases}$$

Soit λ_h la fonction définie de $\mathbb{N}^* \times \mathbb{N}^*$ sur $\{1, \ldots, k\}$ par

$$\begin{aligned} \lambda_h : \mathbb{N}^* \times \mathbb{N}^* &\to \{1, 2, \ldots, k\} \\ (m, k) &\mapsto h. \end{aligned}$$

λ_h est surjective et non injective. L'ensemble des antécédants de h forme une classe notée $C^{(h)}$,

$$C^{(h)} = \{(m,k), k = h \text{ et } m \geq 2^h - 1\} \bigcup \{(m,k), 2^h \leq m \leq 2^{h+1} - 1 \text{ et } k \geq h+1\} \backslash \{(2^{h+1} - 1, h+1)\}$$

et résulte de la construction faite aux pages $54 - 57$.

Le nombre $f_h = 2^h - 1$ de sous-ensembles disjoints intermédiares et le nombre total $\Delta_h = 2^h + 1$ de sous-ensembles disjoints résultent des Lemme 2.2.4, Lemme 2.2.5. □

Remarque 2.2.8. *Soit $X = \mathbb{N}^* \times \mathbb{N}^*$ et définisons sur X une relation $\sim$ par*

$$(m, k) \sim (m', k') \iff \lambda_h(m, k) = \lambda_h(m', k') = h.$$

Il est facile de vérifier que cette relation est une relation d'équivalence. L'ensemble des classes d'équivalence est noté $C^{(h)}$ au lieu de $X/\sim$

2.2.1 Cardinal d'une classe

Dans cette partie nous nous proposons de calculer le cardinal de $C^{(h)}$.

Soient k et m les ordres des suites récurrentes linéaires constituant la suite multiplexée u de classe $C^{(h)}$.

Soit $\lambda = \max(k, m)$.

Nous avons les exemples suivants qui explicitent l'idée de calcul du cardinal d'une classe.

Pour ce faire, nous allons commencer par la classe $C^{(1)}$. Puisque $\lambda = \max(k, m)$, alors la classe $C^{(1)}$ devient :

$$C^{(1)} = \{(m,k), k = 1 \; et \; \lambda \geq m \geq 1\} \bigcup \{(m,k), 2 \leq m \leq 3 \; et \; \lambda \geq k \geq 2\} \setminus \{(3,2)\}$$

Comment se calcule le cardinal de $C^{(1)}$?

Puisque le cardinal de la classe $C^{(1)}$ est le nombre total d'éléments ou de couples appartenant $C^{(1)}$. Alors nous comptons le nombre de couples dans les ensembles $\{(m,k), k = 1 \; et \; \lambda \geq m \geq 1\}$ et $\{(m,k), 2 \leq m \leq 3 \; et \; \lambda \geq k \geq 2\} \setminus \{(3,2)\}$. Donc, le cardinal de $C^{(1)}$ est

$$|C^{(1)}| = \lambda + 2(\lambda - 1) - 1 = 3\lambda - 3 = \lambda(2^1 + 1) - [2^1(1 + 1) - 1].$$

En utilisant le même procédé pour la classe

$$C^{(2)} = \{(m,k), k = 2 \text{ et } \lambda \geq m \geq 3\} \bigcup \{(m,k), 4 \leq m \leq 7 \text{ et } \lambda \geq k \geq 3\} \setminus \{(7,3)\}$$

nous obtenons

$$|C^{(2)}| = (\lambda - 2) + 4(\lambda - 2) - 1 = 5\lambda - 11 = \lambda(2^2 + 1) - [2^2(2 + 1) - 1].$$

En continuant le raisonnement, pour la classe

$$C^{(h)} = \{(m,k), k = h \; et \; \lambda \geq m \geq 2^h - 1\} \cup \{(m,k), 2^h \leq m \leq 2^{h+1} - 1 \; et \; \lambda \geq k \geq h + 1\} \setminus \{(2^{h+1} - 1, h + 1)\})$$

nous obtenons finalement

$$|C^{(h)}| = (\lambda - 2^h + 2) + 2^h(\lambda - h) - 1 = \lambda(2^h + 1) - [2^h(h+1) - 1].$$

De ce fait, nous avons la remarque suivante :

Remarque 2.2.9. *Soit $C^{(h)}$ la classe d'une suite multiplexée u. Alors le cardinal de $C^{(h)}$ est*

1) $|C^{(h)}| = \infty$ *si* $\lambda = \infty$

2) $|C^{(h)}| = \lambda(2^h + 1) - [2^h(h+1) - 1] = \lambda\Delta_h - f_h - h2^h$ *si* $\lambda < \infty$.

Théorème 2.2.10. *Soient u une suite multiplexée de classe $C^{(h)}$ dans $\mathbb{F}_2$ constituée par deux suites récurrentes linéaires et $\lambda = max(m, k)$.*

Alors les propriétés suivantes sont équivalentes :

1) $|C^{(h)}| = \lambda(2^h + 1) - [2^h(h+1) - 1]$ *avec* $\lambda < \infty$

2) $|C^{(h)}| = |C^{(h-1)}| + 2^{h-1} \times [\lambda - (h+2)]$ *pour* $h \geq 2$ *et* $\lambda < \infty$

Démonstration. 1) $\Longrightarrow$ 2)

Supposons que

$$|C^{(h)}| = \lambda(2^h + 1) - [2^h(h+1) - 1]$$

et montrons que

$$|C^{(h)}| = |C^{(h-1)}| + 2^{h-1}[\lambda - (h+2)].$$

Nous avons
$|C^{(h)}| = \lambda(2^h + 1) - [2^h(h+1) - 1]$
Ce qu'on va faire c'est ajouter et retrancher $2^{h-1}[\lambda - (h+1)]$ et nous obtenons

$$\begin{aligned}
|C^{(h)}| &= \lambda(2^h + 1) - [2^h(h+1) - 1] + 2^{h-1}[\lambda - (h+1)] - 2^{h-1}[\lambda - (h+1)] \\
&= \lambda(2^h + 1) - 2^{h-1}[\lambda - (h+1)] - [2^h(h+1) - 1] + 2^{h-1}[\lambda - (h+1)] \\
&= \lambda(2^h + 1) - 2^{h-1}\lambda + 2^{h-1}(h+1)] - [2^h(h+1) - 1] + 2^{h-1}[\lambda - (h+1)] \\
&= \lambda(2^h - 2^{h-1} + 1) + 2^{h-1}(h+1) - [2 \cdot 2^{h-1}(h+1) - 1] + 2^{h-1}[\lambda - (h+1)] \\
&= \lambda(2^h - 2^{h-1} + 1) + 2^{h-1}(h + 1 - 2 \cdot (h+1) + \lambda - (h+1)) + 1 \\
&= \lambda(2^{h-1} + 1) + 2^{h-1}(-2 \cdot (h+1) + \lambda) + 1 \\
&= \lambda(2^{h-1} + 1) + 2^{h-1}(-h) + 1 + 2^{h-1} \cdot (-(h+2) + \lambda) \\
&= \lambda(2^{h-1} + 1) - [2^{h-1}h - 1] + 2^{h-1}(\lambda - (h+2))
\end{aligned}$$

or

$$|C^{(h-1)}| = \lambda(2^{h-1}+1) - [2^{h-1}h - 1]$$

D'où le résultat.

2) $\Longrightarrow$ 1)

Supposons que

$$|C^{(h)}| = |C^{(h-1)}| + 2^{h-1}[\lambda - (h+2)] \text{ pour } h \geq 2$$

et montrons que

$$|C^{(h)}| = \lambda(2^h+1) - [2^h(h+1) - 1].$$

Nous avons

$$|C^{(1)}| = 3\lambda - 3.$$

$$\begin{aligned}
|C^{(2)}| - |C^{(1)}| &= 2^1[\lambda - (2+2)] \\
|C^{(3)}| - |C^{(2)}| &= 2^2[\lambda - (3+2)] \\
\cdots \quad \cdots &= \quad \cdots \\
|C^{(h-1)}| - |C^{(h-2)}| &= 2^{h-2}[\lambda - ((h-1)+2)] \\
|C^{(h)}| - |C^{(h-1)}| &= 2^{h-1}[\lambda - (h+2)]
\end{aligned}$$

En sommant toutes les lignes, nous obtenons

$$|C^{(h)}| - |C^{(1)}| = \lambda \sum_{k=1}^{h-1} 2^k - 2 \times \sum_{k=1}^{h-1} 2^k - \sum_{k=1}^{h-1} (k+1)2^k$$

Pour déterminer la valeur de chaque somme, nous procédons comme suit :
la somme $\sum_{k=1}^{h-1} 2^k = -2 + 2^h$ et pour calculer la somme $\sum_{k=1}^{h-1}(k+1)2^k$, nous avons :
Soit $S_k = \sum_{k=1}^{h-1}(k+1)2^k$ *et* $f(x) = \sum_{k=2}^{h-1}(k+1)x^k$ une fonction définie sur $\mathbb{R}$, alors $f(x)$ admet une primitive

$$\begin{aligned} F(x) &= \sum_{k=1}^{h-1} x^{k+1} \\ &= x^2 \sum_{k=1}^{h-1} x^{k-1} \\ &= x^2 \frac{x^{h-1}-1}{x-1} \\ &= \frac{x^{h+1}-x^2}{x-1}. \end{aligned}$$

Donc,

$$\begin{aligned} f(x) = F'(x) &= \frac{[(h+1)x^h - 2x](x-1) - (x^{h+1}-x^2)}{(x-1)^2} \\ &= \frac{(h+1)x^{h+1} - 2x^2 - (h+1)x^h + 2x - x^{h+1} + x^2}{(x-1)^2} \\ &= \frac{(h+1-1)x^{h+1} - x^2 - (h+1)x^h + 2x}{(x-1)^2} \\ &= \frac{x^h(xh-h-1) - x^2 + 2x}{(x-1)^2} \end{aligned}$$

Alors

$$\begin{aligned} S_k = f(2) &= \frac{2^h(2h-h-1) - 2^2 + 2*2}{(2-1)^2} \\ &= 2^h(h-1). \end{aligned}$$

En remplaçant chaque somme par sa valeur, on obtient :

$$|C^{(h)}| - |C^{(1)}| = \lambda \sum_{k=1}^{h-1} 2^k - 2 * \sum_{k=1}^{h-1} 2^k - \sum_{k=1}^{h-1} (k+1)2^k$$

Donc

$$\begin{aligned} |C^{(h)}| &= |C^{(1)}| + \lambda(-2+2^h) - 2(-2+2^h) - 2^h(h-1) \\ |C^{(h)}| &= \lambda(2^h+1) - [2^h(h+1)-1]. \end{aligned}$$

D'où le résultat.

□

Exemple 2.2.11. *1. Soient $\lambda = 3$ et $h = 1$, alors*

$$\begin{aligned} C^{(1)} &= \{(m,k), k = 1 \text{ et } 1 \leq m \leq 3\} \bigcup \{(m,k), 2 \leq m \leq 3 \text{ et } 2 \leq k \leq 3\} \setminus \{(3,2)\} \\ &= \{(1,1),(2,1),(3,1)\} \bigcup \{(2,2),(2,3),(3,2),(3,3)\} \setminus \{(3,2)\} \\ &= \{(1,1),(2,1),(3,1),(2,2),(2,3),(3,3)\}. \end{aligned}$$

Donc le cardinal de $C^{(1)}$ est $|C^{(1)}| = 6$

2. Soient $\lambda = 4$ et $h = 2$, alors

$$\begin{aligned} C^{(2)} &= \{(m,k), k = 2 \text{ et } 3 \leq m \leq 4\} \bigcup \{(m,k), 4 \leq m \leq 7 \text{ et } 3 \leq k \leq 4\} \setminus \{(7,3)\} \\ &= \{(3,2),(4,2)\} \bigcup \{(4,3),(4,4),(5,3),(5,4),(6,3),(6,4),(7,3),(7,4)\} \setminus \{(3,2)\} \\ &= \{(3,2),(4,2),(4,3),(4,4),(5,3),(5,4),(6,3),(6,4),(7,4)\}. \end{aligned}$$

Donc le cardinal de $C^{(2)}$ est $|C^{(2)}| = 9$

Proposition 2.2.12. *Soient $s = (s_0, s_1, \ldots)$ une suite récurrente linéaire d'ordre k dans $\mathbb{F}_2$, de période maximale et b_n sa représenation binaire. Alors s et b_n ont même période.*

Démonstration. se référer à [20] □

Proposition 2.2.13. *Si u est une suite multiplexée de classe $C^{(h)}$, constituée de suites de périodes maximales s et t, et b_n la représentation binaire de s est connue. Alors la suite $s_0, s_1, \ldots$ peut être déterminé par l'algorithme de Berlekamp-Massey.*

Démonstration. Puisque $C^{(h)}$ est la classe de u, alors h est connu.
Du Lemme 2.2.4 nous avons b_n est périodique, de période $2^k - 1$. D'où l'on connait la valeur de k.

Puisque b_n est connue, ce que nous allons faire c'est la confondre avec sa représentation binaire $(s_{n+j_1}, s_{n+j_2}, \cdots, s_{n+j_h})$ où $0 < j_1 < j_2 < \cdots < j_h \leq k-1$ et $1 \leq h \leq k$.

De plus $j_{i+1} = j_i + 1$ pour $i = 1, \cdots, h$, donc

$$(s_{n+j_1}, s_{n+j_2}, \cdots, s_{n+j_h}) = (s_{n+j_1}, s_{n+j_1+1}, \cdots, s_{n+j_{1+(h-1)}}).$$

Ce qui permet de bien visualiser les termes consécutifs de la suite s.

Finalement, nous pouvons identifier les $2k$ termes de la suite récurrente linéaire s, donc on peut utiliser l'algorithme de Berlekamp-Massey pour déterminer le polyôme minimal de s et enfin la relation de récurrence. □

Remarque 2.2.14. *b_n est un élément de I_h dans la définition d'une suite multiplexée.*

2.2.2 Détermination de φ

Avant tout φ c'est quoi ?

φ est la fonction injective donnée à la Definition 1.7.1 de la manière suivante

$$\varphi : I_h \to \{0,\ 1,\ \ldots,\ m-1\}$$

avec

$$I_h = \{0, 1, ..., p^h - 1\} \quad si \quad h < k,$$
$$I_h = \{1, 2, ..., p^h - 1\} \quad si \quad h = k.$$

Remarque 2.2.15. *Nous ne pouvons pas donner l'expression exacte de φ, mais nous donnons juste son expression générale.*

Soient $A_m = \{0, 1, 2, \ldots, m-1\}$ et I_h définis ci-dessus. Alors la fonction φ est définie de I_h dans A_m. I_h et A_m sont des parties de $\mathbb{N}$ l'ensemble des entiers positifs.

Donc, φ est une fonction injective linéaire ou affine. D'où la formule générale

$$\varphi(x) = (ax + b)(\mod m), \forall x \in I_h, a \neq 0, b \in A_m.$$

En fait, connaissant les images de deux éléments de I_h, on pourra déterminer la valeur exacte de φ.

Remarque 2.2.16. *Soit r la période de b_n et φ une fonction injective définie de I_h dans A_m. Alors*

$$\varphi(x) = (ax + b)(\mod m), \forall x \in I_h, a \neq 0, b \in A_m$$

et

$$(\sum_{i=0}^{r-1} \varphi(b_{n+i}))(\mod m) = (a \sum_{i=0}^{r-1} b_{n+i} + rb)(\mod m)$$

Chapitre 3

Rapprochement entre la Classification et le Polynôme minimal d'une Suite Multiplexée

Dans ce chapitre, nous avons fait un rapprochement entre la classification faite dans le chapitre précédent et le polynôme minimal d'une suite multiplexée plus précisément avec le degré du polynôme minimal d'une suite multiplexée.

De plus, nous allons montrer comment calculer les complexités des suites récurrentes linéaires de périodes maximales constituant une suite multiplexée.

Nous allons commencer par présenter quelques algorithmes issus des résultats du chapitre précédent.

3.1 Algorithmes

Dans cette partie, nous présentons une méthode pour calculer la valeur de h et une autre méthode pour déterminer les classes des suites multiplexées via des algorithmes.

L'algoritthme suivant permet de calculer la valeur de h.

Algorithme 1.

Entrée *: k, m*

Sortie *: h*

1. *$i \longleftarrow 0$*
2. *Si $(2^k - 1) \leq m$ alors*
3. *$h \longleftarrow k$*
4. *Sinon*
5. *Tant que $(2^{k-i}) > m$ faire*
6. *$h \longleftarrow k - i$;*
7. *$i \longleftarrow i + 1$;*
8. *Fin Tant que*
9. *Fin Si*
10. *Retourner (h)*

Exemple 3.1.1. *Soit $(m, k) = (5, 3)$. Déterminons la valeur de h pour le couple $(5, 3)$ en utilisant l'algorithme.*

L'algorithme fonctionne comme suit :

Si $h = k = 3$, alors $2^3 - 1 = 7 > 5$ donc $h \neq k = 3$.

Donc nous passons à la condition suivante

Si 2^{k-1} est inférieur à $m = 5$.

On a $2^2 = 4 < 5$, donc $h = 2$ et l'algorithme s'arrête.

Avec cet algorithme, nous classifions les $N \times N$ premiers couples (m, k) associés à h.

Algorithme 2.

Entrée *: N (N est un entier)*

Sortie *: R (R est un tableau $N \times N$)*

1. *Pour $i \longleftarrow 1..N$ faire*
2. *Pour $j \longleftarrow 1..N$ faire*
3. *$R[i][j] \longleftarrow$ Algorithme 1(i, j) ;*
4. *afficher(i, j, R[i][j]) ;*
5. *Fin Pour*
6. *Fin Pour*

Tous ces algorithmes sont implémentés sous maple.

Exemple 3.1.2. *L'algorithme prend N en entrée et calcule la valeur de h de chaque couples (m, k). Les i et j dans l'Algorithme 2 représentent k et m respectivement. Nous avons pour $N = 4$ le tableau suivant afin d'avoir une bonne visibilité de l'algorithme.*

m/k	*1*	*2*	*3*	*4*
1	*1*	*0*	*0*	*0*
2	*1*	*1*	*1*	*1*
3	*1*	*2*	*1*	*1*
4	*1*	*2*	*2*	*2*

où $1 \leq h \leq N$, alors les couples pour lesquels $h = 0$ sont exclus de la classification, il s'agit de l'ensemble $\{(1, 2), (1, 3), (1, 4)\}$. La classification débute alors avec $h = 1$

qui lui correspond à l'ensemble $\{(1,1),(2,1),(2,2),(2,3),(2,4),(3,1),(3,3),(3,4),(4,1)\}$.

Et avec cet algorithme, pour $h=2$, *nous avons le début de la classe* $C^{(2)}$:

$\{(3,2),(4,2),(4,3),(4,4),\ldots\}$.

Ainsi nous obtenons les résultats suivants à l'aide de la classification (voir [17]) et des polynômes minimaux (voir [21]) .

3.2 Degré du polynôme minimal d'une suite multiplexée

Le théorème suivant nous permet de mettre en évidence le degré du polynôme minimal d'une suite multiplexée à l'aide des complexités des suites la constituant comme suit :

Théorème 3.2.1. *Soit* u *une suite multiplexée de classe* $C^{(h)}$ *avec* $1 \leq h \leq k$ *dans* $\mathbb{F}_2$ *et* $H(x)$ *son polynôme minimal. Alors*

1) si $h=1$ *et* $k>1$, *alors*

$$\deg(H(x)) = 2(1+k) \quad ou \quad \deg(H(x)) = 3(1+k).$$

2) si $2 \leq h \leq k-1$, *alors*

$$2^h \sum_{i=0}^{h} \binom{k}{i} \leq \deg(H(x)) \leq (2^{h+1}-1) \sum_{i=0}^{h} \binom{k}{i}.$$

3) si $h=k$, *alors*

$\deg(H(x)) > (f_k)^2$ *avec* $f_k = 2^k - 1$ *(le nombre total de sous-ensembles internédiaires de la classe* $C^{(k)}$) .

Démonstration. 1) Soit u une suite multiplexée de classe $C^{(1)}$ *et* $k > 1$, alors il existe deux suites de périodes maximales v et w d'ordres respectifs $k \geq 2$ et $2 \leq m \leq 3$ tels que

$$u_t = w_{t+\varphi(b_t)} \quad pour \quad tout \quad t = 0, 1, \ldots$$

avec $b_t = (v_t, v_{t+1}, \ldots, v_{t+h})$ pour tout $t \geq 0$.

Puisque m est un entier, alors $m = 2 \quad or \quad m = 3. \quad (*)$

De plus $h = 1$, alors de [21] il résulte

$$\deg(H(x)) = m(1+k). \quad (**)$$

Donc, d'après $(*)$ et $(**)$ nous obtenons :

$$\deg(H(x)) = 2(1+k) \quad ou \quad \deg(H(x)) = 3(1+k).$$

2) Soit $C^{(h)}$ la classe de u dans $\mathbb{F}_2$ avec $1 < h < k$, alors $2^h \leq m \leq 2^{h+1} - 1$ (voir [17]).

D'où nous avons les résultats suivants :

$$\deg(H(x)) = m. \sum_{i=0}^{h} \binom{k}{i}$$

(d'après [21]).

En multipliant $2^h \leq m \leq 2^{h+1} - 1 \quad par \quad \sum_{i=0}^{h} \binom{k}{i}$,

nous obtenons

$$2^h \sum_{i=0}^{h} \binom{k}{i} \leq \deg(H(x)) \leq (2^{h+1}-1) \sum_{i=0}^{h} \binom{k}{i}.$$

3) Soit $C^{(k)}$ une classe de u, alors $m \geq 2^k - 1$.

En outre, la multiplication de $m \geq 2^k - 1$ par $2^k - 1$ donne $m(2^k - 1) \geq (2^k - 1)^2$.

De plus,

$$\deg(H(x)) = m(2^k - 1) \quad où \quad 2^k - 1 = f_h = f_k \quad car \quad h = k.$$

(lequel est le nombre total de sous-ensembles disjoints intermédiaires de la classe $C^{(k)}$), ceci implique que $(2^k - 1)^2 = (f_k)^2$.

Donc $\deg(H(x)) \geq (f_k)^2$.

□

3.3 Quelques cas particuliers

Avec le corrolaire suivant, nous obtenons les valeurs des polynômes minimaux $f(x)$ et $g(x)$ des suites constituant une suite multiplexée de classe $C^{(1)}$.

Corollaire 3.3.1. *Soit u une suite multiplexée de classe $C^{(1)}$. Soient k et m les ordres respectifs des suites de périodes maximales, de polynômes minimaux $f(x)$ et $g(x)$ constituant la suite multiplexée u. Alors,*

1) si $k = 1$, alors $f(x) \in \{x,\ x+1\}$.

De plus

$$\deg(H(x)) = 2m$$

2) si $k > 1$, alors

$$g(x) \in \{x^2 + x + 1,\ x^3 + x + 1,\ x^3 + x^2 + 1\}$$

Démonstration. Soit u une suite multiplexée de classe $C^{(1)}$, alors il existe un couple $(m, k) \in C^{(1)}$ ordres respectifs des suites v et w constituant u.

Soient $f(x)$ *et* $g(x)$ les polynômes minimaux de v et w.

Puisque v et w sont des suites de périodes maximales, alors $f(x)$ *et* $g(x)$ sont des polynômes primitifs de degrés k et m (irréductibles dans $\mathbb{F}_2[x]$).

De plus,

1) si k le degré $f(x)$ est égal à 1, alors d'après [20], nous avons les résultats suivants

   $f(x) = x$ *ou* $f(x) = x + 1$.

   Donc,

   $$\textit{puisque}\quad k = 1,\ \textit{alors}\ deg(H(x)) = m(k+1) = m(1+1) = 2m$$

2) si $k > 1$, alors m le degré de $g(x)$ est égal à 2 ou 3.

   a) si $m = 2$, alors il résulte de [20] que $g(x) = x^2 + x + 1$.

   b) si $m = 3$, alors il résulte de [20] $g(x) = x^3 + x + 1$ *ou* $x^3 + x^2 + 1$.

   D'où

   $$g(x) \in \{x^2 + x + 1,\ x^3 + x + 1,\ x^3 + x^2 + 1\}.$$

□

Remarque 3.3.2. *Soit s une suite de période maximale, d'ordre k dans $\mathbb{F}_2$, alors le h-uplet $(s_{n+j_1}, s_{n+j_2}, \ldots, s_{n+j_h})$ pour $n = 0, 1, \ldots$ est la représentation en base 2 (binaire) de la suite $b_n \in I_h \subset \mathbb{F}_{2^h}$; et $j_1, j_2, \ldots, j_h$ sont des entiers tels que $0 \leq j_1 < j_2 < \cdots < j_h \leq k - 1$.*

Puisque s est une suite récurrente linéaire, alors elle satisfait à la relation de récurrence

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n$$

Maintenant, démontrons que la suite b_n est une suite récurrente linéaire.

Pour cela, nous identifions b_n avec sa représentation binaire $(s_{n+j_1}, s_{n+j_2}, \ldots, s_{n+j_h})$.

Ainsi, nous avons $b_n = (s_{n+j_1}, s_{n+j_2}, \ldots, s_{n+j_h})$ pour tout $n = 0, 1, \ldots$

où $j_2 = j_1 + 1, j_3 = j_2 + 1 = j_1 + 2, \ldots, j_h = j_1 + h - 1$.

Posons $j_1 = 0$, alors $j_2 = 1, \ldots, j_h = h - 1$ et $b_n = (s_n, s_{n+1}, \ldots, s_{n+h-1})$

Alors,

$$\begin{aligned} b_0 &= (s_0, s_1, \ldots, s_{h-1}), \\ b_1 &= (s_1, s_2, \ldots, s_h), \\ &\vdots \\ b_{k-1} &= (s_{k-1}, s_k, \ldots, s_{k+h-2}), \\ b_k &= (s_k, s_{k+1}, \ldots, s_{k+h-1}), \end{aligned}$$

Puisque

$$b_k = (s_k, s_{k+1}, \ldots, s_{k+h-1}),$$

Alors en remplaçant chacun de ces termes par leur valeur, on obtient :

$b_k = (a_{k-1}s_{k-1} + a_{k-2}s_{k-2} + \cdots + a_0 s_0,\ a_{k-1}s_k + a_{k-2}s_{k-1} + \cdots +$

$a_0 s_1,\ \ldots, a_{k-1}s_{k+h-2} + a_{k-2}s_{k+h-3} + \cdots + a_0 s_{h-1}),$

$= (a_{k-1}s_{k-1}, a_{k-1}s_k, \ldots, a_{k-1}s_{k+h-2}) + (a_{k-2}s_{k-2}, a_{k-1}s_{k-3}, \ldots, a_{k-2}s_{k+h-3}) +$

$\cdots + (a_0 s_0, a_0 s_1 \ldots, a_0 s_{h-1})$,

$= a_{k-1}(s_{k-1}, s_k, \ldots, s_{k+h-2}) + a_{k-2}(s_{k-2}, s_{k-3}, \ldots, s_{k+h-3}) + \cdots + a_0(s_0, s_1, \ldots, s_{h-1})$,

$b_k = a_{k-1}b_{k-1} + a_{k-2}b_{k-2} + \cdots + a_0 b_0$,

$b_{k+1} = a_{k-1}b_k + a_{k-1}b_{k-2} + \cdots + a_0 b_1$,

$b_{k+2} = a_{k-1}b_{k+1} + a_{k-2}b_k + \cdots + a_0 b_2$,

$\forall n \geq 0,\ b_{n+k} = a_{k-1}b_{n+k-1} + a_{k-2}b_{n+k-2} + \cdots + a_0 b_n$.

La suite $(b_n)_{n\geq 0} \in I_h \subseteq \mathbb{F}_{2^h}$ *où* $\mathbb{F}_{2^h}$ *est un corps d'extension de* $\mathbb{F}_2$, *et tous les* $a_{k-1}, a_{k-2}, \ldots, a_0 \in \mathbb{F}_{2^h}$. *La suite* $(b_n)_{n\geq 0}$ *est une suite récurrence linéaire et son polynôme est*

$$f_{b_n}(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0 \in \mathbb{F}_{2^h}[x].$$

3.4 Détermination des complexités m et k

Pour déterminer les complexités des suites de périodes maximales constituant une suite multiplexée, nous avons le théorème suivant :

Théorème 3.4.1. *Soit* u *une suite multiplexée de classe* $C^{(h)}$ *et* $H(x)$ *son polynôme minimal. Alors*

i) il existe $(b_n) \in \mathbb{F}_{2^h}$, *une suite récurrente linéaire d'ordre* k *satisfaisant à la relation*

$$u_n = w_{n+\varphi(b_n)} \text{ pour } n = 0, 1, \ldots$$

ii) soit h *un entier tel que* $2 \leq h \leq k-1$ *et* $\text{pgcd}(m, k) = d$. *Alors*

a) si $d = k$, *alors il existe un unique entier* α *tel que*

$$\frac{2^h}{k} \leq \alpha \leq \frac{2^{h+1}-1}{k} \quad et \quad m = k\alpha.$$

b) si $d = m$, alors il existe un unique entier β tel que

$$\frac{k}{2^{h+1}-1} \leq \beta \leq \frac{k}{2^h} \quad et \quad k = m\beta.$$

iii) Soit h un entier tel que $2 \leq h \leq k-1$, alors

$$2^h \sum_{i=0}^{h} \binom{k}{i} \leq \deg(H(x)) \leq (2^{h+1}-1) \sum_{i=0}^{h} \binom{k}{i}.$$

Démonstration. i) Soit u une suite multiplexée de classe $C^{(h)}$, alors il existe v et w, deux suites de période maximales d'ordres respectifs k et m constituant u tel que $u_n = w_{n+\varphi(b_n)}$ où $b_n = (v_n, v_{n+1}, \ldots, v_{n+h-1})$

ii) pour $2 \leq h \leq k-1$ et $d > 1$,

a) si $d = k$, alors m est un multiple de k. Alors il existe un entier positif α tel que $m = k\alpha$. Comme $2^h \leq m \leq 2^{h+1} - 1$, alors nous obtenons $2^h \leq k\alpha \leq 2^{h+1} - 1$.

Puisque $k > 0$ est un entier positif, alors $\frac{2^h}{k} \leq \alpha \leq \frac{2^{h+1}-1}{k}$.

Pour montrer que α est unique, nous allons raisonner par l'absurde ; en supposant qu'il exite deux entiers α_1 et α_2 tel que $\alpha_1 \neq \alpha_2$ vérifiant les conditions suivantes :

$$\frac{2^h}{k} \leq \alpha_1 \leq \frac{2^{h+1}-1}{k} \; et \; m = k\alpha_1$$

et

$$\frac{2^h}{k} \leq \alpha_2 \leq \frac{2^{h+1}-1}{k} \; et \; m = k\alpha_2$$

Alors, nous avons $m = k\alpha_1 = k\alpha_2 \Rightarrow k\alpha_1 - k\alpha_2 = k(\alpha_1 - \alpha_2) = 0$. Puique $k > 0$, alors $\alpha_1 - \alpha_2 = 0$ c'est-à-dire $\alpha_1 = \alpha_2$. Ce qui est absurde. Donc α est unique.

b) si $d = m$, alors k est un multiple de m. Alors il existe un entier positif β tel que $k = m\beta$. Comme, $2^h \leq m \leq 2^h - 1$, alors $\frac{k}{2^{h+1}-1} \leq \beta \leq \frac{k}{2^h}$. Pour montrer que β est unique, nous allons raisonner par l'absurde ; en supposant qu'il existe deux entiers β_1 et β_2 tel que $\beta_1 \neq \beta_2$ vérifiant les conditions suivantes :

$$\frac{k}{2^{h+1}-1} \leq \beta_1 \leq \frac{k}{2^h} \; et \; m = k\beta_1$$

et

$$\frac{k}{2^{h+1}-1} \leq \beta_2 \leq \frac{k}{2^h} \; et \; m = k\beta_2$$

Alors, $m = k\beta_1 = k\beta_2 \Rightarrow k\beta_1 - k\beta_2 = k(\beta_1 - \beta_2) = 0$.

Puique $k > 0$, alors $\beta_1 - \beta_2 = 0$ c'est-à-dire $\beta_1 = \beta_2$. Ce qui est absurde. Donc β est unique.

iii) Voir Théorème 3.2.1 pour la preuve.

□

Remarque 3.4.2. *L'exemple suivant montre qu'il est possible de trouver les valeurs de* $\text{pgcd}(m,k) \neq k$ *et* $\text{pgcd}(m,k) \neq m$. *Soit* $d = \text{pgcd}(m,k)$.

a) si $1 < d < m$ *et* $1 < d < k$, *il existe des cas pour lesquels il est possible de calculer la valeur de* m *quand* k *et* h *sont connus.*

Par exemple pour $k = 100$ *et* $h = 2$, *alors* $4 \leq m \leq 7$. *Trouvons la bonne valeur de* m.

Pour cela, nous avons le tableau suivant

h	k	*diviseurs de* k	m	*diviseurs de* m	$d = \text{pgcd}(m,k) \neq 1$, m *et* k
2	100	$2, 4, 5, 10, 20, 25, 50, 100$	4	$2, 4$	–
			5	5	–
			6	$2, 3, 6$	2
			7	7	–

Puisque $d = pgcd(m,k) \neq 1, k$ *et* m *alors les valeurs* $m = 4$ *ou* 5 *ou* 7 *sont exclus car* $pgcd(7,100) = 1$, $pgcd(4,100) = 4$ *et* $pgcd(5,100) = 5$.

Alors il ne reste que la valeur $d = (100,6) = 2$ *qui est différente de tout élément de l'ensemble* $\{1, 6, 100\}$. *Donc en conclusion la valeur cherchée est* $m = 6$.

D'après la remarque 3.3.2, nous avons :

Soit u *une suite multiplexée de classe* $C^{(h)}$ *constituée par deux suites récurrentes linéaires* v *et* w, *de périodes maximales respectives* $2^k - 1$ *et* $2^m - 1$. *Alors il existe une suite récurrente linéaire* $(b_n) \in \mathbb{F}_{2^h}$ *de période maximale* $2^k - 1$ *et d'ordre* k *telle que*

$$u_n = w_{n+\varphi(b_n)} \text{ pour } n = 0, 1, \ldots$$

où φ *est une fonction définie de* I_h *dans* $\{0, 1, \ldots, m\}$ *avec*

$$\begin{cases} I_h = \{0, 1, \ldots, 2^h - 1\}, & si\ h < k, \\ I_h = \{1, \ldots, 2^h - 1\}, & si\ h = k. \end{cases}$$

et b_n *est la représentation binaire de* v.

De plus, si h *est un entier avec* $2 \leq h \leq k-1$ *et* $H(x)$ *le polynôme minimal de* u, *alors*

$$2^h \sum_{i=0}^{h} \binom{k}{i} \leq \deg(H(x)) \leq (2^{h+1}-1) \sum_{i=0}^{h} \binom{k}{i}.$$

On a remarqué que la difficulté pour trouver la valeur exacte de m s'accroît avec celle de h.

En résumé, dans les cas où

$$pgcd(m,k) = k \quad ou \quad pgcd(m,k) = m,$$

nous avons pu calculer les complexités k et m des suites récurrentes linéaires de périodes maximales constituant une suite multiplexée (où k et m sont les degrés respectifs des polynômes minimaux).

Conclusion et perspectives

Les suites multiplexées nées pour remédier à l'insécurité des suites récurrentes linéaires, ne sont pas elles aussi à l'abri de nouvelles attaques. Nous avons pu dans cette thèse élaborer des méthodes qui nous ont permi de borner, minorer les complexités des suites de longueurs maximales constituant une suite multiplexée afin de déterminer leur valeurs k et m suivant que $pgcd(m,k) = m$ ou $pgcd(m,k) = k$.

Cependant, les suites multiplexées restent très complexes, et de plus elles ont permi de surmonter l'attaque en clair basée sur la linéarité des suites récurrentes linéaires. En plus de cela, elles possèdent de très grandes périodes de l'ordre de $(2^k-1)(2^m-1)$ si $pgcd(m,k) = 1$.

Par ailleurs, avec cette classification nous avons vu que, plus h est grand plus le nombre d'éléments de $C^{(h)}$ s'accroient, trouver les valeurs de m et de k s'avére difficile. D'où l'intérêt de calculer la complexité d'une suite multiplexée afin de faire un bon choix des m-séquences qui vont constituées notre suite multiplexée que l'on va choisir comme générateur aléatoire (générateur de clés) dans notre chiffrement par flot.

De plus, par analogie avec l'Algorithme de Berlekamp-Massey, mettre en place un algorithme pour déterminer le polynôme minimal des suites de ce genre reste un atout majeur. En résumé, il serait intéressant de voir ce qu'il en est lorsque

$$pgcd(m,k) \neq k \quad et \quad pgcd(m,k) \neq m,$$

et montrer comment déterminer les polynômes minimaux des suites récurrentes linéaires de périodes maximales constituant une suite multiplexée afin de la reconstituer.

Bibliographie

[1] Alin Bostan, - Algoithmes rapides des polynômes, Séries formelles et matrices, Vol.1, n°2, 2010, pp.75-262.

[2] C. Ding, Tor Helleseth, H. Niederreiter. - Sequences and their applications, SETA'98 Proceedings, Discrete Mathématics and Theorical Computer Science, Springer, 1999.

[3] Guang Gong, - Sequence Analysis, Lecture Notes for Co739x, University of Waterloo, 1999.

[4] Guang Gong, Amr M. Youssef. - Cryptographic Properties of the Wilch-Gong Transformation Sequences Gerators, IEEE Transformations on Information Theory, Vol.48, N°11, 2002.

[5] G. H. Hardy, E. M. Wright, - An Introduction to the Theory of Numbers, Clarendon Press, Oxford, 1960.

[6] Jean Bertel, Maurice Mignotte. - Deux propriétés décidables des suites récurrentes linéaires, Bull. Soc. Math. France, Vol. 104, 1976, pp.175-184.

[7] Jean Paul Bezivin, - Factorisation des suites récurrentes linéaires et applications, Bull. Soc. Mth. France, Vol.112, 1984,pp.365-376.

[8] James L. massey, Shirlee Serconek. - A Fourier transform approach to the linear complexity of nonlinear filtered sequences, Springer-Verlag, 1998.

[9] Jovan Dj. Golic, - Towards Fast Correlation Attacks on Irregularty Clocked Shift Registers, Springer-Verlag, 1998.

[10] Keqin Feng, Peter Jan-Shyong Shine, Qing Yiang. - On Aperiodic and Periodic Complementary Binary Sequences, IEEE Transformation on Information theory, 1998.

[11] K. B. Magleby. - The synthesis of nonlinear feedback shift registers, Technical Report, n°6207-1, 1963.

[12] L. Cerlieno, M. Mignotte, F. Piras - Suites récurrentes linéaires, Propriétés algébriques et arithmétiques, L'Enseign. Math, tome 33, 1987, pp. 67-108.

[13] Marcin Skubiszewski. - Binary Periodic Synchronizing Sequences, Theoretical Computer Science, part A, vol.99, 1992.

[14] M. Mignotte. - Suites Recurrentes Lineaires, Séminaire Delange-Pisot-Poitou :Théorie des Nombres 15(2) (1973-1974), G14-1-G14-9.

[15] MiuLan Liu, Zhe-xian Wan. - Generalized Multiplexed Sequences, Springer-Verlag, 1998.

[16] O. Diankha. - Suites Recurrentes Lineaires sur les corps finis : Théorie et Applications, Afrika Matematica, serie 3, Vol. 18, 2007, pp.46-60.

[17] O. Diankha, C. B. Deme. - Linear recurrent sequence over finite field and their applications in cryptogrphy, JP Journal of Algebra, Number Theory and Application,Vol.22, Number 2, 2011, pp 205-221.

[18] O. Diankha and C. B. Deme, - Connection between classification and the minimal polynomial of the multiplexed sequence, Accepté en publication par le Far East Journal of Mathematical Sciences (FJMS).

[19] R. F. Babindamana. - Liens entre codes de Gabidulin et les codes de Reed Solomon Généralisés, Thèse, Université Cheikh Anta Diop Dakar-Senegal, 2010, pp.18-20.

[20] R. Lidl and H. Niederreiter, - Introductionto Finite Fields and their Applications, Addison-Wesley, Cambridge University Press, 1994.

[21] S. M. Jennings. - Multiplexed Sequences : Some properties of the minimal polynomial, Springer-Verlag, 1998.

[22] S. W. COLOMB. - Shift Register Sequences, AEGEAN Park Press, 1982.

[23] Seung Anh Park, - The period and the linear complexity of certain linear recurring sequences in the finite field $\mathbb{F}_q$, Bull Korean Math.Soc 29, n°1,1992, p.89-99.

[24] Serdar Boztas. - Lower Bounds on the Maximum Periodic and Aperiodic Correlation of Signal Sets with Arbitrary Energy Distribution, National Conference publication, 1994.

[25] Tor Helleseth, P. V. Kumar. - Pseudonoise sequences, Chapter 8 : The Mobile Communications Handbook, Jerry D. Gibson, ed., CRC Press, 1996.

[26] Tor Helleseth, P. V. Kumar. - Sequences with low correlation, Handbook of Coding Theory, V. Pless and G. Huffimann, eds., Kluwer Acad. Publ., 1998.