# Conception Vectorielle de Registre à rétroaction avec retenue sur les corps finis.

Abdelaziz Marjane

**UNIVERSITÉ Paris 13 - Villetaneuse**

ÉCOLE DOCTORALE
**INSTITUT GALILÉE**

LABORATOIRE
**ANALYSE, GÉOMÉTRIE ET APPLICATION (LAGA), UMR 7539**

# T H È S E

pour obtenir le titre de

**Docteur**

de l'Université Paris 13
**Mention : Mathématique**

Présentée et soutenue publiquement par

Abdelaziz Marjane

# Conception Vectorielle de Registre à rétroaction avec retenue sur les corps finis.

soutenue le 08/07/2011

**Jury :**

| | | | |
|---|---|---|---|
| *Examinateurs :* | Pascal BOYER | - | Université Paris 13 |
| | Claude CARLET | - | Université Paris 8. |
| *Directeur de thèse :* | Farid MOKRANE | - | Université Paris 13 |
| *Rapporteurs :* | François RODIER | - | Université Aix-Marseille 2 |
| | Patrick SOLÉ | - | Telecom Paris-Tech |

# Remerciement

Je tiens à remercier en premier lieu mon directeur de thèse, le professeur Farid MOKRANE, pour m'avoir offert cette chance de faire de la recherche et pour m'avoir guidé durant ces trois années de thèse.

Je tiens aussi à remercier Daniel BARSKY et Maher ZERZERI pour m'avoir aidé et pour avoir relu et corrigé ma thèse.

Je n'oublie pas mon collègue Boufeldja ALLAILOU avec qui j'ai formé une équipe de recherche et avec qui j'ai pu avancer dans mes travaux et publier mes premiers résultats.

Je remercie également Mr le Professeur Patrick SOLÉ et Mr le Professeur François RODIER qui ont eu la patience de lire et de relire ma thèse en vue d'en faire un rapport. Je remercie le Professeur Claude CARLET et le Professeur Pascal BOYER pour avoir accepté de participer au jury de cette thèse.

J'adresse aussi mes remerciements aux doctorants de l'équipe du LAGA de Paris 13, à l'équipe MAATICAH de Paris 8, ainsi qu'à tous les membres du LAGA que j'ai pu côtoyer durant toutes ces années.

Enfin, je tiens à exprimer mon affection envers tous les membres ma famille pour leur soutien qui m'a été très précieux.

# Table des matières

# Table des figures

# Liste des tableaux

# Chapitre 1

# Introduction

## 1.1 Les séquences pseudo-aléatoires

Les séquences (définition 2.1.1) pseudo-aléatoires sont un outil très utilisé en communication et en cryptologie depuis 1948. La liste des domaines est longue : radar, banque, internet, téléphone, satellite, numérique, clé d'identification, commerce électronique, CDMA (Code Design Mutiple Access)... Plus particulièrement, l'avènement du net et du multimédia ont posé de nouveaux problèmes en termes de cryptographie. En effet, le multimédia réunit à la fois plusieurs services, comme l'audio et la vidéo.

La notion de pseudo-aléa désigne une suite de nombres qui s'approche d'un aléa statistiquement presque parfait, puisque par le procédé algorithmique utilisé pour générer cette séquence, on ne peut considérer une telle séquence comme aléatoire. Les chercheurs ont donc développé des outils afin de mesurer les propriétés dites aléatoires ou imprévisibles de telles séquences. L'étude des séquences pseudo-aléatoires se situe alors sur deux plans : le premier étant la conception du modèle générateur (définition 2.3.1) et le deuxième étant la mesure de la qualité de ces séquences (voir page 127).

La cryptographie a pour but de fournir des méthodes de communications sécurisées, fiables et efficaces. Elle est utile non seulement pour le chiffrement des messages, mais aussi pour l'authentification, l'identification... Au départ, les techniques de communication étaient analogiques, elles sont devenues par la suite numériques. Le numérique fait intervenir les techniques de chiffrement qui utilisent des séquences pseudo-aléatoires ou nombres pseudo-aléatoires. Les cryptographes ont du développer différents modèles algorithmiques de générateur d'aléa appelés PSG (Pseudo-random Sequence Generators) pour générer ces séquences pseudo-aléatoires dont le but est de servir de clé de chiffrement.

## 1.2 Les critères de pseudo-aléa

Pour la mesure de la qualité aléatoire des PSGs, on utilise plusieurs critères classiques [1] :

1. Une longue période : on cherche à générer des séquences périodiques avec une très grande période. Les paramètres des PSGs définissent en général une borne supérieure pour la période des séquences générées. Le but est de trouver des séquences atteignant cette limite. Par exemple pour les FSRs (présentés ci-dessous) construits sur un corps fini à $q$ éléments $\mathbb{F}_q$ de taille $r$, les séquences de sorties sont toutes périodiques de période inférieure ou égale à $q^r - 1$.
2. La Propriété d'équilibre (balanced property) : dans une période d'une séquence binaire périodique, le nombre de uns et le nombre de zéros doivent être égaux à une unité près.
3. La Propriété des répétitions (run property) : dans une période, les séries de la forme $(\mu, \lambda, \lambda, \ldots, \lambda, \delta)$, avec $\mu \neq \lambda$ et $\delta \neq \lambda$, doivent apparaître suivant une bonne répartition. Par exemple pour les séquences de période $q^r - 1$, les mots de taille $1 \leq k \leq r-2$ doivent apparaître $(q-1)q^{r-k-2}$ fois.
4. Une distribution idéale des $n$-uplets : dans une période, les $n$-uplets de la forme $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ doivent obéir à une distribution idéale. Par exemple, pour les séquences de période $q^r - 1$, les $n$-uplets non-nuls doivent apparaître $q^{r-n}$ fois pour $1 \leq n \leq r$ et les $n$-uplets nuls doivent apparaître $q^{r-n} - 1$ fois.
5. Une auto-corrélation de niveau 2 ou auto-corrélation idéale (définition 5.22.1).
6. Une faible inter-corrélation (définition 5.22.1).
7. Une grande complexité linéaire (linear span ou linear complexity) : on cherche à ce que la taille du plus petit registre générant la séquence donnée soit très grande afin de rendre difficile la reproduction du système.

La propriété d'équilibre, la propriété des répétitions et la propriété de l'auto-corrélation idéale forment les trois postulats pour un bon aléa proposés par Golomb [2].

**Exemple 1.2.1.**

$$(000100110101111000100110101111000100110101111\ldots)$$

*Cette séquence est de période* $15 = 2^4 - 1$. *Elle vérifie la propriété d'équilibre puisqu'il y a* 7 *zéros et* 8 *uns. Elle vérifie la propriété des répétitions puisqu'il y a deux séries de la forme* (0)*, deux séries de la forme* (1)*, une série de la forme* (00)*, une série de la forme* (11)*, une série de la forme* (000) *et une série de la forme* (1111)*. Enfin elle possède une distribution idéale des* 4*-uplets puisque chaque 4-uplet apparaît une seule fois.*

## 1.3 Modèles de Générateurs Pseudo-Aléatoires

Pour le problème de conception, il existe un modèle classique, *les FSRs (Feedback Shift Register) ou Registres à décalage et à rétroaction* (définition 2.5.2). Ce sont des registres à décalage avec une entrée et une sorties utilisant comme fonction de retour une fonction booléenne. La figure 1.1 représente le fonctionnement d'un Feedback Shift Register. La plupart des séquences pseudo-aléatoires vérifiant les postulats désirés peuvent être générées par ces FSRs. Ces registres sont simples et facilement programmables. Ils sont utilisés depuis 1950.

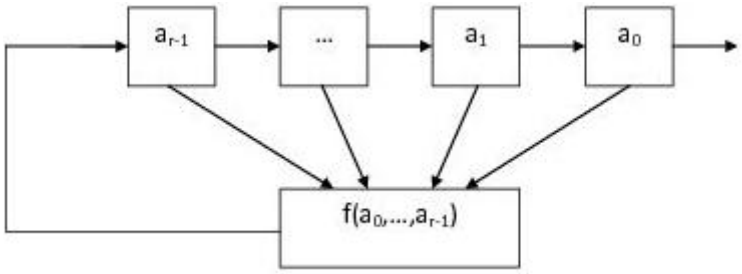



FIGURE 1.1 – Registre à décalage et à rétroaction ou FSR.

### 1.3.1 Registres à décalage et à rétroaction linéaire ou LFSR.

Le plus connu de tous les registres à décalage et à rétroaction est le *Linear Feedback Shift Register ou LFSR* (voir définition 5.2.1) dont les séquences de sorties sont appelées *séquences récurrentes linéaires*. Leur particularité étant que la fonction de retour est une fonction linéaire, ils jouissent donc d'une structure mathématique élégante. Les LFSRs sont étudiés depuis 1930 dans leur aspect purement théorique construits le plus souvent sur un corps fini. De 1948 à 1969, les LFSRs sont utilisés comme PSG dans les cryptosystèmes puisqu'ils peuvent générer des séquences binaires de période maximale, à savoir une période égale à $2^r - 1$ si le registre est de taille $r$. Ces séquences sont appelées les *m-séquences ou maximal length sequences* (voir définition 5.14.2). La recherche de séquence à très grande période devient un problème crucial dans les années 50. En plus d'avoir une période maximale, les $m$-séquences vérifient tous les postulats aléatoires qui leur confèrent une bonne qualité aléatoire.

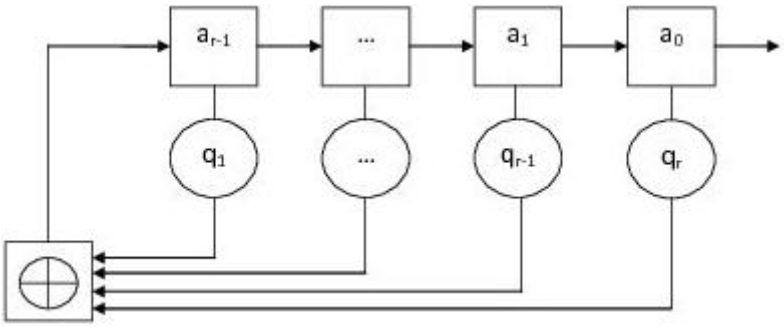



FIGURE 1.2 – Registre à décalage et à rétroaction linéaire ou LFSR.

### 1.3.2 Étude algébrique des LFSRs : les séries formelles.

L'essentiel des résultats théoriques sur les LFSRs séquences se trouvent dans [2]. Les objets algébriques permettant d'étudier les séquences récurrentes linéaires est l'anneau

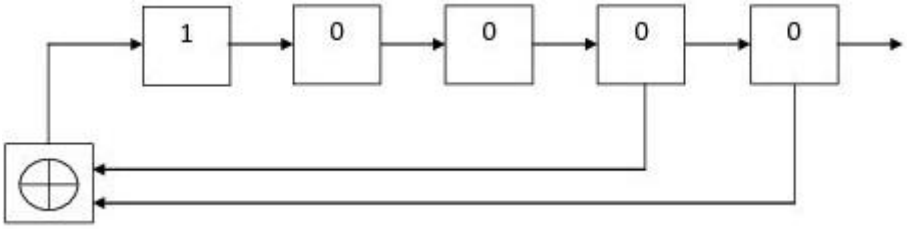



FIGURE 1.3 – Complexité linéaire égale à 5.

des séries formelles (voir définition 3.10.4). Très brièvement, l'étude théorique des LFSRs sur un corps fini $\mathbb{F}_{p^n}$ où $p$ est premier et $n \geq 1$ consistent à associer à la séquence de sorties $(a_0, a_1, a_2, \ldots)$ du registre la série formelle

$$a_0 + a_1 X + a_2 X^2 + \ldots \in \mathbb{F}_{p^n}[[X]].$$

La relation de récurrence linéaire transforme cette série formelle en fraction rationnelle dont le dénominateur est déterminé par la fonction de retour. Ce polynôme que l'on note $q(X)$ est appelé polynôme de connexion du LFSR. Toute séquence de sorties d'une LFSR est périodique et la période est inférieure ou égale à $p^{nr} - 1$. Inversement toute séquence périodique peut être générée par un LFSR. En particulier, si $q(X)$ est irréductible, alors la période de la séquence de sorties est l'ordre de $q(X)$ (l'ordre de $q(X)$ le plus petit entier $T$ tel que $q(X)$ divise $X^T - 1$). Si en plus de cela $q(X)$ est primitif, alors la période est maximale c'est-à-dire égale à $p^{nr} - 1$, ce sont les fameuses $m$-séquences. La recherche de polynôme primitifs irréductibles dans $\mathbb{F}_{p^n}$ permet donc la génération des $m$-séquences.

Pour l'étude inverse, à savoir étudier une séquence périodique et chercher les LFSRs qui la génèrent, on sait qu'il existe un polynôme minimal qui définit le LFSR de taille minimale générant une séquence donnée. La taille de cette LFSR est appelée *durée ou complexité linéaire* (*linear Span ou linear complexity*). Le problème étant de savoir comment trouver la complexité linéaire et comment générer des séquences à très grande complexité linéaire afin de contrer les techniques de cryptanalyse du système ? En 1969, Massey présente un algorithme pour trouver le polynôme minimal d'une séquence périodique appelé *Algorithme de Berlekamp-Massey* [3]. Une autre méthode *(théorème de Blahut)*, consistant à calculer le poids de Hamming de la transformée de Fourier discrète de la séquence en question, donne seulement la complexité linéaire sans fournir les paramètres du registre.

**Exemple 1.3.1.** *Considérons le LFSR de fonction de retour définie à partir de* $f(x_0, x_1, x_2, x_3, x_4) = x_0 + x_1$. *La complexité linéaire de la séquence de sorties* $(00001\ldots)$ *est* 5 *puisque on ne peut pas générer ce début de séquence avec une LFSR de taille strictement inférieur à* 5. *Voir la figure 1.3 .*

Les LFSRs possèdent plusieurs représentations. La représentation par la trace permet de démontrer plusieurs résultats classiques des LFSRs (voir définition 5.16.1). Le résultat

le plus important est le théorème de Gold sur *les gold-pair séquences*. La cross-corrélation entre une $m$-séquence et une $s$-décimation (définition 5.19.1) telle que $s$ soit de la forme $2^k + 1$ avec $k$ et $r$ premiers entre eux est à trois niveaux $(-1, -1 \pm 2^{\frac{n+1}{2}})$ [1].

Tous ces résultats font des LFSRs séquences un outil très utilisé dans les systèmes de chiffrement par flot, les CDMA et bien d'autres applications. À partir de 1969, l'algorithme de Berlekamp Massey signe la fin de vie des $m$-séquence en cryptographie. Il suffit de capter $2r$ bits consécutifs d'une $m$-séquences de période $2^r - 1$ pour reconstruire la séquence entièrement. Les LFSRs ne sont plus aptes à une utilisation cryptographique. Les scientifiques ont donc cherchés à construire de nouveaux PSGs, cette fois ci, non-linéaire, *les NLFSRs ou Non-Linear Feedback Shift Registers*. Cependant, il est très difficile de choisir des fonctions de retour non-linéaires pour générer des séquences vérifiant les postulats aléatoires décrits précédemment. Les NLFSRs s'avèrent être très résistants aux techniques algébriques d'analyse et les propriétés les plus simples comme la périodicité restent inconnues dans un cadre général. Les scientifiques se tournent alors vers d'autres méthodes toujours basées sur les LFSRs.

### 1.3.3 La communication CDMA (Code Division Multiple Access)

Le CDMA est une technique de communication récente utilisée dans les communications mobiles permettant d'optimiser la façon dont sont allouées les ressources radio entre plusieurs utilisateurs. Elle consiste à attribuer à chaque utilisateur de mobile un code au début de chaque communication qui est "orthogonal" aux codes des autres utilisateurs. Pour écouter un message reçu d'un utilisateur, il suffit alors de multiplier le signal par le code associé à cette utilisateur. Pour illustrer par un modèle simplifié, considérons un ensemble d'utilisateurs $\{1, 2, \ldots, N\}$ transmettant simultanément des informations dans un même canal. On suppose que la transmission se fait sans coordination ni synchronisation. En sortie du canal, le récepteur reçoit la somme des signaux émis par chacun des utilisateurs (on se place ici dans la situation idéale où la transmission n'est pas altérée par le bruit). Il s'agit alors de retrouver l'information transmise par chacun des utilisateurs. À l'utilisateur $j$, on attribue une suite $\underline{u}_j = (u_0^j, u_1^j, \ldots)$ de 1 et de $-1$ de période $2^n - 1$. Ces suites sont appelées suites "porteuses". Pour envoyer un bit $a_j$, l'utilisateur transmet la suite $(-1)^{a_j}\underline{u}_j$. Le signal reçu en sortie est la suite "somme" notée $\underline{s}$ et définie par

$$s_i = \sum_{j=0}^{j=N-1} (-1)^{a_j} u_{i+\tau_j}^j.$$

Le décalage $\tau_j$ représente le retard de transmission relatif à l'utilisateur $j$. Les retards de transmission sont inconnus du récepteur si on suppose qu'il n'y a aucune coordination dans la transmission des messages. Pour obtenir le bit $a_j$, il faut calculer l'inter-corrélation pour tout décalage entre $\underline{s}$ la suite "somme" des messages et $\underline{u}_j$ la suite attribuée à

l'utilisateur $j$. La formule de l'inter-corrélation donne :

$$\begin{aligned}
\mathcal{C}_{\underline{s},\underline{u}_j}(\tau) &= \sum_{i=0}^{i=2^n-2} s_i u^j_{i+\tau} \\
&= \sum_{i=0}^{i=2^n-2} \sum_{k=0}^{k=N-1} (-1)^{a_k} u^k_{i+\tau_k} u^j_{i+\tau} \\
&= \sum_{k=0}^{k=N-1} \sum_{i=0}^{i=2^n-2} (-1)^{a_k} u^k_{i+\tau_k} u^j_{i+\tau} \\
&= \sum_{i=0}^{i=2^n-2} (-1)^{a_j} u^j_{i+\tau_j} u^j_{i+\tau} + \sum_{k\neq j} \sum_{i=0}^{i=2^n-2} (-1)^{a_k} u^k_{i+\tau_k} u^j_{i+\tau} \\
&= (-1)^{a_j} \mathcal{C}_{\underline{u}_j,\underline{u}_j}(\tau-\tau_j) + \sum_{k\neq j} (-1)^{a_k} \mathcal{C}_{\underline{u}_k,\underline{u}_j}(\tau-\tau_k).
\end{aligned}$$

L'inter-corrélation entre $\underline{s}$ et $\underline{u}_j$ dépend alors de l'auto-corrélation de $\underline{u}_j$ et de l'inter-corrélation entre $\underline{u}_j$ et $\underline{u}_k$ pour tout $k \neq j$. L'idée consiste à trouver et à utiliser comme suites porteuses une famille de suites $\underline{u}_j$ "orthogonales" par rapport à l'inter-corrélation.

Les LFSRs sont utilisés dans les CDMAs pour la génération des suites porteuses qui doivent être des $m$-séquences, c'est-à-dire de période $2^n - 1$, ayant une inter-corrélation idéale. Les séquences de Gold ou les Gold-pair séquences sont particulièrement adaptées à cet effet. C'est une bonne illustration des applications des LFSRs dans la télécommunication. Cet exemple montre aussi l'importance de résoudre le problème de génération de familles de séquences pseudo-aléatoires de grande période et ayant une inter-corrélation idéale (faible).

### 1.3.4 Les PSGs non linéaires à base de LFSRs.

**Les Générateurs à combinaison non linéaire.**

En 1971, Groth développe *les Générateurs à combinaison non linéaire ou Combinatorial Function Generators ou encore CFG* qui consistent à opérer une fonction booléenne sur plusieurs LFSRs distincts et simultanés. Cette construction représentée par la figure 1.4 détruit la linéarité inhérente des LFSRs.

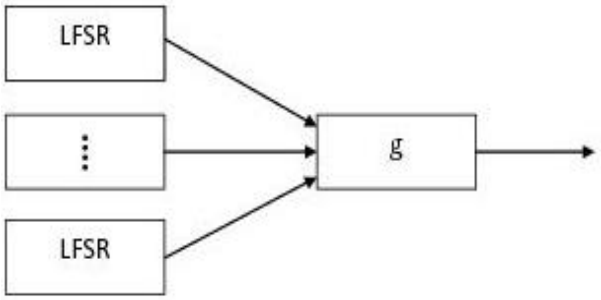



FIGURE 1.4 – Générateur à combinaison linéaire.

**Les Générateurs à base de LFSRs filtrés.**

En 1973, Key introduit *les LFSRs filtrés ou les Filter Function Generators ou encore les Feedforward Generator* qui consistent en un LFSR filtré par une fonction booléenne. À chaque étape du registre, la fonction de sorties $f$ prend comme entrée un certain nombre de bits de l'état du LFSR (voir figure 1.5). En 1984 d'autres types de PSG sont

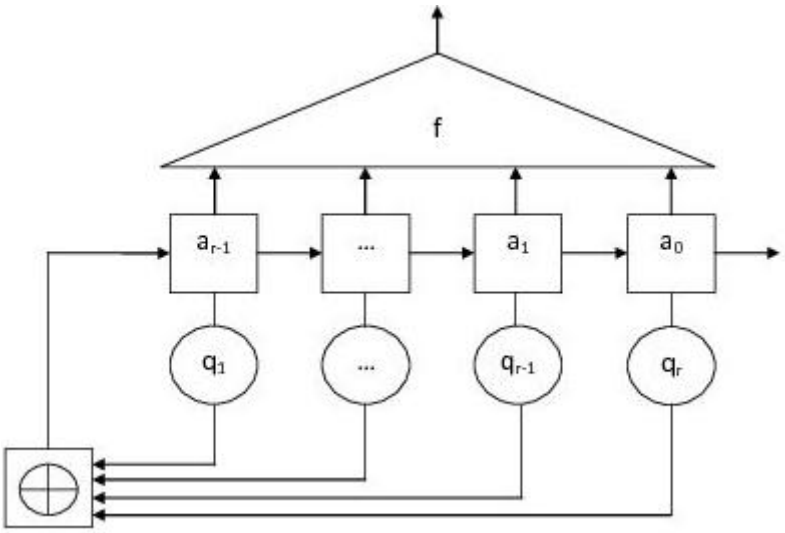



FIGURE 1.5 – Registre à décalage et à rétroaction linéaire filtré.

introduits dans l'étude des séquences pseudo-aléatoires comme les GMW séquences ou les générateurs contrôlés par une horloge (Clock controlled Generators).

**Les Générateurs par combinaison avec retenue**

Une autre manière de construire des générateurs de flot de chiffrement plus complexes est d'ajouter une retenue durant le processus de génération. Ces registres sont appelés *Générateur par combinaison avec mémoire*. Le générateur utilise plusieurs LFSRs simultanément et un registre de retenues dont la mémoire initiale est nulle. Pour chaque top d'horloge, les sorties des LFSRs sont additionnées. On applique à la somme obtenue notée $S$ la fonction (`mod2`) et la fonction (`div2`) qui sont respectivement le reste et le quotient de la division euclidienne de $S$ par 2. On retient en sortie le reste et en retenue le quotient. La figure 1.6 représente ce modèle de registre.

**Les Générateurs par rétrécissement**

Dans cette catégorie de générateur, on trouve deux variantes, *le générateur rétrécissant ou shrinking generator* et *le générateur auto-rétrécissant ou self-shrinking generator*.

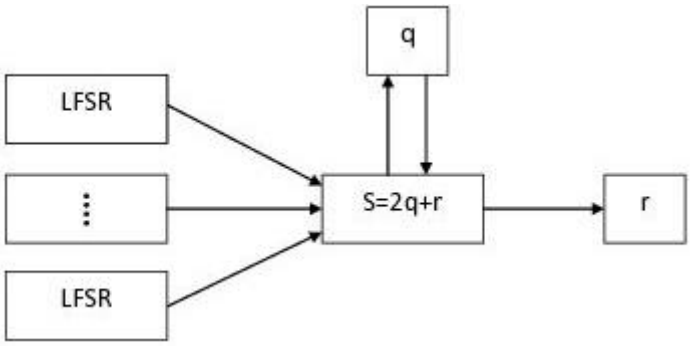



FIGURE 1.6 – Générateur par combinaison avec retenue.

**Le générateur rétrécissant** Dans [4][5], Don Coppersmith, Hugo Krawczyk et Yishay Mansour ont introduit le principe de ce nouveau PSG. Le principe représenté par la figure 1.7 consiste à prendre deux LFSRs $LFSR1$ et $LFSR2$, générant respectivement les $m$-séquences $(a_0, a_1, \ldots)$ et $(b_0, b_1, \ldots)$. La sortie du générateur est construite selon la règle suivante :

- si $b_i = 1$, le bit $a_i$ est envoyé en sortie et
- si $b_i = 0$, le bit $a_i$ est supprimé et aucun bit n'est envoyé en sortie.

Ainsi, même en connaissant une partie de la séquence de sorties, on ne peut trouver une correspondance entre les $a_i$ et les bits de sorties. Le gros désavantage de cette approche est une diminution du taux de génération qui devient par la même occasion irrégulier.

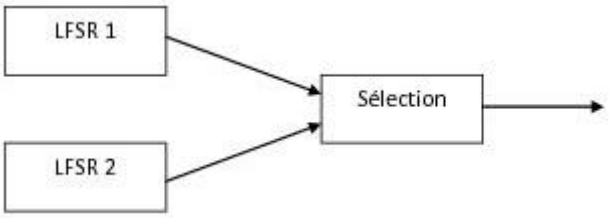



FIGURE 1.7 – Générateur rétrécissant.

**Le générateur auto-rétrécissant (self-shrinking)** Le générateur auto-rétrécissant est une version modifiée et plus simple du générateur rétrécissant. Ce modèle a été présenté par W. Meier et O. Staffelbach dans [5]. Le générateur auto-rétrécissant comme présenté sur la figure 1.8 exige un seul LFSR. Le LFSR génère une $m$-séquence $(a_0, a_1, \ldots)$. La règle de sélection est identique à celle du générateur rétrécissant, tout en prenant la séquence formée des bits d'index impair $(a_1, a_3, \ldots)$ comme première séquence et la séquence formée des bits d'index pair $(a_0, a_2, \ldots)$ comme seconde séquence. Explicitement, on retient en sortie le bit $a_{2i+1}$ si $a_{2i} = 1$, sinon on passe à l'étape suivante. En dépit de

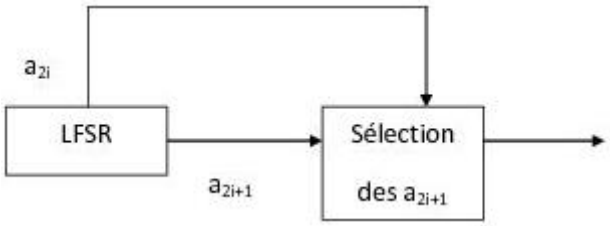



FIGURE 1.8 – Générateur auto-rétrécissant.

leur similitude, le générateur auto-rétrécissant a montré une résistance à la cryptanalyse encore plus forte que le générateur rétrécissant [6].

Jusque là, la plupart des PSGs ont une structure basée sur les LFSRs et ont été utilisés dans les systèmes de chiffrement par flot ou par bloc et les générateurs pseudo-aléatoires de nombres.

### 1.3.5 Registres à décalage et à rétroaction avec retenue ou FCSR.

En 1993, Goresky et Klapper développent un nouveau type de registre à décalage qui ne se base pas sur les LFSRs : *les registres à décalage et à rétroaction avec retenue ou Feedback with Carry Shift Registers ou encore FCSR* [7] (voir définition 6.3.1). Ils se différencient des LFSRs par l'ajout d'une mémoire qui varie suivant les étapes du registre. "Carry" désigne l'ajout de la mémoire. Le registre se subdivise en deux registres : le registre principal contenant les bits initiaux de la séquence appartenant au corps premier $\mathbb{F}_p$ (corps fini à $p$ éléments avec $p$ premier) et le registre de retenue contenant la mémoire initiale appartenant à l'anneau des entiers relatifs $\mathbb{Z}$. La fonction de retour consiste en une fonction linéaire dont les variables sont les bits initiaux, à laquelle on ajoute la mémoire initiale pour obtenir un entier $\sigma$. Les calculs se font dans $\mathbb{Z}$. La division euclidienne de $\sigma$ par $p$ donne le bit et la retenue suivante.

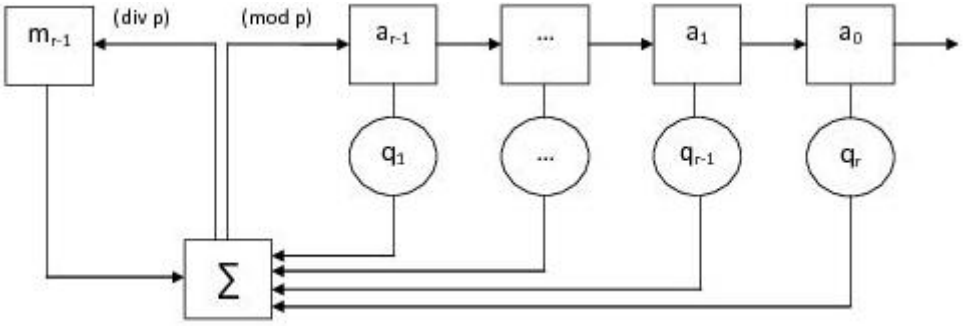



FIGURE 1.9 – Registre à décalage et à rétroaction linéaire avec retenue.

### 1.3.6 Étude algébrique des FCSRs : l'anneau des entiers $p$-adiques $\mathbb{Z}_2$.

Pour analyser les FCSRs, Goresky et Klapper utilisent l'anneau des entiers $p$-adiques [8] (voir définition 3.10.6). Ils associent à la séquence de sorties son développement $p$-adique :

$$a_0 + a_1 p + a_2 p^2 + \ldots \in \mathbb{Z}_p$$

L'addition dans l'anneau des séries formelles se fait coefficient à coefficient tandis que dans l'anneau des entiers $p$-adiques, elle se fait avec une retenue. La relation de récurrence qui définit le registre transforme cet entier $p$-adique en un rationnel $\frac{s}{q}$ où $q$ est un entier déterminé par le FCSR. L'entier $q$ est appelé entier de connexion du FCSR. La période divise l'ordre de $p$ modulo $q$ (l'ordre de $p$ modulo $q$ est le plus petit entier $T$ tel que $q$ divise $p^T - 1$). La période est maximale si $q$ est premier et si $p$ est une racine primitive modulo $q$. Dans ce cas, on a une séquence de période $q - 1$. Les FCSRs séquences de période maximale sont appelées *l-séquences ou longer sequences* [9] (voir définition 6.11.1). Elles jouent un rôle similaire à celui des $m$-séquences. La recherche d'entiers premiers $q$ dont $p$ est une racine primitive modulo $q$ résout la recherche de telles séquences.

En général, les FCSR séquences ont une grande complexité linéaire. Cependant elles restent vulnérables à un autre type de mesure : la complexité 2-adique [10] [11]. *L'algorithme d'approximation rationnelle* [8] permet de construire le plus petit FCSR qui génère une séquence FCSR en connaissant seulement $(2r + 2\ logr)$ bits, où $r$ est le nombre de cellules du registre principal (la taille du registre). Par conséquent, un FCSR ne peut pas être utilisé directement comme générateur de chiffrement par flot.

Toutefois, les bonnes propriétés statistiques vérifiées par les FCSR séquences font de ces séquences un outil tentant et important pour la construction de générateur de chiffrement. Tout comme les LFSRs, les FCSRs peuvent être la base de tels registres en reprenant les différentes construction abordées précédemment. On peut citer notamment la construction d'une nouvelle famille de chiffrement par flot *FCSR filtrés ou Filtred Feedback With Carry Shift Register ou encore F-FCSR* proposée par Arnault et al. pour le projet e-STREAM [12] [13][14][15][16] .

### 1.3.7 Les $d$-FCSRs et les extensions totalement ramifiés de $\mathbb{Z}_p$.

En 1994, Goresky et Klapper proposent un nouveau type de FSRs semblables aux FCSRs : *les d-FCSRs* [17]. La principale différence réside dans l'ajout d'un saut de longueur $d$ dans la case mémoire. Ce saut se traduit algébriquement par une structure algébrique sous-jacente étant une extension totalement ramifiée des entiers $p$-adiques de degré de ramification $d$. L'analyse des $d$-FCSR séquences s'associe donc à l'étude des entiers dits $\pi$-adiques où $\pi$ est une solution de l'équation irréductible sur $\mathbb{Q}$ :

$$\pi^d = p \text{ avec } p \text{ premier.}$$

L'analyse des $d$-FCSRs montre que la séquence de sorties a pour développement $\pi$-adique une fraction dans le corps de nombres algébriques $\mathbb{Q}[\pi]$. En 2004, ils démontrent les propriétés basiques de périodicité et de distribution des $d$-FCSR séquences [18] [19].

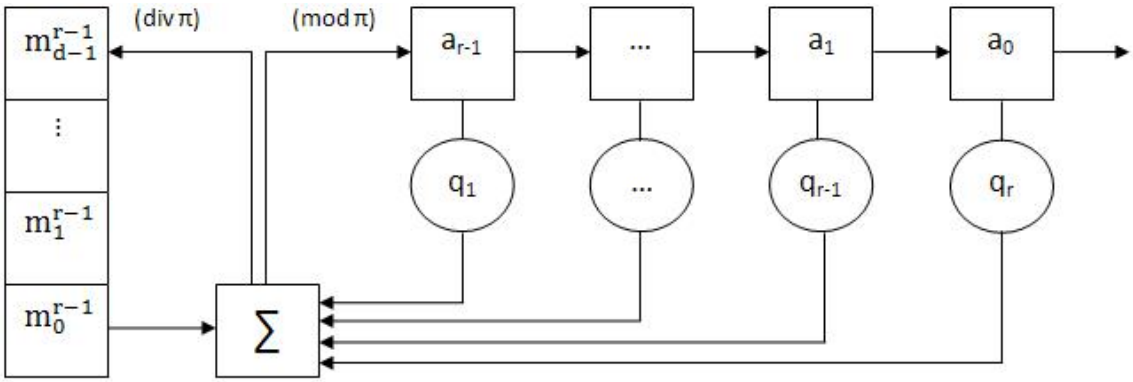



FIGURE 1.10 – Registre à décalage et à rétroaction avec retenue et saut.

### 1.3.8 Algebraic Feedback Shift Registers

Les $d$-FCSRs constituent avec les LFSRs et les FCSRs une classe particulière des FSRs. Ce sont des registres à décalage et à rétroaction reposant sur une structure algébrique sous-jacente. Les LFSRs reposent sur l'anneau des séries formelles sur un corps fini, les FCSRs reposent sur l'anneau des entiers $p$-adiques pour $p$ premier et les $d$-FCSRs reposent sur une extension totalement ramifiée de l'anneau des entiers $p$-adiques et de degré de ramification $d$. Ainsi, en 1999, Klapper et Xu introduisent *les Algebraic Feedback Shift Registers ou AFSRs* [20] [21] qui consistent en une généralisation des registres cités précédemment. Ils sont construits sur un triplet $(A, \pi, S)$ où $A$ est anneau intègre et commutatif, $\pi$ un élément de $A$ et $S$ un système de représentants de $A/\pi A$. Le fonctionnement des AFSRs est identique au fonctionnement des FCSRs. Le cas intéressant des AFSRs est celui où $A/\pi A$ est un corps fini. Si $A = \mathbb{F}_{p^n}[X]$ et $\pi = X$, le registre est un LFSR, si $A = \mathbb{Z}$ et $\pi = p$ premier, alors le registre est un FCSR et si $A = \mathbb{Z}[\pi]$ et $\pi$ est racine $d$-ième de $p$ premier, alors le registre est un $d$-FCSR. Dans l'analyse, ils utilisent la topologie $\pi$-adique sur $A$ et considèrent la complétion de cet anneau topologique. Si $A$ est noethérien, la complétion pour cette topologie $\pi$-adique est l'ensemble des séries formelles $S[[\pi]]$. Le développement $\pi$-adique des séquences de sorties correspond à un élément $\frac{u}{q}$ dans le corps des fractions de $A$ où $q$ est toujours l'entier de connexion du registre. Sous certaines conditions, la séquence de sorties a une représentation exponentielle et sa période divise l'ordre de $\pi$ modulo $q$.

## 1.4 Classification des registres via la théorie algébrique des nombres.

L'idée des AFSRs amènent à penser à une classification des registres en suivant la classification des anneaux de valuations discrètes complets. En effet, l'analyse des FSRs construits sur un corps fini $\mathbb{F}_{p^n}$ repose sur la correspondance entre la séquence de sorties

infinie $(a_0, a_1, \ldots)$ et une série ayant un sens de convergence dans un espace. Ces espaces là ne peuvent être que les anneaux de valuation discrète complets de corps résiduel fini $\mathbb{F}_{p^n}$ dont les éléments sont représentés par des séries convergentes de la forme $\sum_{i=0}^{i=+\infty} a_i \pi^i$. La théorie algébrique des nombres classifie ces anneaux en deux catégories :

1. L'anneau de valuation discrète complet et son corps résiduel sont de même caractéristique.
2. L'anneau de valuation discrète complet est de caractéristique nulle et son corps résiduel est de caractéristique $p$ premier.

Dans le premier cas, l'anneau de valuation discrète complet de corps résiduel $\mathbb{F}_{p^n}$ est isomorphe à l'anneau des séries formelles $\mathbb{F}_{p^n}[[X]]$ et dans le second cas, il est une extension finie de l'anneau des entiers $p$-adiques $\mathbb{Z}_p$. Le degré de l'extension est $nd$ où $d$ est le degré de ramification. Les LFSRs correspondent à l'anneau des séries formelles $\mathbb{F}_{p^n}[[X]]$, les FCSRs sur $\mathbb{F}_p$ à l'anneau des entiers $p$-adiques $\mathbb{Z}_p$ et les $d$-FCSRs à l'anneau $\mathbb{Z}_p[\pi]$ extension totalement ramifiée des entiers $p$-adiques de degré de ramification $d$.

## 1.5 Les différents modes de connexion des FSRs.

La fonction de retour et les entrées des LFSRs et des FCSRs se traduisent sous forme de connexion entre les cellules du registre. Le mode le plus naturel est le mode dit de Fibonacci. Il est appelé ainsi car la suite de Fibonacci se représente dans ce mode. En 2002, Goresky et Klapper introduisent un tout autre mode appelé le mode de Galois [22] (voir définition 5.23.1). Le mode de Fibonacci met à jour une seule cellule du registre principale puis opère par décalage tandis que le mode de Galois met à jour simultanément toutes les cellules du registre. En 2004, Mrugalski et Al. développent un nouveau mode de connexion pour les LFSRs appelé le mode Ring [23] (voir définition 5.24.1). Il est appelé ainsi car ce mode garde les décalages qui forment un anneau avec les cellules juxtaposées tandis que les connexions entre cellules non-juxtaposées sont aléatoires. En 2009, Arnault et al. ont adapté le mode Ring aux FCSRs [24] [25].

## 1.6 Travaux développés dans cette thèse : les FCSRs vectoriels.

Dans le cadre de cette thèse, nous avons développé la conception vectorielle des FCSRs. Sachant que les FCSRs se construisent principalement sur le corps premier $\mathbb{F}_p$, Klapper tente en 1994 d'étendre leur conception sur tout corps fini $\mathbb{F}_{p^n}$ [26]. Les FCSRs sur $\mathbb{F}_{p^n}$ correspondent à l'anneau des vecteurs de Witt sur $\mathbb{F}_{p^n}$. C'est une structure algébrique sous-jacente très difficilement utilisable. Klapper décrit alors brièvement une conception vectorielle mais se cantonne à une analyse purement formelle dont les résultats sont difficilement implémentables.

Nous avons développé une analyse vectorielle complète fournissant tous les résultats fondamentaux dont on dispose déjà pour le cas d'un corps premier comme la période,

la mémoire, les propriétés pseudo-aléatoires, la recherche et la génération de $l$-séquences ... etc. Ces résultats ont été publiés dans SETA 2010 [27]. Après avoir développé l'analyse

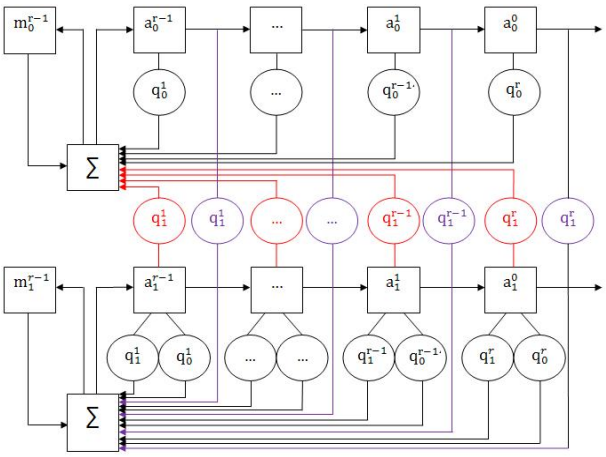


FIGURE 1.11 – FCSR vectoriel quadratique en mode Fibonacci.

vectorielle des FCSRs ou VFCSRs, nous nous sommes intéressés au mode Galois des FCSRs vectoriels. Nous avons construit le formalisme de ces FCSRs vectoriels en mode Galois et nous avons développé en détail le cas quadratique (FCSR construit sur $\mathbb{F}_{2^2}$). En effet, c'est le cas le plus naturel après le cas binaire qui a déjà été l'objet des travaux de Goresky et Klapper. On montre que les FCSRs vectoriels en mode Galois ont de bonnes propriétés statistiques tout comme les FCSRs vectoriels en mode Fibonacci pour des choix adéquats des paramètres. Ils passent en particulier tous les tests statistiques du NIST et ils sont simples à mettre en œuvre.

Comme constaté dans [28], le mode de Fibonacci n'est pas adapté pour les applications de cryptographie alors que le mode de Galois semble meilleur. Nous avons construit une famille de chiffrement par flot à base de FCSRs vectoriels filtrés et nous avons simulé une version hardware : F-VFCSR-H. Notre générateur de flot de chiffrement semble présenter une résistance à l'attaque de Hell et Johansson [29]. Il offre aussi un débit double par rapport au F-FCSR-H v3 [24]. L'introduction de cette nouvelle famille de chiffrement par flot et les résultats obtenus ont été publiés dans WISA 2010 [30]. Cependant, nous n'explicitons pas, dans la suite, ces applications hardware des VFCSRs en mode Galois.

Enfin, nous présentons le mode généralisé ou mode Ring des FCSRs vectoriels. On parle alors de FCRs vectoriels ou Vectorial Feedback with Carry Registers ou registres vectoriels avec retenues. Nous fournissons les résultats basiques de l'analyse et comparons les propriétés de périodicité avec un FCSR binaire en mode Ring de taille double. On constate que les périodes maximales sont identiques tout en gagnant en structure algébrique permettant de faciliter l'analyse. En réalité un VFCR de taille $r$ s'apparente à un FCR de taille $2r$, mais cette ressemblance n'est valable que d'un point de vue matériel, car les VFCRs obéissent à une structure algébrique.

On note enfin que l'introduction des VFCSRs, nous permet de compléter la classification des registres à décalage et à rétroaction.

## 1.7 Plan de la Thèse

Dans un premier temps, nous définissons les notions générales et élémentaires sur les séquences et les générateurs. En deuxième partie, on rappelle les résultats classiques sur les anneaux de valuations discrètes complets et leur classification. En troisième partie, on développe les vecteurs de Witt et l'anneau $\mathbb{Z}_{p^n}$. En quatrième, on rappelle tous les résultats fondamentaux sur les LFSRs. En cinquième partie, on développe les résultats sur les FCSRs. Enfin en sixième partie, on présente notre analyse vectorielle des FCSRs en mode Fibonacci, en mode Galois et en mode généralisé. Pour conclure, nous présentons les perspectives futures.

# Chapitre 2

# Généralités sur les séquences et les générateurs pseudo-aléatoires

Dans ce chapitre, nous abordons les définitions élémentaires concernant les séquences et les générateurs de séquences.

## 2.1 Séquences

Dans cette section, nous décrivons les notions de bases concernant les séquences.

**Définition 2.1.1** (séquence)**.** *Soit $A$ un ensemble. Considérons l'ensemble des suites de la forme $(a_0, a_1, \ldots, a_i, \ldots)$ où les $a_i$ sont des éléments dans $A$.*

- *On note la suite $(a_0, a_1, \ldots, a_i, \ldots)$ par $\underline{a}$.*
- *Si $A$ est discret, c'est-à-dire fini ou dénombrable, on dit que $A$ est un alphabet et $a_i$ un symbole ou un coefficient de la suite.*
- *Si $A = \{0, 1, \ldots, p-1\}$ où $p$ est un entier, on dit que $\underline{a}$ est une séquence $p$-aire (séquence binaire pour $p = 2$).*

**Définition 2.1.2** (périodicité)**.** *Soit $\underline{a}$ une séquence.*

- *$\underline{a}$ est dite strictement périodique s'il existe $T > 0$ tel que $a_{i+T} = a_i$ pour tout $i \in \mathbb{N}$.*
- *$\underline{a}$ est ultimement périodique s'il existe $T > 0$ et $N > 0$ tels que $a_{i+T} = a_i$ pour tout $i \geq N$ et tels que $\underline{a}$ ne soit pas strictement périodique. Dans ce cas, le plus petit $N$ vérifiant cela est appelé pré-période de $\underline{a}$.*
- *On dit que $\underline{a}$ est périodique si elle est strictement ou ultimement périodique.*
- *On dit que $T$ est une longueur de $\underline{a}$ et on appelle période de $\underline{a}$ la plus petite des longueurs non nulles.*

**Lemme 2.1.1.** *Soit $\underline{a}$ une séquence périodique de période $T$, alors toute longueur est un multiple de $T$.*

*Démonstration.* Soit $L$ une longueur de $\underline{a}$. La division euclidienne de $L$ par $T$ donne $L = Tq + r$ où $0 \leq r < T$.

$$a_i = a_{i+L} = a_{i+Tq+r} = a_{i+r}$$

$r$ est donc une longueur de $\underline{a}$ strictement plus petite que $T$. L'entier $T$ étant la plus petite longueur, alors $r = 0$. Donc $L = Tq$. □

## 2.2 Décalages et isomorphismes de séquences

**Définition 2.2.1** (décalage). *Soient $A$ un alphabet, $\underline{a}$ et $\underline{b}$ deux séquences de $A$.*

- *On dit que $\underline{b}$ est un décalage de $\underline{a}$ s'il existe $\tau \geq 0$ tel que $b_i = a_{i+\tau}$ pour tout $i \in \mathbb{N}$.*
- *Si $\underline{b}$ n'est aucun décalage de $\underline{a}$, on dit que $\underline{a}$ et $\underline{b}$ sont de décalage distinct.*
- *Si $\underline{a}$ et $\underline{b}$ sont périodiques de même période et si $\underline{b}$ est un décalage de $\underline{a}$, on dit que $\underline{b}$ est un décalage cyclique de $\underline{a}$.*
- *Si $\underline{a}$ et $\underline{b}$ sont périodiques de même période et si $\underline{b}$ n'est pas un décalage de $\underline{a}$, on dit que $\underline{a}$ et $\underline{b}$ sont cycliquement distinctes.*

**Définition 2.2.2** (isomorphisme de séquences). *Soient $A$ et $B$ deux alphabets et soient $\underline{a}$ et $\underline{b}$ deux séquences respectivement dans $A$ et dans $B$.*

- *On dit que $\underline{a}$ et $\underline{b}$ sont isomorphes s'il existe une bijection $\sigma : A \to B$ telle que $\sigma(a_i) = b_i$ pour tout $i \in \mathbb{N}$.*
- *Si $A = B$, $\sigma$ est une permutation.*
- *On dit que $\underline{a}$ et $\underline{b}$ sont isomorphes par décalage s'il existe une bijection $\sigma : A \to B$ et un entier $\tau$ tels que $\sigma(a_{i+\tau}) = b_i$ pour tout $i \in \mathbb{N}$.*
- *S'il n'existe pas de bijection $\sigma$ et de décalage $\tau$, alors $\underline{a}$ et $\underline{b}$ sont dites non-isomorphes cycliquement distinctes.*

## 2.3 Modèle de générateur de séquences ou Automate

Pour la construction de séquences, nous devons donner un formalisme définissant les générateurs de séquences.

**Définition 2.3.1** (automate). *On appelle générateur de séquences (ou machine à état discret avec sortie ou automate) tout quadruplet $F = (U, \sum, f, g)$ où $U$ est un ensemble d'états, $\sum$ un alphabet de valeurs de sorties, $f : U \to U$ une fonction de transition et $g : U \to \sigma$ une fonction de sorties. L'ensemble $U$ est supposé discret (fini ou dénombrable). Le premier état d'un automate est appelé état initial. Pour tout état initial $s$ dans $U$, la séquence de sorties du générateur $F$ est*

$$F(s) = (g(s), g(f(s)), g(f^2(s)), \ldots, \ldots)$$

*où $g(f^i(s)) \in \sum$ pour tout $i \in \mathbb{N}$.*

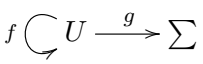



FIGURE 2.1 – Formalisme d'un générateur de séquences.

**Définition 2.3.2** (état périodique)**.** *Soit un automate* $(U, \sum, f, g)$.

- *Un état $s$ est dit strictement périodique s'il existe un entier $L$ strictement positif tel que $f^L(s) = s$. La période est le plus petit $L$ vérifiant cela.*
- *Un état $s$ est dit ultimement périodique s'il existe un entier $L$ strictement positif et un entier $N$ strictement positif tel que pour tout $0 \leq i < N$, l'état $f^i(s)$ n'est pas strictement périodique et l'état $f^N(s)$ est strictement périodique.*
- *Un état est dit périodique s'il est strictement ou ultimement périodique.*
- *Un état $s$ est dit apériodique dans le cas contraire.*
- *On appelle diagramme des états le digramme représentant la succession des états d'un automate.*

**Proposition 2.3.1.** *Si $U$ est fini alors tout état est périodique.*

*Démonstration.* C'est évident. □

**Définition 2.3.3.** *Un ensemble d'état est dit complet si tous ses états sont périodiques.*

**Proposition 2.3.2.** *Si un état $s$ est strictement (ou ultimement) périodique alors la séquence de sorties $F(s)$ est strictement (ou ultimement) périodique.*

La preuve est évidente. Par contre l'inverse est faux !

**Exemple 2.3.1.** *Soit le générateur $F = (\mathbb{N}, 0, 1, f, g)$ où $f(n) = n + 1$ et $g(n) = 0$ pour tout $n \in \mathbb{N}$. Toute séquence de sorties est nulle donc strictement périodique alors qu'aucun état n'est périodique puisque qu'il n'existe pas d'entier $n$ et d'entier $L > 0$ tels que $f^L(n) = n + L = n$ (voir Figure 2.2).*

$$U = \mathbb{N} \qquad \sum = 0, 1$$

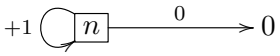



FIGURE 2.2 – Exemple de séquence périodique dont l'état est apériodique.

## 2.4 Homomorphisme de générateurs

**Définition 2.4.1** (homomorphisme d'automates)**.** *Soient $F = (U, \sum, f, g)$ et $G = (V, \sum, f', g')$ deux générateurs de séquences. Un homomorphisme entre $F$ et $G$ est une application partielle $\psi : U \to V$ telle que :*

- *Si $a$ appartient à l'espace de départ de $\psi$, alors $f(a)$ appartient aussi à l'espace de départ de $\psi$.*
- *Le diagramme de la figure 2.3 commute, c'est-à-dire que pour tout $a$ dans l'espace de départ de l'application $\psi$, $g'(\psi(a)) = g(a)$ et $\psi(f(a)) = f'(\psi(a))$.*

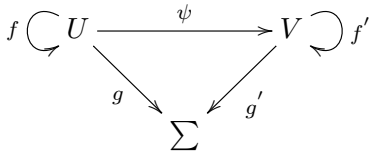



FIGURE 2.3 – Homomorphisme d'automate.

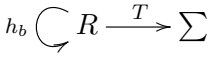



FIGURE 2.4 – Automate $R^{b,T}$.

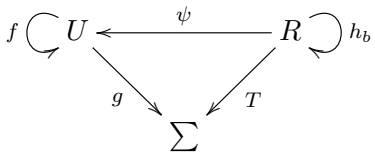



FIGURE 2.5 – Modèle Injectif.

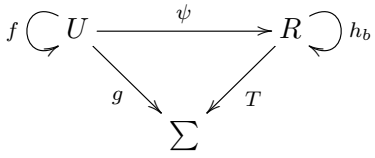



FIGURE 2.6 – Modèle Projectif.

**Définition 2.4.2.** *Soient $R$ un anneau et $b$ un élément de $R$. On note $h_b$ la multiplication par $b$ dans $R$.*

$$h_b : \begin{cases} R & \to & R \\ x & \mapsto & bx. \end{cases}$$

*Pour toute application $T : R \to \sum$, le quadruplet $R^{b,T} = (R, \sum, h_b, T)$ est un générateur de séquences (voir figure 2.4).*

**Définition 2.4.3** (modèle algébrique)**.** *Soit $F = (U, \sum, f, g)$ un automate.*

- *On appelle modèle algébrique pour $F$ un homomorphisme d'automate $\psi$ entre $F$ et $R^{b,T}$ pour un certain anneau $R$, un élément $b \in R$ et une application $T : R \to \sum$.*
- *Le modèle est dit injectif si $\psi : R^{b,T} \to F$ (voir 2.5).*
- *Le modèle est dit projectif si $\psi : F \to R^{b,T}$ (voir 2.6).*

**Définition 2.4.4** (représentation exponentielle)**.** *Si le modèle algébrique est injectif, pour tout $a \in R$, la séquence générée par l'automate $F$ à partir de l'état $\psi(a) \in U$ est sous la*

*forme exponentielle suivante :*

$$\begin{aligned} F(\psi(a)) &= (g(\psi(a)), g(f(\psi(a))), g(f^2(\psi(a))), \ldots) \\ &= (T(a), T(h_b(a)), T(h_b^2(a)), \ldots) \\ &= (T(a), T(ba), T(b^2a), \ldots). \end{aligned}$$

*Si le modèle algébrique est projectif, pour tout $s \in U$, la séquence générée par l'automate $F$ à partir de l'état $s$ est sous la forme exponentielle suivante :*

$$\begin{aligned} F(s) &= (g(s), g(f(s)), g(f^2(s)), \ldots) \\ &= (T(\psi(s)), T(\psi(f(s))), T(\psi(f^2(s))), \ldots) \\ &= (T(\psi(s)), T(h_b(\psi(s))), T(h_b^2(\psi(s))), \ldots) \\ &= (T(\psi(s)), T(b\psi(s)), T(b^2\psi(s)), \ldots). \end{aligned}$$

**Proposition 2.4.1.** *Si $R$ est un corps fini, alors toute séquence de sorties de l'automate $R$ est strictement périodique.*

*Démonstration.* En effet, si $b \neq 0$, alors $b^{|R|-1} = 1$.

$$R(a) = (T(a), T(ba), T(b^2a), \ldots, T(b^{|R|-2}a), T(a), \ldots).$$

□

Si l'homomorphisme $\psi$ est un isomorphisme, alors on peut transformer un modèle injectif en un modèle projectif, et inversement. Dans la suite, nous présentons plusieurs types d'automate (générateurs de séquences) avec leur modèle algébrique et nous étudions les propriétés des séquences générées par ces automates.

## 2.5 Registres à décalage et à rétroaction (Feedback Shift Registers)

Dans cette section, nous introduisons une classe spéciale d'automate : les registres à décalage et à rétroaction appelés Feedback Shift Registers ou FSR.

**Définition 2.5.1** (fonction booléenne)**.** *Considérons $\mathbb{F}_{p^n}$ le corps à $p^n$ éléments et l'espace vectoriel de dimension $r$ sur $\mathbb{F}_{p^n}$ défini par*

$$\mathbb{F}_{p^n}^{(r)} = \{(a_0, a_1, \ldots, a_{r-1})\,;\, \forall\, 0 \leq i \leq r-1,\, a_i \in \mathbb{F}_{p^n}\}\,.$$

*Une fonction booléenne à $r$ variables est une fonction à $r$ entrées et une sortie dans $\mathbb{F}_{p^n}$ $f : \mathbb{F}_{p^n}^{(r)} \to \mathbb{F}_{p^n}$.*

**Théorème 2.5.1.** *Il existe $(p^n)^{(p^n)^r}$ fonctions booléennes $f : (\mathbb{F}_{p^n})^r \to \mathbb{F}_{p^n}$.*

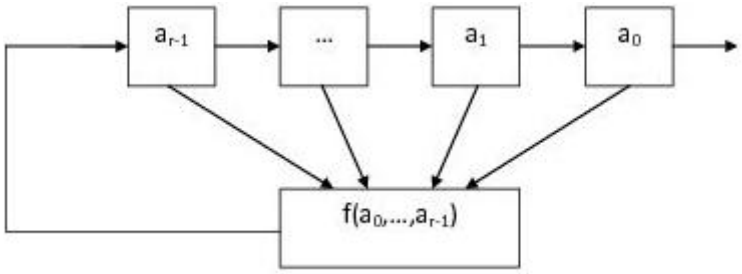



FIGURE 2.7 – Registre à décalage et à rétroaction ou FSR.

**Définition 2.5.2** (Feedback Shift Registers)**.** *Un registre à décalage et à rétroaction ou Feedback Shift Registers est un automate* $((\mathbb{F}_{p^n})^r, \mathbb{F}_{p^n}, h, g))$ *avec pour fonction de retour (feedback fonction)* $h$ *définie par une fonction booléenne* $f$ *à* $r$ *variables sur* $\mathbb{F}_{p^n}$ *:*

$$\begin{aligned} h(x_0, x_1, \ldots, x_{r-1}) = &\quad (x_1, \ldots, x_{r-1}, f(x_0, x_1, \ldots, x_{r-1})) \text{ où} \\ f(x_0, x_1, \ldots, x_{r-1}) = &\sum_{0 \leq i_1, i_2, \ldots, i_t \leq r-1} q_{i_1,\ldots,i_t} x_{i_1} \ldots x_{i_t}; \end{aligned}$$

*et pour fonction de sorties* $g : {\mathbb{F}_{p^n}}^r \to \mathbb{F}_{p^n}$ *définie par* $g(x_0, x_1, \ldots, x_{r-1}) = x_0$*. On appelle* $r$ *la taille du registre. La séquence de sorties* $\underline{a} = (a_0, a_1, \ldots)$ *vérifie la relation de récurrence*

$$a_{i+n} = f(a_i, a_{i+1}, \ldots, a_{i+n-1}).$$

$\underline{a}$ *est une FSR-séquence* $p^n$*-ary.*

La figure 2.7 représente un Feedback Shift Register.

**Définition 2.5.3** (cas linéaire et cas non-linéaire)**.**

- *Si* $f$ *est linéaire, le FSR est un registre à décalage et à rétroaction linéaire ou un Linear Feedback Shift Register ou encore un LFSR. Les séquences de sorties des LFSRs sont appelées LFSR séquences (linear feedback shift register sequence).*
- *Si* $f$ *est non-linéaire, le FSR est un registre à décalage et à rétroaction non-linéaire ou un Non-Linear Feedback Shift Register ou encore un NLFSR. Les séquences de sorties des NLFSRs sont appelées NLFSR séquences (non-linear feedback shift register sequences).*

**Théorème 2.5.2.** *Soit un FSR* $\mathcal{F} = ((\mathbb{F}_{p^n})^r, \mathbb{F}_{p^n}, f, g)$*. Toute séquence de sorties est périodique avec une période inférieure ou égale à* $p^{nr}$*.*

*Démonstration.* Toute séquence de sorties $\underline{a}$ est déterminée par l'état initial $(a_0, a_1, \ldots, a_{r-1})$ et par $f$ en posant la relation de récurrence $a_{i+n} = f(a_i, a_{i+1}, \ldots, a_{i+n-1})$. Or il y a $p^{nr}$ états de taille $r$ à coefficients dans $\mathbb{F}_{p^n}$. Entre l'état initial et l'état $(a_{p^{nr}}, a_{p^{nr}+1}, \ldots, a_{p^{nr}+r-1})$, $p^{nr} + 1$ états se succèdent par décalage à droite. Donc il y a forcément un état $s =$

$(a_r, a_{r+1}, \ldots, a_{r+n-1})$ qui se répète avec $r \leq q^n$. Cette état est périodique, d'après la proposition 2.3.2, la séquence $F(s)$ est strictement périodique et

$$F(s) = (a_r, a_{r+1}, \ldots).$$

Si $s$ est l'état initial, alors $\underline{a}$ est strictement périodique ; sinon à partir de $r$, la séquence $\underline{a}$ est strictement périodique, donc elle est ultimement périodique. □

**Exemple 2.5.1.** *Soit le FSR ayant pour fonction de retour* $f(x_0, x_1, x_2, x_3) = x_2 + x_3$. *L'état initial* (0001) *génère la séquence* (00011011011...). *C'est une LFSR séquence, elle est ultimement périodique avec* $N = 2$ *et la période est* $T = 3$.

**Exemple 2.5.2.** *Soit le NLFSR ayant pour fonction de retour* $f(x_0, x_1, x_2) = x_0x_1$. *Le diagramme des états est représenté dans la figure 2.8. Ce diagramme nous montre que les séquences de sorties se subdivisent en 4 catégories :*

- *quatre séquences sont de période 2 dont deux ultimement périodiques de pré-période 2 et deux strictement périodiques.*
- *trois séquences ultimement périodiques de période 1.*
- *Les séquences triviales (nulle et celle composée de uns).*

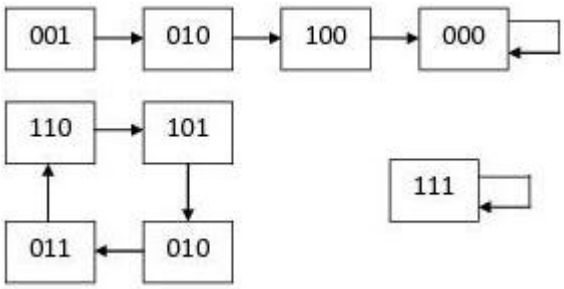



FIGURE 2.8 – Diagramme des états pour la fonction de retour $f(x_0, x_1, x_2) = x_0x_1$.

**Exemple 2.5.3.** *Soit le LFSR ayant pour fonction de retour* $f(x_0, x_1, x_2) = x_0 + x_1$. *Le diagramme des états est représenté dans la figure 2.9. La séquence de sorties est une LFSR séquence. Pour tout état initial non-nul, la séquence de sorties est de période* $7 = 2^3 - 1$.

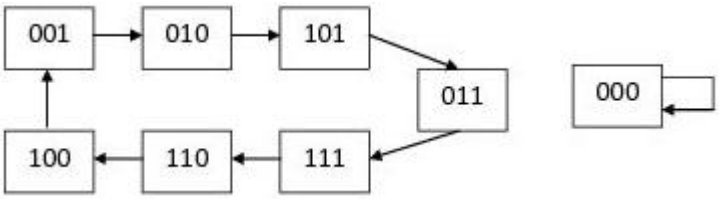



FIGURE 2.9 – Diagramme des états pour la fonction de retour $f(x_0, x_1, x_2) = x_0 + x_1$.

# Chapitre 3

# Corps valués et classification

## 3.1 Introduction

Dans ce chapitre, nous abordons la théorie des valuations. On rappelle les résultats classiques en prenant pour sources les livres [31], [32], [33], [34], [35], [36], [37] et [38]. Le but étant de présenter la classification des corps de valuation discrète complets de corps résiduel fini ou de manière équivalente les anneaux de valuations discrètes (a.v.d.) complets de corps résiduel fini. Nous ne démontrerons pas les résultats énoncés dans ce chapitre en nous référant à ces huit livres qui contiennent déjà les arguments nécessaires pour prouver ces résultats. Notre intérêt pour les valuations discrètes se justifie par le fait que les anneaux de valuation discrète ont des objets qui se définissent comme des séries formelles ayant un sens (convergence) dans ces espaces là. Or l'idée centrale pour l'étude d'un registre est d'associer les séquences de sorties à des objets existant dans des espaces avec des lois qui permettent d'étudier les propriétés de ces objets pour ensuite transporter ces propriétés via la correspondance qui les lie avec les séquences de sorties. Les objets naturels qui sont les plus adaptés, voir les seuls adaptés sont les séries formelles. La figure 3.1 illustre bien ce parallèle. Il existe deux cas principaux :

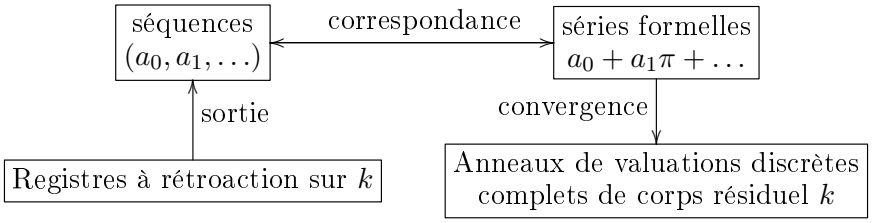



FIGURE 3.1 – Lien entre les a.v.ds et les registres à rétroaction.

1. les séries formelles dont les sommes se font terme à terme.
2. les séries formelles dont les sommes se font avec des retenues.

Dans le cas des retenues, il y a deux sous cas :

1. le premier étant le cas sans "saut" et

2. le deuxième étant le cas avec "saut".

Cela se traduit en théorie algébrique des nombres par les trois cas obtenus par la classification des anneaux de valuation discrète complets :

1. le cas d'égale caractéristique,
2. le cas d'inégale caractéristique absolument non-ramifié et
3. le cas d'inégale caractéristique totalement ramifié.

Dans les premières sections, nous présentons la classification des a.v.d complets. En conclusion, nous développons ce lien essentiel et constructif qui existe entre ces anneaux de valuations discrètes complets et les registres à rétroaction générant des séquences sur un corps fini.

## 3.2 Valuations

**Définition 3.2.1** (valeur absolue)**.** *Soit $K$ un corps commutatif. Une valeur absolue sur $K$ est une application $v : K \to \mathbb{R}_+$ qui vérifient les trois conditions suivantes :*

1. $v(a) = 0 \Leftrightarrow a = 0$,
2. *pour tout* $a, b \in K$, $v(ab) = v(a)v(b)$ *et*
3. *pour tout* $a, b \in K$, $v(a + b) \leq v(a) + v(b)$.

*Une valeur absolue qui vérifie la condition plus forte :*

$$\textit{pour tout } a, b \in K, v(a + b) \leq \max(v(a), v(b)),$$

*est appelée valeur absolue non-archimédienne ou valeur absolue ultramétrique.*
*Sinon on dit que $v$ est une valeur absolue archimédienne.*
*La valeur absolue définie par $v(0) = 0$ et $v(a) = 1$ pour tout $a \neq 0$ est appelée valeur absolue triviale ou impropre.*
*Un corps muni d'une valeur absolue est dit corps valué. Si $v$ est (non-)archimédienne, on dit que $K$ est un corps valué (non-)archimédien.*

**Proposition 3.2.1.** *Tout corps fini possède uniquement la valeur absolue triviale.*

**Définition 3.2.2** (valeurs absolues équivalentes)**.** *Soient $v_1$ et $v_2$ deux valeurs absolues sur un corps $K$. Elles sont équivalentes si :*

$$\textit{pour tout } a \in K,\ v_1(a) < 1 \Leftrightarrow v_2(a) < 1.$$

**Proposition 3.2.2.** *Soit $v_1$ et $v_2$ deux valeur absolues équivalentes sur un corps $K$. Alors il existe $s > 0$ tel que pour tout $a \in K$, $v_1(a) = v_2(a)^s$.*

**Théorème 3.2.1.** *Toute valeur absolue sur un corps $K$ de caractéristique $p$ premier est une valeur absolue non-archimédienne. Si $v$ est une valeur absolue archimédienne sur un corps $K$, alors $K$ est de caractéristique $0$.*

## 3.3 Valeur absolue sur $\mathbb{Q}$

**Définition 3.3.1** (valeur absolue $p$-adique). *Soit un nombre rationnel $a = \frac{m}{n} \in \mathbb{Q}$. Il existe deux entiers naturels $r$ et $s$ et deux entiers $m'$ et $n'$ premiers avec $p$ tels que :*

$$m = m'p^r \text{ et } n = n'p^s.$$

*On appelle valeur absolue $p$-adique l'application $v_p : \mathbb{Q} \to \mathbb{R}_+$ qui à tout $a$ associe la valeur $\frac{1}{p^{r-s}}$.*

**Proposition 3.3.1.** *La valeur absolue $p$-adique sur $\mathbb{Q}$ est une valeur absolue non-archimédienne sur $\mathbb{Q}$.*

**Définition 3.3.2** (valeur absolue ordinaire). *Le corps $\mathbb{Q}$ possède aussi la valeur absolue ordinaire notée $v_\infty$ définie par $v_\infty(a) = a$ si $a > 0$ et $v_\infty(a) = -a$ si $a < 0$.*

**Théorème 3.3.1** (Ostrowski). *Toute valeur absolue sur $\mathbb{Q}$ est soit équivalente à la valeur absolue ordinaire $v_\infty$, soit équivalente à la valeur absolue $p$-adique $v_p$ pour un certain $p$ premier, soit triviale.*

## 3.4 Anneau de valuation, Corps résiduel et Groupe des Valeurs

**Définition 3.4.1** (groupe des valeurs). *Soit $v$ une valeur absolue. On appelle groupe des valeurs de $v$ l'image dans $\mathbb{R}_+$ de $v$ et on le note $\Gamma$.*

$$\Gamma = \{y \in \mathbb{R}_+ \text{ tel que } \exists a \in K, v(a) = x\}.$$

**Proposition 3.4.1.** *Le groupe des valeurs d'une valeur absolue est un sous groupe multiplicatif de $\mathbb{R}_+$.*

**Définition 3.4.2** (anneau de valuation). *Soit un corps $K$ muni d'une valeur absolue $v$ non-archimédienne. On appelle anneau de valuation pour $v$ l'ensemble des éléments de $K$ tels que leur valeur absolue soit strictement inférieure ou égale à 1. On note cet ensemble $\mathcal{O}$.*

$$\mathcal{O} = \{a \in K \text{ tel que } v(a) \leq 1\}.$$

**Proposition 3.4.2.** *L'anneau de valuation d'un corps valué $K$ non- archimédien est un anneau local, c'est-à-dire qu'il possède un unique idéal maximal noté $\mathcal{M}$ et*

$$\mathcal{M} = \{a \in K \text{ tel que } v(a) < 1\}.$$

*Pour tout $x \in K$, si $x \notin \mathcal{O}$, alors $x^{-1} \in \mathcal{O}$. L'ensemble $\mathcal{O} \setminus \mathcal{M}$ forme le sous groupe multiplicatif des éléments inversibles de $\mathcal{O}$ noté $\mathcal{O}^*$. Le corps $K$ se décompose de la manière suivante :*

$$K = \mathcal{M} \cup \mathcal{O}^* \cup (\mathcal{M} \setminus \{0\})^{-1}.$$

**Définition 3.4.3** (corps résiduel). *Le corps quotient $\mathcal{O}/\mathcal{M}$ est appelé corps résiduel de $K$ ou de $\mathcal{O}$. On le note $k$.*

## 3.5 Complétion d'un corps valué

Soit $K$ un corps muni d'une valeur absolue $v$ non-triviale. L'espace $K$ est un espace métrique. La distance entre deux éléments $a$ et $b$ est définie par

$$d(a,b) = v(a-b).$$

**Définition 3.5.1** (suite de Cauchy)**.** *Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments dans $K$. On dit que cette suite est de Cauchy si elle vérifie la propriété suivante :*

*Pour tout $\epsilon > 0$, il existe un entier $N_\epsilon \geq 0$ tel que pour tout $n, m \geq N_\epsilon$, $d(a_n, a_m) < \epsilon$.*

*On dit que $K$ est complet si toute suite de Cauchy dans $K$ converge dans $K$.*

**Notation 3.5.1.** *Notons $\mathcal{C}(K)$ l'ensemble des suites de Cauchy de $K$. Notons $\mathcal{M}(K)$ l'ensemble des suites de $K$ convergentes vers $0$.*

**Théorème 3.5.1.** *$\mathcal{C}(K)$ est un anneau unitaire et $\mathcal{M}(K)$ un idéal maximal de $\mathcal{C}(K)$. L'espace $\mathcal{C}(K)/\mathcal{M}(K)$ est un corps. La valeur absolue $v$ se prolonge dans $\mathcal{C}(K)/\mathcal{M}(K)$ par la valeur absolue $\hat{v}$ définie par :*

$$\hat{v}((a_n)_{n\in\mathbb{N}}) = \lim_{n\to+\infty} v(a_n).$$

*$\mathcal{C}(K)/\mathcal{M}(K)$ est complet pour cette valeur absolue. Le corps $K$ s'injecte dans $\hat{K}$ par l'application "diagonale" $x \mapsto (x, x, \ldots)$. Le sous-espace $K$ est dense dans $\hat{K}$. Le corps $\hat{K}$ est l'unique extension valuée complète de $K$ à isomorphisme près vérifiant ces propriétés.*

**Définition 3.5.2.** *$\mathcal{C}(K)/\mathcal{M}(K)$ est appelé le complété de $K$ et est noté $\hat{K}$.*

**Proposition 3.5.1.** *Le corps résiduel de $\hat{K}$ est isomorphe au corps résiduel de $K$.*

**Proposition 3.5.2.** *Le groupe des valeurs de $\hat{K}$ est isomorphe au groupe des valeurs de $K$.*

**Définition 3.5.3.** *Le complété de $\mathbb{Q}$ pour la valeur absolue p-adique est noté $\mathbb{Q}_p$ et son anneau de valuation est noté $\mathbb{Z}_p$.*

**Théorème 3.5.2.** *Le complété de $\mathbb{Q}$ pour la valeur absolue ordinaire est le corps des réels $\mathbb{R}$.*

## 3.6 Valeur absolue discrète

**Définition 3.6.1** (Valeur absolue discrète)**.** *On dit qu'une valeur absolue non archimédienne est discrète si son groupe des valeurs est monogène. Par abus de langage, on dit aussi que c'est une valuation discrète. Il existe donc un unique élément $\pi$ de $\mathcal{O}$ à un inversible près tel que pour tout $a \in K$, il existe $r \in \mathbb{Z}$ tel que $v(a) = v(\pi)^r$. L'élément $\pi$ est une uniformisante de $K$ pour $v$. L'entier $r$ est appelé valuation de $a$. Si $k$ est muni d'une telle valeur absolue, on dit qu'il est un corps de valuation discrète.*

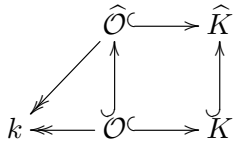



FIGURE 3.2 – Complété d'un corps muni d'une valuation discrète.

**Proposition 3.6.1.** *Soit $K$ un corps de valuation discrète. L'anneau $\mathcal{O}$ est un anneau principal qui admet pour unique idéal premier son idéal maximal $\mathcal{M}$ et $\pi$ est l'unique élément irréductible à un inversible près dans $\mathcal{O}$. L'idéal $\mathcal{M}$ est engendré par $\pi$ et est noté $\pi\mathcal{O}$.*

**Définition 3.6.2** (anneau de valuation discrète)**.** *Un anneau principal qui possède un unique idéal premier est appelé anneau de valuation discrète.*

**Définition 3.6.3** (uniformisante)**.** *L'unique élément irréductible à un inversible près d'un anneau de valuation discrète est appelé une uniformisante.*

**Proposition 3.6.2.** *Le corps des fractions d'un anneau de valuation discrète est un corps de valuation discrète. Inversement, l'anneau de valuation d'un corps de valuation discrète est un anneau de valuation discrète et son uniformisante pour cette valuation est l'uniformisante de l'anneau de valuation.*

**Théorème 3.6.1.** *Soit $K$ un corps de valuation discrète. Son complété $\hat{K}$ est un corps de valuation discrète dont les éléments se développent de manière unique en série convergente dans $\hat{K}$ de la forme*

$$a = \sum_{-\infty<<n} a_n \pi^n,$$

*à coefficients dans le corps résiduel de $K$. L'anneau de valuation $\hat{\mathcal{O}}$ correspond à l'ensemble des séries indéxées sur $\mathbb{N}$. C'est un anneau de valuation discrète complet.*

## 3.7 Extension et Degré de ramification

**Définition 3.7.1** (extension de corps)**.** *Soit $K$ un corps. Un corps $K'$ est une extension de $K$ si $K'$ est un corps contenant $K$.*

**Théorème 3.7.1.** *Soit $K$ un corps muni d'une valeur absolue $v$. Soit $K'$ une extension de $K$. Alors $v$ se prolonge en une valeur absolue sur $K'$.*

**Proposition 3.7.1.** *Soit $K$ un corps muni d'une valeur absolue $v$ de groupe des valeurs $\Gamma$. Soient $K'$ une extension finie de $K$ et $\Gamma'$ le groupe des valeurs de $K'$ pour un prolongement de $v$ sur $K'$. Alors :*

$$[\Gamma' : \Gamma] \leq [K' : K].$$

**Définition 3.7.2** (degré de ramification). *On appelle degré de ramification d'une extension finie de corps valués $K' \supseteq K$ l'ordre du groupe quotient $\Gamma'/\Gamma$ c'est-à-dire la valeur $[\Gamma' : \Gamma]$.*

**Proposition 3.7.2.** *Soit $K$ un corps muni d'une valeur absolue $v$ de corps résiduel $k$ et de groupe des valeurs $\Gamma$. Soit $K'$ une extension finie de corps résiduel $k'$ et de groupe des valeurs $\Gamma'$ pour le prolongement de $v$ sur $K'$. Alors :*

$$[\Gamma' : \Gamma].[k' : k] \leq [K' : K].$$

**Définition 3.7.3** (degré résiduel). *On appelle degré résiduel d'une extension finie de corps valués $K' \supseteq K$ la dimension de $k'$ comme $k$-espace vectoriel, soit la valeur $[k' : k]$.*

**Proposition 3.7.3.** *Soit $K$ un corps muni d'une valuation discrète $v$ et complet pour cette valuation. Soit $K'$ une extension finie de $K$. Alors :*

$$[\Gamma' : \Gamma].[k' : k] = [K' : K].$$

**Définition 3.7.4.** *Une extension est dite absolument non-ramifiée si son degré de ramification est 1.*

$$[\Gamma' : \Gamma] = 1.$$

*Une extension est dite totalement ramifiée si son degré de ramification est égale à son degré d'extension et donc si son degré résiduel est égale à 1.*

$$[\Gamma' : \Gamma] = [K' : K] \text{ et } [k' : k] = 1.$$

## 3.8 Classification des corps de valuation discrète complet avec un corps résiduel parfait

**Définition 3.8.1** (corps parfait). *Un corps $K$ est parfait si et seulement s'il est de caractéristique nulle, ou, lorsqu'il est de caractéristique $p > 0$, l'endomorphisme de Frobenius $x \mapsto x^p$ est surjectif (autrement dit tout élément de $K$ possède une racine $p$-ième dans $K$). En particulier tout corps fini est parfait.*

**Théorème 3.8.1** (Cas d'égale caractéristique). *Soit $K$ un corps de valuation discrète complet dont le corps résiduel $k$ est parfait. Si $K$ et $k$ sont de caractéristique égale alors $K$ est isomorphe au corps des séries formelles à une variable sur $k$ :*

$$K \cong k((X)).$$

**Proposition 3.8.1.** *Soit $K$ un corps de valuation discrète complet dont le corps résiduel $k$ est parfait. Si $K$ et $k$ sont de caractéristiques différentes, alors $K$ est de caractéristique $0$ et $k$ est de caractéristique $p$ premier. Nous avons le diagramme suivant d'homomorphismes injectifs :*

$$\begin{array}{ccccc} \mathbb{Q} & \hookrightarrow & \mathbb{Q}_p & \hookrightarrow & K \\ \uparrow & & \uparrow & & \uparrow \\ \mathbb{Z} & \hookrightarrow & \mathbb{Z}_p & \hookrightarrow & \mathcal{O} \end{array}$$

*Si $v(p) = v(\pi)^e$ alors l'extension $K \supseteq \mathbb{Q}_p$ est d'indice de ramification égale à $e$. Si $k$ est fini alors $K$ est une extension finie de $\mathbb{Q}_p$ de dimension :*

$$[K : \mathbb{Q}_p] = e.[k : \mathbb{F}_p].$$

*L'anneau de valuation de $K$ est un $\mathbb{Z}_p$-module de rang $e.[k : \mathbb{F}_p]$.*

**Définition 3.8.2** (degré de ramification absolu)**.** *Soit $K$ un corps de valuation discrète $v$ et complet pour cette valuation, de caractéristique 0 et de corps résiduel parfait de caractéristique $p$ premier. Soit $\pi$ l'uniformisante de $K$ pour cette valuation. Alors l'indice $e$ tel que $v(p) = v(\pi)^e$ est appelé indice de ramification absolu.*

**Théorème 3.8.2** (Cas d'inégale caractéristique absolument non-ramifié)**.** *Soit $K$ un corps de valuation discrète complet dont le corps résiduel $k$ est parfait et de caractéristique différente de $K$. Si $K$ est absolument non ramifié, alors $K$ est isomorphe au corps des fractions de $W(k)$ l'anneau des vecteurs de Witt sur $k$ et $\mathcal{O}$ est isomorphe à $W(k)$.*

$$K \cong \texttt{Frac}(W(k)).$$

**Théorème 3.8.3** (Cas d'inégale caractéristique ramifié)**.** *Soit $K$ un corps de valuation discrète complet dont le corps résiduel $k$ est parfait et de caractéristique différente de $K$. Si $K$ est ramifié et $e$ est son indice de ramification absolu, alors nous avons le diagramme d'homomorphismes injectifs suivants :*

$$\begin{array}{ccccccc}
\mathbb{Q} & \hookrightarrow & \mathbb{Q}_p & \hookrightarrow & \texttt{Frac}(W(k)) & \hookrightarrow & K \\
\uparrow & & \uparrow & & \uparrow & & \uparrow \\
\mathbb{Z} & \hookrightarrow & \mathbb{Z}_p & \hookrightarrow & W(k) & \hookrightarrow & \mathcal{O}
\end{array}$$

*$K$ est une extension totalement ramifiée de $\texttt{Frac}(W(k))$ et son anneau de valuation $\mathcal{O}$ est un $W(k)$-module libre de rang $e$. Si $k$ est fini, alors $K$ est un $\mathbb{Q}_p$-espace vectoriel de dimension $e.[k : \mathbb{F}_p]$ et $\mathcal{O}$ est un $\mathbb{Z}_p$-module libre de rang $e.[k : \mathbb{F}_p]$.*

Ces résultats d'existence et d'unicité sont valables pour les anneaux de valuation discrète complets de corps résiduel parfait.

## 3.9 Classification des corps de valuation archimédienne complet

**Définition 3.9.1** (valeur absolue ordinaire sur $\mathbb{R}$ et sur $\mathbb{C}$)**.** *La valeur absolue ordinaire sur $\mathbb{R}$ est définie par $v(a) = a$ pour tout $a \geq 0$ et $v(a) = -a$ pour tout $a \leq 0$. La valeur absolue ordinaire sur $\mathbb{C}$ est définie par $v(a + ib) = \sqrt{a^2 + b^2}$ pour tout $a, b \in \mathbb{R}$.*

**Théorème 3.9.1.** *Tout corps valué archimédien complet est isomorphe à $\mathbb{R}$ ou à $\mathbb{C}$.*

## 3.10 Séries formelles et entiers $p$-adiques.

Nous présentons dans la suite les trois exemples fondamentaux qui nous intéressent dans cette thèse à savoir : (dans cette section) le cas d'égale caractéristique représenté par les séries formelles et le cas d'inégale caractéristique absolument non ramifié de corps résiduel premier $\mathbb{F}_p$ représenté par les entiers $p$-adiques ; et (dans le chapitre suivant) le cas d'inégale caractéristique absolument non ramifié de corps résiduel $\mathbb{F}_{p^n}$ avec $n \geq 1$ représenté par l'anneau des vecteurs de Witt, $W(\mathbb{F}_{p^n})$. On ignorera le cas totalement ramifié correspond aux $d$-FCSRs que l'on n'aborde pas dans la suite.

### 3.10.1 Localisation

Soit $A$ un anneau commutatif.

**Définition 3.10.1** (partie multiplicative)**.** *Soit $A$ un anneau commutatif unitaire. L'ensemble $S$ est une partie multiplicative de $A$ si elle est stable par multiplication et si elle contient l'unité de $A$.*

**Définition 3.10.2** (localisé)**.** *Considérons un anneau commutatif $A$ et une partie multiplicative $S$. Soit l'ensemble produit $A \times S$ muni de la relation d'équivalence définie par $(a, s) \sim (b, r)$ s'il existe $t \in S$ tel que $t(ar - bs) = 0$.*

*$A \times S$ quotienté par cette relation d'équivalence muni de l'addition $(a, s) + (b, r) = (ar + bs, sr)$ et du produit $(a, s).(b, r) = (ab, sr)$ est un anneau commutatif. On l'appelle l'anneau localisé de $A$ en $S$ et on le note $S^{-1}A$.*

*Le corps des fractions $K$ d'un anneau intègre est le localisé de $A$ en $A \setminus \{0\}$.*

*Si $S$ est le complémentaire d'un idéal premier $P$ de $A$, alors l'anneau localisé de $A$ en $A \setminus P$ est un anneau local noté $A_P$.*

### 3.10.2 Valuation $X$-adique.

Soit $k$ un corps commutatif. Considérons l'anneau euclidien $k[X]$ des polynômes à coefficients dans $k$ et son corps des fractions $k(X)$ des fractions rationnelles à coefficients dans $k$.

**Définition 3.10.3** (valuation ou ordre $X$-adique)**.** *Tout polynôme $P(X)$ peut s'écrire comme produit $X^{r(P)}P_0(X)$ avec $P_0(X)$ premier avec $X$. Pour toute fraction rationnelle $f(X) = \frac{P(X)}{Q(X)}$, on lui associe l'entier $r(f) = r(P) - r(Q)$ appelé ordre $X$-adique de $f$ et on définit l'application $r : k(X) \to \mathbb{Z}$. Considérons un réel $0 < \alpha < 1$ arbitraire. On définit la valuation $X$-adique d'une fraction rationnelle $f(X)$ par $v(f(X)) = \alpha^{r(f)}$. C'est une application $v : k(X) \to \mathbb{R}_+$.*

**Proposition 3.10.1.** *La valuation $X$-adique est une valuation discrète sur $k(X)$ d'uniformisante $X$.*

*Démonstration.* Il est évident qu'il s'agit d'une valuation. Il reste à prouver la propriété dite ultra-métrique.

$$\begin{aligned} v\Big(\tfrac{P(X)}{Q(X)}+\tfrac{R(X)}{S(X)}\Big) &= v\Big(\tfrac{P(X)S(X)+R(X)Q(X)}{Q(X)S(X)}\Big) = \alpha^{r(PS+RQ)-r(QS)} = \alpha^{\min(r(PS),r(RQ))-r(QS)} \\ &= \max(\alpha^{r(PS)},\alpha^{r(RQ)})\alpha^{-r(QS)} = \max(\alpha^{r(PS)-r(QS)},\alpha^{r(RQ)-r(QS)}) \\ &= \max(\alpha^{r(P)-r(Q)},\alpha^{r(R)-r(S)}) = \max(v(\tfrac{P}{Q}),v(\tfrac{R}{S})\Big). \end{aligned}$$

□

**Proposition 3.10.2.** *L'anneau de valuation de $k(X)$ pour la valuation $X$-adique est l'anneau localisé de $k[X]$ en $k[X]\setminus(X)$. L'idéal maximal $(X)$ est l'unique idéal premier de cet anneau. Son corps résiduel est $k$ et on note cet anneau local $k[X]_{(X)}$.*

*Démonstration.* $k(X)$ est un corps muni d'une valuation discrète et son anneau de valuation $\mathcal{O}$ est l'ensemble des éléments de valuation $X$-adique inférieur ou égale à 1.

$$\begin{aligned} \tfrac{P(X)}{Q(X)}\in\mathcal{O} &\Leftrightarrow r(P)-r(Q)\geq 0 \\ &\Leftrightarrow \tfrac{P(X)}{Q(X)}=\tfrac{X^{r(P)-r(Q)}P_0(X)}{Q_0(X)} \\ &\Leftrightarrow \tfrac{P(X)}{Q(X)}\in(k[X]\setminus(X))^{-1}k[X]. \end{aligned}$$

L'ensemble $k[X]_{(X)}\setminus(X)$ est constitué des éléments inversibles de l'anneau $k[X]_{(X)}$ et donc l'idéal engendré par $X$ dans cet anneau est maximal, c'est même l'unique idéal premier. Le corps résiduel de $k[X]_{(X)}$ est le corps $k$. En effet, en utilisant l'homomorphisme surjectif d'anneau de $k[X]_{(X)}$ dans $k$ qui à toute fraction rationnelle $\frac{P(X)}{Q(X)}$ associe l'élément $P(X)\texttt{mod}X(Q(X)\texttt{mod}X)^{-1}$, on trouve que le noyau est l'idéal engendré par $X$ et le reste suit. □

**Proposition 3.10.3.** *Le complété de $k(X)$ pour la valuation $X$-adique est le corps des séries de Laurent $k((X))$ dont les éléments sont toutes les séries de la forme*

$$\sum_{-\infty<<i} a_iX^i$$

*avec les $a_i$ éléments du corps $k$. L'anneau de valuation de $k((X))$ est l'anneau des séries formelles $k[[X]]$ dont les éléments sont les séries de la forme*

$$\sum_{i\in\mathbb{N}} a_iX^i$$

*avec les $a_i$ éléments du corps $k$. C'est un anneau de valuation discrète dont l'idéal maximal est $(X)=Xk[[X]]$. L'ensemble $k[[X]]\setminus(X)$ est constitué des éléments inversibles de $k[[X]]$.*

*Démonstration.* Cette proposition est une conséquence directe du théorème 3.6.1. □

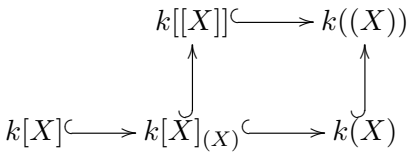



FIGURE 3.3 – Séries formelles

### 3.10.3 Séquences périodiques, séquences récurrentes linéaires et séries formelles

**Définition 3.10.4** (L'anneau des séries formelles)**.** *L'anneau des séries formelles sur $k$ est défini comme l'ensemble des séries infinies de la forme $a(X) = \sum_{i\in\mathbb{N}} a_i X^i$ muni de la somme terme à terme et de la multiplication suivante :*

$$\sum_{i\in\mathbb{N}} a_i X^i + \sum_{i\in\mathbb{N}} b_i X^i = \sum_{i\in\mathbb{N}} (a_i + b_i) X^i$$
$$\sum_{i\in\mathbb{N}} a_i X^i . \sum_{i\in\mathbb{N}} b_i X^i = \sum_{i\in\mathbb{N}} \Big( \sum_{j=0}^{j=i} a_j b_{i-j} \Big) X^i .$$

**Lemme 3.10.1.** *Une série formelle $\sum_{i=0}^{i=+\infty} a_i X^i$ est inversible si et seulement si $a_0 \neq 0$.*

*Démonstration.* C'est un résultat déjà énoncé précédemment. En effet $k[[X]]$ est un anneau de valuation discrète. L'idéal engendré par $X$ est son unique d'idéal premier et le complémentaire de cet idéal est l'ensemble des inversibles de $k[[X]]$. C'est aussi l'ensemble des éléments dont le premier coefficient $a_0$ est non nul. On peut le prouver directement par construction en remarquant qu'une série formelle $\sum_{i=0}^{i=+\infty} a_i X^i$ est inversible si et seulement s'il existe une série formelle $\sum_{i=0}^{i=+\infty} b_i X^i$ telle que

$$\begin{aligned} a(X)b(X) = 1 &\Leftrightarrow a_0 b_0 + (a_0 b_1 + a_1 b_0) X + \ldots = 1 \\ &\Leftrightarrow a_0 b_0 = 1 \text{ et } \sum_{j=0}^{j=i} a_j b_{i-j} = 0 \text{ pour tout } i \geq 1 \\ &\Leftrightarrow \begin{cases} a_0 \neq 0 \\ b_0 = a_0^{-1} \\ b_1 = -a_0^{-1} a_1 b_0 \\ \vdots \end{cases} \end{aligned}$$

Donc la série formelle est inversible si et seulement si $a_0 \neq 0$ et son inverse se construit par récurrence. □

**Remarque 3.10.1.** *L'inverse de $-(X^T - 1)$ est la série formelle $1 + X^T + X^{2T} + \ldots$.*

**Lemme 3.10.2.** *$k[X]_{(X)}$ le localisé de $k[X]$ en $k[X] \setminus (X)$ s'injecte naturellement dans l'anneau des séries formelles $k[[X]]$ par l'application qui à toute fraction rationnelle $\frac{a(X)}{b(X)}$ avec $b(0) \neq 0$ associe le produit $a(X)b(X)^{-1}$ où $b(X)^{-1}$ est l'inverse de $b(X)$ en tant que série formelle.*

*Démonstration.* En effet, le polynôme $b(X)$ est identifié canoniquement à sa série formelle finie et la condition $b_0 = b(0) \neq 0$ implique d'après le lemme 3.10.1 l'inversibilité de $b(X)$. □

**Théorème 3.10.1.** *Soit $a(X)$ une série formelle non-nulle et $\underline{a}$ la séquence extraite. Considérons les assertions suivantes :*

1. *$a(X) \in k[X]_{(X)}$ ; c'est-à-dire que $a(X) = \frac{f(X)}{q(X)}$ tel que $q(0) \neq 0$.*
2. *$\underline{a}$ est récurrente linéaire, c'est-à-dire qu'elle vérifie la relation de récurrence linéaire*

$$q_0 a_n + q_1 a_{n-1} + \ldots + q_r a_{n-r} = 0,$$

   *pour tout $n \geq N$ tel que $N \geq r$, $q_0 \neq 0$ et $q_r \neq 0$.*
3. *$\underline{a}$ est strictement périodique (ou ultimement périodique de pré-période $t \geq 1$) de période $T \geq 1$.*
4. *$a(X) = \frac{h(X)}{X^T - 1}$ tel que $T \geq 1$ est minimal et $\deg(h) \leq T - 1$ (ou $\deg(h) = T + t - 1$ avec $t \geq 1$).*

*Alors 1) $\Leftrightarrow$ 2) $\Leftarrow$ 3) $\Leftrightarrow$ 4).*
*Si $k$ est fini, alors 1) $\Leftrightarrow$ 2) $\Leftrightarrow$ 3) $\Leftrightarrow$ 4). Dans ce cas, la période divise $\mathtt{ord}_q(X)$.*
*Si en plus $f$ et $q$ sont premiers entre eux, alors la période est $\mathtt{ord}_q(X)$.*

*Démonstration.* Si $a(X) \in k[X]_{(X)}$ alors par définition, $a(X) = \frac{f(X)}{q(X)}$ avec $X$ ne divisant pas $q(X)$ ce qui équivaut à dire que $q(0) \neq 0$. L'équation $q(X)a(X) = f(X)$ se traduit sur les coefficients par :

$$\begin{aligned} q_0 a_0 &= f_0 \\ q_1 a_0 + q_0 a_1 &= f_1 \\ &\vdots \\ q_r a_{m-r} + \ldots + q_1 a_{m-1} + q_0 a_m &= 0 \\ q_r a_{m+1-r} + \ldots + q_1 a_m + q_0 a_{m+1} &= 0 \\ &\vdots \end{aligned}$$

avec $m = \max(\deg(f) + 1, \deg(q))$. Donc $\underline{a}$ vérifie une relation de récurrente linéaire à partir de $N = \max(\deg(f) + 1, \deg(q))$.

Inversement, si $\underline{a}$ vérifie la relation de récurrence linéaire à partir du rang $N \geq r$ :

$$q_0 a_n + \ldots + q_r a_{n-r} = 0.$$

En posant $q(X) = q_r X^r + \ldots + q_1 X + q_0$, on trouve que

$$q(X)a(X) = q_0 a_0 + (q_1 a_0 + q_0 a_1)X + \ldots + (q_r a_0 + \ldots + q_0 a_r)X^r + \ldots + (q_r a_{N-r} + \ldots + q_0 a_N)X^N + \ldots$$

$q(X)a(X)$ est donc un polynôme de degré inférieur ou égale à $N-1$. Comme $q_0 \neq 0$, $q(X)$ est inversible dans $k[[X]]$ et $a(X) = \frac{f(X)}{q(X)}$ avec $\deg(f) \leq N-1$. On trouve alors que $N \geq \max(\deg(f)+1, \deg(q))$.

Si $\underline{a}$ est ultimement périodique de période $T$ et de pré-période $t \geq 1$, alors :

$$\begin{aligned} a(X) = & \quad a_0 + \ldots + a_{t-1}X^{t-1} + X^t(a_t + \ldots + a_{t+T-1}X^{T-1})(1 + X^T + X^{2T} + \ldots) \\ = & \quad g(X) - X^t \tfrac{f(X)}{X^T-1}, \end{aligned}$$

où $\deg(g) \leq t-1$ et $\deg(f) \leq T-1$. On pose $h(X) = g(X)(X^T-1) - X^t f(X)$ et on trouve $a(X) = \frac{h(X)}{X^T-1}$. Le coefficient dominant de $h(X)$ est $a_{t-1} - a_{T+t-1}$ qui est non-nul car sinon la séquence serait de pré-période inférieure ou égale à $t-1$.

Si $\underline{a}$ est strictement périodique de période $T$, alors $h(X) = -(a_0 + \ldots + a_{T-1}X^{T-1})$ et $\deg(h) \leq T-1$.

Inversement, si $a(X) = \frac{h(X)}{X^T-1}$ tel que $\deg(h) \leq T-1$, alors $a(X) = h(X)(X^T-1)^{-1} = -h(X)(1 + X^T + \ldots)$. En posant $-h(X) = a_0 + \ldots + a_{T-1}X^{T-1}$, on a que

$$a(X) = a_0 + \ldots + a_{T-1}X^{T-1} + a_0X^T + \ldots + a_{2T-1}X^{2T-1} + \ldots$$

$\underline{a}$ est strictement périodique. La période est le plus petit $T$.

Si $a(X) = \frac{h(X)}{X^T-1}$ avec $\deg(h) \geq T$ et $T \geq 1$ minimal, alors on peut faire la division euclidienne de $h(X)$ par $X^T-1$ puisque $k[X]$ est euclidien. Il existe $u(X)$ et $v(X)$ tels que $h(X) = (X^T-1)u(X) + v(X)$ et $\deg(v) < T$.

$$a(X) = u(X) + \frac{v(X)}{X^T-1}.$$

La suite extraite de $\frac{v(X)}{X^T-1}$ est strictement périodique de longueur $T$. La séquence extraite de $u(X)$ est ultimement périodique de période 1 et de pré-période $\deg(u)$. La séquence $\underline{a}$ s'obtient en sommant terme à terme ces deux séquences extraites. La séquence $\underline{a}$ est ultimement périodique de pré-période $t' \leq \deg(v)$ et de période $T' \leq T$. Alors $a(X) = \frac{s(X)}{X^{T'}-1}$ avec $\deg(s) = T' + t' - 1$. Comme $T$ est minimal, on en déduit que $T = T'$ puis que $s(X) = h(X)$. La pré-période vérifie alors $\deg(h) = T + t' - 1$.

Une séquence périodique est évidemment récurrente linéaire. L'assertion 3) implique l'assertion 2). Parallèlement 4) $\Rightarrow$ 1) en prenant $q(X) = X^T - 1$.

Si $k$ est fini, 1) $\Rightarrow$ 4) car $q(X)$ vérifiant $q(0) \neq 0$ possède un ordre, c'est un plus petit entier $T$ tel que $q(X)$ divise $X^T-1$. C'est aussi l'ordre de $X$ modulo $q(X)$. La période de $\underline{a}$ divise donc $\mathtt{ord}_q(X)$. Si en plus $f$ et $q$ sont premiers entre eux, $q$ divise $X^T-1$ avec $T$ minimal. Donc $\mathtt{ord}_q(X)$ divise $T$ la période. Parallèlement si $k$ est fini, alors 2) $\Rightarrow$ 3). En effet si $\underline{a}$ est récurrente linéaire, posons les états $e_n = (a_{n-r}, \ldots, a_{n-1})$ pour $n \geq N$. L'état $e_{n+1}$ est déterminé à partir de $e_n$ par la relation de récurrence linéaire. Il y a $|k|^r$ états différents, donc il y a un premier état $e_t$ qui est récurrent, c'est à dire qu'il existe un plus petit $t$ et un plus petit $T \leq |k|^r$, tels que $e_{t+T} = e(t)$. À partir de là, on voit que la suite des états est périodique et donc que la séquence est périodique. □

### 3.10.4 Valuation $p$-adique

Considérons $\mathbb{Z}$ l'anneau euclidien des entiers relatifs et son corps des fractions $\mathbb{Q}$.

**Définition 3.10.5** (valuation ou ordre $p$-adique)**.** *Tout entier $z$ peut s'écrire comme produit $p^{r(z)}z_0$ avec $z_0$ premier avec $p$. Pour toute fraction rationnelle $f = \frac{x}{y}$, on lui associe l'entier $r(f) = r(x) - r(y)$ appelé l'ordre $p$-adique de $f$. On définit alors l'application $r : \mathbb{Z} \to \mathbb{Z}$. On définit la valuation $p$-adique d'une fraction rationnelle $f$ par $v(f) = \frac{1}{p^{r(f)}}$. C'est une application $v : \mathbb{Z} \to \mathbb{R}_+$.*

**Proposition 3.10.4.** *La valuation $p$-adique est une valuation discrète sur $\mathbb{Q}$ d'uniformisante $p$.*

*Démonstration.* La démonstration utilise les mêmes arguments que la démonstration de la proposition 3.10.1. □

**Proposition 3.10.5.** *L'anneau de valuation de $\mathbb{Q}$ pour la valuation $p$-adique est l'anneau localisé de $\mathbb{Z}$ en $\mathbb{Z} \setminus (p)$. L'idéal maximal $(p)$ est l'unique idéal premier de cet anneau. Son corps résiduel est $\mathbb{F}_p$ et on note cet anneau local $\mathbb{Z}_{(p)}$.*

*Démonstration.* $\mathbb{Q}$ est un corps muni d'une valuation discrète et son anneau de valuation $\mathcal{O}$ est l'ensemble des éléments de valuation $p$-adique inférieure ou égale à 1.

$$\begin{aligned} f = \tfrac{x}{y} \in \mathcal{O} &\Leftrightarrow r(x) - r(y) \geq 0 \\ &\Leftrightarrow f = \tfrac{p^{r(x)-r(y)}x_0}{y_0} \\ &\Leftrightarrow f \in (\mathbb{Z} \setminus (p))^{-1}\mathbb{Z}. \end{aligned}$$

L'ensemble $\mathbb{Z} \setminus (p)$ est constitué des éléments inversibles de l'anneau $\mathbb{Z}_{(p)}$ et donc l'idéal engendré par $p$ dans cet anneau est maximal, c'est même l'unique idéal premier. Le corps résiduel de $\mathbb{Z}_{(p)}$ est le corps $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. En effet, en utilisant l'homomorphisme surjectif d'anneau de $\mathbb{Z}_{(p)}$ dans $\mathbb{F}_p$ qui à toute fraction rationnelle $\frac{x}{y}$ associe l'élément $x(\mathtt{mod}p)(y(\mathtt{mod}p))^{-1}$, on trouve que le noyau est l'idéal engendré par $p$ et le reste suit. □

**Proposition 3.10.6.** *Le complété de $\mathbb{Q}$ pour la valuation $p$-adique est le corps des nombres $p$-adiques $\mathbb{Q}_p$ dont les éléments sont toutes les séries de la forme*

$$\sum_{-\infty<<i} a_i p^i$$

*avec $a_i$ éléments du corps $\mathbb{F}_p$. L'anneau de valuation de $\mathbb{Q}_p$ est l'anneau des entiers $p$-adiques $\mathbb{Z}_p$ dont les éléments sont les séries de la forme*

$$\sum_{i\in\mathbb{N}} a_i p^i$$

*avec $a_i$ éléments du corps $\mathbb{F}_p$. C'est un anneau de valuation discrète dont l'idéal maximal est $p\mathbb{Z}_p$. L'ensemble $\mathbb{Z}_p \setminus (p)$ est constitué des éléments inversibles de $\mathbb{Z}_p$.*

*Démonstration.* Cette proposition est une conséquence directe du thèorème 3.6.1. □

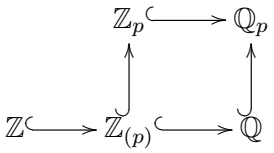



FIGURE 3.4 – Entiers $p$-adiques

### 3.10.5 Séquences périodiques, séquences récurrentes linéaires avec retenue et entiers $p$-adiques

Pour la suite, on notera respectivement $z(\texttt{div}p)$ et $z(\texttt{mod}p)$ le quotient et le reste de la division euclidienne de $z$ par $p$ dans $\mathbb{Z}$.

**Définition 3.10.6** (L'anneau des entiers $p$-adiques)**.** *L'anneau des entiers $p$-adiques est défini comme l'ensemble des séries infinies de la forme $a(X) = \sum_{i\in\mathbb{N}} a_i p^i$ muni de la somme avec retenue et de la multiplication avec retenue opérant de la manière suivante :*

$$\sum_{i\in\mathbb{N}} a_i p^i + \sum_{i\in\mathbb{N}} b_i p^i = \sum_{i\in\mathbb{N}} c_i X^i$$

*où les $c_i$ sont déterminés par l'algorithme suivant :*

$$\begin{aligned}
a_0 + b_0 = pm_1 + c_0 \quad & \textit{avec } m_1 = (a_0 + b_0)(\texttt{div}p) \\
& \textit{et } c_0 = (a_0 + b_0)(\texttt{mod}p) \\
a_1 + b_1 + m_1 = pm_2 + c_1 \quad & \textit{avec } m_2 = (a_1 + b_1 + m_1)(\texttt{div}p) \\
& \textit{et } c_1 = (a_1 + b_1 + m(1))(\texttt{mod}p) \\
a_2 + b_2 + m_2 = pm_3 + c_2 \quad & \textit{avec } m_3 = (a_2 + b_2 + m_2)(\texttt{div}p) \\
& \textit{et } c_2 = (a_2 + b_2 + m(2))(\texttt{mod}p) \\
& \vdots
\end{aligned}$$

$$\sum_{i\in\mathbb{N}} a_i X^i . \sum_{i\in\mathbb{N}} b_i X^i = \sum_{i\in\mathbb{N}} d_i X^i .$$

*où les $d_i$ sont déterminés par l'algorithme suivant :*

$$\begin{aligned}
a_0 b_0 = pn_1 + d_0 \quad & \textit{avec } n_1 = (a_0 b_0)(\texttt{div}p) \\
& \textit{et } d_0 = (a_0 b_0)(\texttt{mod}p) \\
a_1 b_0 + a_0 b_1 + n_1 = pn_2 + d_1 \quad & \textit{avec } n_2 = (a_1 b_0 + a_0 b_1 + n_1)(\texttt{div}p) \\
& \textit{et } d_1 = (a_1 b_0 + a_0 b_1 + n_1)(\texttt{mod}p) \\
a_2 b_0 + a_1 b_1 + a_0 b_2 + n_3 = pn_3 + d_2 \quad & \textit{avec } n3 = (a_2 b_0 + a_1 b_1 + a_0 b_2 + n_3)(\texttt{div}p) \\
& \textit{et } d_2 = (a_2 b_0 + a_1 b_1 + a_0 b_2 + n_3)(\texttt{mod}p) \\
& \vdots
\end{aligned}$$

**Lemme 3.10.3.** *Un entier $p$-adique $\sum_{i=0}^{i=+\infty} a_i p^i$ est inversible si et seulement si $a_0 \neq 0$.*

*Démonstration.* C'est un résultat déjà énoncé précédemment. En effet $\mathbb{Z}_p$ est un anneau de valuation discrète. L'idéal $p\mathbb{Z}_p$ engendré par $p$ est son unique d'idéal premier et $\mathbb{Z}_p \backslash p\mathbb{Z}_p$ le complémentaire de cet idéal est l'ensemble des inversibles de $\mathbb{Z}_p$. C'est l'ensemble des éléments dont le premier coefficient $a_0$ est non nul. On peut le prouver directement par construction en remarquant qu'un entier $p$-adique $a = \sum_{i=0}^{i=+\infty} a_i p^i$ est inversible si et seulement si il existe un autre entier $p$-adique $b = \sum_{i=0}^{i=+\infty} b_i p^i$ tel que $ab = 1$. En reprenant les notations des régles de la multiplication, on obtient que :

$$\begin{aligned} ab = 1 &\Leftrightarrow \exists b_0, b_1, \dots \text{ tels que } d_0 = 1 \text{ et } d_i = 0 \\ &\Leftrightarrow \exists b_0, b_1, \dots \text{ tels que } \begin{cases} d_0 = b_0 a_0 (\mathtt{mod} p) = 1, \\ d_1 = b_1 a_0 + b_0 a_1 + n_1 (\mathtt{mod} p) = 0, \\ \vdots \end{cases} \\ &\Leftrightarrow \begin{cases} a_0 \neq 0 \\ b_0 = a_0^{-1} (\mathtt{mod} p) \\ b_1 = -a_0^{-1} (b_0 a_1 + n_1) (\mathtt{mod} p) \\ \vdots \end{cases} \end{aligned}$$

Donc $a$ est inversible si et seulement si $a_0 \neq 0$ et son inverse se construit par récurrence. □

**Remarque 3.10.2.** *L'inverse de $-(p^T - 1)$ est l'entier $p$-adique $1 + p^T + p^{2T} + \dots$.*

**Lemme 3.10.4.** *$\mathbb{Z}_{(p)}$ le localisé de $\mathbb{Z}$ en $\mathbb{Z} \backslash p\mathbb{Z}$ s'injecte naturellement dans $\mathbb{Z}_p$, l'anneau des entiers $p$-adiques, par l'application qui à toute fraction $\frac{a}{b}$ telle que $b(0) \neq 0$ associe le produit $ab^{-1}$ où $b^{-1}$ est l'inverse de $b$ en tant qu'entier $p$-adique.*

*Démonstration.* En effet, $b$ est identifié canoniquement à lui-même en tant qu'entier $p$-adique fini et la condition $b_0 = b(0) \neq 0$ implique d'après le lemme 3.10.3 l'inversibilité de $b$. □

**Proposition 3.10.7.** *Soit $a$ un entier $p$-adique. Alors*

$$a \in \mathbb{Q} \Leftrightarrow a \in \mathbb{Z}_{(p)}$$

*Démonstration.* Si $a \in \mathbb{Q}$, alors il existe deux entiers $s$ et $q$ premiers entre eux tels que $a = \frac{s}{q}$. Si $p$ divise $s$, alors il ne divise pas $q$ et donc $a \in \mathbb{Z}_{(p)}$. Sinon $s$ est un entier inversible dans $\mathbb{Z}_p$. Du coup $\frac{1}{q} = s^{-1} a \in \mathbb{Z}_p$. Or $\frac{1}{q}$ est l'inverse de $q$ dans $\mathbb{Q} \subseteq \mathbb{Q}_p$. C'est aussi l'inverse de $q$ dans $\mathbb{Z}_p$. D'après le lemme 3.10.3, on en conclut que $p$ ne peut pas diviser $q$. □

**Théorème 3.10.2.** *Soit $a$ un entier $p$-adique et $\underline{a}$ sa séquence associée. Alors :*

1. *$\underline{a}$ est périodique si et seulement si $a \in \mathbb{Q}$.*

2. *$\underline{a}$ est strictement périodique de période $T$ si et seulement si $a = \frac{s}{q} \in \mathbb{Q}$ tel que $-q \leq s \leq 0$, $\texttt{PGCD}(s,q) = 1$ et $\texttt{ord}_q(p) = T$. L'écriture est unique.*
3. *$\underline{a}$ est ultimement périodique de pré-période $t$ et de période $T$ si et seulement si $a = u + p^t \frac{s}{q} \in \mathbb{Q}$ tel que $-q \leq s \leq 0$, $0 \leq u \leq p^t - 1$, $\texttt{PGCD}(s,q) = 1$, $t$ est minimal et $\texttt{ord}_q(p) = T$. L'écriture est unique.*

*Démonstration.* Si $\underline{a}$ est strictement périodique de période $T$, alors

$$\begin{aligned} a &= (a_0 + \ldots + a_{T-1}p^{T-1})(1 + p^T + p^{2T} + \ldots) \\ &= \tfrac{f}{p^T-1}, \end{aligned}$$

où $f = -(a_0 + \ldots + a_{T-1}p^{T-1})$. On vérifie que $-(p^T - 1) \leq f \leq 0$. Si on pose $a = \frac{s}{q}$ avec $s$ et $q$ premiers entre eux, on trouve que $-q \leq s \leq 0$ et $q$ divise $p^T - 1$. Donc $\texttt{ord}_q(p)$ existe et $\texttt{ord}_q(p)$ divise $T = \texttt{per}(\underline{a})$.

Inversement, si $a = \frac{s}{q}$ vérifie les conditions de 1), alors $p \in (\mathbb{Z}/q\mathbb{Z})^*$ et l'ordre de $p$ modulo $q$ existe. Il existe un entier $T \geq 1$ tel que $q$ divise $p^T - 1$.

$$a = \frac{s\frac{p^T-1}{q}}{p^T-1} = \frac{f}{p^T-1}.$$

$-(p^T - 1) \leq f = \frac{s}{q}(p^T - 1) \leq 0$ implique que $-f$ admet un développement $p$-adique fini $-f = a_0 + \ldots + a_{T-1}p^{T-1}$. L'inverse de $-(p^T - 1)$ dans $\mathbb{Z}_p$ est $1 + p^T + p^{2T} + \ldots$. On obtient alors :

$$a = (a_0 + \ldots + a_{T-1}p^{T-1})(1 + p^T + p^{2T} + \ldots).$$

$\underline{a}$ est donc une séquence strictement périodique de longueur $T$. On a prouvé précédemment que $a = \frac{g}{p^{\texttt{per}(\underline{a})}-1}$ et on vient de prouver que $\texttt{per}(\underline{a}) \leq T$. Comme $s$ et $q$ sont premiers entre eux, alors $q$ divise $p^{\texttt{per}(\underline{a})} - 1$. Par définition de l'ordre d'un entier modulo $q$, $T \leq \texttt{per}(\underline{a})$. La condition $s$ et $q$ premiers entre eux implique donc que $\texttt{per}(\underline{a}) = \texttt{ord}_q(p)$. Le point 2) est prouvé.

Si $\underline{a}$ est ultimement périodique de période $T$ et de pré-période $t \geq 1$, alors le développement $p$-adique de $a$ s'écrit :

$$\begin{aligned} a &= a_0 + \ldots + a_{t-1}p^{t-1} + p^t(a_t + \ldots + a_{T-1}p^{T-1})(1 + p^T + p^{2T} + \ldots) \\ &= (a_0 + \ldots + a_{t-1}p^{t-1}) - p^t\tfrac{a_t+\ldots+a_{T-1}p^{T-1}}{p^T-1} \\ &= v + p^t\tfrac{f}{p^T-1}, \end{aligned}$$

où $0 \leq v \leq p^t - 1$ et $-(p^T - 1) \leq f \leq 0$. En posant $a = u + p^t\frac{s}{q}$ tel que $s$ et $q$ soient premiers entre eux, on trouve que $q$ divise $(uq + p^t s)(p^T - 1)$. L'entier $p^t$ est premier avec $q$, d'après le lemme 3.10.7. On en déduit que $q$ est premier à $uq + p^t s$, donc $q$ divise $p^T - 1$ et par définition de l'ordre de $p$ modulo $q$, $\texttt{ord}_q(p)$ divise $\texttt{per}(\underline{a})$. Les inégalités sont

vérifiées. Par définition, la pré-période est le minimum des $t \geq 1$ vérifiant cette équation.

Inversement, supposons que $a = u + p^t \frac{s}{q}$ vérifie les conditions du 3). La fraction $\frac{s}{q}$ a un développement $p$-adique strictement périodique de période $\mathtt{ord}_q(p)$. Les conditions du 3) donnent les développements $p$-adiques suivants :

$$u = a_0 + \ldots + a_{t-1}p^{t-1} \text{ et } -s\frac{p^T-1}{q} = a_t + \ldots + a_{t+T-1}p^{T-1}.$$

On obtient une séquence $\underline{a}$ périodique de période $\mathtt{ord}_q(p)$. Supposons que $\underline{a}$ soit strictement périodique, alors le $t$ minimal serait 0 ce qui n'est pas le cas, donc $\underline{a}$ est ultimement périodique de pré-période $t$ et de période $\mathtt{ord}_q(p)$. Le point 3) est prouvé.

On a aussi prouvé la première implication du point 1).

Montrons que si $a$ est rationnel alors $\underline{a}$ est périodique. Supposons que $a = \frac{s}{q}$ avec $s$ et $q$ premiers entre eux. D'après la proposition 3.10.7, $p$ ne divise pas $q$. Posons $s = p^r s'$ avec $p$ ne divisant pas $s'$. Comme $p$ ne divise pas $q$, alors l'ordre de $p$ modulo $q$ existe, ce qui signifie que pour $T = \mathtt{ord}_q(p) \geq 1$, $q$ divise $p^T - 1$. On a donc $a = p^r \frac{s' \frac{p^T-1}{q}}{p^T-1} = p^r \frac{f}{p^T-1}$. On cherche à écrire $f$ sous la forme $(p^T-1)u - p^t v$ tels que $t \geq 0$, $0 \leq u \leq p^t - 1$ et $0 \leq v \leq p^T - 1$.

Si $f = 0$, alors $a = 0$ et $\underline{a}$ est la séquence nulle, donc strictement périodique.

Si $f > 0$, alors il existe un plus petit $t$ tel que $0 < f \leq p^t - 1$. Les entiers $p^t$ et $p^T - 1$ sont premiers entre eux. Le théorème de Bézout implique l'existence de $u$ et $v$ tels que $(p^T-1)u - p^t v = 1$. En multipliant par $f$, on trouve alors l'existence d'une solution pour l'équation $(p^T-1)u - p^t v = f$. La division euclidienne de $u$ par $p^t$ donne l'existence de $u'$ et $u''$ tels que $u = p^t u' + u''$ et $0 \leq u'' < p^t$. On a alors comme solution le couple $(u'', v-(p^T-1)u')$. Au final, il existe donc un couple $(u, v)$ solution de $(p^T-1)u - p^t v = f$ tel que $0 \leq u < p^t$. Dans ce cas, $0 \leq v \leq p^T - 1$. En effet :

$$\begin{aligned} 0 < f < p^t &\Rightarrow p^t v < (p^T-1)u < p^t(v+1) \Rightarrow \left\{ \begin{array}{l} p^t(v+1) > 0 \\ p^t v < (p^T-1)u < (p^T-1)p^t \end{array} \right. \\ &\Rightarrow \left\{ \begin{array}{l} v > -1 \\ v < (p^T-1) \end{array} \right. \end{aligned}$$

Donc, nous avons trouvé une solution $(u, v)$ vérifiant les conditions recherchées. En écrivant le développement $p$-adique de $u = a_0 + \ldots + a_{t-1}p^{t-1}$, $v = a_t + \ldots + a_{t+T-1}p^{T-1}$ et $-(p^T-1) = 1 + p^T + p^{2T} + \ldots$, On trouve que le développement $p$-adique de $\frac{f}{p^T-1}$ est de la forme

$$u - p^t \frac{v}{p^T-1} = (a_0 + \ldots + a_{t-1}p^{t-1}) + a_t p^t + \ldots + a_{t+T-1}p^{t+T-1} + \ldots$$

En multipliant par $p^r$, on décale la séquence vers la droite et on a

$$a = p^r u - p^{r+t} \frac{v}{p^T-1},$$

$$\underline{a} = (\underbrace{0, \ldots, 0}_{r}, \underbrace{a_0, \ldots, a_{t-1}}_{t}, \underbrace{a_t, \ldots, a_{t+T-1}}_{T}, \ldots$$

On obtient une séquence périodique. Le point 1) est démontré. La période divise $\mathtt{ord}_q(p)$. Comme $\underline{a}$ est périodique, on a vu précédemment que $a = \frac{g}{p^{\mathtt{per}(\underline{a})}-1}$. Les entiers $s$ et $q$ étant premiers entre eux, alors $q$ divise $p^{\mathtt{per}(\underline{a})}-1$. Par définition, $\mathtt{ord}_q(p)$ divise $\mathtt{per}(\underline{a})$, donc ils sont égaux. Si $f > 0$, la séquence est ultimement périodique. La pré-période est comprise entre $r$ et $r+t$. Avec $t$ minimal, on obtient la pré-période. Donc $a$ s'écrit comme dans le point 2) avec toutes les conditions posées.

Si $-(p^T-1) \leq f < 0$, $\underline{a}$ est strictement périodique si et seulement si $r = 0$. La séquence $\underline{a}$ est ultimement périodique si et seulement si $r > 0$. La période est $\mathtt{ord}_q(p)$. On le prouve avec les arguments précédents.

Si $f < -(p^T-1)$, alors la séquence ne peut pas être strictement périodique. Soit le plus petit entier $t$ tel que $-(p^t-1) \leq f < -(p^T-1)$. Comme précédemment, on trouve des $u$ et $v$ tels que $(p^T-1)u - p^t v = f$. La division euclidienne de $u$ par $p^t$ donne l'existence de $u^{'}$ et $u^{''}$ tels que $u = p^t u^{'} + u^{''}$ et $0 \leq u^{''} < p^t$. On a alors comme solution le couple $(u^{''}, v-(p^T-1)u^{'})$. Au final, il existe donc un couple $(u,v)$ solution de $(p^T-1)u - p^t v = f$ tel que $0 \leq u < p^t$. Dans ce cas, $0 \leq v \leq p^T - 1$. En effet :

$$\begin{aligned}
-p^t < (p^T-1)u - p^t v < -(p^T-1) &\Leftrightarrow \begin{cases} p^t(v-1) < (p^T-1)u \\ (p^T-1)(u+1) < p^t v \end{cases} \\
&\Leftrightarrow \begin{cases} p^t(v-1) < (p^T-1)p^t \\ (p^T-1) < p^t v \end{cases} \\
&\Leftrightarrow \begin{cases} v < p^T \\ 0 < \frac{p^T-1}{p^t} < v \end{cases}
\end{aligned}$$

$a$ s'écrit sous la forme $p^r u - p^{t+r}\frac{v}{p^T-1}$ avec les conditions recherchées, donc $\underline{a}$ est ultimement périodique de pré-période $r+t$ où $t$ est minimal et de période $\mathtt{ord}_q(p)$.

Il reste à montrer l'unicité. Supposons que l'on ait deux écritures vérifiant les conditions du 2).

$$a = u + 2^t\frac{s}{q} = u^{'} + p^{t^{'}}\frac{s^{'}}{q^{'}}$$

Par définition de la minimalité $t$ est unique, donc $t = t^{'}$. Les arguments précédant prouvent que $q$ divise $q^{'}$ et réciproquement $q^{'}$ divise $q$. Donc $q = q^{'}$. On trouve alors que $(u-u^{'})q = (s^{'}-s)p^t$. Les entiers $q$ et $p$ étant premiers entre eux, alors $p^t$ est premier avec $q$, donc $p^t$ divise $u-u^{'}$. Par hypothèse $0 \leq u, u^{'} \leq p^t - 1$, donc $-p^t < u - u^{'} < p^t$. La seule possibilité est $u - u^{'} = 0$, ce qui implique $s - s^{'} = 0$. L'unicité de cette écriture est démontrée.

□

**Remarque 3.10.3.** *Dans le cas des séries formelles, la séquence correspondante est périodique si et seulement si la série formelle peut s'écrire sous forme de fraction rationnelle*

*de dénominateur $X^T - 1$ et elle est récurrente linéaire si et seulement si le dénominateur ne s'annule pas en 0. Il y a équivalence entre la périodicité et la récurrence linéaire si $k$ est fini. L'argument central est l'existence dans le cas fini de l'ordre de $X$ modulo $q(X)$ si $q(X)$ est premier avec $X$.*

*Dans le cas des entiers p-adiques, le corps $k$ est $\mathbb{F}_p$, il est donc fini, ce qui implique l'existence de l'ordre de $p$ modulo $q$ pour tout $q$ premier avec $p$. Il y a directement équivalence entre la périodicité et l'écriture en fraction de dénominateur $q$ premier avec $p$. C'est pourquoi la notion de récurrence linéaire avec retenue n'a pas besoin d'apparaître ici. Le théorème suivant fait le lien entre périodicité, récurrence linéaire avec retenue et écriture sous forme d'un rationnel.*

**Théorème 3.10.3.** *Soit $a$ un entier p-adique et $\underline{a}$ sa séquence extraite. Les assertions suivantes sont équivalentes :*

1. *$\underline{a}$ est périodique.*
2. *$a \in \mathbb{Z}_{(p)}$, c'est-à-dire $a = \frac{s}{q}$ tel que $p$ et $q$ premiers entre eux.*
3. *$\underline{a}$ est récurrente linéaire avec retenue, c'est-à-dire qu'elle vérifie la relation*

$$q_0 a_n + \ldots + q_r a_0 + m_{n-1} = p m_n,$$

*pour tout $n \geq N \geq r$ où $(m_{n-1}, m_n, \ldots)$ est une suite entière déterminée, $q_0 \neq 0$ et $q_r \neq 0$.*

*Démonstration.* Les points 1) et 2) sont équivalents d'après le théorème 3.10.2.

Si $a = \frac{s}{q}$ avec $q$ et $p$ premiers entre eux. Alors $q$ peut s'écrire $q = q_r p^r + \ldots + q_1 p + q_0$ avec $q_0 \neq 0$ et $q_r \neq 0$. L'égalité $qa = s$ se traduit sur les coefficients par identification

$$\begin{aligned}
(q_0 a_0)(\texttt{mod}p) &= s_0 \\
(q_0 a_0)(\texttt{div}p) &= m_0 \\
(q_0 a_1 + q_1 a_0 + m_0)(\texttt{mod}p) &= s_1 \\
(q_0 a_1 + q_1 a_0 + m_0)(\texttt{div}p) &= m_1 \\
&\vdots \\
(q_0 a_n + \ldots + q_r a_{n-r} + m_{n-1})(\texttt{mod}p) &= 0 \\
(q_0 a_n + \ldots + q_r a_{n-r} + m_{n-1})(\texttt{div}p) &= m_n \\
&\vdots
\end{aligned}$$

On a donc construit la suite des retenues $(m_{n-1}, m_n, \ldots)$ telles que $\underline{a}$ vérifie la relation de récurrence avec cette suite de retenue pour tout $n \geq N = \max([\log_p(s)] + 1, [\log_p(q)])$.

Inversement, si $\underline{a}$ vérifie cette relation, alors par calcul direct, on a :

$$\begin{aligned}
qa &= q_0 a_0 + (q_1 a_0 + q_0 a_1)p + \ldots + (q_r a_{N-r} + \ldots + q_0 a_N)p^N + \ldots \\
&= q_0 a_0 + (q_1 a_0 + q_0 a_1)p + \ldots + (p m_N - m_{N-1})p^N + (p m_{N+1} - m_N)p^{N+1} \ldots \\
&= q_0 a_0 + \ldots + (q_{N-1} a_0 + \ldots + q_r a_{N-1-r})p^{N-1} - m_{N-1} p^N \\
qa &\in \mathbb{Z}
\end{aligned}$$

Comme $q_0 \neq 0$, alors $q$ est inversible dans $\mathbb{Z}_p$. Donc $a = \frac{s}{q}$ dans $\mathbb{Z}_p$. On a prouvé que les points 2) et 3) sont équivalents. □

## 3.11 Conclusion : Lien entre Valuations discrètes, séquences et Registres à Rétroaction

Dans notre étude, nous nous intéressons aux registres à rétroaction ou feedback registers (FR) construits sur un corps fini $k = \mathbb{F}_{p^f}$. Les séquences de sorties $(a_0, a_1, \ldots)$ sont associées à la série formelle $\sum_{i=0}^{i=+\infty} a_i \pi^i$ ayant un sens dans un espace, en l'occurrence les corps de valuation discrète complets de corps résiduel $k$ et d'uniformisante $\pi$.

**Classification des a.v.d complets** D'après les résultats développés dans ce chapitre, si le corps résiduel est fini, il existe trois cas qui nous intéressent :

1. le cas d'égale caractéristique : $K \cong k((X))$ et $\mathcal{O} \cong k[[X]]$.
2. le cas d'inégale caractéristique absolument non-ramifié : $K \cong \texttt{Frac}(W(k))$ et $\mathcal{O} \cong W(k)$. Le corps $K$ est $\mathbb{Q}_p$-espace vectoriel de dimension $f$.
3. le cas d'inégale caractéristique totalement ramifié : $K$ est un $\mathbb{Q}_p$-espace vectoriel de dimension $ef$ où $e$ est l'indice de ramification absolu.

L'idée principale de notre thèse est qu'il existe une classification des registres à rétroaction équivalente ou semblable à la classification des anneaux de valuation discrète complets de corps résiduel fini.

**Classification des registres à rétroaction**

1. Les LFSRs étant des registres linéaires dont la fonction de rétroaction est basée sur une addition sans retenue correspondent au premier cas. Les LFSRs se construisent facilement sur $\mathbb{F}_{p^f}$ pour tout $f \geq 1$. La figure 3.5 illustre le mode opératoire d'un LFSR et sa relation avec l'anneau des séries formelles.

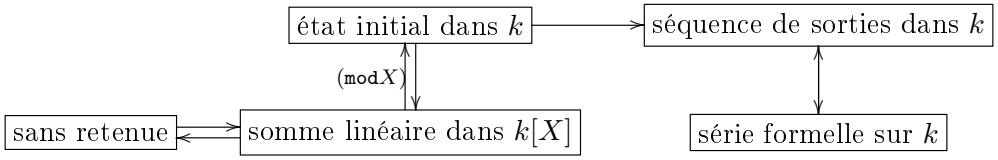



FIGURE 3.5 – LFSR et Anneau des séries formelles.

2. Les FCSRs étant des registres dont la fonction de rétroaction est basée sur une addition avec retenue correspondent au deuxième cas. Les FCSRs ont surtout été développés sur le corps premier $\mathbb{F}_p$. Leur construction sur $\mathbb{F}_{p^f}$ et l'analyse des séquences de sorties nécessitent l'utilisation des vecteurs de Witt sur $\mathbb{F}_{p^f}$. Les vecteurs de Witt ont une structure d'anneau où l'addition et la multiplication sont compliquées. C'est pourquoi nous avons développé l'analyse vectorielle des FCSRs. La figure 3.6 illustre le mode opératoire d'un FCSR et sa relation avec l'anneau des entiers $p$-adiques.

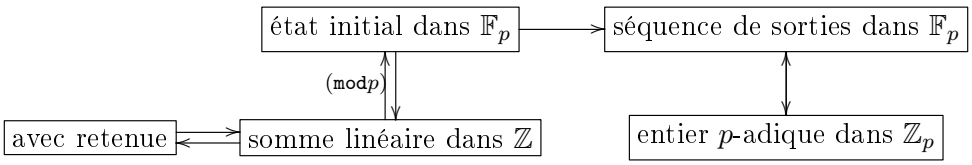



FIGURE 3.6 – FCSR et Anneau des entiers $p$-adiques.

3. Les $d$-FCSRs sont des registres dont la fonction de rétroaction est basée sur une addition avec retenues et un saut. Le saut s'interprète comme le degré de ramification. Les $d$-FCSRs correspondent donc au troisième cas avec $e = d$. De même les $d$-FCSRs ont surtout été développés sur les corps premiers $\mathbb{F}_p$. Il reste donc à étendre leur conception sur tout corps fini. On suggère d'utiliser la conception vectorielle et l'analyse vectorielle comme outil pour étudier ces registres. La figure 3.7 illustre le mode opératoire d'un LFSR et sa relation avec l'anneau des séries formelles.

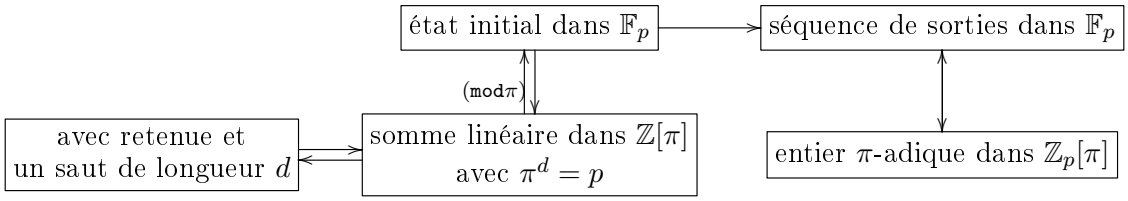



FIGURE 3.7 – $d$-FCSR et Anneau des entiers $\pi$-adiques.

Le tableau 3.1 résume l'idée centrale de cette thèse :

| Caractéristique | Degré de ramification | Corps résiduel | Uniformisante | Anneaux de valuation discrète | Registre correspondant |
|---|---|---|---|---|---|
| $\mathtt{car}(K) = p$<br>$\mathtt{car}(k) = p$ | | $\mathbb{F}_{p^f}$ | $X$ | $\mathbb{F}_{p^f}[[X]]$ | LFSR sur $\mathbb{F}_{p^f}$ |
| $\mathtt{car}(K) = 0$ | $d = 1$ | $\mathbb{F}_p$ | $p$ | $W(\mathbb{F}_p) = \mathbb{Z}_p$ | FCSR |
| | | $\mathbb{F}_{p^f}, f > 1$ | $p$ | $W(\mathbb{F}_{p^f})$ | VFCSR |
| $\mathtt{car}(k) = p$ | $d > 1$ | $\mathbb{F}_p$ | $\pi; \pi^d = p$ | $W(\mathbb{F}_p)[\pi] = \mathbb{Z}_p[\pi]$ | $d$-FCSR |
| | | $\mathbb{F}_{p^f}, f > 1$ | $\pi; \pi^d = p$ | $W(\mathbb{F}_{p^f})[\pi]$ | $d$-VFCSR |

TABLE 3.1 – Classification des a.v.ds et des registres à rétroaction.

**Classification des séquences récurrentes linéaires avec ou sans retenue** On peut ajouter que les séquences récurrentes linéaires peuvent être classifiées en trois catégories :

1. Les séquences "purement" récurrentes linéaires dans $k$, c'est-à-dire qu'elles vérifient une relation de récurrence linéaire $q_0 a_n + \ldots + q_r a_{n-r} = 0$, pour tout $n \geq N$ où $N$ est un certain entier plus grand que $r$ et où $q_0, \ldots, q_r$ sont des coefficients dans $k$ avec $q_0, q_r \neq 0$.
2. Les séquences récurrentes linéaires dans $\mathbb{F}_p$ avec retenues entières, c'est-à-dire qu'elles vérifient une relation de récurrence linéaire avec retenue $q_0 a_n + \ldots + q_r a_{n-r} + m_{n-1} = pm_n$, pour tout $n \geq N$ où $N$ est un certain entier plus grand que $r$, où $q_0, \ldots, q_r$ sont des coefficients dans $\mathbb{F}_p$ avec $q_0$ et $q_r \neq 0$ et où $(m_{n-1}, m_n, \ldots)$ est une suite déterminée dans $\mathbb{Z}$.
3. Les séquences récurrentes linéaires dans $\mathbb{F}_p$ avec retenues et avec saut, c'est-à-dire qu'elles vérifient une relation de récurrence linéaire avec retenue $q_0 a_n + \ldots + q_r a_{n-r} + m_{n-1} = \pi m_n$, pour tout $n \geq N$ où $N$ est un certain entier plus grand que $r$, où $q_0, \ldots, q_r$ sont des coefficients dans $\mathbb{F}_p$ avec $q_0, q_r \neq 0$, où $\pi^d = p$ et où $(m_{n-1}, m_n, \ldots)$ est une suite déterminée dans $\mathbb{Z}[\pi]$.

Les séquences sur les corps finis et vérifiant ces relations, les registres à décalage et à rétroaction construits sur les corps finis et les anneaux de valuation discrète complets de corps résiduel fini se subdivisent tous en trois catégories. Le tableau 3.2 illustre ce parallèle.

| Familles de séquences | Anneaux de valuation discrète complets | registres à décalage et à rétroaction |
|---|---|---|
| récurrentes linéaires | $\mathbb{F}_{p^f}[[X]]$ | LFSR sur $\mathbb{F}_{p^f}$ |
| récurrentes linéaires avec retenue | $W(\mathbb{F}_p) = \mathbb{Z}_p$ | FCSR |
| vectorielles récurrentes linéaires avec retenue | $W(\mathbb{F}_{p^f}) \cong \mathbb{Z}_p[X]/(P)$, $f > 1$ | VFCSR |
| récurrentes linéaires avec retenue et avec saut | $W(\mathbb{F}_p)[\pi] = \mathbb{Z}_p[\pi]$ | $d$-FCSR |
| vectorielles récurrentes linéaires avec retenue et avec saut | $W(\mathbb{F}_{p^f})[\pi] = \mathbb{Z}_p[\pi, X]/(P)$, $f > 1$ | $d$-VFCSR |

TABLE 3.2 – Classification des a.v.ds, des séquences récurrentes et des FSRs.

# Chapitre 4

# Vecteurs de Witt relatifs à un nombre premier $p$ et Anneau $\mathbb{Z}_{p^n}$

## 4.1 Introduction

Dans ce chapitre, nous présentons les vecteurs de Witt à coefficient dans le corps fini $\mathbb{F}_{p^n}$ et leur relation avec les entiers $p$-adiques. L'anneau des vecteurs de Witt est l'unique anneau de valuation discrète complet de corps résiduel $\mathbb{F}_{p^n}$. Il joue donc un rôle central dans notre étude. Cependant la structure algébrique des vecteurs de Witt est assez complexe pour ne pas être appliquée à l'étude des registres à décalage et à rétroaction avec retenue construits sur $\mathbb{F}_{p^n}$. On utilisera donc une autre représentation des vecteurs de Witt. La majorité des démonstration sont tirées de [39] et de [32].

## 4.2 Polynômes de Witt

Soit $p$ un nombre premier et soit $\{X_i\}_{i\in\mathbb{N}}$ une suite d'indéterminées.

**Définition 4.2.1.** *Pour tout entier naturel $n$, on appelle $n$-ième polynôme de Witt de $\mathbb{Z}[X_0,\ldots,X_n]$ l'élément :*

$$\mathrm{W}_n(X_0,\ldots,X_n)=\sum_{i=0}^{i=n}p^iX_i^{p^{n-i}}=X_0^{p^n}+pX_1^{p^{n-1}}+\cdots+p^nX_n.$$

On notera abusivement ce polynôme par $\mathrm{W}_n$. On a en particulier :

$$\begin{aligned}\mathrm{W}_0 &= X_0\\ \mathrm{W}_1 &= X_0^p+pX_1\\ &\vdots\end{aligned}$$

Soit une autre suite d'indéterminées $\{Y_i\}_{i\in\mathbb{N}}$.

**Théorème 4.2.1.** *Pour tout polynôme $\Phi \in \mathbb{Z}[X,Y]$, il existe une unique suite $\{\phi_i\}_{i\in\mathbb{N}}$ de polynômes de $\mathbb{Z}[X_i,Y_i]_{i\in\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, $\phi_n \in \mathbb{Z}[X_0,\ldots,X_n,Y_0,\ldots,Y_n]$ et telle que l'on ait, pour tout $n \in \mathbb{N}$ :*

$$\mathrm{W}_n(\phi_0(X_0,Y_0),\ldots,\phi_n(X_0,\ldots,X_n,Y_0,\ldots,Y_n)) = \Phi(\mathrm{W}_n(X_0,\ldots,X_n),\mathrm{W}_n(Y_0,\ldots,Y_n)).$$

*Démonstration.* L'existence et l'unicité de cette suite dans $\mathbb{Z}[\frac{1}{p}][X_i,Y_i]_{i\in\mathbb{N}}$ est évidente. En effet, on trouve :

$$\begin{array}{lll}
n=0, & \mathrm{W}_0(\phi_0(X_0,Y_0)) & = \Phi(\mathrm{W}_0(X_0),\mathrm{W}_0(Y_0)) \\
& \Rightarrow \phi_0(X_0,Y_0) & = \Phi(X_0,Y_0), \\
n=1 & \mathrm{W}_1(\phi_0,\phi_1) & = \Phi(\mathrm{W}_1(X_0,X_1),\mathrm{W}_1(Y_0,Y_1)) \\
& \Rightarrow \phi_0^p + p\phi_1 & = \Phi(X_0^p+pX_1,Y_0^p+pY_1) \\
& \Rightarrow \phi_1(X_0,X_1,Y_0,Y_1) & = \frac{1}{p}(\Phi(X_0^p+pX_1,Y_0^p+pY_1) - \Phi(X_0,Y_0)^p), \\
& \vdots &
\end{array}$$

Montrons par récurrence que cette suite est à coefficients entiers.
Pour $n=0$, c'est évident puisque $\phi(X_0,Y_0) = \Phi(X_0,Y_0) \in \mathbb{Z}[X_0,Y_0]$.
Pour $n=1$, on voit que $\Phi(X_0^p+pX_1,Y_0^p+pY_1) \equiv \Phi(X_0^p,Y_0^p) \mod p$
et $\Phi(X_0,Y_0)^p \equiv \Phi(X_0^p,Y_0^p) \mod p$. Donc $p\phi_1 \equiv 0 \mod p$. On en déduit que $\phi_1$ est à coefficients entiers.
Supposons que la suite est à coefficient entier jusqu'à un rang $n-1$ quelconque fixé. Montrons que cela est vrai pour $\phi_n$. Par construction des polynômes de Witt :

$$\begin{array}{rcl}
\mathrm{W}_n(X_0,\ldots,X_n) & = & \mathrm{W}_{n-1}(X_0^p,\ldots,X_{n-1}^p) + p^n X_n \\
& \equiv & \mathrm{W}_{n-1}(X_0^p,\ldots,X_{n-1}^p) \mod p^n.
\end{array}$$

Par définition des $\phi_n$ :

$$\begin{array}{rcll}
\mathrm{W}_n(\phi_0,\ldots,\phi_n) & = & \Phi(\mathrm{W}_n(X_0,\ldots,X_n),\mathrm{W}_n(Y_0,\ldots,Y_n)) & \\
& \equiv & \Phi(\mathrm{W}_{n-1}(X_0^p,\ldots,X_{n-1}^p),\mathrm{W}_{n-1}(Y_0^p,\ldots,Y_{n-1}^p)) & \mod p^n \\
& \equiv & \mathrm{W}_{n-1}(\phi_0(X_0^p,Y_0^p),\ldots,\phi_{n-1}(X_0^p,\ldots,X_{n-1}^p,Y_0^p,\ldots,Y_{n-1}^p)) & \mod p^n \\
& \equiv & \phi_0(X_0^p,Y_0^p)^{p^{n-1}} + \ldots + p^{n-1}\phi_{n-1}(X_0^p,\ldots,X_{n-1}^p,Y_0^p,\ldots,Y_{n-1}^p) & \mod p^n.
\end{array}$$

De manière générale, soit un polynôme $\Psi(X) \in \mathbb{Z}[X]$ et $j$ un entier naturel. On trouve que $\Psi(X^p) \equiv \Psi(X)^p \mod p$ et $\Psi(X^p)^{p^j} \equiv \Psi(X)^{p^{j+1}} \mod p^{j+1}$. Ceci est vrai pour n'importe quel nombre d'indéterminées. On en déduit :

$$\begin{array}{rcl}
\mathrm{W}_n(\phi_0,\ldots,\phi_n) & \equiv & \phi_0^{p^n} + \ldots + p^{n-1}\phi_{n-1}^p \mod p^n \\
p^n\phi_n & \equiv & 0 \mod p^n.
\end{array}$$

Autrement dit $\phi_n$ est à coefficient entier. □

Dans la suite, on utilisera l'existence et l'unicité de ces polynômes à coefficients entiers en les indéterminées $\{X_n\}_{n\in\mathbb{N}}$ pour $\Phi(X,Y) = X+Y$ et $\Phi(X,Y) = XY$ et on utilisera les notations suivantes :

**Notation 4.2.1.** *On notera* $\{\mathrm{S}_n\}_{n\in\mathbb{N}}$ *les polynômes uniques vérifiant :*

$$\mathrm{W}_n(\mathrm{S}_0(X_0,Y_0),\ldots,\mathrm{S}_n(X_0,\ldots,X_n,Y_0,\ldots,Y_n)) = \mathrm{W}_n(X_0,\ldots,X_n)+\mathrm{W}_n(Y_0,\ldots,Y_n).$$

*On notera* $\{\mathrm{P}_n\}_{n\in\mathbb{N}}$ *les polynômes uniques vérifiant :*

$$\mathrm{W}_n(\mathrm{P}_0(X_0,Y_0),\ldots,\mathrm{P}_n(X_0,\ldots,X_n,Y_0,\ldots,Y_n)) = \mathrm{W}_n(X_0,\ldots,X_n)\mathrm{W}_n(Y_0,\ldots,Y_n).$$

On peut calculer ces polynômes pour les valeurs initiales :

$$\begin{array}{rcl}
\mathrm{S}_0(X_0,Y_0) & = & X_0+Y_0 \\
\mathrm{S}_1(X_0,X_1,Y_0,Y_1) & = & X_1+Y_1-\displaystyle\sum_{i=1}^{i=p-1}\frac{p!}{(p-i)!i!p}X_0^iY_0^{p-i} \\
\mathrm{P}_0(X_0,Y_0) & = & X_0Y_0 \\
\mathrm{P}_1(X_0,X_1,Y_0,Y_1) & = & X_0^pY_1+X_1Y_0^p+pX_1Y_1 \\
 & \vdots &
\end{array}$$

**Proposition 4.2.1.** *Il existe une unique suite de polynômes* $\{\mathrm{I}_i\}_{i\in\mathbb{N}}$ *dans* $\mathbb{Z}[X_i]_{i\in\mathbb{N}}$ *telle que* $\mathrm{I}_n\in\mathbb{Z}[X_0,\ldots,X_n]$ *et telle que l'on ait :*

$$\mathrm{W}_n(X_0,\ldots,X_n)+\mathrm{W}_n(\mathrm{I}_0,\ldots,\mathrm{I}_n)=0.$$

*Démonstration.* Cette suite $\{\mathrm{I}_i\}_{i\in\mathbb{N}}$ vérifie, pour tout $n\in\mathbb{N}$ :

$$\begin{array}{rcl}
\mathrm{W}_n(\mathrm{I}_0,\ldots,\mathrm{I}_n) & = & -\mathrm{W}_n(X_0,\ldots,X_n) \\
\mathrm{I}_0^{p^n}+\ldots+p^n\mathrm{I}_n & = & -X_0^{p^n}-\ldots-p^nX_n.
\end{array}$$

Pour $n=0$, on trouve $\mathrm{I}_0(X_0)=-X_0$.
Si $p\neq 2$, alors $p$ est impair. Dans ce cas, les polynômes $\mathrm{I}_n$ doivent vérifier :

$$\mathrm{I}_0^{p^n}+\ldots+p^n\mathrm{I}_n=(-X_0)^{p^n}+\ldots+p^n(-X_n).$$

On en déduit que pour $p\neq 2$, cette suite vérifie $\mathrm{I}_n(X_0,\ldots,X_n)=-X_n$ pour tout $n\in\mathbb{N}$.
Si $p=2$, l'existence et l'unicité de ces polynômes est évidente sur $\mathbb{Z}[\frac{1}{2}][X_i]_{i\in\mathbb{N}}$. Montrons par récurrence que pour tout $n\in\mathbb{N}$, $2^n\mathrm{I}_n\equiv 0 \mod 2^n$.

$$\begin{array}{rcl}
\mathrm{I}_0(X_0) & = & -X_0 \\
\mathrm{I}_1(X_0,X_1) & = & -X_0^2-X_1.
\end{array}$$

Supposons que ce soit vérifié jusqu'à un rang $n-1$ fixé. Montrons que c'est vrai pour $n$.

$$\begin{array}{rcl}
\mathrm{W}_n(\mathrm{I}_0,\ldots,\mathrm{I}_n) & = & -\mathrm{W}_n(X_0,\ldots,X_n) \\
 & \equiv & -\mathrm{W}_{n-1}(X_0^2,\ldots,X_{n-1}^2) \mod 2^n \\
 & \equiv & \mathrm{W}_{n-1}(\mathrm{I}_0(X_0^2),\ldots,\mathrm{I}_{n-1}(X_0^2,\ldots,X_{n-1}^2)) \mod 2^n \\
 & \equiv & \mathrm{I}_0(X_0^2)^{2^{n-1}}+\ldots+2^{n-1}\mathrm{I}_{n-1}(X_0^2,\ldots,X_{n-1}^2) \mod 2^n \\
 & \equiv & \mathrm{I}_0(X_0)^{2^n}+\ldots+2^{n-1}\mathrm{I}_{n-1}(X_0,\ldots,X_{n-1})^2 \mod 2^n \\
\mathrm{I}_0^{2^n}+\ldots+2^{n-1}\mathrm{I}_{n-1}^2+2^n\mathrm{I}_n & \equiv & \mathrm{I}_0^{2^n}+\ldots+2^{n-1}\mathrm{I}_{n-1}^2 \mod 2^n \\
2^n\mathrm{I}_n & \equiv & 0 \mod 2^n.
\end{array}$$

Donc on a prouvé l'unicité, l'existence et le fait que les coefficients soient entiers. □

**Théorème 4.2.2.** *Il existe une unique suite $\{\mathrm{F}_i\}_{i\in\mathbb{N}}$ de polynômes de $\mathbb{Z}[X_i]_{i\in\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, $\mathrm{F}_n \in \mathbb{Z}[X_0, \ldots, X_{n+1}]$ et telle que l'on ait, pour tout $n \in \mathbb{N}$ :*

$$\mathrm{W}_n(\mathrm{F}_0(X_0, X_1), \ldots, \mathrm{F}_n(X_0, \ldots, X_{n+1})) = \mathrm{W}_{n+1}(X_0, \ldots, X_{n+1}).$$

*Démonstration.* L'existence et l'unicité est évidente dans $\mathbb{Z}[\frac{1}{p}][X_i, Y_i]_{i\in\mathbb{N}}$ est évidente. En effet, on trouve :

$$\begin{array}{lll}
n=0, & \mathrm{W}_0(\mathrm{F}_0(X_0,X_1)) & = \mathrm{W}_1(X_0,X_1), \\
& \Rightarrow \mathrm{F}_0(X_0,X_1) & = X_0^p + pX_1, \\
n=1 & \mathrm{W}_1(\mathrm{F}_0,\mathrm{F}_1) & = \mathrm{W}_2(X_0,X_1,X_2) \\
& \Rightarrow \mathrm{F}_0^p + p\mathrm{F}_1 & = X_0^{p^2} + pX_1^p + p^2X_2 \\
& \Rightarrow \mathrm{F}_1(X_0,X_1,X_2) & = \frac{1}{p}(X_0^{p^2} + pX_1^p + p^2X_2 - (X_0^p + pX_1)^p), \\
& \vdots &
\end{array}$$

Montrons par récurrence que pour tout $n \in \mathbb{N}$, $\mathrm{F}_n(X_0, \ldots, X_{n+1}) \equiv X_n^p \mod p$.
Pour $n = 0$, c'est évident.
Pour $n = 1$, on voit que $(X_0^p + pX_1)^p \equiv X_0^p \mod p^2$
donc $X_0^{p^2} + pX_1^p + p^2X_2 - (X_0^p + pX_1)^p \equiv pX_1^p \mod p^2$. Donc $\mathrm{F}_1 \equiv X_1^p \mod p$. On en déduit que $\mathrm{F}_1$ est à coefficients entiers.
Supposons que c'est vrai jusqu'à un $n-1$ quelconque fixé.
Montrons que c'est vrai pour $\mathrm{F}_n$.
Par définition des $\mathrm{F}_n$ :

$$\begin{array}{rcl}
\mathrm{W}_n(\mathrm{F}_0, \ldots, \mathrm{F}_n) & = & W_{n+1}(X_0, \ldots, X_{n+1}) \\
\mathrm{F}_0^{p^n} + \ldots + p^{n-1}\mathrm{F}_{n-1}^p + p^n\mathrm{F}_n & = & X_0^{p^{n+1}} + \ldots + p^{n-1}X_{n-1}^{p^2} + p^nX_n^p + p^{n+1}X_{n+1} \\
X_0^{p^{n+1}} + \ldots + p^{n-1}X_{n-1}^{p^2} + p^n\mathrm{F}_n & \equiv & X_0^{p^{n+1}} + \ldots + p^{n-1}X_{n-1}^{p^2} + p^nX_n^p \mod p^{n+1} \\
p^n\mathrm{F}_n & \equiv & p^nX_n^p \mod p^{n+1} \\
\mathrm{F}_n & \equiv & X_n^p \mod p.
\end{array}$$

Autrement dit $\mathrm{F}_n$ est à coefficients entiers. □

On peut calculer les polynômes $\mathrm{F}_n$ pour les valeurs initiales :

$$\begin{array}{rcl}
\mathrm{F}_0(X_0, X_1) & = & X_0^p + pX_1 \\
\mathrm{F}_1(X_0, X_1, X_2) & = & X_1^p + pX_2 - \displaystyle\sum_{i=0}^{i=p-1} \frac{p!p^{p-i-1}}{(p-i)!i!} X_0^{p^i} X_1^{p-i} \\
& \vdots &
\end{array}$$

Tous ces éléments vont nous aider à construire l'anneau des vecteurs de Witt.

## 4.3 L'anneau $\mathrm{W}(A)$ des vecteurs de Witt

Soit $A$ un anneau quelconque. On considère l'ensemble $A^{\mathbb{N}}$.

**Notation 4.3.1.** *On notera la séquence $(a_n)_{n\in\mathbb{N}}$ par $\underline{a}$.*

On définit une autre structure différente de la structure d'anneau produit de $A^{\mathbb{N}}$.

**Définition 4.3.1.** *Pour tout $\underline{a}$ et $\underline{b}$ de $A^{\mathbb{N}}$, on définit les compositions et applications suivantes :*

$$\boxed{\begin{array}{rcl} \underline{a}\oplus\underline{b} & = & (\mathrm{S}_0(\underline{a},\underline{b}),\ldots,\mathrm{S}_n(\underline{a},\underline{b}),\ldots) \\ \underline{a}\otimes\underline{b} & = & (\mathrm{P}_0(\underline{a},\underline{b}),\ldots,\mathrm{P}_n(\underline{a},\underline{b}),\ldots) \\ \mathrm{I}_A(\underline{a}) & = & (\mathrm{I}_0(\underline{a}),\ldots,\mathrm{I}_n(\underline{a}),\ldots) \\ \mathrm{F}_A(\underline{a}) & = & (\mathrm{F}_0(\underline{a}),\ldots,\mathrm{F}_n(\underline{a}),\ldots). \end{array}}$$

*On notera $\mathrm{W}(A)$ l'ensemble $(A^{\mathbb{N}},\oplus,\otimes)$.*

Remarquons qu'ici, on considère les polynôme $\mathrm{S}_n$, $\mathrm{P}_n$, $\mathrm{I}_n$ et $\mathrm{F}_n$ comme des polynômes en les indéterminées $\{X_i\}_{i\in\mathbb{N}}$ et $\{Y_i\}_{i\in\mathbb{N}}$ mais ne dépendant que des $n$ premières.
Nous allons montrer que $\mathrm{W}(A)$ est un anneau pour ces deux compositions. Tout d'abord ces deux compositions sont évidemment des lois internes de $A^{\mathbb{N}}$. Il reste à montrer les autres propriétés des lois d'un anneau.

**Définition 4.3.2.** *On définit l'application $\mathcal{W}_A$ de $\mathrm{W}(A)$ dans $A^{\mathbb{N}}$ de la manière suivante :*

$$\mathcal{W}_A : \left\{ \begin{array}{rcl} \mathrm{W}(A) & \to & A^{\mathbb{N}} \\ \underline{a} & \mapsto & (\mathrm{W}_n(\underline{a}))_{n\in\mathbb{N}}. \end{array}\right.$$

*L'élément $\mathrm{W}_n(\underline{a})$ est appelée la composante fantôme d'indice $n$ de $\underline{a}$.*

Cet homomorphisme va nous permettre de démontrer le fait que $\mathrm{W}(A)$ est un anneau. Dans la suite on notera l'élément $p.1_A = \underbrace{1_A+\ldots+1_A}_{p}$ par $p$ tout simplement.

**Proposition 4.3.1.** *Si $p$ ne divise pas $0$ dans $A$, alors l'application $\mathcal{W}_A$ est injective. Si $p$ est inversible dans $A$, alors l'application $\mathcal{W}_A$ est bijective.*

*Démonstration.*

$$\mathcal{W}_A(\underline{a}) = \mathcal{W}_A(\underline{b}) \Leftrightarrow \forall n\in\mathbb{N},\ \mathrm{W}_n(\underline{a}) = \mathrm{W}_n(\underline{b}).$$

Par récurrence on trouve :

$$\left\{\begin{array}{rcl} \mathrm{W}_0(\underline{a}) & = & \mathrm{W}_0(\underline{b}) \\ \mathrm{W}_1(\underline{a}) & = & \mathrm{W}_1(\underline{b}) \\ & \vdots & \\ \mathrm{W}_n(\underline{a}) & = & \mathrm{W}_n(\underline{b}) \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} a_0 & = & b_0 \\ p(a_1-b_1) & = & 0 \\ & \vdots & \\ p^n(a_n-b_n) & = & 0 \end{array}\right.$$

On en déduit que si $p$ ne divise pas 0 dans $A$, l'application est injective.

$$\mathcal{W}_A(\underline{a}) = \underline{b} \Leftrightarrow \forall n \in \mathbb{N},\ \mathrm{W}_n(\underline{a}) = \underline{b}.$$

$$\left\{\begin{array}{rcl} \mathrm{W}_0(\underline{a}) &=& \underline{b} \\ \mathrm{W}_1(\underline{a}) &=& \underline{b} \\ &\vdots& \\ \mathrm{W}_n(\underline{a}) &=& \underline{b} \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} a_0 &=& b_0 \\ pa_1 &=& b_1 - b_0^p \\ &\vdots& \\ p^n a_n &=& b_n - a_0^{p^n} - \ldots - p^{n-1} a_{n-1}^p \end{array}\right.$$

On en déduit que si $p$ est inversible dans $A$, l'application est bijective et on a :

$$\begin{array}{rcl} a_0 &=& b_0 \\ a_1 &=& \frac{1}{p}(b_1 - b_0^p) \\ &\vdots& \end{array}$$

□

**Proposition 4.3.2.** *Pour tout $\underline{a}$ et pour tout $\underline{b}$ :*

$$\boxed{\begin{array}{rcl} \mathcal{W}_A(\underline{a} \oplus \underline{b}) &=& \mathcal{W}_A(\underline{a}) + \mathcal{W}_A(\underline{b}) \\ \mathcal{W}_A(\underline{a} \otimes \underline{b}) &=& \mathcal{W}_A(\underline{a}).\mathcal{W}_A(\underline{b}) \\ \mathcal{W}_A(\mathrm{I}_A(\underline{a})) &=& -\mathcal{W}_A(\underline{a}) \\ \mathcal{W}_A(\underline{0}) &=& \underline{0} \\ \mathcal{W}_A(1,0,0,\ldots) &=& \underline{1}. \end{array}}$$

*Démonstration.*

$$\begin{array}{rcl} \mathcal{W}_A(\underline{a} \oplus \underline{b}) &=& (\mathrm{W}_n(\underline{a} \oplus \underline{b}))_{n\in\mathbb{N}} \\ &=& (\mathrm{W}_n(S_0(\underline{a},\underline{b}),\ldots,S_n(\underline{a},\underline{b})))_{n\in\mathbb{N}} \\ &=& (\mathrm{W}_n(\underline{a}) + \mathrm{W}_n(\underline{b}))_{n\in\mathbb{N}} \\ &=& (\mathrm{W}_n(\underline{a}))_{n\in\mathbb{N}} + (\mathrm{W}_n(\underline{b}))_{n\in\mathbb{N}} \\ &=& \mathcal{W}_A(\underline{a}) + \mathcal{W}_A(\underline{b}). \end{array}$$

La preuve est similaire pour les autres égalités. □

**Notation 4.3.2.** *Soit $B$ un anneau et soit $\rho : B \to A$ un homomorphisme d'anneaux. On notera par $\mathrm{W}(\rho)$ l'homomorphisme*

$$\mathrm{W}(\rho) = \rho^{\mathbb{N}} : \left\{\begin{array}{rcl} B^{\mathbb{N}} &\to& A^{\mathbb{N}} \\ \underline{b} &\mapsto& (\rho(b_n))_{n\in\mathbb{N}}. \end{array}\right.$$

Il résulte de ces définitions, les propriétés suivantes :

**Propriété 4.3.1.** *Pour tout $\underline{a}$ et $\underline{b}$ dans $B^{\mathbb{N}}$, on a :*

$$\boxed{\begin{array}{rcl} \mathrm{W}(\rho)(\underline{a} \oplus \underline{b}) &=& \mathrm{W}(\rho)(\underline{a}) \oplus \mathrm{W}(\rho)(\underline{b}) \\ \mathrm{W}(\rho)(\underline{a} \otimes \underline{b}) &=& \mathrm{W}(\rho)(\underline{a}) \otimes \mathrm{W}(\rho)(\underline{b}) \\ \mathrm{W}(\rho) \circ \mathrm{I}_B(\underline{a}) &=& \mathrm{I}_A \circ \mathrm{W}(\rho)(\underline{a}) \\ \mathrm{W}(\rho) \circ \mathrm{F}_B(\underline{a}) &=& \mathrm{F}_A \circ \mathrm{W}(\rho)(\underline{a}) \\ \mathrm{W}(\rho)(1,0,0,\ldots) &=& (1,0,0,\ldots). \end{array}}$$

*Démonstration.* Nous ferons la preuve évidente seulement pour la première égalité.

$$\begin{aligned} \mathrm{W}(\rho)(\underline{a} \oplus \underline{b}) &= \mathrm{W}(\rho)(\mathrm{S}_n(\underline{a}, \underline{b}))_{n\in\mathbb{N}} \\ &= (\rho(\mathrm{S}_n(\underline{a}, \underline{b})))_{n\in\mathbb{N}} \\ &= (\mathrm{S}_n(\mathrm{W}(\rho)(\underline{a}), \mathrm{W}(\rho)(\underline{b})))_{n\in\mathbb{N}} \\ &= \mathrm{W}(\rho)(\underline{a}) \oplus \mathrm{W}(\rho)(\underline{b}). \end{aligned}$$

□

**Lemme 4.3.1.** *Soit un anneau $A$. Il existe un anneau $B$ et un homomorphisme surjectif d'anneaux $\rho : B \to A$ tels que $p$ ne divise pas 0 dans $B$ et tels qu'il existe un endomorphisme $\sigma$ de $B$ tel que $\sigma(b) \equiv b^p \mod p.B$ pour tout $b \in B$.*

*Démonstration.* Soit $B = \mathbb{Z}[X_a]_{a\in A}$. L'entier $p$ ne divise pas 0 dans $B$. De plus, nous avons l'homomorphisme $\rho : \left\{ \begin{array}{ccc} B & \to & A \\ X_a & \mapsto & a \end{array} \right.$. Cet homomorphisme est naturellement surjectif. On définit l'endomorphisme $\sigma : \left\{ \begin{array}{ccc} B & \to & B \\ R(X_a)_{a\in A} & \mapsto & R(X_a{}^p)_{a\in A} \end{array} \right.$. Par le petit théorème de Fermat, on voit que $\sigma(R) \equiv R^p \mod p.B$. □

**Théorème 4.3.1.** *Soit $A$ un anneau. Alors $\mathrm{W}_A$ est un anneau pour l'addition $\oplus$ et la multiplication $\otimes$. L'élément neutre pour l'addition est la séquence $\underline{0} = (0, 0, \ldots)$. L'opposé d'un élément $\underline{a}$ de $\mathrm{W}(A)$ est $\ominus\underline{a} = \mathrm{I}_A(\underline{a})$. L'élément neutre pour la multiplication est $1_{\mathrm{W}(A)} = (1, 0, 0, \ldots)$.*

*Si $\rho : B \to A$ est un homomorphisme d'anneau alors $\mathrm{W}(\rho) : \mathrm{W}(B) \to \mathrm{W}(A)$ est un homomorphisme d'anneaux. L'application $\mathcal{W}_A$ est un homomorphisme d'anneaux de $\mathrm{W}(A)$ dans $A^{\mathbb{N}}$ et les composantes fantômes sont elles aussi des homomorphismes d'anneaux.*

*Démonstration.* Les lois sont internes. Il reste à prouver le reste des propriétés d'un anneau. Considérons l'anneau $B = \mathbb{Z}[X_a]_{a\in A}$. L'application $\mathcal{W}_B$ est injective car $p$ ne

$$\begin{array}{ccc} \mathbb{Z}[X_a]_{a\in A} & \xrightarrow{\rho} & A \\ \Big\downarrow \mathrm{W} & & \Big\downarrow \mathrm{W} \\ \mathrm{W}(\mathbb{Z}[X_a]_{a\in A}) & \xrightarrow{\mathrm{W}(\rho)} & \mathrm{W}(A) \end{array}$$

FIGURE 4.1 – Foncteur W

divise pas 0 dans $B$. D'après 4.3.2

$$\mathcal{W}_B(\underline{0} \oplus \underline{b}) = \mathcal{W}_B(\underline{0}) + \mathcal{W}_B(\underline{b}) = \underline{0} + \mathcal{W}_B(\underline{b}) = \mathcal{W}_B(\underline{b}).$$

$$\mathcal{W}_B(\underline{b} \oplus \mathrm{I}(\underline{b})) = \mathcal{W}_B(\underline{b}) + \mathcal{W}_B(\mathrm{I}(\underline{b})) = \mathcal{W}_B(\underline{b}) - \mathcal{W}_B(\underline{b}) = \underline{0} = \mathcal{W}_B(\underline{0}).$$

Par injectivité : $\underline{0}\oplus\underline{b} = \underline{b}$ et $\underline{b}\oplus \mathrm{I}(\underline{b}) = 0$. Tout élément admet un inverse $\ominus\underline{b}$. L'associativité et la commutativité de l'addition se montrent de la même manière. Donc l'addition est bien une loi de groupe abélien sur $B$.

$$\mathcal{W}_B(\underline{b}\otimes 1_{\mathrm{W}(A)}) = \mathcal{W}_B(\underline{b}).\underline{1} = \mathcal{W}_B(\underline{b}).$$

Par injectivité, l'élément neutre pour la multiplication est $1_{\mathrm{W}(A)}$. On démontre de même que la multiplication est associative et distributive par rapport à l'addition. Tout ceci est vrai pour un anneau dont $p$ ne divise pas 0.

L'application $\mathrm{W}(\rho) : \mathrm{W}(B) \to \mathrm{W}(A)$ est surjective. Donc pour tout $\underline{a}$, il existe $\underline{a}'$ telle que $\mathrm{W}(\rho)(\underline{a}') = \underline{a}$. D'après 4.3.1 :

$$\begin{aligned}\underline{a}\oplus \mathrm{I}_A(\underline{a}) &= \mathrm{W}(\rho)(\underline{a}')\oplus \mathrm{I}_A(\mathrm{W}(\rho)(\underline{a}')) = \mathrm{W}(\rho)(\underline{a}')\oplus \mathrm{W}(\rho)(\mathrm{I}_B(\underline{a}')) = \mathrm{W}(\rho)(\underline{a}'\oplus \mathrm{I}_B(\underline{a}'))\\ &= \mathrm{W}(\rho)(\underline{0}) = \underline{0}.\end{aligned}$$

$$\underline{a}\otimes 1_{\mathrm{W}(A)} = \mathrm{W}(\rho)(\underline{a}')\otimes \mathrm{W}(\rho)(1_{\mathrm{W}(B)}) = \mathrm{W}(\rho)(\underline{a}'\otimes 1_{\mathrm{W}(B)}) = \mathrm{W}(\rho)(\underline{a}') = \underline{a}.$$

On démontre de la même manière toutes les hypothèses d'un anneau sur $\mathrm{W}(A)$ et donc $\mathrm{W}(A)$ est un anneau. Du coup, $\mathrm{W}(\rho)$ et $\mathcal{W}(A)$ sont aussi des homomorphismes d'anneaux.

Si $A$ est commutatif, les formules des polynômes de $\mathrm{S}_A$ et $\mathrm{P}_A$ montrent que la commutativité de $A$ implique celle de $\mathrm{W}(A)$.

□

**Définition 4.3.3.** *Soit $A$ un anneau. L'anneau $\mathrm{W}(A)$ est appelé l'anneau des vecteurs de Witt à coefficients dans $A$.*

Ainsi W est un foncteur de la catégorie des anneaux, puisqu'il transforme un anneau $A$ en un anneau $\mathrm{W}(A)$ et un homomorphisme d'anneaux $p : B \to A$ en un homomorphisme d'anneaux $\mathrm{W}(p) : \mathrm{W}(B) \to \mathrm{W}(A)$. Si $p$ est inversible, $\mathrm{W}(A)$ est isomorphe à $A^{\mathbb{N}}$.

## 4.4 L'homomorphisme de Frobenius et l'opérateur de décalage sur $\mathrm{W}(A)$

Soit $A$ un anneau. Dans la suite, on notera $1_{\mathrm{W}(A)}$ par 1 tout simplement.

**Définition 4.4.1.** *On appelle homomorphisme de Frobenius l'application $\mathrm{F}_A$ que l'on notera* F *lorsqu'il est question d'un seul anneau.*
*On appelle opérateur de décalage et on le note $\mathrm{V}_A$ ou tout simplement* V *lorsqu'il est question d'un seul anneau, l'application suivante :*

$$\mathrm{V}_A : \left\{\begin{array}{rcl}\mathrm{W}(A) & \to & \mathrm{W}(A)\\ (a_0, a_1, \ldots) & \mapsto & (0, a_0, a_1, \ldots).\end{array}\right.$$

*On définit deux autres applications :*

$$v_A : \left\{\begin{array}{rcl}A^{\mathbb{N}} & \to & A^{\mathbb{N}}\\ (a_0, a_1, a_2, \ldots) & \mapsto & (0, pa_0, pa_1, \ldots).\end{array}\right.$$

$$f_A : \left\{ \begin{array}{rcl} A^{\mathbb{N}} & \to & A^{\mathbb{N}} \\ (a_0, a_1, a_2, \ldots) & \mapsto & (a_1, a_2, a_3, \ldots). \end{array} \right.$$

$f_A$ est évidemment un endomorphisme de l'anneau $A^{\mathbb{N}}$ tandis que $v_A$ est un endomorphisme du groupe additif sous-jacent à $A^{\mathbb{N}}$.

**Proposition 4.4.1.** *Pour tout $\underline{a} \in \mathrm{W}(A)$ :*

$$\boxed{\begin{array}{rcl} \mathcal{W}_A \circ \mathrm{F}_A(\underline{a}) & = & f_A \circ \mathcal{W}_A(\underline{a}) \\ \mathcal{W}_A \circ \mathrm{V}_A(\underline{a}) & = & v_A \circ \mathcal{W}_A(\underline{a}). \end{array}}$$

*Les figures 4.4.1 et 4.4.1 représentent la commutativité de ces homomorphismes.*

$$\begin{array}{ccc} \mathrm{W}(A) & \xrightarrow{\mathrm{F}_A} & \mathrm{W}(A) \\ \downarrow{\scriptstyle \mathcal{W}_A} & & \downarrow{\scriptstyle \mathcal{W}_A} \\ A^{\mathbb{N}} & \xrightarrow{f_A} & A^{\mathbb{N}} \end{array}$$

$$\begin{array}{ccc} \mathrm{W}(A) & \xrightarrow{\mathrm{V}_A} & \mathrm{W}(A) \\ \downarrow{\scriptstyle \mathcal{W}_A} & & \downarrow{\scriptstyle \mathcal{W}_A} \\ A^{\mathbb{N}} & \xrightarrow{v_A} & A^{\mathbb{N}} \end{array}$$

*Démonstration.* Le théorème 4.2.2 démontre la première égalité. Pour la deuxième égalité, il suffit de remarquer que $\mathrm{W}_{n+1}(\underline{a}) = {a_0}^{p^{n+1}} + p\mathrm{W}_n(a_1, \ldots, a_{n+1})$. On en déduit que :

$$\begin{array}{rcl} \mathrm{W}_0(\mathrm{V}_A(\underline{a})) & = & 0 \\ \mathrm{W}_{n+1}(\mathrm{V}_A(\underline{a})) & = & \mathrm{W}_{n+1}(0, a_0, a_1, \ldots) = p\mathrm{W}_n(a_0, \ldots, a_n) \\ \mathcal{W}_A \circ \mathrm{V}_A(\underline{a}) & = & (0, p\mathrm{W}_1(\underline{a}), p\mathrm{W}_2(\underline{a}), \ldots) = v_A \circ \mathcal{W}_A(\underline{a}). \end{array}$$

□

**Propriété 4.4.1.** *Soit $\rho$ un homomorphisme d'anneaux. Nous possédons les relations suivantes, pour tout $\underline{a} \in \mathrm{W}(B)$ :*

$$\boxed{\mathrm{W}(\rho) \circ \mathrm{V}_B(\underline{a}) = \mathrm{V}_A \circ \mathrm{W}(\rho)(\underline{a}).}$$

*Démonstration.*

$$\begin{array}{rcl} \mathrm{W}(\rho) \circ \mathrm{V}_B(\underline{a}) & = & \mathrm{W}(\rho)(0, a_0, a_1, \ldots) \\ & = & (0, \rho(a_0), \rho(a_1), \ldots) \\ & = & \mathrm{V}_A(\rho(a_0), \rho(a_1), \ldots) \\ & = & \mathrm{V}_A \circ \mathrm{W}(\rho)(\underline{a}). \end{array}$$

□

Dans la suite, nous allons étudier les propriétés de calculs pour ces deux applications.

**Notation 4.4.1.** *Dans l'anneau* $\mathrm{W}(A)$*, on note :* $p.\underline{a} = \underbrace{\underline{a} \oplus \ldots \oplus \underline{a}}_{p}$ *et* $\underline{a}^{*p} = \underbrace{\underline{a} \otimes \ldots \otimes \underline{a}}_{p}$.

**Théorème 4.4.1.** *Soit $A$ un anneau. L'application $\mathrm{F}_A$ est un endomorphisme de l'anneau $\mathrm{W}(A)$. L'application $\mathrm{V}_A$ est un endomorphisme du groupe additif sous-jacent à l'anneau $\mathrm{W}(A)$.*
*Pour tout $\underline{a}$ et $\underline{b}$ de $\mathrm{W}(A)$, on a :*

$$\boxed{\begin{array}{rcl} \mathrm{F}_A \circ \mathrm{V}_A(\underline{a}) & = & p.\underline{a} \\ \mathrm{V}_A \circ \mathrm{F}_A(\underline{a}) & = & (0,1,0,0,\ldots) \otimes \underline{a} \\ \mathrm{V}_A(\underline{a} \otimes \mathrm{F}_A(\underline{b})) & = & \mathrm{V}_A(\underline{a}) \otimes \underline{b} \\ \mathrm{V}_A(\underline{a}) \otimes \mathrm{V}_A(\underline{b}) & = & p.\mathrm{V}_A(\underline{a} \otimes \underline{b}). \end{array}}$$

*Démonstration.* Si on reprend les éléments de la démonstration du théorème 4.3.1, on possède l'anneau $B = \mathbb{Z}[X_a]_{a \in A}$ et un homomorphisme surjetic $\rho : B \to A$. On rappelle aussi que $\mathrm{W}(\rho)$ est homomorphisme surjectif, que $\mathcal{W}_B$ est homomorphisme injectif et que $f_B$ est homomorphisme d'anneaux. Donc pour tout $\underline{a} \in \mathrm{W}_A$, il existe $\underline{a}^{'} \in \mathrm{W}_B$

$$\begin{array}{rcl} \mathrm{F}_A(\underline{a} \oplus \underline{b}) & = & \mathrm{F}_A(\mathrm{W}(\rho)(\underline{a}^{'}) \oplus \mathrm{W}(\rho)(\underline{b}^{'})) \\ & = & \mathrm{F}_A \circ \mathrm{W}(\rho)(\underline{a}^{'} \oplus \underline{b}^{'}) \\ & = & \mathrm{W}(\rho) \circ \mathrm{F}_B(\underline{a}^{'} \oplus \underline{b}^{'}) \text{ et} \\ \mathcal{W}_B \circ \mathrm{F}_B(\underline{a}^{'} \oplus \underline{b}^{'}) & = & f_B \circ \mathcal{W}_B(\underline{a}^{'} \oplus \underline{b}^{'}) \\ & = & f_B \circ \mathcal{W}_B(\underline{a}^{'}) + f_B \circ \mathcal{W}_B(\underline{b}^{'}) \\ & = & \mathcal{W}_B \circ \mathrm{F}_B(\underline{a}^{'}) + \mathcal{W}_B \circ \mathrm{F}_B(\underline{b}^{'}) \\ & = & \mathcal{W}_B(\mathrm{F}_B(\underline{a}^{'}) \oplus \mathrm{F}_B(\underline{b}^{'})). \end{array}$$

L'injectivité de $\mathcal{W}_B$ implique $\mathrm{F}_B(\underline{a}^{'}) \oplus \mathrm{F}_B(\underline{b}^{'}) = \mathrm{F}_B(\underline{a}^{'} \oplus \underline{b}^{'})$. D'où :

$$\begin{array}{rcl} \mathrm{F}_A(\underline{a} \oplus \underline{b}) & = & \mathrm{W}(\rho)(\mathrm{F}_B(\underline{a}^{'}) \oplus \mathrm{F}_B(\underline{b}^{'})) \\ & = & \mathrm{W}(\rho) \circ \mathrm{F}_B(\underline{a}^{'}) \oplus \mathrm{W}(\rho) \circ \mathrm{F}_B(\underline{b}^{'}) \\ & = & \mathrm{F}_A \circ \mathrm{W}(\rho)(\underline{a}^{'}) \oplus \mathrm{F}_A \circ \mathrm{W}(\rho)(\underline{b}^{'}) \\ & = & \mathrm{F}_A(\underline{a}) \oplus \mathrm{F}_A(\underline{b}). \end{array}$$

La preuve pour la multiplication est identique et repose sur le fait que $f$ est un homomorphisme d'anneaux. Pour montrer que $\mathrm{V}_A$ est un homomorphisme de groupe additif sous-jacent, on utilise les mêmes calculs et le fait que $v$ est seulement un homomorphisme de groupe additif sous-jacent. On utilise les mêmes procédés pour les autres points du théorème.

$$\begin{array}{rcl} \mathcal{W}_B \circ \mathrm{F}_B \circ \mathrm{V}_B(\underline{a}^{'}) & = & f_B \circ v_B \circ \mathcal{W}_B(\underline{a}^{'}) \\ & = & (p.\mathrm{W}_n(\underline{a}^{'}))_{n \in \mathbb{N}}. \end{array}$$

$$\begin{array}{rcl} \mathcal{W}_B(p.\underline{a}^{'}) & = & p.\mathcal{W}_B(\underline{a}^{'}) \\ & = & (p.\mathrm{W}_n(\underline{a}^{'}))_{n \in \mathbb{N}}. \end{array}$$

L'injectivité de $\mathcal{W}_B$ et le même procédé implique que $\mathrm{F}_A \circ \mathrm{V}_A(\underline{a}) = p.\underline{a}$.
Pour montrer $\mathrm{V}_A(\underline{a} \otimes \mathrm{F}_A(\underline{b})) = \mathrm{V}_A(\underline{a}) \otimes \underline{b}$, on relève dans l'anneau $\mathrm{W}(B)$ et on a :

$$\begin{aligned} \mathrm{W}_B \circ \mathrm{V}_B(\underline{a}^{'} \otimes \mathrm{F}_B(\underline{b}^{'})) &= v_B \circ \mathcal{W}_B(\underline{a}^{'} \otimes \mathrm{F}_B(\underline{b}^{'})) \\ &= v_B(\mathcal{W}_B(\underline{a}^{'}) \times \mathcal{W}_B \circ \mathrm{F}_B(\underline{b}^{'})) \\ &= v_B(\mathcal{W}_B(\underline{a}^{'}) \times f_B \circ \mathcal{W}_B(\underline{b}^{'})). \end{aligned}$$

$$\mathrm{W}_B(\mathrm{V}_B(\underline{a}^{'}) \otimes \underline{b}^{'}) = v_B \circ \mathrm{W}_B(\underline{a}^{'}) \times \mathrm{W}_B(\underline{b}^{'}).$$

Il reste à prouver que $v_B(\alpha \times f_B(\beta)) = v_B(\alpha) \times \beta$.

$$\begin{aligned} v_B(\alpha \times f_B(\beta)) &= v_B(\alpha_n \beta_{n+1})_{n \in \mathbb{N}} \\ &= (0, p\alpha_0\beta_1, p\alpha_1\beta_2, \ldots). \end{aligned}$$

$$\begin{aligned} v_B(\alpha) \times \beta &= (0, p\alpha_1, p\alpha_2, \ldots) \times \beta \\ &= (0, p\alpha_0\beta_1, p\alpha_1\beta_2, \ldots). \end{aligned}$$

Il en résulte le résultat que $\mathrm{V}_A(\underline{a} \otimes \mathrm{F}_A(\underline{b})) = \mathrm{V}_A(\underline{a}) \otimes \underline{b}$. On déduit directement de cela en remplaçant $\underline{a}$ par $1_{\mathrm{W}(A)}$ que $\mathrm{V}_A \circ \mathrm{F}_A(\underline{b}) = (0, 1, 0, 0, \ldots) \otimes \underline{b}$. Maintenant il reste à prouver que $\mathrm{V}_A(\underline{a}) \otimes \mathrm{V}_A(\underline{b}) = p.\mathrm{V}_A(\underline{a} \otimes \underline{b})$. On se replace dans l'anneau $B$ et on a :

$$\begin{aligned} \mathcal{W}_B(\mathrm{V}_B(\underline{a}^{'}) \otimes \mathrm{V}_B(\underline{b}')) &= \mathcal{W}_B \circ \mathrm{V}_B(\underline{a}^{'}) \times \mathcal{W}_B \circ \mathrm{V}_B(\underline{b}^{'}) \\ &= v_B \circ \mathcal{W}_B(\underline{a}^{'}) \times v_B \circ \mathcal{W}_B(\underline{b}^{'}) \\ &= (0, p^2\mathrm{W}_0(\underline{a}^{'})\mathrm{W}_0(\underline{b}^{'}), p^2\mathrm{W}_1(\underline{a}^{'})\mathrm{W}_1(\underline{b}^{'}), \ldots) \\ &= p.(0, p\mathrm{W}_0(\underline{a}^{'})\mathrm{W}_0(\underline{b}^{'}), p\mathrm{W}_1(\underline{a}^{'})\mathrm{W}_1(\underline{b}^{'}), \ldots) \\ &= p.v_B(\mathrm{W}_B(\underline{a}^{'}) \times \mathrm{W}_B(\underline{b}^{'})) \\ &= p.v_B \circ \mathrm{W}_B(\underline{a}^{'} \otimes \underline{b}^{'}) \\ &= p.\mathrm{W}_B \circ \mathrm{V}_B(\underline{a}^{'} \otimes \underline{b}^{'}) \\ &= \mathrm{W}_B(p.\mathrm{V}_B(\underline{a}^{'} \otimes \underline{b}^{'})). \end{aligned}$$

L'injectivité de $\mathcal{W}_B$ et la surjectivité de $\mathrm{W}(\rho)$ impliquent que l'égalité est vérifiée. □

Ces opérateurs permettent d'introduire une filtration sur le groupe additif sous-jacent à $\mathrm{W}(A)$. Cette filtration définit une topologie sur $\mathrm{W}(A)$

## 4.5 Vecteurs de Witt sur anneau de caractéristique $p$ et Topologie

Grâce à l'opérateur de décalage V, nous allons construire une suite décroissante d'idéaux dans $\mathrm{W}(A)$. Tout d'abord, énonçons un lemme très important :

**Lemme 4.5.1.** *Soit $A$ un anneau et $n$ un entier naturel. Pour tout $\underline{a} \in \mathrm{W}(A)$, on a :*

$$\underline{a} = (a_0, \ldots, a_{n-1}, 0, \ldots) \oplus (\underbrace{0, \ldots, 0}_{n}, a_n, \ldots).$$

*Démonstration.* On se replace dans l'anneau $B = \mathbb{Z}[X_a]_{a\in A}$.

$$\mathcal{W}_B((a_0,\ldots,a_{n-1},0,\ldots)\oplus(\underbrace{0,\ldots,0}_{n},a_n,\ldots)) = \mathcal{W}_B(a_0,\ldots,a_{n-1},0,\ldots)+\mathcal{W}_B(\underbrace{0,\ldots,0}_{n},a_n,\ldots).$$

Si $k < n$, alors :

$$\begin{array}{rcl} \mathrm{W}_k(a_0,\ldots,a_{n-1},0,\ldots) & = & \mathrm{W}_k(\underline{a}) \\ \mathrm{W}_k((\underbrace{0,\ldots,0}_{n},a_n,\ldots)) & = & 0. \end{array}$$

Si $k \geq n$, alors :

$$\begin{array}{rcl} \mathrm{W}_k(a_0,\ldots,a_{n-1},0,\ldots) & = & \sum_{i=0}^{i=n-1} p^i a_i^{p^{n-i}} \\ \mathrm{W}_k((\underbrace{0,\ldots,0}_{n},a_n,\ldots)) & = & \sum_{i=n}^{i=k} p^i a_i^{p^{n-i}}. \end{array}$$

Donc pour tout $k \in \mathbb{N}$ : $\mathrm{W}_k(a_0,\ldots,a_{n-1},0,\ldots) + \mathrm{W}_k((\underbrace{0,\ldots,0}_{n},a_n,\ldots)) = \mathrm{W}_k(\underline{a})$. On en déduit que : $\mathcal{W}_B((a_0,\ldots,a_{n-1},0,\ldots) \oplus (\underbrace{0,\ldots,0}_{n},a_n,\ldots)) = \mathcal{W}_B(\underline{a})$. Par injectivité, on a alors l'égalité sur $B$ et on remonte dans $A$ par surjectivité de l'homomorphisme $\mathrm{W}(\rho)$. □

### 4.5.1 Filtration sur l'anneau des vecteurs de Witt

**Définition 4.5.1.** *Soit $A$ un anneau. Pour tout $n$ entier naturel, on pose :*

$$\mathrm{V}_m(A) = \mathrm{V}^m(\mathrm{W}(A)) = \left\{\mathrm{V}^m(\underline{a}); \underline{a} \in \mathrm{W}(A)\right\}.$$

*C'est l'ensemble des vecteurs de Witt tels que les $n$ premiers termes soient nuls.*

**Proposition 4.5.1.** *Pour tout $n$ entier naturel, pour tout $\underline{a}$ et $\underline{b}$ :*

$$\boxed{\begin{array}{rcl} \mathrm{V}^n(\underline{a}\oplus\underline{b}) & = & \mathrm{V}^n(\underline{a})\oplus\mathrm{V}^n(\underline{b}) \\ \mathrm{V}^n(\underline{a})\otimes\underline{b} & = & \mathrm{V}^n(\underline{a}\otimes\mathrm{F}^n(\underline{b})). \end{array}}$$

*Démonstration.* Cette proposition se démontre par récurrence à partir des résultats du théorème 4.4.1 □

**Corollaire 4.5.1.** *Pour tout $n$ entier naturel, $\mathrm{V}_n(A)$ est un idéal de $\mathrm{W}(A)$.*

*Démonstration.* La proposition 4.5.1 montre clairement que $\mathrm{V}_n(A)$ est un idéal. □

**Définition 4.5.2.** *On appelle filtration décroissante sur un groupe $G$ une suite décroissante $\{G_n\}_{n\in\mathbb{Z}}$de sous-groupes. Le groupe $G$ est appelé un groupe filtré.*
*La filtration est dite séparée si $\bigcap_{n\in\mathbb{Z}} G_n = 0$. Soit un anneau $A$. On dit qu'une filtration $\{A_n\}_{n\in\mathbb{Z}}$ sur le groupe additif sous-jacent à l'anneau est compatible à la structure d'anneau si $\forall n,m \in \mathbb{Z}$, $A_nA_m \subseteq A_{n+m}$ et $1 \in A_0$. L'anneau $A$ est appelé un anneau filtré.*

On voit qu'une filtration sur un anneau compatible avec la structure d'anneau est une suite décroissante d'idéaux de $A_0$ dont $A_0$ est un sous-anneau de $A$. On pose $\mathrm{V}_n(A) = \mathrm{W}(A)$ pour tout $n \leq 0$. La suite des $\{\mathrm{V}_n(A)\}_{n\in\mathbb{Z}}$ est une filtration décroissante du groupe additif sous-jacent de $A$.

$$\mathrm{W}(A) = \mathrm{V}_0(A) \supseteq \mathrm{V}_1(A) \supseteq \ldots \supseteq \mathrm{V}_n(A) \ldots$$

Cette filtration du groupe additif sous-jacent est séparée.

$$\bigcap_{m\in\mathbb{N}} \mathrm{V}_m(A) = \{0\}\,.$$

L'élément 1 appartient à $\mathrm{V}_0(A)$. Cependant il reste à voir si cette filtration est compatible avec la structure d'anneau des vecteurs de Witt.

**Théorème 4.5.1.** *Soit $A$ un anneau. L'anneau $\mathrm{W}(A)$ est filtré si et seulement si $A$ est de caractéristique $p$.*

*Démonstration.* Si $\mathrm{W}(A)$ est un anneau filtré alors $\mathrm{V}_1(A)\mathrm{V}_1(A) \subseteq \mathrm{V}_2(A)$. D'après les formules des polynômes du produit $\mathrm{P}_n$, on a

$$(0, a_1, a_2, \ldots) \otimes (0, b_1, b_2, \ldots) = (0, pa_1b_1, \ldots),$$

pour tout $a_1$ et tout $b_1$ dans $A$, alors $px = 0$ pour tout $x \in A$. Ce qui signifie que $A$ est un anneau de caractéristique $p$. La réciproque nécessite des résultats préliminaires sur l'homomorphisme de Frobenius et l'opérateur de décalage. □

### 4.5.2 Vecteurs de Witt sur un anneau de caractéristique $p$

**Proposition 4.5.2.** *Soit un anneau de caractéristique $p$. Pour tout $\underline{a}$ et tout $\underline{b}$ de $\mathrm{W}(A)$ et pour tout entier naturel $n$ et tout $m$, on a :*

$$\begin{gathered}\mathrm{F}(\underline{a}) = (a_n{}^p)_{n\in\mathbb{N}} \\ p.\underline{a} = \mathrm{F}_A \circ \mathrm{V}(\underline{a}) = \mathrm{V} \circ \mathrm{F}(\underline{a}) = (0, 1, 0, 0, \ldots) \otimes \underline{a} = (0, a_0{}^p, a_1{}^p, \ldots) \\ \mathrm{V}^m(\underline{a}) \otimes \mathrm{V}^n(\underline{b}) = \mathrm{V}^{n+m}(\mathrm{F}^n(\underline{a}) \otimes \mathrm{F}^m(\underline{b})).\end{gathered}$$

*Démonstration.* Dans la démonstration du théorème 4.2.2, on prouve que $\mathrm{F}_n \equiv X_n^p \mod p$. Cette congruence s'interprète dans un anneau de caractéristique $p$ par $\mathrm{F}_n(\underline{a}) = a_n{}^p$. La première assertion est prouvée. D'après le théorème 4.4.1,

$$p.\underline{a} = \mathrm{F} \circ \mathrm{V}(\underline{a}) = \mathrm{F}(0, a_0, a_1, \ldots) = (0, a_0{}^p, a_1{}^p, \ldots) \text{ et}$$

$$(0, 1, 0, 0, \ldots) \otimes \underline{a} = \mathrm{V} \circ \mathrm{F}(\underline{a}) = \mathrm{V}(a_0{}^p, a_1{}^p, \ldots) = (0, a_0{}^p, a_1{}^p, \ldots).$$

La deuxième assertion est donc prouvée. D'après la proposition 4.5.1, on a :

$$\mathrm{V}^m(\underline{a}) \otimes \mathrm{V}^n(\underline{b}) = \mathrm{V}^m(\underline{a} \otimes \mathrm{F}^m \circ \mathrm{V}^n(\underline{b})).$$

Par commutativité de F avec V démontrée ci-dessus, on a :

$$\mathrm{V}^m(\underline{a}) \otimes \mathrm{V}^n(\underline{b}) = \mathrm{V}^m(\underline{a} \otimes \mathrm{V}^n \circ \mathrm{F}^m(\underline{b})).$$

D'après la proposition 4.5.1, on a :

$$\underline{a} \otimes \mathrm{V}^n \circ \mathrm{F}^m(\underline{b}) = \mathrm{V}^n(\mathrm{F}^n(\underline{a}) \otimes \mathrm{F}^m(\underline{b})).$$

On en déduit la dernière assertion de la proposition à savoir :

$$\begin{aligned} \mathrm{V}^m(\underline{a}) \otimes \mathrm{V}^n(\underline{b}) &= \mathrm{V}^m \circ \mathrm{V}^n(\mathrm{F}^n(\underline{a}) \otimes \mathrm{F}^m(\underline{b})) \\ &= \mathrm{V}^{n+m}(\mathrm{F}^n(\underline{a}) \otimes \mathrm{F}^m(\underline{b})). \end{aligned}$$

□

**Corollaire 4.5.2.** *Si $A$ est un anneau de caractéristique $p$ alors la filtration $\{\mathrm{V}_n(A)\}_{n\in\mathbb{Z}}$ est compatible avec la structure d'anneau de $A$.*

*Démonstration.* En effet, on a vu qu'il suffisait de démontrer que :

$$\boxed{\mathrm{V}_m(A) \otimes \mathrm{V}_n(A) \subseteq \mathrm{V}_{n+m}(A).}$$

Or pour tout $\underline{a}$ et tout $\underline{b}$, on a vu ci-dessus que $\mathrm{V}^m(\underline{a}) \otimes \mathrm{V}^n(\underline{b}) = \mathrm{V}^{n+m}(\mathrm{F}^n(\underline{a}) \otimes \mathrm{F}^m(\underline{b}))$. Autrement dit $\mathrm{V}_m(A) \otimes \mathrm{V}_n(A) \subseteq \mathrm{V}_{n+m}(A)$. □

*fin de la démonstration du théorème 4.5.1*
Ce corollaire achève donc la preuve du fait que $\mathrm{W}(A)$ est un anneau filtré si et seulement si $A$ est un anneau de caractéristique $p$. Cette filtration définit une topologie sur l'anneau des vecteurs de Witt.

### 4.5.3 Topologie et Représentant de Teichmuller

Munissons $\mathrm{W}(A)$ de la topologie associée à la filtration $\{\mathrm{V}_m(A)\}_{m\in\mathbb{Z}}$. Cette topologie est compatible à la structure d'anneau de $\mathrm{W}(A)$ si $A$ est de caractéristique $p$.
Pour tout $\underline{a} \in \mathrm{W}(A)$, pour tout $m \in \mathbb{Z}$, les ensembles $\underline{a} \oplus \mathrm{V}_m(A)$ sont des voisinages de $\underline{a}$. D'après le lemme 4.5.1, $\underline{a} \oplus \mathrm{V}_m(A)$ est l'ensemble des éléments $\underline{b}$ tels que pour tout $0 \leq i \leq m-1$, $b_i = a_i$.

$$\underline{a} \oplus \mathrm{V}_m(A) = \{(a_0, \ldots, a_{m-1}, b_m, b_{m+1}, \ldots); \forall i \geq m, b_i \in A\}.$$

**Proposition 4.5.3.** *Muni de la topologie associée à la filtration $\{V_k(A)\}_{k\in\mathbb{N}}$, $\mathrm{W}(A)$ est un anneau topologique séparé et complet.*

*Démonstration.* Soient $\underline{a}$ et $\underline{b}$ deux vecteurs de Witt tels que pour tout voisinage de $\underline{a}$ et voisinage de $\underline{b}$, l'intersection de ces deux voisinages soit non-vide, c'est-à-dire pour tout $n$ et $k$ entiers, $\{\underline{a} \oplus \mathrm{V}_k(A)\} \cap \{\underline{b} \oplus \mathrm{V}_n(A)\} \neq 0$. Donc pour tout $k$ et $n$ entiers, il existe un élément $\underline{c}_{n,k} \in \{\underline{a} \oplus \mathrm{V}_k(A)\} \cap \{\underline{b} \oplus \mathrm{V}_n(A)\}$. Supposons que $k \leq n$, comme la filtration est décroissante alors $\underline{c}_{n,k} \ominus \underline{a}$ et $\underline{c}_{n,k} \ominus \underline{b}$ sont dans $\mathrm{V}_k(A)$ qui est un idéal, donc

$\underline{a} \ominus \underline{b} \in \mathrm{V}_k(A)$. Ceci étant vérifié pour tout $k$ entier et la filtration étant séparée alors $\underline{a} \ominus \underline{b} = 0$. On a démontré que la topologie associée à cette filtration est séparée.

Soit $\{\underline{a}_n\}_{n\in\mathbb{N}}$ une suite de Cauchy de vecteurs de Witt pour la topologie associée à cette filtration.

$$\forall k \in \mathbb{N}, \quad \exists n_k \in \mathbb{N}; \quad \forall n, m \geq n_k, \quad \underline{a}_n \ominus \underline{a}_m \in \mathrm{V}_k(A).$$

Pour $k = 1$, il existe un plus petit entier $n_1$ tel que pour tout $n, m \geq n_1$, $\underline{a}_n \ominus \underline{a}_m \in \mathrm{V}_1(A)$. Ce qui équivaut à dire qu'il existe $a_0 \in A$ tel que pour tout $n \geq n_1$, le vecteur de Witt $\underline{a}_n$ ait pour première composante $a_0$. Pour $k = 2$, il existe $n_2$ tel que pour tout $n, m \geq n_2$, $\underline{a}_n \ominus \underline{a}_m \in \mathrm{V}_2(A)$. La filtration est décroissante, donc $n_2 \geq n_1$. C'est équivalent à dire qu'il existe $a_1 \in A$ tel que pour tout $n \geq n_2$, le vecteur de Witt $\underline{a}_n$ a pour deuxième composante $a_1$. Par récurrence sur $k$, on obtient une suite d'entiers croissantes

$$\ldots \geq n_k \geq \ldots \geq n_2 \geq n_1 \geq 0.$$

et une suite $(a_0, a_1, \ldots, a_k, \ldots)$ d'éléments dans $A$ qui constitue un vecteur de Witt que l'on note $\underline{a}$ tel que pour tout $n \geq n_k$, $\underline{a}_n \ominus \underline{a} \in \mathrm{V}_k(A)$. Autrement dit la suite des $\underline{a}_n$ est convergente et converge vers $\underline{a}$ pour cette topologie. □

**Définition 4.5.3.** *Soit $\tau_A$ l'application de $A$ dans $\mathrm{W}(A)$ définie par :*

$$\tau_A : \left\{ \begin{array}{ccc} A & \to & \mathrm{W}(A) \\ a & \mapsto & (a, 0, \ldots) \end{array} \right.$$

*Cette application est appelée le représentant de Teichmuller. Il sera noté $\tau$ quand il sera question d'un seul anneau.*

**Proposition 4.5.4.** *Soient $a$ et $b$ deux éléments de $A$ et soit un homomorphisme d'anneaux $\rho : B \to A$. soit $\underline{c} \in \mathrm{W}(A)$. On a :*

$$\boxed{\begin{array}{rcl} \mathcal{W}_A \circ \tau_A(a) & = & (a^{p^n})_{n\in\mathbb{N}} \\ \mathrm{W}(\rho) \circ \tau_B & = & \tau_A \circ \rho \\ \tau_A(ab) & = & \tau_A(a) \otimes \tau_A(b) \\ \tau_A(a) \otimes \underline{c} & = & (a^{p^n} c_n)_{n\in\mathbb{N}}. \end{array}}$$

*Démonstration.* Par les formules de $\mathrm{W}_n$, la première assertion est évidente. La deuxième assertion est aussi évidente. Pour la troisième assertion, on se replace dans l'anneau $B = \mathbb{Z}[X_a]_{a\in A}$. L'élément $p$ n'étant pas un diviseur de 0, alors $\mathcal{W}_B$ est injective.

$$\begin{array}{rcl} \mathcal{W}_B(\tau_B(a') \otimes \tau_B(b')) & = & \mathcal{W}_B \circ \tau_B(a') \times \mathcal{W}_B \circ \tau_B(b') \\ & = & (a'^{p^n})_{n\in\mathbb{N}} \times (b'^{p^n})_{n\in\mathbb{N}} \\ & = & ((a'b')^{p^n})_{n\in\mathbb{N}} \\ & = & \mathcal{W}_B \circ \tau_B(a'b'). \end{array}$$

Donc $\tau_B(a^{'}) \otimes \tau_B(b^{'}) = \tau_B(a^{'}b^{'})$. Comme $\rho$ est surjectif, pour tout $a$ et $b$, il existe $a^{'}$ et $b^{'}$ tels que $\rho(a^{'}) = a$ et $\rho(b^{'}) = b$.

$$\begin{aligned} \tau_A(a) \otimes \tau_A(b) &= \tau_A \circ \rho(a^{'}) \otimes \tau_A \circ \rho(b^{'}) \\ &= \mathrm{W}(\rho) \circ \tau_B(a^{'}) \otimes \mathrm{W}(\rho) \circ \tau_B(b^{'}) \\ &= \mathrm{W}(\rho) \circ \tau_B(a^{'}b^{'}) \\ &= \tau_A(ab). \end{aligned}$$

On procède de la même manière pour démontrer la dernière assertion. □

**Proposition 4.5.5.** *Munissons l'anneau* $\mathrm{W}(A)$ *de la topologie associée à la filtration* $\{\mathrm{V}_m(A)\}_{m\in\mathbb{Z}}$. *Soit* $\underline{a} = (a_n)_{n\in\mathbb{N}}$ *alors la série de terme général* $\mathrm{V}^n(\tau(a_n))$ *converge vers* $\underline{a}$.

$$\underline{a} = \sum_{n=0}^{n=+\infty} \mathrm{V}^n(\tau(a_n)).$$

*Démonstration.*

$$\mathrm{V}^n(\tau(a_n)) = (\underbrace{0, \ldots, 0}_{n}, a_n, 0, \ldots).$$

D'après le lemme 4.5.1, pour tout $n$ : $\underline{a} \in \sum_{k=0}^{k=n} \mathrm{V}^k(\tau(a_k)) \oplus \mathrm{V}_n(A)$. D'après le corollaire 4.5.1, la suite des $V_k(A)$ est une suite d'idéaux décroissante, donc pour tout $n$ et pour tout $m \geq n$ : $\sum_{k=0}^{k=m} \mathrm{V}^k(\tau(a_k)) \ominus \underline{a} \in \mathrm{V}_m(A) \subseteq \mathrm{V}_n(A)$.

En d'autres termes : $\forall n \in \mathbb{N}, \quad \forall m \geq n, \quad \sum_{k=0}^{k=m} \mathrm{V}^k(\tau(a_k)) \ominus \underline{a} \in \mathrm{V}_n(A)$. La série de terme général $\mathrm{V}^k(\tau(a_k))$ converge donc vers $\underline{a}$ pour la topologie associée à la filtration $\mathrm{V}_k(A)$. □

Il existe d'autres topologies sur l'anneau des vecteurs de Witt : la topologie $\mathrm{V}_1(A)$-adique et la topologie $p$-adique.

$$\mathrm{W}(A) \supseteq \mathrm{V}_1(A) \supseteq \mathrm{V}_1(A)^2 \supseteq \ldots \supseteq \mathrm{V}_1(A)^k \supseteq \ldots$$

$$\mathrm{W}(A) \supseteq p.\mathrm{W}(A) \supseteq p^2.\mathrm{W}(A) \supseteq \ldots \supseteq p^k.\mathrm{W}(A) \supseteq \ldots$$

Elles sont intéressantes dans le cas où $A$ est un anneau parfait de caractéristique $p$ car dans ce cas, elles coincident et sont plus fines que la topologie associée à la filtration $\{\mathrm{V}_m(A)\}_{m\in\mathbb{Z}}$.

### 4.5.4 Vecteurs de Witt sur un anneau parfait de caractéristique $p$ et topologie $p$-adique

Soit $A$ un anneau . La topologie $\mathrm{V}_1(A)$-adique et la topologie $p$-adique coincident sur l'anneau des vecteurs de Witt, $\mathrm{W}(A)$, si et seulement si $A$ est de caractéristique $p$. En effet :

**Proposition 4.5.6.** *Soit $A$ un anneau quelconque. Pour tout $k$ entier, on :*

$$\mathrm{V}_1(A)^k = p^{k-1}.\mathrm{V}_1(A).$$

*Démonstration.* D'après le théorème 4.4.1, pour tout couple de vecteurs de Witt, on a :

$$\mathrm{V}(\underline{a}) \otimes \mathrm{V}(\underline{b}) = p.\mathrm{V}(\underline{a} \otimes \underline{b}).$$

On en déduit directement que $\mathrm{V}_1(A)^2 \subseteq p.\mathrm{V}_1(A)$. D'autre part, soit $p.\mathrm{V}(\underline{a}) \in p.\mathrm{V}_1(A)$.

$$p.\mathrm{V}(\underline{a}) = p.\mathrm{V}(\underline{a} \otimes 1_{\mathrm{W}(A)}) = \mathrm{V}(\underline{a}) \otimes \mathrm{V}(1_{\mathrm{W}(A)}).$$

On en déduit directement l'inclusion inverse. Donc la proposition est vérifiée pour $k = 2$ et elle est évidente pour $k = 1$. Supposons que cela soit vrai pour un $k$ quelconque fixé.

$$\mathrm{V}_1(A)^{k+1} = \mathrm{V}_1(A)^k \mathrm{V}_1(A) = p^{k-1}.\mathrm{V}_1(A)\mathrm{V}_1(A) = p^{k-1}.\mathrm{V}_1(A)^2 = p^k.\mathrm{V}_1(A).$$

□

**Proposition 4.5.7.** *La topologie $p$-adique est plus fine que la topologie $\mathrm{V}_1(A)$-adique si et seulement si $A$ est un anneau de caractéristique $p$.*

*La topologie $\mathrm{V}_1(A)$-adique est plus fine que la topologie associée à la filtration $\{\mathrm{V}_m(A)\}_{m\in\mathbb{N}}$ si et seulement si $A$ est un anneau de caractéristique $p$.*

*L'anneau $\mathrm{W}(A)$ est séparé et complet pour ces trois topologies.*

*Démonstration.* Si la topologie $p$-adique est plus fine que la topologie $\mathrm{V}_1(A)$-adique alors $p.\mathrm{W}(A) \subseteq \mathrm{V}_1(A)$. Donc pour tout $\underline{a} \in \mathrm{W}(A)$, $p.\underline{a} \in \mathrm{V}_1(A) = \mathrm{V}(\mathrm{W}(A))$.

$$p.(a_0, a_1, \ldots) = (p.a_0, *, \ldots) = (0, *, \ldots).$$

On en déduit que pour tout $a_0 \in A$, $p.a_0 = 0$, ce qui signifie que $A$ est de caractéristique $p$.
Si la topologie $\mathrm{V}_1(A)$-adique est plus fine que la topologie associée à la filtration $\{\mathrm{V}_m(A)\}_{m\in\mathbb{N}}$, alors $\mathrm{V}_1(A)^2 \subseteq \mathrm{V}_2(A)$. Donc pour tout $\underline{a}$ et pour tout $\underline{b}$ dans $\mathrm{W}(A)$, $\mathrm{V}(\underline{a})\otimes\mathrm{V}(\underline{b}) \in \mathrm{V}_2(A)$.

$$(0, a_0, \ldots) \otimes (0, b_0, \ldots) = (0, p.a_0.b_0, \ldots) = (0, 0, *, \ldots).$$

On en déduit que pour tout $a \in A$, $p.a = 0$, ce qui signifie que $A$ est de caractéristique $p$.

Inversement si $A$ est de caractéristique $p$, d'après la proposition 4.5.2 :

$$p.\mathrm{W}(A) \subseteq \mathrm{V}(\mathrm{W}(A)) \subseteq \mathrm{V}_1(A).$$

On déduit de cela que $p^2.\mathrm{W}(A) \subseteq p.\mathrm{V}_1(A)$. De la proposition 4.5.6, on a $p.\mathrm{V}_1(A) = \mathrm{V}_1(A)^2$. Du corollaire 4.5.2, on a $\mathrm{V}_1(A)^2 \subseteq \mathrm{V}_2(A)$ et plus généralement $\mathrm{V}_1(A)^k \subseteq \mathrm{V}_k(A)$.

$$p^2.\mathrm{W}(A) \subseteq \mathrm{V}_1(A)^2 \subseteq \mathrm{V}_2(A).$$

Supposons que cela soit vrai pour $k-1$ quelconque. alors :

$$\begin{aligned} p^k.\mathrm{W}(A) &= p.p^{k-1}.\mathrm{W}(A) \subseteq p.\mathrm{V}_1(A)^{k-1} = p.\mathrm{V}_1(A)\mathrm{V}_1(A)^{k-2} \\ &= \mathrm{V}_1(A)^2\mathrm{V}_1(A)^{k-2} = \mathrm{V}_1(A)^k \subseteq \mathrm{V}_k(A). \end{aligned}$$

Les deux premières assertions sont démontrées. De manière analogue à la démonstration de la proposition 4.5.3, ces deux topologies sont séparées car $\bigcap_{k\in\mathbb{N}} p^k.\mathrm{W}(A) = \{0\}$ $\bigcap_{k\in\mathbb{N}} \mathrm{V}_1(A)^k = \{0\}$. La démonstration de la complétude est identique à celle de la proposition 4.5.3. □

**Proposition 4.5.8.** *La topologie $\mathrm{V}_1(A)$-adique, la topologie $p$-adique et la topologie associée à la filtration $\{\mathrm{V}_m(A)\}_{m\in\mathbb{N}}$ coincident sur l'anneau des vecteurs de Witt $\mathrm{W}(A)$ si et seulement si $A$ est parfait de caractéristique $p$.*

*Démonstration.* Si $A$ est un anneau parfait de caractéristique $p$, alors on en déduit grâce à la proposition 4.5.7 que pour tout $k$ entier, $p^k.\mathrm{W}(A) \subseteq \mathrm{V}_1(A)^k \subseteq \mathrm{V}_k(A)$. Comme $A$ est parfait alors d'après la proposition 4.5.2, F est un automorphisme de l'anneau $\mathrm{W}(A)$. Soit $\underline{a} \in \mathrm{V}_1(A)$, il existe $\underline{b} \in \mathrm{W}(A)$ tel que $\underline{a} = \mathrm{V}(\underline{b})$ et il existe $\underline{c}$ tel que $\underline{b} = \mathrm{F}(\underline{c})$. Donc $\underline{a} = \mathrm{V}(\mathrm{F}(\underline{c})) = p.\underline{c}$. Autrement dit $\mathrm{V}_1(A) = p.\mathrm{W}(A)$. La proposition 4.5.2 donne par commutativité en multipliant par $p.1_{\mathrm{W}(A)}$, $\mathrm{V}_1(A)^k = (p.\mathrm{W}(A))^k \subseteq p^k.\mathrm{W}(A)$. Autrement dit $p^k.\mathrm{W}(A) = \mathrm{V}_1(A)^k$. Avec l'automorphisme F et par commutativité de F et V, on a aussi :

$$\mathrm{V}_k(A) = \mathrm{V}^k(\mathrm{W}(A)) = \mathrm{V}^k \circ \mathrm{F}^k \circ \mathrm{F}^{-k}(\mathrm{W}(A)) = \underbrace{\mathrm{V}\circ\mathrm{F}}_{k} \circ \mathrm{F}^{-k}(\mathrm{W}(A)) = p^k.\mathrm{W}(A).$$

Donc les topologies coincident. Inversement, si les topologies coincident, d'après la proposition 4.5.7, $A$ est de caractéristique $p$. Il reste à montrer qu'il est parfait en sachant que $\mathrm{V}_1(A) = p.\mathrm{W}(A)$. Pour tout $\underline{a} \in \mathrm{W}(A)$, il existe $\underline{b} \in \mathrm{W}(A)$ tel que $V(\underline{a}) = p.\underline{b}$. D'après la proposition 4.5.2, on a : $(0, a_0, \ldots) = (0, b_0^p, \ldots)$. Donc pour tout $a \in A$, il existe $b \in A$ tel que $a = b^p$, autrement dit $A$ est parfait. □

Avec cette topologie $p$-adique, dans le cas où $A$ est un anneau parfait de caractéristique $p$, on peut redéfinir la série de terme général $\mathrm{V}^n(\tau(a_n))$ qui converge vers $\underline{a}$.

**Théorème 4.5.2.** *Soit un anneau parfait de caractéristique $p$. Munissons l'anneau $\mathrm{W}(A)$ de la topologie $p$-adique. Soit $\underline{a} = (a_n)_{n\in\mathbb{N}}$ alors la série de terme général $p^n.\tau({a_n}^{p^{-n}})$ converge vers $\underline{a}$.*

$$\underline{a} = \sum_{n=0}^{n=+\infty} p^n.\tau({a_n}^{p^{-n}}).$$

*Démonstration.* Si $A$ est parfait de caractéristique $p$, alors la topologie $p$-adique et la topologie associée à la filtration $\{\mathrm{V}_m(A)\}_{m\in\mathbb{N}}$ coincident. D'après les propositions 4.5.2 et 4.5.5 :

$$\underline{a} = \sum_{n=0}^{n=+\infty} \mathrm{V}^n(\tau(a_n)) = \sum_{n=0}^{n=+\infty} \mathrm{V}^n\circ\mathrm{F}^n\circ\mathrm{F}^{-n}(\tau(a_n)) = \sum_{n=0}^{n=+\infty} (\mathrm{V}\circ\mathrm{F})^n(\tau(a_n^{p^{-n}})) = \sum_{n=0}^{n=+\infty} p^n.\tau({a_n}^{p^{-n}}).$$

□

**Proposition 4.5.9.** *Soit $A$ un anneau de caractéristique $p$. La première composante fantôme $\mathrm{W}_0$ induit un isomorphisme de l'anneau quotient $\mathrm{W}(A)/\mathrm{V}_1(A)$ sur $A$. Si en plus $A$ est parfait, alors $\mathrm{W}_0$ induit un isomorphisme de l'anneau quotient $\mathrm{W}(A)/p.\mathrm{W}(A)$ sur $A$.*

*Démonstration.*

$$\mathrm{W}_0 : \left\{ \begin{array}{ccc} \mathrm{W}(A) & \to & A \\ \underline{a} & \mapsto & a_0. \end{array} \right.$$

C'est un homomorphisme d'anneau surjectif car pour tout $a \in A, \mathrm{W}_0(\tau(a)) = a$. Le noyau est l'ensemble des vecteurs de Witt tels que $a_0 = 0$, autrement dit l'idéal $\mathrm{V}_1(A)$. Si $A$ est parfait de caractéristique $p$ alors $\mathrm{V}_1(A) = p.\mathrm{W}(A)$. Donc $\mathrm{W}(A)/p.\mathrm{W}(A) \cong A$. □

## 4.6 Vecteurs de Witt sur un corps parfait de caractéristique $p$ et valuation discrète

Cette fois-ci, nous nous placerons dans le cas ou $A$ est un corps de caractéristique $p$ que l'on notera $k$. La structure de corps de $k$ fait de l'anneau des vecteurs de Witt $\mathrm{W}(k)$ un anneau local d'idéal maximal $p.\mathrm{W}(k)$.

**Proposition 4.6.1.** *Soit $k$ un corps de caractéristique $p$. Alors l'anneau $\mathrm{W}(k)$ est un anneau local intègre séparé et complet, d'idéal maximal $\mathrm{V}_1(k)$ et de corps résiduel $k$.*

*Démonstration.* On a démontré dans les parties précédentes que l'anneau est séparé et complet. De la proposition 4.5.9, on a que $\mathrm{W}(k)/\mathrm{V}_1(k)$ est isomorphe à $k$. L'espace $k$ étant un corps, on en déduit que $\mathrm{V}_1(k)$ est maximal.
Soit $\underline{a} \notin \mathrm{V}_1(k)$. Donc $a_0 \neq 0$ et il existe $a_0^{-1} \in k$. On cherche $\underline{b}$ tel que $\underline{a} \otimes \underline{b} = 1_{\mathrm{W}(A)} = (1, 0, 0, \ldots)$.

$$\mathrm{P}_0(\underline{a}, \underline{b}) = 1 \Rightarrow a_0 b_0 = 1 \Rightarrow b_0 = a_0^{-1}.$$

$$\mathrm{P}_1(\underline{a}, \underline{b}) = 0 \Rightarrow a_0^p b_1 + a_1 b_0^p = 0 \Rightarrow b_1 = -a_1 a_0^{-2p}.$$

Ainsi de suite par récurrence, on trouve qu'un inverse de $\underline{a}$ dans $\mathrm{W}(k)$ si $\underline{a} \notin \mathrm{V}_1(k)$.

$$\mathrm{W}(k) = \mathrm{V}_1(k) \coprod \mathrm{W}(k)^*.$$

On déduit que tout idéal est inclus dans $\mathrm{V}_1(k)$. L'idéal $\mathrm{V}_1(k)$ est donc l'unique idéal maximal. L'anneau $\mathrm{W}(k)$ est local et son corps résiduel est $k$.

Soient $\underline{a}$ et $\underline{b}$ deux vecteurs de Witt non-nuls. Il existe donc au moins un coefficient non nul pour chacun des deux vecteurs. Prenons les premiers coefficients non nuls notés $a_m$ et $b_n$. Alors $\underline{a} = \mathrm{V}^m(\underline{a}')$ et $\underline{b} = \mathrm{V}^n(\underline{b}')$ avec $\underline{a}' = (a_m, a_{m+1}, \ldots)$ et $\underline{b}' = (b_n, b_{n+1}, \ldots)$. D'après la proposition 4.5.2 :

$$\underline{a} \otimes \underline{b} = \mathrm{V}^m(\underline{a}') \otimes \mathrm{V}^n(\underline{b}') = \mathrm{V}^{m+n}(\mathrm{F}^n(\underline{a}) \otimes \mathrm{F}^m(\underline{b})) = \mathrm{V}^{m+n}((a_m^{p^n}.b_n^{p^m}, *, \ldots) \neq \underline{0}.$$

$\mathrm{W}(k)$ est un anneau intègre. □

**Théorème 4.6.1.** *Soit $k$ un corps parfait de caractéristique $p$. Alors l'anneau $\mathrm{W}(k)$ est un anneau de valuation discrète et son idéal maximal est $p.\mathrm{W}(k)$*

*Démonstration.* Si $k$ est parfait, d'après la proposition 4.5.9, l'idéal maximal est $\mathrm{V}_1(k) = p.\mathrm{W}(k)$. Si $k$ est de caractéristique $p$, sommer $p$ fois revient à multiplier par $p = p.1_{\mathrm{W}(k)} = (0, 1, 0, \ldots)$. Donc $p.\mathrm{W}(k) = p.1_{\mathrm{W}(k)} \otimes \mathrm{W}(k)$ est engendré par l'élément $p.1_{\mathrm{W}(k)} = (0, 1, 0, \ldots)$. Cet élément est non-nilpotent, car pour tout $n$ entier $(p.1_{\mathrm{W}(k)})^n = p^n.1_{\mathrm{W}(k)} = (\underbrace{0, \ldots, 0}_{n}, 1, 0 \ldots) \neq \underline{0}$. D'après le théorème précédent, $\mathrm{W}(k)$ est local, d'idéal maximal principal engendré par un élément non-nilpotent, intègre, séparé et complet. On en déduit que c'est un anneau de valuation discrète de corps résiduel $k$. En effet on démontre que tout idéal premier ne peut être que l'idéal maximal. Et le fait que l'idéal maximal soit principal implique que $\mathrm{W}(k)$ est principal. □

## 4.7 Vecteurs de Witt de longueur finie et Entiers $p$-adiques

Il existe une relation entre les vecteurs de Witt relatifs à un nombre premier $p$ et les entiers $p$-adiques. En effet, $\mathrm{W}(\mathbb{F}_p)$ l'anneau des vecteurs de Witt sur $\mathbb{F}_p$ est isomorphe à $\mathbb{Z}_p$ l'anneau des entiers $p$-adiques. Cet isomorphisme se construit avec l'anneau des vecteurs de Witt de longueur finie que nous allons introduire et les limites projectives.

### 4.7.1 Généralités

#### Vecteurs de Witt de longueur finie

**Définition 4.7.1.** *Soit $A$ un anneau quelconque et $n$ un entier strictement positif. On appelle anneau des vecteurs de Witt de longueur $n$ l'anneau quotient $\mathrm{W}_n(A) = \mathrm{W}(A)/\mathrm{V}_n(A)$.*

Cet anneau est en bijection avec l'anneau produit $A^n$ à travers l'application naturelle :

$$\begin{array}{rcl} \mathrm{W}_n(A) & \to & A^n \\ [a_0, \ldots, a_{n-1}, *, \ldots] & \mapsto & (a_0, \ldots, a_{n-1}). \end{array}$$

Les classes sont représentées par l'élément $(a_0, \ldots, a_{n-1}, 0, \ldots)$ que l'on notera $[a_0, \ldots, a_{n-1}]$. Les opérations sur $\mathrm{W}_n(A)$ sont définies par :

$$\begin{array}{rcl} [a_0, \ldots, a_{n-1}] \oplus [b_0, \ldots, b_{n-1}] & = & [\mathrm{S}_0(a_0, b_0), \ldots, \mathrm{S}_{n-1}(a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1})] \\ \\ [a_0, \ldots, a_{n-1}] \otimes [b_0, \ldots, b_{n-1}] & = & [\mathrm{P}_0(a_0, b_0), \ldots, \mathrm{P}_{n-1}(a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1})]\,. \end{array}$$

L'élément neutre pour l'addition est la classe de la séquence nulle notée $[\underline{0}]$ et celui de la multiplication est la classe de $1_{\mathrm{W}(A)}$ notée $[1, 0, \ldots, 0]$.

**Exemple 4.7.1.** *L'anneau* $\mathrm{W}_1(A)$ *est isomorphe à l'anneau* $A$ *puisque l'application est un homomorphisme d'anneau et les opérations sont données par*

$$[a_0] \oplus [b_0] = [\mathrm{S}_0(a_0, b_0)] = [a_0 + b_0]$$

$$[a_0] \otimes [b_0] = [\mathrm{P}_0(a_0, b_0)] = [a_0 \times b_0]\,.$$

**Exemple 4.7.2.** *Les opérations explicites sur* $\mathrm{W}_2(A)$ *sont :*

$$[a_0, a_1] \oplus [b_0, b_1] = \left[a_0 + b_0, a_1 + b_1 - \sum_{i=1}^{i=p-1} \frac{p!}{(p-i)!i!p} a_0^i a_0^{p-i}\right]$$

$$[a_0, a_1] \otimes [b_0, b_1] = [a_0 Y_0, a_0^p b_1 + a_1 b_0^p + p a_1 b_1]\,.$$

### Projections

**Notation 4.7.1.** *On notera l'homomorphisme surjectif canonique de* $\mathrm{W}(A)$ *dans* $\mathrm{W}_n(A)$ *par* $\pi_n$ *:*

$$\pi_n : \left\{ \begin{array}{ccc} \mathrm{W}(A) & \longrightarrow & \mathrm{W}_n(A) \\ \underline{a} & \mapsto & [a_0, \ldots, a_{n-1}]\,. \end{array} \right.$$

*On notera l'homomorphisme canonique de* $\mathrm{W}(A)$ *dans l'anneau du produit direct* $\prod_{n\in\mathbb{N}} \mathrm{W}_n(A)$ *par* $\pi$ *:*

$$\pi : \left\{ \begin{array}{ccc} \mathrm{W}(A) & \longrightarrow & \prod\limits_{n\geq 1} \mathrm{W}_n(A) \\ \underline{a} & \mapsto & (\pi_n(\underline{a}))_{n\in\mathbb{N}}. \end{array} \right.$$

### Foncteur

Soit $\rho$ un homomorphisme d'anneaux de $B$ dans $A$, on définit l'application $\mathrm{W}_n(\rho)$ par passage aux quotients de l'homomorphisme $\mathrm{W}(\rho)$. C'est bien un homomorphisme. $\mathrm{W}_n$ est donc un foncteur de la catégorie des anneaux. On a pour tout vecteur $\underline{b}$ dans $\mathrm{W}_n(B)$ :

$$\mathrm{W}_n(\rho)\,[b_0, \ldots, b_{n-1}] = [(p(b_0, \ldots, \rho(b_{n-1})]$$

$\mathrm{W}_n$ est donc un foncteur pour la catégorie des anneaux (voir figure 4.2).

### L'homomorphisme $\mathcal{W}_n$

Avec les polynômes, on peut définir des homomorphismes de $\mathrm{W}_n(A)$ dans $A$.

**Définition 4.7.2.** *Pour tout* $n$ *strictement positif, pour tout* $i < n$*, on définit les applications suivantes :*

$$\mathrm{W}_i^n : \left\{ \begin{array}{ccc} \mathrm{W}_n(A) & \to & A \\ [a_0, \ldots, a_{n-1}] & \mapsto & \mathrm{W}_i(a_0, \ldots, a_{n-1}) \end{array} \right.$$

*où* $\mathrm{W}_i$ *est la composante fantôme d'indice* $i$ *de la définition 4.3.2.*

$$\begin{array}{ccc} B & \xrightarrow{\rho} & A \\ \downarrow{\scriptstyle \mathrm{W}} & & \downarrow{\scriptstyle \mathrm{W}} \\ \mathrm{W}(B) & \xrightarrow{\mathrm{W}(\rho)} & \mathrm{W}(A) \\ \downarrow{\scriptstyle \pi_n} & & \downarrow{\scriptstyle \pi_n} \\ \mathrm{W}_n(B) & \xrightarrow{\mathrm{W}_n(\rho)} & \mathrm{W}_n(A) \end{array}$$

FIGURE 4.2 – Foncteur $\mathrm{W}_n$

On peut alors définir l'homomorphisme d'anneaux $\mathcal{W}_n : \mathrm{W}_n(A) \to A^n$ qui correspond au passage au quotient de l'homomorphisme $\mathcal{W} : \mathrm{W}(A) \to A^{\mathbb{N}}$.

$$\mathcal{W}_n : \left\{ \begin{array}{rcl} \mathrm{W}_n(A) & \to & A^n \\ [a_0, \ldots, a_{n-1}] & \to & \{\mathrm{W}_i(a_0, \ldots, a_{n-1})\}_{0 \leq i \leq n-1} \end{array} \right.$$

En effet, l'ensemble des vecteurs dans $A^{\mathbb{N}}$ tels que les $n$ premiers coefficients soient nuls est un idéal et l'image de $\mathrm{V}_n(A)$ par $\mathcal{W}$ est contenu dans cet idéal. Par passage au quotient, on a le diagramme suivant :

$$\begin{array}{ccc} \mathrm{W}(A) & \xrightarrow{\mathcal{W}} & A^{\mathbb{N}} \\ \downarrow{\scriptstyle \pi_n} & & \downarrow \\ \mathcal{W}_n(A) & \xrightarrow{\mathcal{W}_n} & A^n \end{array}$$

FIGURE 4.3 – L'homomorphisme $\mathcal{W}_n$

### 4.7.2 Limite projective

Pour tout $n$ entier, la filtration $\{\mathrm{V}_m(A)\}_{m \in \mathbb{N}}$ étant décroissante, on peut construire un homomorphisme surjectif de $\mathrm{W}_m(A)$ sur $\mathrm{W}_n(A)$ pour toute paire d'entiers strictement positifs $m$ et $n$ tels que $m > n$.

**Définition 4.7.3.** *Soit une famille d'anneau $\{A_n\}_{n \in \mathbb{N}}$ munie d'une famille d'homomorphismes d'anneaux $\pi_{i,j} : A_j \to A_i$ pour tout $i \leq j$ telle que :*

- *$\pi_{i,i}$ est l'identité de $A_i$.*
- *$\pi_{i,k} = \pi_{i,j} \circ \pi_{j,k}$ pour tout triplet $i \leq j \leq k$.*

*Alors on appelle cette famille $(A_n, \pi_{n,m})$ un système projectif d'anneaux. On définit la limite projective de ce système par :*

$$\varprojlim A_n = \left\{ (x_n)_{n \in \mathbb{N}} \in \prod_{n \in \mathbb{N}} A_n; \quad \forall i \leq j, \quad a_i = \pi_{i,j}(a_j) \right\}$$

La limite projective d'un système projectif d'anneaux est un sous-anneau de l'anneau produit direct $\prod_{n\in\mathbb{N}} A_n$. On construit les homomorphismes canoniques de projection suivant pour toute paire $(n,m)$ telle que $n \leq m$,

$$\pi_{n,m} : \left\{ \begin{array}{ccc} \mathrm{W}_m(A) & \to & \mathrm{W}_n(A) \\ [a_0,\ldots,a_{m-1}] & \mapsto & [a_0,\ldots,a_{n-1}]\,. \end{array} \right.$$

Il est évident que la famille $(\mathrm{W}_n(A),\pi_{n,m})$ est un système projectif.

**Proposition 4.7.1.** *L'homomorphisme $\pi$ est un isomorphisme d'anneaux de $\mathrm{W}(A)$ dans $\varprojlim \mathrm{W}_n(A)$.*

*Démonstration.* L'image de $\pi$ est l'ensemble :

$$\left\{ (x_n)_{n\geq 1} \in \prod_{n\in\mathbb{N}} \mathrm{W}_n(A); \quad \exists \underline{a} \in \mathrm{W}(A), \quad \forall n \geq 1, \quad x_n = \pi_n(\underline{a}) \right\}.$$

Soit $(x_n)_{n\geq 1} \in \varprojlim \mathrm{W}_n(A)$. Par définition de la limite projective, $\pi_{n,n+1}(x_{n+1}) = x_n$.

$$\begin{array}{rcl} & & \exists a_0 \in A; \quad x_1 = [a_0] \\ \pi_{1,2}(x_2) = x_1 & \Rightarrow & \exists a_1 \in A; x_1 = [a_0,a_1] \\ & \vdots & \\ \pi_{n,n+1}(x_{n+1}) = x_n & \Rightarrow & \exists a_n \in A; x_{n+1} = [a_0,\ldots,a_n]\,. \end{array}$$

On a construit une suite $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ telle que pour tout $n$, $x_n = [a_0,\ldots,a_{n-1}]$. Cette suite correspond à un vecteur de Witt $\underline{a}$ tel que $\pi(\underline{a}) = (x_n)_{n\geq 1}$.
Soit $(\pi_n(\underline{a}))_{n\geq 1} \in \mathcal{I}m(\pi)$. Par définition des homomorphismes de projection $\pi_{n,m}$, pour tout $m \geq n$, $\pi_{n,m} \circ \pi_m(\underline{a}) = \pi_n(\underline{a})$. On a prouvé $\mathcal{I}m(\pi) = \varprojlim \mathrm{W}_n(A)$. L'homomorphisme $\pi$ est injectif. En effet :

$$(\pi_n(\underline{a}))_{n\geq 1} = 0 \Leftrightarrow \forall n \in \mathbb{N}, \quad [a_0,\ldots,a_{n-1}] = 0 \Leftrightarrow \forall n \in \mathbb{N}, \quad a_n = 0 \Leftrightarrow \underline{a} = 0.$$

Donc $\pi$ est un isomorphisme d'anneaux de $\mathrm{W}(A)$ dans $\varprojlim \mathrm{W}_n(A)$. □

### 4.7.3 Vecteurs de Witt sur $\mathbb{F}_p$ et Entiers $p$-adiques

Considérons l'anneau des vecteurs de Witt de longueur finie $\mathrm{W}_n(\mathbb{Z})$.

**Lemme 4.7.1.** *Soient $[a_0,\ldots,a_{n-1}]$ et $[b_0,\ldots,b_{n-1}]$ deux vecteurs dans $\mathrm{W}_n(\mathbb{Z})$. Si pour tout $0 \leq i \leq n-1$, $a_i \equiv b_i \mod p$, alors : $\mathrm{W}^n_{n-1}[a_0,\ldots,a_{n-1}] \equiv \mathrm{W}^n_{n-1}[b_0,\ldots,b_{n-1}] \mod p^n$.*

*Démonstration.* Si pour tout $0 \leq i \leq n-1$, $a_i \equiv b_i \mod p$, alors pour tout $0 \leq i \leq n-1$,

$$(a_i^{p^{n-1-i}}) \equiv (b_i^{p^{n-1-i}}) \mod p^{n-i} \Rightarrow (p^i a_i^{p^{n-1-i}}) \equiv (p^i b_i^{p^{n-1-i}}) \mod p^n.$$

$$\begin{aligned} \mathrm{W}_{n-1}^{n}\left[a_0,\ldots,a_{n-1}\right] &= \left(\sum_{i=0}^{i=n-1} p^i a_i^{p^{n-1-i}}\right) \\ &\equiv \left(\sum_{i=0}^{i=n-1} p^i b_i^{p^{n-1-i}}\right) \mod p^n \\ &= \mathrm{W}_{n-1}^{n}\left[b_0,\ldots,b_{n-1}\right] \mod p^n. \end{aligned}$$

□

En considérant la projection de $\rho : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ et en utilisant le fait que $\mathrm{W}_n$ est un foncteur pour la catégorie des anneaux, on obtient le diagramme 4.7.3. On peut

$$\begin{array}{ccccccc} \mathbb{Z} & \xrightarrow{\mathcal{W}_n} & \mathrm{W}_n(\mathbb{Z}) & \xrightarrow{\mathcal{W}_n^{n-1}} & \mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/p^n\mathbb{Z} \\ \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \mathrm{W}_n(\rho)} & & \downarrow & & \\ \mathbb{Z}/p\mathbb{Z} & \xrightarrow{\mathcal{W}_n} & \mathrm{W}_n(\mathbb{Z}/p\mathbb{Z}) & \xrightarrow{\mathcal{W}_n^{n-1}} & \mathbb{Z}/p\mathbb{Z} & & \end{array}$$

alors construire une application de $\Psi_n$ de $\mathrm{W}_n(\mathbb{Z}/p\mathbb{Z})$ dans $\mathbb{Z}/p^n\mathbb{Z}$. Pour tout vecteur dans $\mathrm{W}_n(\mathbb{Z}/p\mathbb{Z})$, on prend un relèvement dans $\mathrm{W}_n(\mathbb{Z})$, puis on prend son image dans $\mathbb{Z}$ modulo $p^n$. Si on prend deux relèvement différents, $[a_0,\ldots,a_{n-1}]$ et $[b_0,\ldots,b_{n-1}]$, alors pour tout $0 \leq i \leq n-1$, $a_i \equiv b_i \mod p$. D'après le lemme précédent, on trouve que leur image par $\mathrm{W}_{n-1}^n$ sont congrues modulo $p^n$. Autrement dit $\Psi_n$ est bien définie. C'est évidemment un homomorphisme d'anneaux.

**Proposition 4.7.2.** *L'homomorphisme $\Psi_n : \mathrm{W}_n(\mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p^n\mathbb{Z}$ est un isomorphisme d'anneau.*

*Démonstration.*

$$\Psi_n([1,0,\ldots,0] = 1$$

Donc 1 appartient à l'image de $\Psi_n$. L'application $\Psi_n$ étant un homomorphisme, pour tout $0 \leq k \leq p^n - 1$, $\Psi_n(k.[1,0,\ldots,0] = k.\Psi_n([1,0,\ldots,0] = k$. Autrement dit, $\Psi_n$ est surjectif et par cardinalité, c'est une bijection. □

**Théorème 4.7.1.** *L'anneau des vecteurs de Witt sur $\mathbb{F}_p$ est isomorphe à l'anneau des entiers p-adiques $\mathbb{Z}_p$.*

$$\mathrm{W}(\mathbb{F}_p) \cong \varprojlim \mathrm{W}_n(\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$$

*Démonstration.* Pour tout $m \geq n$, l'unique homomorphisme d'anneaux de $\mathbb{Z}/p^m\mathbb{Z}$ dans $\mathbb{Z}/p^n\mathbb{Z}$ est l'homomorphisme surjectif qui à la classe de tout entier modulo $p^m$ lui associe sa classe modulo $p^n$. On le note $\delta_{n,m}$ et on obtient le diagramme commutatif suivant 4.7.3. Soit l'homomorphisme $\Psi$ produit direct des homomorphismes d'anneaux $\Psi_n$ de $\varprojlim \mathrm{W}_n(\mathbb{F}_p)$ dans le produit direct $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$.

$$\Psi : \left\{ \begin{array}{ccc} \varprojlim \mathrm{W}_n(\mathbb{F}_p) & \to & \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} \\ ([a_0,\ldots,a_{n-1}])_{n\in\mathbb{N}} & \mapsto & (\Psi_n\left[a_0,\ldots,a_{n-1}\right])_{n\geq 1}. \end{array} \right.$$

$$\begin{array}{ccc} \mathrm{W}_m(\mathbb{F}_p) & \xrightarrow{\pi_{n,m}} & \mathrm{W}_n(\mathbb{F}_p) \\ \downarrow{\scriptstyle \Psi_m} & & \downarrow{\scriptstyle \Psi_n} \\ \mathbb{Z}/p^m\mathbb{Z} & \xrightarrow{\delta_{n,m}} & \mathbb{Z}/p^n\mathbb{Z} \end{array}$$

On cherche le noyau. On identifiera $a_n$ à son relèvement dans $\mathbb{Z}$.

$$\begin{array}{rcl} \Psi([a_0,\ldots,a_{n-1}])_{n\in\mathbb{N}} = 0 & \Leftrightarrow & \forall n \geq 1, \quad \Psi_n\left[a_0,\ldots,a_{n-1}\right] = 0 \\ & \Rightarrow & a_0 \mod p = 0 \Rightarrow a_0 = 0 \\ & \Rightarrow & pa_1 \mod p^2 = 0 \Rightarrow a_1 = 0 \\ & & \vdots \\ & \Rightarrow & p^{n-1}a_{n-1} \mod p^n = 0 \Rightarrow a_{n-1} = 0 \\ & & \vdots \end{array}$$

$\Psi$ est donc injectif. Soit $(\Psi_n\left[a_0,\ldots,a_{n-1}\right])_{n\geq 1}$ un élément de $\mathcal{I}m(\Psi)$. Alors pour tout $m \geq n$,

$$\begin{array}{rcl} \Psi_n\left[a_0,\ldots,a_{n-1}\right] & = & \Psi_n \circ \pi_{n,m}\left[a_0,\ldots,a_{m-1}\right] \\ & = & \delta_{n,m} \circ \Psi_m\left[a_0,\ldots,a_{m-1}.\right] \end{array}$$

Donc $\mathcal{I}m(\Psi) \subseteq \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Inversement, soit $(y_n)_{n\geq 1}$ un élément de $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Par isomorphisme des $\Psi_n$, pour tout $n$, il existe $x_n$ élément de $\varprojlim \mathrm{W}_n(\mathbb{F}_p)$ tel que $\Psi_n(x_n) = y_n$. Pour tout $m \geq n$, $\delta_{n,m}(y_m) = y_n$. En réutilisant le diagramme commutatif, on trouve :

$$\begin{array}{rcl} \delta_{n,m}(y_m) = y_n & \Rightarrow & \delta_{n,m} \circ \Psi_m(x_m) = \Psi_n(x_n) \\ & \Rightarrow & \Psi_n \circ \pi_{n,m}(x_m) = \Psi_n(x_n) \\ & \Rightarrow & \pi_{n,m}(x_m) = \Psi_n^{-1} \circ \Psi_n(x_n) = x_n \end{array}$$

Donc $\mathcal{I}m(\Psi) = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. □

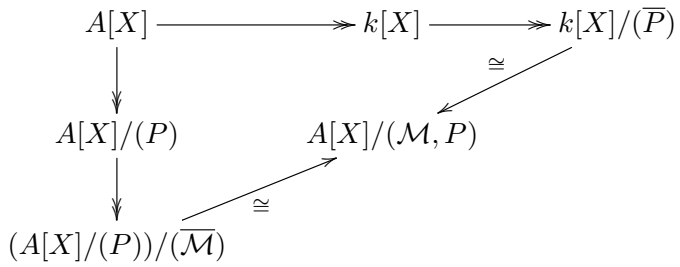
## 4.8 L'anneau $\mathbb{Z}_{p^n}$

L'anneau des vecteurs de Witt étant une structure algébrique difficilement applicable pour la conception d'un registre à décalage et à rétroaction avec retenue, on doit introduire une autre représentation de l'anneau de valuation discrète complet de corps résiduel $\mathbb{F}_{p^n}$.

Soit $A$ un anneau local de corps résiduel $k$ et d'idéal maximal $\mathcal{M}$. Considérons $A[X]$ l'anneau des polynômes à coefficient dans $A$ et $P(X) \in A[X]$ un polynôme de degré $n$. L'anneau quotient $A[X]/(P(X))$ est une $A$-algèbre libre de type fini de rang $n$. La base canonique est $\left\{1, \bar{X}, \ldots, \bar{X}^{n-1}\right\}$ où $\bar{X}$ représente la classe de $X$ modulo $P(X)$. L'ensemble $\mathcal{M}[X]$ définie par les polynômes à coefficient dans $\mathcal{M}$ est un idéal de $A[X]$. Notons les idéaux $(P(X)) = P(X).A[X]$, $\mathcal{M}[X]$ et $P(X).A[X] + \mathcal{M}[X]$ par les notations abusives $(P)$, $(\mathcal{M})$ et $(P, \mathcal{M})$. On a les isomorphismes suivants :

$$A[X]/(\mathcal{M}) \cong (A/\mathcal{M})[X] \cong k[X].$$

Notons $\overline{P}$ la classe de $P(X)$ modulo $\mathcal{M}$ et $(\overline{M})$ la classe de $(\mathcal{M})$ modulo $P(X)$.




Comme $k$ est un corps, alors $k[X]$ est euclidien donc principal et factoriel. Il existe donc une décomposition en facteurs irréductibles de $\overline{P(X)}$ : $\overline{P(X)} = \prod_{i\in I} \overline{P_i(X)}^{n_i}$ où $I$ est une sous sensemble fini de $\mathbb{N}$.

**Lemme 4.8.1.** *Les idéaux maximaux de $A[X]/(P)$ sont les idéaux de la forme $(\overline{\mathcal{M}}, \overline{P_i})$ pour tout $i \in I$. Ils sont deux à deux distincts. L'anneau quotient $(A[X]/(P))/(\overline{\mathcal{M}}, \overline{P_i})$ est le corps $k[X]/(\overline{P_i})$.*

**Proposition 4.8.1.** *Si $A$ est un anneau de valuation discrète complet de corps résiduel $k$ et d'idéal maximal $\mathcal{M}$ et si $\overline{P}$ la classe d'un polynôme $P(X) \in A[X]$ est irréductible dans $k[X]$, alors $A[X]/(P)$ est un anneau de valuation discrète complet d'idéal maximal $\overline{\mathcal{M}}$ et de corps résiduel $k[X]/(\overline{P})$.*

**Corollaire 4.8.1.** *Soit $P(X)$ un polynôme de $\mathbb{Z}_p[X]$ tel que $\overline{P}$ sa classe modulo $p$ soit un polynôme irréductible de degré $n$. Alors l'anneau $\mathbb{Z}_p[X]/(P)$ est un anneau de valuation discrète complet d'idéal maximal $p.\mathbb{Z}_p[X]/(P)$ et de corps résiduel $\mathbb{F}_{p^n}$. C'est aussi un $\mathbb{Z}_p$-module libre de rang $n$.*

Le corps des fractions de $\mathbb{Z}_p[X]/(P)$ est $\mathbb{Q}_p[X]/(P)$. C'est aussi une extension finie du corps $\mathbb{Q}_p$ complète pour le prolongement de la valuation $p$-adique.

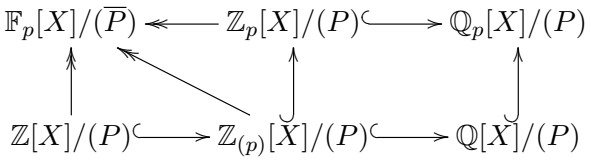



FIGURE 4.4 – Anneau $\mathbb{Z}_{p^n}$.

**Corollaire 4.8.2.** *Soit $P(X) \in \mathbb{Z}_p[X]$ un polynôme dont la classe modulo $p$ est un polynôme irréductible de degré $n$. L'anneau de valuation discrète complet $\mathbb{Z}_p[X]/(P)$ est isomorphe à l'anneau des vecteurs de Witt $W(\mathbb{F}_{p^n})$.*

**Définition 4.8.1** (l'anneau $\mathbb{Z}_{p^n}$)**.** *L'anneau $\mathbb{Z}_p[X]/(P)$ unique à isomorphisme près est noté par $\mathbb{Z}_{p^n}$.*

### 4.8.1 Lien entre $\mathbb{Z}_{p^n}$ et les registres vectoriels à décalage et à rétroaction avec retenue

Dans la suite, nous construisons les registres vectoriels à rétroaction avec retenue (le décalage n'est pas important puisqu'il existe un mode général qui contient d'autres connexions que le décalage) en utilisant l'anneau $\mathbb{Z}_{p^n}$. On rappelle que :

1. L'analyse des LFSRs sur $\mathbb{F}_{p^n}$ utilise l'anneau des séries formelles $\mathbb{F}_{p^n}[[X]]$.
2. L'analyse des FCSRs sur $\mathbb{F}_p$ utilise l'anneau des entiers $p$-adiques $\mathbb{Z}_p$.
3. L'analyse des $d$-FCSRs sur $\mathbb{F}_p$ utilise une extension totalement ramifiée de $\mathbb{Z}_p$ de degré de ramification $d$.

Pour la conception et l'analyse des FCSRs sur $\mathbb{F}_{p^n}$, on utilisera l'anneau $\mathbb{Z}_{p^n}$. Pour construire ces registres, on utilise la conception vectorielle suivante :

- On prend un polynôme $P(X)$ unitaire de degré $n$ irréductible sur $\mathbb{F}_p$ de la forme $X^n - \ldots - 1$.
- On considère les relèvements canoniques de $P(X)$ dans $\mathbb{Z}[X]$ et $\mathbb{Z}_p[X]$.
- On considère $\mathbb{F}_{p^n}$ comme un $\mathbb{F}_p$-espace vectoriel de dimension $n$ puisqu'il est isomorphe au quotient $\mathbb{F}_p[X]/(P)$. Les états et les coefficients de connexion du registre sont des états dans $(\mathbb{F}_p)^n$ où les coefficients sont des vecteurs de dimension $n$ sur $\mathbb{F}_p$.
- On considère $\mathbb{Z}[X]/(P)$ le $\mathbb{Z}$-module libre de rang $n$. Les lois d'addition et de multiplication sont définies par $P(X)$. La base canonique de $\mathbb{Z}[X]/(P)$ est $\left\{1, \ldots, \bar{X}^{n-1}\right\}$. On prend un relèvement de l'état du registre et des coefficients de connexion dans $\mathbb{Z}[X]/(P)$ respectivement par rapport à la base canonique. Tous ces éléments sont vus comme des vecteurs d'entiers dans $\mathbb{Z}^n$.
- La retenue initiale est un vecteur dans $\mathbb{Z}^n$. Les calculs du registre se font dans $\mathbb{Z}[X]/(P)$ et on applique les fonctions ($\mathtt{mod}p$) et ($\mathtt{div}p$) composante par composante.

L'analyse du registre repose sur la correspondance entre les séquences dans $\mathbb{F}_{p^n}$ et les séries dans $\mathbb{Z}_{p^n}$ :

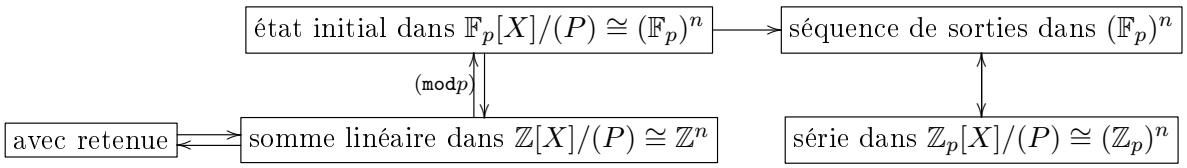



FIGURE 4.5 – FCSR vectoriel et Anneau $\mathbb{Z}_{p^n}$.

# Chapitre 5

# Registre à décalage et à rétroaction linéaire ou LFSR

## 5.1 Introduction

Dans ce chapitre, nous allons revoir les résultats classiques sur les LFSR séquences et leur démonstration en nous inspirant de [1] et [40]. Certains des résultats présentés dans ce chapitre sont connus depuis plus d'un siècle.

En plus d'être des objets mathématiques intéressants, les LFSR séquences ou les séquences récurrentes linéaires se sont révélées très utiles dans le domaine de la communication et du cryptage.

Les LFSR séquences jouissent d'une structure linéaire qui rend leur analyse très simple. On démontre facilement leur périodicité, leur propriétés pseudo-aléatoires (distribution des bits), l'existence de LFSR séquences de période maximale, leur complexité linéaire ...

Essentiellement, leur analyse se fait via les séries formelles en associant à toute séquence d'une sortie la série formelle correspondante. L'analyse des LFSR séquences revient alors à l'étude des fractions rationnelles.

## 5.2 Definitions et Conception

Dans cette section, nous allons définir un *Linear Feedback Shift Register* ou un *Registre Linéaire à Rétroaction et à Décalage* sur un corps fini $\mathbb{F}_{p^n}$ où $p$ est premier et $n \geq 1$.

**Définition 5.2.1** (LFSR). *Un Linear Feedback Shift Register en mode Fibonacci sur $\mathbb{F}_{p^n}$ de taille $r$ et de coefficients de connexion $q_1, \ldots, q_r \in \mathbb{F}_{p^n}$ est un automate ou générateur de séquence dont les états sont définis de la manière suivante :*

$$s = (a_0, \ldots, a_{r-1}) \in (\mathbb{F}_{p^n})^r.$$

*et dont l'opération de changement d'état est la suivante : Calculons*

$$a_r = \sum_{i=1}^{i=r} q_i a_{r-i}.$$

*L'addition et la multiplication se font dans le corps fini* $\mathbb{F}_{p^n}$. *La fonction de retour est* $f(a_0, \ldots, a_{r-1}) = (a_1, \ldots, a_r)$ *et la fonction de sorties est* $g(x_0, \ldots, x_{r-1}) = x_0$. *On répète ce procédé à l'infini. Le LFSR génère la séquence infinie*

$$(g(s), g(f(s)), g(f^2(s)), \ldots) = (a_0, a_1, a_2, \ldots)$$

*appelée séquence de sorties. L'état* $s$ *est appelé l'état initial de la séquence de sorties,* $r$ *la taille du LFSR et* $q_1, \ldots, q_r$ *les coefficients de connexion du LFSR.*

Avec cette définition, un LFSR est un triplet $\mathcal{L} = (\mathbb{F}_{p^n}, r, (q_1, \ldots, q_r))$. En tant qu'automate, on définit aussi le LFSR par $\mathcal{L} = (U, \sum, f, g)$ avec $U = (\mathbb{F}_{p^n})^r$ et $\sum = \mathbb{F}_{p^n}$. La

$$f \circlearrowright U \xrightarrow{g} \mathbb{F}_{p^n}$$

FIGURE 5.1 – Formalisme d'un LFSR.

figure 5.2 représente le mode Fibonacci d'un LFSR.

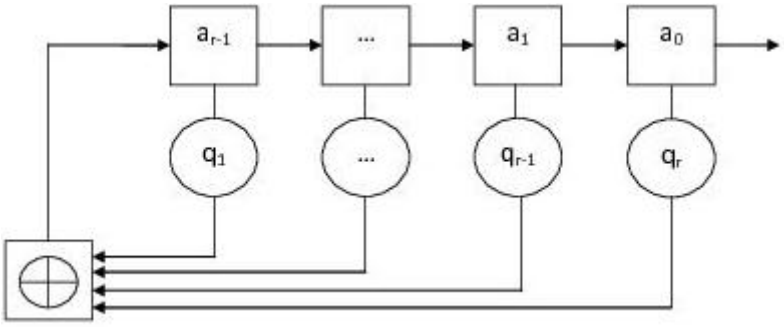



FIGURE 5.2 – Registre à décalage et à rétroaction linéaire ou LFSR.

**Définition 5.2.2.** *Les séquences générées par des LFSR sont appelées LFSR séquences.*

**Définition 5.2.3** (séquence récurrente linéaire)**.** *Une séquence* $\underline{a} = (a_0, a_1, \ldots)$ *dans* $\mathbb{F}_{p^n}$ *est dite linéairement récurrente s'il existe un entier* $r \geq 1$ *et un vecteur* $(q_1, \ldots, q_r)$ *dans* $\mathbb{F}_{p^n}$ *tel que pour tout* $i \geq r$,

$$a_i = \sum_{j=1}^{j=r} q_j a_{i-j} = q_1 a_{i-1} + \ldots + q_r a_{i-r}.$$

*Cette équation est appelée relation de récurrence linéaire.*

Autrement dit, une séquence dans $\mathbb{F}_{p^n}$ est linéairement récurrente s'il existe un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$ qui génère cette séquence et inversement toute séquence de sorties d'un LFSR est récurrente linéaire. Ces deux définitions sont équivalentes. On les appelle aussi les LFSR séquences.

## 5.3 Périodicité et Exemple

La périodicité est la propriété la plus fondamentale pour les séquences. Dans cette section, nous allons démontrer la périodicité des LFSR séquences sans donner leur période exacte tout en illustrant par des exemples.

**Proposition 5.3.1.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, (q_1, \ldots, q_r))$. Toute séquence de sorties est ultimement périodique. La période est inférieur ou égale à $p^{nr}$.*

*Démonstration.* Si l'état initial est nul, alors la séquence de sorties est nulle. Si l'état nul apparait au fur est à mesure des étapes du registre, la séquence devient nulle. Dans ces deux cas, la séquence est périodique de période 1. Si l'état nul n'apparait jamais, alors il existe $p^{nr} - 1$ états possibles. Donc après $p^{nr} - 1$ étapes, le registre reitère forcément un état. La période est donc inférieur ou égale à $p^{nr} - 1$. □

Dans la suite nous verrons qu'on peut déterminer de manière exacte la période d'une séquence de sorties. Notons que cette proposition équivaut à dire que les séquences récurrentes linéaires sont périodiques.

**Exemple 5.3.1.** *Soit le LFSR $(\mathbb{F}_2, 3, (1, 1, 0))$. Ou bien la séquence de sorties est nulle ou bien elle est strictement périodique de période $2^3 - 1 = 7$. Le diagramme des états est représenté dans la figure 5.3. Pour l'état initial $(001)$, la séquence de sorties est*

$$\underline{a} = (0010111001\ldots).$$

## 5.4 Fonction génératrice d'une séquence et Polynôme de connexion d'un LFSR

### 5.4.1 Analyse

Dans cette section, nous allons étudier les LFSR séquences via les séries formelles correspondantes. En effet, on construit la correspondance entre les séries formelles et les séquences extraites à partir de leurs coefficients. Soit l'application suivante :

$$\begin{array}{rccc} \Theta : & (\mathbb{F}_{p^n})^{\mathbb{N}} & \to & \mathbb{F}_{p^n}[[X]] \\ & \underline{a} = (a_0, a_1, \ldots) & \mapsto & a(X) = \sum_{i=0}^{i=+\infty} a_i X^i. \end{array}$$

$\Theta$ est un isomorphisme entre l'anneau produit infini $(\mathbb{F}_{p^n})^{\mathbb{N}}$ et l'anneau des séries formelles $\mathbb{F}_{p^n}[[X]]$. C'est un même un morphisme de $\mathbb{F}_{p^n}$-algèbre.

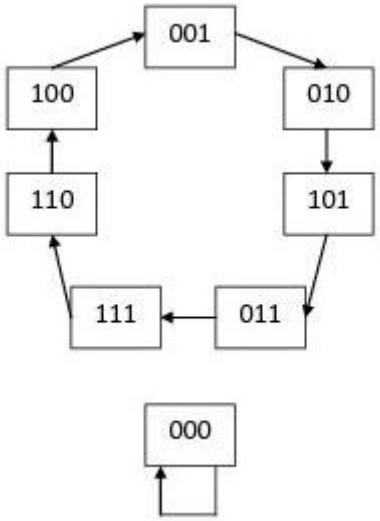



FIGURE 5.3 – Diagramme des états.

**Définition 5.4.1** (fonction génératrice)**.** *La série formelle $a(X)$ est appelée la fonction génératrice de $\underline{a}$. Inversement, on appelle $\underline{a}$ la séquence associée ou extraite de $a(X)$ dans $\mathbb{F}_{p^n}$ et on la note $\mathtt{seq}_{p^n}(a(X))$.*

**Définition 5.4.2** (polynôme de connexion)**.** *Soit un LFSR $\mathcal{L} = \mathcal{L} = (\mathbb{F}_{p^n}, r, (q_1, \ldots, q_r))$. On appelle polynôme de connexion de $\mathcal{L}$ le polynôme défini par*

$$q(X) = \sum_{i=1}^{i=r} q_i X^i - 1 \in \mathbb{F}_{p^n}[X].$$

**Exemple 5.4.1.** *Le LFSR $(\mathbb{F}_2, 3, (1, 1, 0))$ a pour polynôme de connexion $X^3 + X^2 - 1$.*

On peut donc définir un LFSR par le triplet $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$. Par contre, définir un LFSR par son seul polynôme de connexion est sujet à confusion. En effet, il est nécessaire de définir la taille $r$ puisque pour deux tailles différentes, on peut obtenir le même polynôme de connexion. Il suffit pour cela de prendre un polynôme $q(X)$ et le LFSR $\mathcal{L} = (\mathbb{F}_{p^n} \deg(q), q(X))$. Ensuite pour construire un autre LFSR, on ajoute des cases et des zéros pour coefficients de connexion correspondant à ces cases (voir figure 5.4).

**Exemple 5.4.2.** *Prenons $p = 2$ et $q(X) = X^3 + X^2 - 1$ comme polynôme de connexion. Les deux registres des figures 5.5 et 5.6 sont deux LFSRs distincts ayant $q(X)$ pour polynôme de connexion.*

**Remarque 5.4.1.** *Toutefois, il reste à noter que le triplet $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$ est un LFSR à la seule condition que $r \geq \deg(q)$. Par définition, on ne peut pas avoir un polynôme de connexion de degré supérieur à la taille du registre. Donc dans la suite, on supposera toujours que $r \geq \deg(q)$.*

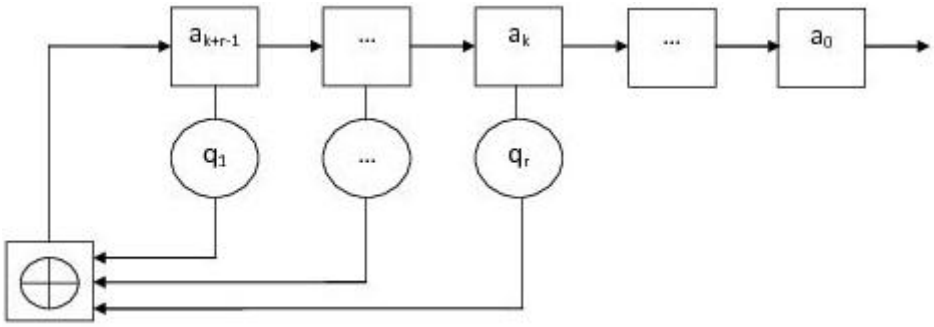



FIGURE 5.4 – Ajout de cases.

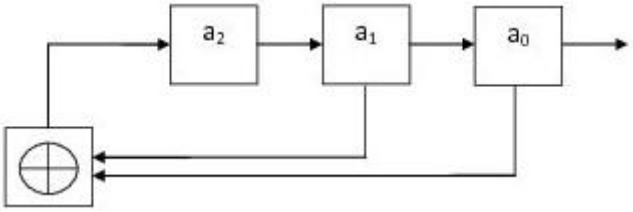



FIGURE 5.5 – Exemple 1.

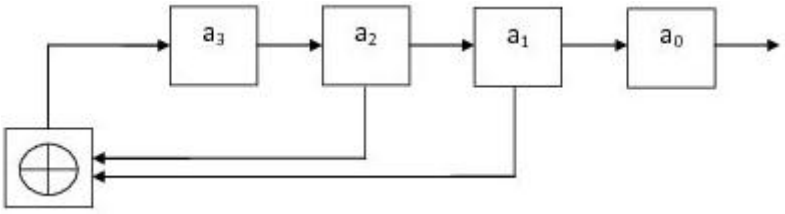



FIGURE 5.6 – Exemple 2.

**Théorème 5.4.1.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$ tel que $q(X) \neq -1$. Soit un état initial $(a_0, \ldots, a_{r-1})$ et soit $\underline{a}$ la séquence de sorties correspondante. Alors la fonction génératrice de $\underline{a}$ est une fraction rationnelle dans $\mathbb{F}_{p^n}(X)$ de la forme suivante :*

$$a(X) = \frac{f(X)}{q(X)} \text{ avec } f(X) = \sum_{j=1}^{j=r-1} \sum_{i=0}^{i=r-j-1} q_j a_i X^{i+j} - \sum_{i=0}^{i=r-1} a_i X^i.$$

*Démonstration.* La séquence $\underline{a}$ vérifie la relation de récurrence pour tout $i \geq r$, $a_i =$

$\sum_{j=1}^{j=r} q_j a_{i-j}$. Sa fonction génératrice vérifie donc

$$\begin{aligned}
a(X) &= \sum_{i=0}^{i=r-1} a_i X^i + \sum_{i=r}^{i=+\infty} a_i X^i \\
&= \sum_{i=0}^{i=r-1} a_i X^i + \sum_{i=r}^{i=+\infty} \sum_{j=1}^{j=r} q_j a_{i-j} X^i \\
&= \sum_{i=0}^{i=r-1} a_i X^i + \sum_{j=1}^{j=r} q_j X^j \sum_{i=r}^{i=+\infty} a_{i-j} X^{i-j} \\
&= \sum_{i=0}^{i=r-1} a_i X^i + \sum_{j=1}^{j=r} q_j X^j (a(X) - \sum_{i=0}^{i=r-j-1} a_i X^i \\
&= \sum_{i=0}^{i=r-1} a_i X^i + \sum_{j=1}^{j=r} q_j X^j a(X) - \sum_{j=1}^{j=r} \sum_{i=0}^{i=r-j-1} q_j a_i X^{i+j} \\
(1 - \sum_{j=1}^{j=r} q_j X^j) a(X) &= -f(X) \\
a(X) &= \tfrac{f(X)}{q(X)}.
\end{aligned}$$

□

**Corollaire 5.4.1.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, -1)$. Soit un état initial $(a_0, \ldots, a_{r-1})$ et soit $\underline{a}$ la séquence de sorties correspondante. Alors $\underline{a} = (a_0, \ldots, a_{r-1}, 0, 0, \ldots)$ et sa fonction génératrice est $a(X) = \sum_{i=0}^{i=r-1} a_i X^i$.*

*Démonstration.* La preuve est évidente. □

### 5.4.2 Période et ordre du Polynôme de connexion

**Définition 5.4.3.** *Soit $\underline{a}$ une séquence périodique et $a(X)$ sa fonction génératrice. La série formelle $a(X)$ est une fraction rationnelle, on note $\deg(a)$ la différence entre le degré du numérateur et le degré du dénominateur.*

**Corollaire 5.4.2.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$. Les séquences de sorties sont périodiques. Soit $\underline{a}$ une séquence de sorties et $\frac{f(X)}{q(X)}$ sa fontion génératrice $\frac{f(X)}{q(X)}$. Alors :*

1. *La période divise l'ordre de $q$ dans $\mathbb{F}_{p^n}[X]$ noté $\mathtt{ord}(q)$.*
2. *L'ordre de $q(X)$ divise $|(\mathbb{F}_{p^n}[X]/(q))^*|$.*
3. *Si $f(X)$ et $q(X)$ sont premiers entre eux, alors la période de $\underline{a}$ est égale à $\mathtt{ord}(q)$.*
4. *La séquence de sorties est strictement périodique si et seulement si $\deg(f) < \deg(q)$.*
5. *Si $q_r \neq 0$, alors la séquence de sorties est strictement périodique.*
6. *Si $\deg(q) \leq \deg(f)$, alors $\underline{a}$ est de pré-période $\deg(a) + 1$.*

*Démonstration.* Les séquences de sorties ont pour fonction génératrice la fraction rationnelle $\frac{f(X)}{q(X)}$ où $f$ est déterminée à partir de l'état initial et des coefficients de connexion et où $q(X)$ est le polynôme de connexion. Le polynôme $q(X)$ est de la forme $q_r X^r + \ldots + q_1 X - 1$. Si $q(X) = -1$, alors les séquences de sorties sont nulles, donc strictement périodiques de période 1. Si $q(X) \neq -1$, alors il existe un coefficient de connexion non nul. Autrement dit $\deg(q) \geq 1$ et $q(0) = -1$. Donc l'ordre de $q$ existe [41] et $q(X)$ divise $X^{\mathtt{ord}(q)} - 1$.

$$a(X) = \frac{f(X)\frac{X^{\mathtt{ord}(q)}-1}{q}}{X^{\mathtt{ord}(q)}-1} = \frac{u(X)}{X^{\mathtt{ord}(q)}-1}.$$

En effectuant la division euclidienne de $u$ par $X^{\mathtt{ord}(q)}-1$ dans $\mathbb{F}_{p_n}[X]$, $u(X) = (X^{\mathtt{ord}(q)}-1)v(X) + w(X)$ avec $\deg(w) < \mathtt{ord}(q)$, on obtient

$$\begin{aligned} a(X) &= v(X) + \frac{w(X)}{X^{\mathtt{ord}(q)}-1} = v(X) + \frac{\sum_{i=0}^{i=\mathtt{ord}(q)-1} w_i X^i}{X^{\mathtt{ord}(q)}-1} \\ &= v(X) - \Big(\sum_{i=0}^{i=\mathtt{ord}(q)-1} w_i X^i\Big)\Big(1 + X^{\mathtt{ord}(q)} + X^{2\mathtt{ord}(q)} + \ldots\Big) \end{aligned}$$

La séquence extraite de $v(X) = \sum_{i=0}^{i=k} v_i X^i$ est $(v_0, \ldots, v_k, 0, 0, \ldots)$ tandis que celle extraite du second membre est $(w_0, \ldots, w_{\mathtt{ord}(q)-1}, w_0, \ldots, w_{\mathtt{ord}(q)-1}, \ldots)$. On en déduit que

$$\underline{a} = \mathtt{seq}_{p^n}(a(X)) = (v_0, \ldots, v_k, 0, 0, \ldots) - (w_0, \ldots, w_{\mathtt{ord}(q)-1}, w_0, \ldots, w_{\mathtt{ord}(q)-1}, \ldots).$$

La soustraction se fait composante par composante dans $\mathbb{F}_{p^n}$, ainsi $\underline{a}$ est éventuelement périodique de pré-période $k+1$ ou strictement périodique. La période divise $\mathtt{ord}(q)$. L'ordre de $q$ est le plus petit entier tel que $X^T \equiv 1 \mod q$. Dans ce cas $X$ est inversible modulo $q$ et donc l'ordre de $q$ est l'ordre de $X$ modulo $q$.

$$\mathtt{ord}(q) = \mathtt{ord}_q(X).$$

Cet ordre divise l'ordre du sous groupe multiplicatif $\Big(\mathbb{F}_{p^n}[X]/(q)\Big)^*$. Si $f(X)$ et $q(X)$ sont premiers entre eux, alors $\underline{a}$ étant périodique, on note $T$ sa période et on a

$$a(X) = \frac{f(X)}{q(X)} = \frac{g(X)}{X^T-1} = \frac{-\sum_{i=0}^{i=T-1} a_i X^i}{X^T-1}.$$

Donc $q$ divise $X^T-1$. Alors $\mathtt{ord}(q)$ divise $T$. Dans ce cas, la période de $\underline{a}$ est $\mathtt{ord}(q)$. Grâce aux calculs précédents, on voit bien que $\underline{a}$ est strictement périodique si et seulement si $v(X) = 0$ ce qui signifie que $\deg(u) < \mathtt{ord}(q)$. Or $\deg(f) - \deg(q) = \deg(u) - \mathtt{ord}(q) < 0$, donc $\deg(f) < \deg(q)$. Pour la dernière assertion, c'est un cas particulier. En effet, on remarque que $\deg(f) \leq r-1$ par construction. Si $q_r \neq 0$, alors $\deg(q) = r$. Et donc on

vérifie la condition équivalente pour la stricte périodicité. Si $\deg(q) \leq \deg(f)$, alors la séquence est ultimement périodique. Soit $t$ sa pré-période et $T$ sa période. Alors

$$a(X) = \sum_{i=0}^{i=t-1} a_i X^i - X^t \frac{\sum_{i=0}^{i=T-1} a_{i+t} X^i}{X^T - 1} = \frac{(a_{t-1} - a_{t+T-1})X^{T+t-1} + \dots}{X^T - 1}.$$

La fonction génératrice a un numérateur de degré $t+T-1$ et un dénominateur de degré $T$. En effet, le degré du numérateur est inférieur ou égal à $t+T-1$. S'il est strictement inférieur à $t+T-1$, alors cela signifie que $a_{t-1} = a_{t-1+T}$, autrement dit la pré-période est inférieure à $t-1$. C'est absurde. Le degré de $a(X)$ est $t+T-1-T = t-1$. Donc $t = \deg(a)+1$. □

**Corollaire 5.4.3.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$.*

1. *Si $q(X)$ est irréductible et ne divise pas $f(X)$, alors la période de $\underline{a}$ est égale à* $\texttt{ord}(q)$ *et divise donc $|(\mathbb{F}_{p^n}[X]/(q))^*| = p^{n\deg(q)} - 1$.*
2. *Si en plus $q(X)$ est primitif, alors la période de $\underline{a}$ est $p^{n\deg(q)} - 1$.*

*Démonstration.* Si $q(X)$ est irréductible et $q(X)$ ne divise pas $f(X)$, alors $q(X)$ et $f(X)$ sont premiers entre eux. D'après le point 3) du corollaire 5.4.2, $\texttt{per}(\underline{a}) = \texttt{ord}(q)$. De plus, si $q(X)$ est primitif, il admet pour racine un élément primitif de $\mathbb{F}_{p^{n\deg(q)}} \cong \mathbb{F}_{p^n}[X]/(q)$. Donc toutes ses racines sont primitives. Soit $T$ l'ordre de $q(X)$. C'est le plus petit entier tel que $q(X)$ divise $X^T - 1$ et est aussi l'ordre de $X$ modulo $q$ qui est une racine de $q(X)$ dans $\mathbb{F}_{p^{n\deg(q)}}$ donc d'ordre $p^{n\deg(q)} - 1$. Autrement dit $q(X)$ est d'ordre $p^{n\deg(q)} - 1$. □

### 5.4.3 États initiaux

Pour un LFSR fixé, il est évident que deux états initiaux différents génèrent deux séquences différentes et donc toute séquence générée par ce LFSR admet un unique état initial. On vérifie aussi que pour tout $f(X)$ de la forme

$$\sum_{j=1}^{j=r-1} \sum_{i=0}^{i=r-j-1} q_j a_i X^{i+j} - \sum_{i=0}^{i=r-1} a_i X^i$$

, il existe un unique état initial qui génère $\texttt{seq}_{p^n}\left(\frac{f(X)}{q(X)}\right)$.

**Proposition 5.4.1.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$. Pour toute séquence de sorties, il existe un unique état initial. Pour toute fraction de la forme*

$$\frac{f(X)}{q(X)} \text{ avec } f(X) = \sum_{j=1}^{j=r-1} \sum_{i=0}^{i=r-j-1} q_j a_i X^{i+j} - \sum_{i=0}^{i=r-1} a_i X^i,$$

*il existe un unique état initial qui construit $f(X)$.*

*Démonstration.* La première partie de la proposition est évidente. La deuxième partie se démontre en considérant deux états initiaux $(a_0, \ldots, a_{r-1})$ et $(b_0, \ldots, b_{r-1})$ et en supposant que leur fonction génératrice sont égales. On a alors

$$\sum_{j=1}^{j=r-1} \sum_{i=0}^{i=r-j-1} q_j(a_i - b_i)X^{i+j} - \sum_{i=0}^{i=r-1} (a_i - b_i)X^i = 0.$$

Par identification, on trouve

$$\begin{cases} (a_0 - b_0)X^0 = 0 & \Rightarrow \quad a_0 = b_0 \\ (q_1(a_0 - b_0) - (a_1 - b_1))X^1 = 0 & \Rightarrow \quad a_1 = b_1 \\ \vdots \end{cases}$$

Par récurrence, on trouve que les deux états initiaux sont égaux. L'existence est évidente. □

## 5.5 Initialisation et Caractérisation des séquences de sorties d'un LFSR

Les séquences de sorties d'un LFSR donné sont périodiques et leurs fonctions génératrices ont pour numérateur un polynôme de degré inférieur ou égal à $r-1$ et pour dénominateur le polynôme de connexion $q(X)$. On peut donc se poser les questions inverses. Pour une fraction rationnelle $\frac{f(X)}{q(X)}$ avec $\deg(f) \leq r-1$, existe-t-il un état initial $(a_0, \ldots, a_{r-1})$ générant $\mathtt{seq}_{p^n} \frac{f(X)}{q(X)}$ à partir de $\mathcal{L}$ ?

**Proposition 5.5.1.** *Considérons le LFSR $(\mathbb{F}_{p^n}, r, q(X))$. Pour toute fraction rationnelle $\frac{f(X)}{q(X)}$ avec $\deg(f) \leq r-1$, il existe un unique état initial $(a_0, \ldots, a_{r-1})$ qui génère la séquence $\mathtt{seq}_{p^n}\left(\frac{f(X)}{q(X)}\right)$.*

*Démonstration.* Soit $f(X) = f_{r-1}X^{r-1} + \ldots + f_1X + f_0$. On cherche à déterminer $(a_0, \ldots, a_{r-1})$ tel que

$$f_{r-1}X^{r-1} + \ldots + f_1X + f_0 = \sum_{j=1}^{j=r-1} \sum_{i=0}^{i=r-j-1} q_j a_i X^{i+j} - \sum_{i=0}^{i=r-1} a_i X^i.$$

Par identification par rapport au degré, on trouve

$$\begin{cases} f_0 &= a_0 \\ f_1 &= q_1 a_0 - a_1 \\ \vdots & \\ f_{r-1} &= q_1 a_{r-2} + \ldots + q_{r-1} a_0 - a_{r-1}. \end{cases}$$

Par un calcul direct, on trouve que l'unique état initial est $(f_0, q_1 f_0 - f_1, \ldots)$. On peut aussi le démontrer matriciellement. C'est équivalent à résoudre un système linéaire représenté par la matrice suivante :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \ldots & 0 \\ q_1 & -1 & 0 & 0 & \ldots & 0 \\ q_2 & q_1 & -1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ q_r & q_{r-1} & q_{r-2} & q_{r-3} & \ldots & -1 \end{pmatrix}.$$

C'est une matrice triangulaire inférieure donc inversible. La solution existe et est unique. □

On en déduit une caractérisation des séquences de sorties d'un LFSR.

**Théorème 5.5.1.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$. Les séquences de sorties de $\mathcal{L}$ sont les séquences ayant pour fonction génératrice une fraction rationnelle de la forme $\frac{f(X)}{q(X)}$ avec $\deg(f) \leq r-1$. Autrement dit, l'ensemble des séquences de sorties de $\mathcal{L}$ est le suivant*

$$\left\{ seq_{p^n} \frac{f(X)}{q(X)} \text{ telle que } f(X) \in \mathbb{F}_{p^n}[X] \text{ et } \deg(f) \leq r-1 \right\}.$$

*Démonstration.* Toute séquence de sorties de $\mathcal{L}$ est dans cet ensemble d'après le théorème 5.4.1. Toute séquence dans cet ensemble admet un état initial qui la génère à partir de $\mathcal{L}$, d'après la proposition 5.5.1. □

**Définition 5.5.1.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$. On notera par $S(\mathcal{L})$ l'ensemble des séquences de sorties de $\mathcal{L}$.*

$$\begin{aligned} S(\mathcal{L}) &= \left\{ seq_{p^n}\left(\tfrac{f(X)}{q(X)}\right) \text{ telle que } f(X) \in \mathbb{F}_{p^n}[X] \text{ et } \deg(f) \leq r-1 \right\} \\ &= \left\{ \underline{a} \in {\mathbb{F}_{p^n}}^{\mathbb{N}} \text{ telle que } a(X) = \tfrac{f(X)}{q(X)} \text{ et } \deg(f) \leq r-1 \right\}. \end{aligned}$$

*On peut aussi dire que la série formelle $a(X)q(X)$ doit être un polynôme de $\mathbb{F}_{p^n}$ de degré inférieur ou égal à la taille de $\mathcal{L}$ moins un.*

Il y a $p^{nr}$ séquences de sorties différentes pour un LFSR donné de taille $r$. Définissons le diagramme $\mathcal{D}_{\mathcal{L}}$ de la figure 5.7. $\Delta$ associe à tout état initial sa séquence de sorties

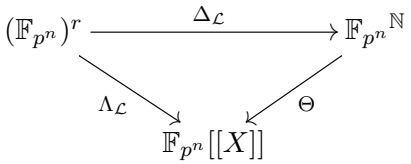



FIGURE 5.7 – Diagramme $\mathcal{D}_{\mathcal{L}}$

générée par $\mathcal{L}$ et $\Lambda$ associe à tout état $(a_0, \ldots, a_{r-1})$ la fraction rationnelle $\frac{f(X)}{q(X)}$ où $f(X) = \sum_{j=1}^{j=r-1} \sum_{i=0}^{i=r-j-1} q_j a_i X^{i+j} - \sum_{i=0}^{i=r-1} a_i X^i$.

**Corollaire 5.5.1.** *Si on se fixe un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$, le diagramme $\mathcal{D}_\mathcal{L}$ vérifie les points suivants :*

1. *$\mathcal{D}_\mathcal{L}$ est commutatif.*
2. *$\Delta_\mathcal{L}$, $\Lambda_\mathcal{L}$ et $\Theta$ sont des morphismes de $\mathbb{F}_{p^n}$-espaces vectoriels.*
3. *$\Theta$ est un isomorphisme.*
4. *$\Delta_\mathcal{L}$ et $\Lambda_\mathcal{L}$ sont injectifs.*
5. *L'image de $\Delta_\mathcal{L}$ est incluse dans l'ensemble des séquences périodiques dont la période divise $\mathtt{ord}(q)$.*
6. *L'image de $\Lambda_\mathcal{L}$ est l'ensemble des fractions rationnelles de dénominateur $q(X)$ et dont le degré du numérateur est inférieur ou ègal à $r-1$.*
7. *$\Delta_\mathcal{L}$ est un isomorphisme de $(\mathbb{F}_{p^n})^r$ dans $\mathcal{S}(\mathcal{L})$.*
8. *$\Lambda_\mathcal{L}$ est isomorphisme de $(\mathbb{F}_{p^n})^r$ dans $\left\{\frac{f(X)}{q(X)}; \deg(f) \leq r-1\right\}$.*

*Démonstration.*

1. Par construction, $\mathcal{D}_\mathcal{L}$ est commutatif.
2. Considérons deux états initiaux $e = (a_0, \ldots, a_{r-1})$ et $e' = (b_0, \ldots, b_{r-1})$. Soit $e'' = (c_0, \ldots, c_{r-1}) = e + e'$. Alors

$$c_r = \sum_{i=1}^{i=r} q_i c_{r-i} = \sum_{i=1}^{i=r} q_i (a_{r-i} + b_{r-i}) = \sum_{i=1}^{i=r} q_i a_{r-i} + \sum_{i=1}^{i=r} q_i b_{r-i} = a_r + b_r.$$

   De même pour la multiplication par un scalaire. L'application $\Delta$ est donc un isomorphisme entre espaces vectoriels.

$$\begin{aligned}
\Lambda(e) + \Lambda(e') &= \sum_{j=1}^{j=r-1} \sum_{i=0}^{i=r-j-1} q_j a_i X^{i+j} - \sum_{i=0}^{i=r-1} a_i X^i + \sum_{j=1}^{j=r-1} \sum_{i=0}^{i=r-j-1} q_j b_i X^{i+j} - \sum_{i=0}^{i=r-1} b_i X^i \\
&= \sum_{j=1}^{j=r-1} \sum_{i=0}^{i=r-j-1} q_j (a_i + b_i) X^{i+j} - \sum_{i=0}^{i=r-1} (a_i + b_i) X^i \\
&= \sum_{j=1}^{j=r-1} \sum_{i=0}^{i=r-j-1} q_j c_i X^{i+j} - \sum_{i=0}^{i=r-1} c_i X^i \\
&= \Lambda(e'') = \Lambda(e + e')
\end{aligned}$$

   De même pour la multiplication par un scalaire. L'application $\Lambda$ est donc un morphisme d'espaces vectoriels.

3. Déjà démontré.

4. D'après la proposition 5.4.1, $\Delta$ et $\Lambda$ sont injectifs.
5. D'après le corollaire 5.4.2, les séquences de sorties sont périodiques et leur périodes divise $\mathtt{ord}(q)$.
6. D'après le théorème 5.4.1 et la proposition 5.5.1, $\mathtt{Im}(\Lambda_{\mathcal{L}}) = \left\{\frac{f(X)}{q(X)}; \deg(f) \leq r-1\right\}$.
7. Comme $\Theta$ est un isomorphisme et que $\mathcal{D}_{\mathcal{L}}$ est commutatif, alors

$$\begin{aligned}\mathtt{Im}(\Delta_{\mathcal{L}}) = \quad & \mathtt{Im}(\Theta^{-1} \circ \Lambda_{\mathcal{L}}) = \Theta^{-1}\left\{\frac{f(X)}{q(X)}; \deg(f) \leq r-1\right\} \\ = \quad & \left\{\frac{f(X)}{q(X)}; \deg(f) \leq r-1\right\} = S(\mathcal{L}).\end{aligned}$$

8. Les points 7 et 8 sont une conséquence directe des points précédents.

□

## 5.6 Initialisation et caractérisation des LFSRs générant une séquence périodique

De manière équivalente, pour une fraction rationnelle $a(X) = \frac{f(X)}{q(X)}$ dont le dénominateur ne s'annule pas en 0, quels sont les LFSRs et les états initiaux qui génèrent $\mathtt{seq}_{p^n}(a(X))$ ? Existe-t-il un LFSR et un état initial générant cette séquence ? Voici un algorithme qui permet d'obtenir un LFSR de polynôme de connexion $q(X)$.

**Algorithme 5.6.1.**

1. *On doit écrire $a(X)$ avec un dénominateur de la forme $q_r X^r + \ldots + q_1 X - 1$. $q(X)$ sécrit $\sum_{i=0}^{i=r} q_i X^i$ avec $q(0) = q_0 \neq 0$ et $q_r \neq 0$. On inverse $q(0)$ dans $\mathbb{F}_{p^n}$. On calcule $a(X) = \dfrac{(-q_0)^{-1} f(X)}{(-q_0)^{-1} q(X)}$ et le dénominateur vérifie donc la condition recherchée. Supposons maintenant que $a(X)$ vérifie déjà cette condition.*
2. *On compare $\deg(f)$ et $\deg(q)$.*
   (a) *Si $\deg(f) + 1 \leq \deg(q)$, alors d'après la proposition 5.5.1, le LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, \deg(q), q(X))$ génère la séquence $\mathtt{seq}_{p^n}(a(X))$ ; l'état initial est déterminé de manière unique par $f$ en suivant le calcul de la démonstration de la proposition 5.5.1.*
   (b) *Si $\deg(f) + 1 > \deg(q)$, alors on écrit $q(X)$ de la forme $\sum_{i=1}^{i=\deg(f)+1} q_i X^i - 1$ avec les $q_i = 0$ pour $\deg(q) + 1 \leq i \leq \deg(f) + 1$. On considère le LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, deg(f)+1, q(X))$. D'après la proposition 5.5.1 et sa démonstration, on peut calculer l'unique état initial qui génère $\mathtt{seq}_{p^n}(a(X))$.*
3. *L'état initial se calcule ainsi*
   (a) *$a_0 = f_0$.*

*(b) Pour tout* $i = 1, \ldots, r-1$, *on calcule* $a_i = \sum_{k=0}^{k=r-1} q_{i-k}a_k - f_k$.

4. *On retient en sortie* $\mathcal{L} = (\mathbb{F}_{p^n}, \max(\deg(f)+1, \deg(q)), q(X))$ *et l'état initial* $(a_0, \ldots, a_{r-1})$.

**Proposition 5.6.1.** *Soit une fraction rationnelle* $\frac{f(X)}{q(X)}$ *avec* $q(0) \neq 0$. *Supposons que l'algorithme 5.6.1 ait été appliqué. Alors le LFSR* $\mathcal{L} = (\mathbb{F}_{p^n}, \max(\deg(f)+1, \deg(q)), -q(0)^{-1}q(X))$ *et l'état initial construit par l'algorithme génèrent la séquence* $\mathtt{seq}_{p^n}\left(\frac{f(X)}{q(X)}\right)$.

Tout d'abord, la proposition 5.6.1 donne le LFSR et l'état initial les plus naturels qui génèrent la séquence $seq_{p^n}\left(\frac{f(X)}{q(X)}\right)$ avec $q(0) \neq 0$. Elle fournit aussi une définition équivalente des LFSR séquences (ou séquences récurrentes linéaires).

**Théorème 5.6.1.** *La séquence* $\underline{a}$ *est une LFSR séquence (ou séquence récurrente linéaire) si et seulement si sa fonction génératrice est une fraction rationnelle dont le dénominateur ne s'annule pas en 0, c'est-à-dire* $a(X)$ *appartient à* $\mathbb{F}_{p^n}[X]_{(X)} = (\mathbb{F}_{p^n}[X]\backslash(X))^{-1}\mathbb{F}_{p^n}[X]$.

*Démonstration.* D'après le théorème 5.4.1, la fonction génératrice d'une LFSR séquence est une fraction rationnelle avec pour dénominateur le polynôme de connexion défini de telle sorte que $q(0) = -1$. Inversement d'après l'algorithme 5.6.1, d'une fraction rationnelle dont le dénominateur ne s'annule pas en 0, on peut construire un LFSR qui génère la séquence extraite du développement en série formelle de la fraction rationnelle. □

C'est une reformulation du thèorème 3.10.1. Nous avons caractériser les séquences de sorties d'un LFSR. Nous donnons dans la suite une caractérisation des LFSRs générant une séquence.

**Définition 5.6.1.** *Soit* $\underline{a}$ *une séquence périodique. Posons* $R(\underline{a})$ *l'ensemble des LFSRs qui génèrent* $\underline{a}$.

$$R(\underline{a}) = \{\mathcal{L} \text{ tel que } \underline{a} \in S(\mathcal{L})\}.$$

**Théorème 5.6.2.** *Pour toute séquence périodique* $\underline{a}$ *de fonction génératrice* $a(X)$,

$$R(\underline{a}) = \left\{ \begin{array}{ll} \mathcal{L} = (\mathbb{F}_{p^n}, r, q(X)) \text{ tel que} & q(0) = -1,\ q(X)a(X) \in \mathbb{F}_{p^n}[X] \\ & \text{et } r \geq \max(\deg(qa)+1, \deg(q)) \end{array} \right\}.$$

*Démonstration.* D'après le théorème 5.4.1, si $\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$ génère $\underline{a}$, alors $a(X) = \frac{f(X)}{q(X)}$ et $\deg(f) \leq r-1$. On en déduit donc que $q(X)a(X)$ est un polynôme de degré inférieur ou égal à $r-1$ et donc que $r \geq \deg(qa)+1$. De plus, par définition le LFSR vérifie $r \geq \deg(q)$ et $q(0) = -1$. Tout LFSR générant $\underline{a}$ est dans cet ensemble.

Inversement, soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$ vérifiant les trois conditions citées dans le théorème. On vérifie bien que c'est un LFSR, c'est-à-dire que $r$ la taille du registre est supérieure au degré du polynôme de connexion $q(X)$ et $q(0) = -1$. De plus, la fonction génératrice $a(X)$ de $\underline{a}$ vérifie les hypothèses de la proposition 5.5.1. Il existe un état initial qui génère $\underline{a}$ à partir de $\mathcal{L}$. □

À partir d'une expression en fraction rationnelle de $a(X)$, on peut décrire tous les LFSRs générant $\underline{a}$. Choisissons $a(X) = \frac{f(X)}{q(X)}$ avec $q(0) = -1$.

Comme dans la remarque 5.4.1, la taille des LFSRs de polynôme de connexion $q(X)$ générant $\underline{a}$ est supérieur ou égale à $\deg(q)$. Le plus naturel, c'est à dire le registre de plus petite taille pour ce polynôme de connexion $q(X)$ est celui généré par l'algo. 5.6.1, $\mathcal{L} = (\mathbb{F}_{p^n}, \max(\deg(f)+1, \deg(q)), q(X))$. Ensuite on peut faire varier la taille en ajoutant des coefficients de connexion $q_{r+1} = q_{r+2} = \ldots = q_{r+k} = 0$. Dans ce cas on aura les LFSRs $(\mathbb{F}_{p^n}, r+k, q(X))$ pour tout $k$ positif.

Pour changer de polynôme de connexion, on peut soit multiplier $a(X)$ par un inversible, soit réduire $a(X)$. Si on multiplie numérateur et dénominateur de la fraction rationnelle par un polynôme $g(X)$ vérifiant $g(0) \neq 0$ , l'algorithme 5.6.1 appliqué à $\frac{f(X)g(X)}{q(X)g(X)}$ donne en sortie un LFSR de taille $\max(\deg(f)+1, \deg(q)) + \deg(g)$ et de polynôme de connexion $g(0)^{-1}g(X)q(X)$. Si on réduit la fraction, on obtient en sortie un LFSR de taille réduite. En effet, soit $g(X)$ un diviseur commun de $f(X)$ et $q(X)$, alors l'algorithme 5.6.1 appliqué à $\frac{f(X)/g(X)}{q(X)/g(X)}$ donne en sortie un LFSR de taille $\Big(\max(\deg(f)+1, \deg(q)) - \deg(g)\Big)$ et de polynôme de connexion $g(0)\frac{q(X)}{g(X)}$. Pour augmenter la taille pour chacun de ces polynômes de connexion, il suffit d'opérer comme précédemment.

En bref, une séquence périodique correspond à une série formelle $a(X)$ qui peut s'écrire comme une fraction rationnelle irréductible $\frac{f(X)}{q(X)}$ avec $q(0) = -1$. Les polynômes de connexion des LFSRs de $R(\underline{a})$ sont donc tous les multiples de $q$ ($q$ multiplié par un polynôme qui prend la valeur -1 en 0). Ensuite la plus petite taille pour chacun de ces polynômes de connexion est leur degré respectif. Pour faire varier la taille, on ne peut que l'augmenter en ajoutant des coefficients de connexion nuls tout en gardant le même polynôme de connexion.

On a donc décrit une méthode qui fournit tous les LFSRs de $R(\underline{a})$. Maintenant, on remarque qu'en réduisant la fraction sous forme irréductible, on obtient le polynôme de connexion de plus bas degré (*polynôme de connexion minimal*) et donc *le LFSR de plus petite taille* dans $R(\underline{a})$.

## 5.7 LFSR de taille minimale et Complexité linéaire

**Définition 5.7.1** (Complexité linéaire)**.** *Soit $\underline{a}$ une séquence périodique. On appelle Complexité linéaire ou complexité linéaire de cette séquence, la taille du plus petit LFSR générant cette séquence. On la note $LS(\underline{a})$.*

$$LS(\underline{a}) = \inf_r \{\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X)) \text{ tel que } \mathcal{L} \in R(\underline{a})\}.$$

*Cette notation vient de l'anglais Linear Span (durée linear) dit aussi linear complexity.*

**Exemple 5.7.1.** *La séquence $\underline{a} = (110110\ldots)$ a une complexité linéaire égale à 2, puisqu'elle est générée par le LFSR $(\mathbb{F}_2, 2, X^2+X-1)$ et qu'elle ne peut pas être générée par un LFSR de plus petite taille, en l'occurrence de taille 1.*

**Proposition 5.7.1.** *Soit une fraction rationnelle* $\frac{f(X)}{q(X)}$ *telle que* $f(X)$ *et* $q(X)$ *soient premiers entre eux et* $q(0) \neq 0$. *Soit* $\mathcal{L}$ *le LFSR en sortie de l'algorithme 5.6.1. Alors* $\mathcal{L}$ *est le LFSR de plus petite taille qui génère* $\mathtt{seq}_{p^n}\left(\frac{f(X)}{q(X)}\right)$. *On a :*

$$LS(\underline{a}) = \max(\deg(f) + 1, \deg(q)).$$

*Démonstration.* Tout d'abord $\mathcal{L}$ a pour polynôme de connexion $-q(0)^{-1}q(X)$ et pour taille

$$\max(\deg(-q(0)^{-1}f) + 1, \deg(-q(0)^{-1}q)) = \max(\deg(f) + 1, \deg(q)).$$

Soit un autre LFSR $\mathcal{L}' = (\mathbb{F}_{p^n}, r', s(X))$ qui génère $\mathtt{seq}_{p^n}\frac{f(X)}{q(X)}$. Alors il existe $g(X) \in \mathbb{F}_{p^n}$ tel que

$$f(X)s(X) = g(X)q(X).$$

Comme $f(X)$ et $q(X)$ sont premiers entre eux alors $q(X)$ divise $s(X)$ et $f(X)$ divise $g(X)$. Donc $\deg(q) \leq \deg(s)$ et $\deg(f) \leq \deg(g)$. Donc $\max(\deg(f)+1, \deg(q)) \leq \max(\deg(g)+1, \deg(s))$. La taille de $\mathcal{L}$ est plus petite que la taille de $\mathcal{L}'$. □

On vient de donner une méthode pour obtenir le plus petit LFSR générant une séquence périodique fixée. Cela consiste en la réduction de la fraction rationnelle représentant sa fonction génératrice. On a en même temps introduit une notion de polynôme de connexion minimal pour une séquence périodique fixée. Il s'obtient en transformant la fonction génératrice de cette séquence en fraction rationnelle irréductible. Ce polynôme divise tous les autres polynômes de connexion des LFSR générant cette séquence. On verra par la suite plus en détail l'étude de ce polynôme minimal de connexion. En particulier :

**Corollaire 5.7.1.** *Si* $q(X)$ *est un polynôme irréductible dans* $\mathbb{F}_{p^n}$, $q(X)$ *ne divise pas* $f(X)$ *et* $q(0) \neq 0$, *alors le LFSR en sortie de l'algorithme 5.6.1 est le plus petit générant* $\mathtt{seq}_{p^n}\left(\frac{f(X)}{q(X)}\right)$.

*Démonstration.* On déduit des hypothèses du corollaire que $f(X)$ et $q(X)$ sont premiers entre eux et donc on se trouve dans un cas particulier de la proposition 5.7.1. □

**Théorème 5.7.1.** *Soit* $\underline{a}$ *une séquence ultimement périodique et* $a(X)$ *sa fonction génératrice.*

$$LS(\underline{a}) = \inf\left\{\max(\deg(qa) + 1, \deg(q)) \text{ tel que } q(X)a(X) \in \mathbb{F}_{p^n}[X] \text{ et } q \neq 0\right\}.$$

*Démonstration.* $q(X)$ est un polynôme de connexion pour $\underline{a}$ si $q(X)a(X) \in \mathbb{F}_{p^n}[X]$ et $q(0) = -1$. Le plus petit LFSR générant $\underline{a}$ de polynôme de connexion noté $m(X)$ est de taille $\max(\deg(ma) + 1, \deg(m))$. Donc la complexité linéaire de $\underline{a}$ est le minimum des $\max(\deg(qa) + 1, \deg(q))$ pour $q(X)a(X) \in \mathbb{F}_{p^n}[X]$ et $q(0) = -1$. Cette dernière condition peut être remplacée par $q \neq 0$. En effet, notons $E$ l'ensemble des polynômes

$q(X)$ tels que $q(X)a(X) \in \mathbb{F}_{p^n}[X]$ et $q \neq 0$ ; et $E^{'}$ le sous-ensemble des polynômes de $E$ tels que $q(0) = -1$. Comme $E^{'} \subseteq E$ alors

$$d = \inf_{q \in E} \{\max(\deg(qa) + 1, \deg(q))\} \leq d^{'} = \inf_{q \in E^{'}} \{\max(\deg(qa) + 1, \deg(q))\}.$$

Soit $m$ un polynôme de $E$ tel que $d = \max(\deg(ma)+1, \deg(m))$. Supposons que $m(0) = 0$, alors il existe $k$ et $m^{'}(X)$ tels que $m(X) = X^k m^{'}(X)$ et $m^{'}(0) \neq 0$. Il existe donc un polynôme $f(X)$ tel que $X^k m^{'}(X)a(X) = f(X) \in \mathbb{F}_{p^n}[X]$. On en déduit que $X^k$ divise $f(X)$. Donc il existe un polynôme $f^{'}(X)$ tel que $f(X) = X^k f^{'}(X)$. Donc $m^{'}(X)a(X) = f^{'}(X)$ et $m^{'}(0) \neq 0$. En multipliant par $-m^{'}(0)^{-1}$ dans $\mathbb{F}_{p^n}$, on peut supposer que $m^{'}(0) = -1$. Donc $m^{'} \in E^{'}$ et $\max(\deg(m^{'}a)+1, \deg(m^{'})) \geq d^{'}$. On observe que $\deg(m^{'}) < \deg(m)$ et $\deg(f^{'}) < \deg(f)$, donc

$$d^{'} \leq \max(\deg(m^{'}a) + 1, \deg(m^{'})) < \max(\deg(ma) + 1, \deg(m)) = d \leq d^{'}.$$

On en déduit que l'hypothèse $m(0) = 0$ est impossible. Donc $m(0) \neq 0$, en multipliant par $-m^{'}(0)^{-1}$, on peut supposer que $m(0) = -1$ et on a $m \in E^{'}$ et donc $d^{'} \leq d$. En conclusion $d = d^{'}$. □

**Corollaire 5.7.2.** *Si $\underline{a}$ est strictement périodique, alors*

$$LS(\underline{a}) = \inf \{\deg(q) \text{ tel que } q(X)a(X) \in \mathbb{F}_{p^n}[X] \text{ et } q \neq 0\}.$$

*Démonstration.* L'argument est simple. La stricte périodicité implique d'après le théorème 5.4.2 que pour toute écriture en fraction rationnelle de $a(X)$, le degré du numérateur $q(X)a(X)$ soit strictement inférieur à celui du dénominateur $q(X)$. Donc le maximum est $\deg(q)$. □

**Théorème 5.7.2.** *Les LFSR séquences sont les séquences périodiques. Soit une séquence périodique $\underline{a}$ dans $\mathbb{F}_{p^n}$ de période $r$ et de pré-période de longueur $T$. Le LFSR $(\mathbb{F}_{p^n}, T + r, X^r - 1)$ génère $\underline{a}$ à partir de l'état initial $(a_0, \ldots, a_{r+T-1})$. Le LFSR de plus petite taille a pour polynôme de connexion*

$$\frac{X^r - 1}{\mathtt{PGCD}\Big(f(X), X^r - 1\Big)}$$

*avec* $f(X) = (X^r - 1) \sum_{i=0}^{i=T-1} a_i X^i - X^T \sum_{i=0}^{i=r-1} a_{i+T} X^i$.

*Démonstration.* D'après le corollaire 5.4.2, une LFSR séquence est périodique. Inversement une séquence périodique a pour fonction génératrice une fraction rationnelle avec pour dénominateur un polynôme premier avec $X$, d'après l'algorithme 5.6.1, il existe donc un LFSR qui la génère, c'est donc une LFSR séquence. Si $\underline{a}$ est de période $r$ et de pré-période $T$, alors

$$a(X) = \sum_{i=0}^{i=T-1} a_i X^i - X^T \frac{\sum_{i=0}^{i=r-1} a_{i+T} X^i}{X^r - 1} = \frac{(X^r - 1) \sum_{i=0}^{i=T-1} a_i X^i - X^T \sum_{i=0}^{i=r-1} a_{i+T} X^i}{X^r - 1}.$$

Le degré du numérateur est $r+T-1$ puisque le coefficient du monôme $X^{r+T-1}$ est $a_{T-1}-a_{r+T-1}$. Or si ce coefficient était nul, la pré-période serait de longueur au plus $T-1$. D'après l'algorithme 5.6.1, le LFSR $(\mathbb{F}_{p^n}, r+T, X^r-1)$ et l'état initial $(a_0,\ldots,a_{r+T-1})$ génère $\underline{a}$.

$$\frac{f(X)}{X^r-1} = \frac{\frac{f(X)}{\mathtt{PGCD}(f(X),X^r-1)}}{\frac{X^r-1}{\mathtt{PGCD}(f(X),X^r-1)}}.$$

$\frac{f(X)}{\mathtt{PGCD}(f(X),X^r-1)}$ et $\frac{X^r-1}{\mathtt{PGCD}(f(X),X^r-1)}$ sont premiers entre eux, d'après la proposition 5.7.1, le plus petit LFSR générant $\underline{a}$ a pour polynôme de connexion $\frac{X^r-1}{\mathtt{PGCD}(f(X),X^r-1)}$. □

## 5.8 Polynôme de connexion minimal

### 5.8.1 Définitions et Généralités

Dans cette section, pour une séquence donnée $\underline{a}$, nous étudions les polynômes de connexion des LFSRs de $R(\underline{a})$, en particulier le polynôme de connexion minimal.

**Définition 5.8.1.** *Soit $\underline{a}$ une séquence périodique, on définit l'ensemble suivant*

$$A(\underline{a}) = \{q(X) \in \mathbb{F}_{p^n}[X] \text{ tel que } q(X)a(X) \in \mathbb{F}_{p^n}[X]\}.$$

*Il contient l'ensemble des polynômes de connexion des LFSRs qui génèrent $\underline{a}$ modulo un inversible :*

$$\left\{q(X) \in \mathbb{F}_{p^n}[X] \text{ tel que } \exists r \in \mathbb{N}^*; (\mathbb{F}_{p^n}, r, -q(0)^{-1}q) \in R(\underline{a})\right\} \subseteq A(\underline{a}).$$

**Proposition 5.8.1.** *Pour toute séquence périodique $\underline{a}$,*

1. *$A(\underline{a}) \neq \{0\}$.*
2. *C'est un idéal de l'anneau $\mathbb{F}_{p^n}[X]$ qui contient une infinité de polynômes.*
3. *$\underline{a} = \underline{0}$ si et seulement si $A(\underline{a}) = \mathbb{F}_{p^n}[X]$.*

*Démonstration.* Soit $r$ la période de $\underline{a}$. Alors d'après le théorème 5.7.2, il existe un LFSR naturel de polynôme de connexion $X^r-1$ qui génère $\underline{a}$. Donc $X^{\mathtt{per}(\underline{a})}-1 \in A(\underline{a})$.
Soient $P$ et $Q$ deux polynômes de $A(\underline{a})$. Soit $R$ un polynôme quelconque de $\mathbb{F}_{p^n}[X]$.

$$(P-Q)(X)a(X) = P(X)a(X) - Q(X)a(X) \in \mathbb{F}_{p^n}[X].$$

$$(RQ)(X)a(X) = R(X)Q(X)a(X) \in \mathbb{F}_{p^n}[X].$$

C'est bien un idéal de $\mathbb{F}_{p^n}[X]$. Il contient l'idéal engendré par $X^r-1$, donc une infinité de polynômes. Tout polynôme $Q$ dans $\mathbb{F}_{p^n}$ vérifie

$$Q(X).0 = 0,$$

où 0 est la fonction génératrice de la séquence nulle, $\underline{0}$. Inversement, si tout polynôme dans $\mathbb{F}_{p^n}[X]$ vérifie cette relation, alors c'est valable pour le polynôme constant 1. Donc

$$1.a(X) = 0 \Rightarrow \underline{a} = \underline{0}.$$

□

**Proposition 5.8.2.** *Pour toute séquence périodique $\underline{a}$, il existe un unique polynôme non-nul de plus bas degré dans $A(\underline{a})$ et de terme constant -1.*

*Démonstration.* Pour l'unicité, soient deux polynômes $Q_1$ et $Q_2$ non-nuls de plus bas degré. Comme $\mathbb{F}_{p^n}[X]$ est euclidien, alors on peut faire la division euclidienne de $Q_1$ par $Q_2$. Il existe donc $P$ et $R$ tels que

$$Q_1(X) = Q_2(X)P(X) + R(X) \text{ tel que } \deg(R) < \deg(Q_2).$$

On a alors

$$\begin{array}{rcl} Q_1(X)a(X) & = & P(X)Q_2(X)a(X) + R(X)a(X) \\ R(X)a(X) & = & Q_1(X)a(X) - P(X)Q_2(X)a(X) \\ R(X)a(X) & \in & \mathbb{F}_{p^n}[X] \end{array}$$

Donc $R$ est un polynôme de $A(\underline{a})$ de degré strictement inférieur au minimum des degrés des polynômes de $A(\underline{a})$. On en déduit que $R = 0$ et donc $Q_2$ divise $Q_1$. Par symétrie, on en conclut que $Q_1$ divise $Q_2$, donc $Q_1 = Q_2$. Pour l'existence, comme $A(\underline{a})$ contient $X^r - 1$, ou bien $X^r - 1$ est de plus bas degré ou bien c'est un autre polynôme de degré strictement inférieur à $r$. Comme le polynôme minimal divise $X^r - 1$, donc son terme constant est non nul, sinon $X$ diviserait $X^r - 1$. Il suffit ensuite de diviser par l'opposé du terme constant. □

**Définition 5.8.2** (polynôme de connexion minimal)**.** *L'unique polynôme de terme constant -1 de plus bas degré de $A(\underline{a})$ est appelé polynôme de connexion minimal de $\underline{a}$.*

**Exemple 5.8.1.** *Le polynôme de connexion minimal de la séquence nulle est le polynôme constant $-1$. C'est le polynôme de connexion du registre de taille $r = 0$, c'est à dire le registre nul $(\mathbb{F}_{p^n}, 0, -1)$. Le polynôme de connexion minimal d'une séquence périodique non-nulle de période 1 est $X - 1$. En effet, toute séquence de la forme $\underline{a} = (a, a, \ldots)$ avec $a \neq 0$, peut être générée par le LFSR $(\mathbb{F}_{p^n}, 1, X - 1)$. Donc $X - 1 \in A(a, a, \ldots)$. Si $X - 1$ n'est pas le polynôme de connexion minimal de $(a, a, \ldots)$, alors c'est un polynôme constant, unitaire, donc c'est la constante $-1$ ce qui impliquerait que $a(X) \in \mathbb{F}_{p^n}[X]$. Or*

$$a(X) = a + aX + \ldots + aX^n + \ldots = \frac{-a}{X - 1}.$$

*On en déduit que $X - 1$ divise $-a$, ce qui est absurde. Le polynôme $X - 1$ est le polynôme de connexion minimal.*

**Théorème 5.8.1.** *Soit $\underline{a}$ une séquence périodique, alors l'idéal $A(\underline{a})$ est un idéal principal généré par le polynôme de connexion minimal de $\underline{a}$.*

*Démonstration.* Pour la séquence nulle, $A(\underline{a})$ est $\mathbb{F}_{p^n}[X]$ qui peut être vu comme l'idéal engendré par 1. L'anneau $\mathbb{F}_{p^n}[X]$ est euclidien donc principal. Tout idéal de $\mathbb{F}_{p^n}[X]$ est principal, donc pour toute séquence périodique non-nulle dans $\mathbb{F}_{p^n}$, il existe un polynôme $m(X) \neq 0$ tel que $A(\underline{a}) = m(X).\mathbb{F}_{p^n}[X]$. On en déduit que $m(X)$ divise le polynôme de connexion minimal de $\underline{a}$, donc il est de degré inférieur ou égal au plus bas degré des

polynômes de $A^*(\underline{a})$. On en déduit qu'il est de plus bas degré. Ainsi $m(X)$ est le polynôme de connexion minimal de $\underline{a}$ à un inversible près. L'idéal $A(\underline{a})$ est généré par le polynôme minimal de $\underline{a}$. D'une autre manière, soit un polynôme $Q(X) \in A(\underline{a})$. Notons $m_{\underline{a}}(X)$ le polynôme de connexion minimal de $\underline{a}$. On fait la division euclidienne de $Q$ par $m_{\underline{a}}$.

$$Q(X) = P(X)m_{\underline{a}}(X) + R(X) \text{ tel que } \deg(R) < \deg(m_{\underline{a}}).$$

On en déduit que $R(X)a(X) = Q(X)a(X) - P(X)m_{\underline{a}}(X)a(X) \in \mathbb{F}_{p^n}[X]$, et donc que $R \in A(\underline{a})$. Or $R$ est de degré strictement inférieur au degré le plus bas, donc $R = 0$. On vient de démontrer que $A(\underline{a}) \subseteq m_{\underline{a}}.\mathbb{F}_{p^n}$. Comme $A(\underline{a})$ est un idéal, alors $m_{\underline{a}}(X).\mathbb{F}_{p^n}[X] \subseteq A(\underline{a})$. □

**Notation 5.8.1.** *Le polynôme de connexion minimal d'une séquence périodique $\underline{a}$ sera noté $m_{\underline{a}}(X)$.*

### 5.8.2 Complexité linéaire

Dans cette sous-section, nous établissons le lien entre la complexité linéaire d'une séquence périodique et son polynôme de connexion minimal. Rappelons que

$$LS(\underline{a}) = \inf\left\{\max(\deg(qa) + 1, \deg(q)) \text{ tel que } q \in A(\underline{a})\right\}.$$

**Théorème 5.8.2.** *Soit $\underline{a}$ une séquence ultimement périodique. Alors*

$$LS(\underline{a}) = \max(\deg(m_{\underline{a}}.a) + 1, \deg(m_{\underline{a}})).$$

*Démonstration.* Soit $q \in A(\underline{a})$ tel que $a(X) = \frac{f(X)}{q(X)} = \frac{h(X)}{m_{\underline{a}}(X)}$. L'étude des degrés donne $\deg(q) \geq \deg(m_{\underline{a}})$ et

$$\begin{array}{rcl} \deg(f) - \deg(q) = \deg(h) - \deg(m_{\underline{a}}) & \Rightarrow & \deg(f) + 1 = \deg(h) + 1 + (\deg(q) - \deg(m_{\underline{a}})) \\ & \Rightarrow & \deg(f) + 1 \geq \deg(h) + 1. \end{array}$$

Donc $\max(\deg(f)+1, \deg(q)) \geq \max(\deg(h)+1, \deg(m_{\underline{a}}))$. Autrement dit, $\max(\deg(m_{\underline{a}}.a)+1, \deg(m_{\underline{a}}))$ est la taille minimale des LFSR générant la séquence en question. C'est donc la complexité linéaire. □

**Corollaire 5.8.1.** *Si $\underline{a}$ est strictement périodique alors*

$$LS(\underline{a}) = \deg(m_{\underline{a}}).$$

*Démonstration.* D'après le corollaire 5.4.2, $\underline{a}$ étant strictement périodique, $\deg(f) < \deg(q)$. Donc $\deg(h) < \deg(m_{\underline{a}})$ et $\max(\deg(h) + 1, \deg(m_{\underline{a}})) = \deg(m_{\underline{a}})$. □

### 5.8.3 Structure de $G(q)$

Dans cette sous-section, nous traitons la question de savoir quelles sont les séquences périodiques ayant pour polynôme de connexion un polynôme donné.

**Définition 5.8.3.** *Soit $q(X)$ un polynôme dans $\mathbb{F}_{p^n}$ de la forme $q(X) = q_r X^r + \ldots + q_1 X - 1$. Posons $G(q)$ l'ensemble des séquences périodiques ayant pour polynôme de connexion $q$.*

$$\begin{aligned} G(q) &= \left\{\underline{a} \in {\mathbb{F}_{p^n}}^{\mathbb{N}} \text{ telle que } a(X)q(X) \in \mathbb{F}_{p^n}[X]\right\} \\ &= \left\{\underline{a} \in {\mathbb{F}_{p^n}}^{\mathbb{N}} \text{ telle que } q(X) \in A(\underline{a})\right\}. \end{aligned}$$

*C'est l'ensemble des séquences telles que leur fonction génératrices soit une fraction rationnelle de dénominateur $q$. Elles sont donc périodiques.*

Munissons l'espace des séries formelles $\mathbb{F}_{p^n}[[X]]$ de sa structure naturelle d'espace vectoriel.

$$a(X) + b(X) = (a_0 + b_0) + \ldots + (a_n + b_n)X^n + \ldots$$
$$\lambda a(X) = (\lambda a_0) + \ldots + (\lambda a_n)X^n + \ldots$$

**Proposition 5.8.3.** *$G(q)$ est un sous espace vectoriel non-vide de ${\mathbb{F}_{p^n}}^{\mathbb{N}}$. Il contient une infinité de séquences périodiques. Pour tout $r \geq \deg(q)$, $S(\mathcal{L}) \subset G(q)$ avec $\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$.*

*Démonstration.* Soient $\underline{a}$ et $\underline{b}$ deux séquences périodiques de $G(q)$. Alors $(a(X)+b(X))q(X) = a(X)q(X) + b(X)q(X) \in \mathbb{F}_{p^n}[X]$. Donc la fonction génératrice de $\underline{a} \oplus \underline{b}$ multipliée par $q$ est un polynôme. De même pour $\lambda\underline{a}$. Donc $G(q)$ est un espace vectoriel.
Soit un entier $r \geq \deg(q)$. On peut définir le LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$. L'ensemble des séquences de sorties $S(\mathcal{L})$ ont pour fonction génératrice $a(X)$ vérifiant $a(X)q(X) \in \mathbb{F}_{p^n}[X]$. Donc $S(\mathcal{L}) \subset G(q)$. L'ensemble $G(q)$ contient donc une infinité de séquences périodiques. □

## 5.9 Période et ordre du Polynôme minimal de connexion

Dans cette section, nous étudions le rapport entre la période d'une séquence donnée et son polynôme de connexion minimal.

**Théorème 5.9.1.** *Soit $\underline{a}$ une séquence périodique. Soit $m_{\underline{a}}$ son polynôme de connexion minimal.*

1. *La période $\underline{a}$ est l'ordre de $m_{\underline{a}}$.*
2. *Si $\deg(m_{\underline{a}}a) < \deg(m_{\underline{a}})$, alors $\underline{a}$ est strictement périodique.*
3. *Sinon $\underline{a}$ est ultimement périodique de pré-période $\deg(a) + 1$.*

*Démonstration.* D'après le corollaire 5.4.2, la période de $\underline{a}$ divise $\mathtt{ord}(m_{\underline{a}})$. Inversement $X^{\mathtt{per}(\underline{a})} - 1 \in A(\underline{a})$. Donc $m_{\underline{a}}$ divise $X^{\mathtt{per}(\underline{a})} - 1$. Alors $\mathtt{ord}(m_{\underline{a}})$ divise $\mathtt{per}\underline{a}$. Donc la période de $\underline{a}$ est l'ordre de $m_{\underline{a}}$. De plus, d'après le théorème 5.4.2, $\deg(m_{\underline{a}}a) < \deg(m_{\underline{a}})$ si et seulement si $\underline{a}$ est strictement périodique. Sinon elle est ultimement périodique de pré-période $\deg(a) + 1$. □

**Corollaire 5.9.1.** *Soit $q$ le polynôme de connexion d'un LFSR $\mathcal{L}$. Supposons que $q$ soit irréductible sur $\mathbb{F}_{p^n}$. Alors toute séquence de sorties $\underline{a}$ non-nulle de $\mathcal{L}$ telle que $q$ ne divise pas $qa$ dans $\mathbb{F}_{p^n}$ est de période $\mathtt{ord}(q)$ .*

*Démonstration.* D'après le corollaire 5.7.1, $q$ est polynôme minimal des séquences de sorties vérifiant les conditions décrites ci-dessus. D'après le théorème 5.9.1, la période est donc $\mathtt{ord}(q)$. □

## 5.10 Polynôme de connexion et Factorisation

### 5.10.1 Produit de polynômes premiers entre eux

Dans cette section, nous étudions la décomposition des LFSR séquences dont le polynôme de connexion est réductible.

Soit $\underline{b}$ et $\underline{c}$ deux séquences périodiques. Notons respectivement $b(X)$ et $c(X)$ leurs fonctions génératrices. Ces deux séquences sont des LFSR séquences et leur fonction génératrice sont deux fractions rationnelles. Soit un LFSR $\mathcal{L}_1 = (\mathbb{F}_{p^n}, r_1, q_1(X))$ qui génère $\underline{b}$ et soit un LFSR $\mathcal{L}_2 = (\mathbb{F}_{p^n}, r_2, q_2(X))$ qui génère $\underline{c}$. Posons $b(X) = \frac{f_1(X)}{q_1(X)}$ et $c(X) = \frac{f_2(X)}{q_2(X)}$. Considérons une combinaison linéaire des ces deux séquences.

$$\underline{a} = \alpha\underline{b} + \beta\underline{c}$$

avec $\alpha$ et $\beta$ deux constantes dans $\mathbb{F}_{p^n}$. La séquence $\underline{a}$ est aussi ultimement périodique, elle est strictement périodique si et seulement si $\underline{b}$ et $\underline{c}$ le sont aussi. La fonction génératrice $a(X)$ est la combinaison linéaire $\alpha b(X) + \beta c(X)$. En effet,

$$a(X) = \sum_{i=0}^{i=+\infty} a_i X^i = \sum_{i=0}^{i=+\infty} (\alpha b_i + \beta c_i) X^i = \alpha \sum_{i=0}^{i=+\infty} b_i X^i + \beta \sum_{i=0}^{i=+\infty} c_i X^i = \alpha b(X) + \beta c(X).$$

Il existe un LFSR de polynôme de connexion $q = q_1 q_2$ qui génère $\underline{a}$.

**Proposition 5.10.1.** *Soit $\underline{b}$ et $\underline{c}$ deux LFSR séquences générées par $\mathcal{L}_1$ et $\mathcal{L}_2$. Posons $b(X) = \frac{f_1(X)}{q_1(X)}$ et $c(X) = \frac{f_2(X)}{q_2(X)}$.*

1. *Toute combinaison linéaire $\underline{a} = \alpha\underline{b} + \beta\underline{c}$ est une LFSR séquence.*
2. *Il existe un LFSR de polynôme de connexion $q_1 q_2$ et un état initial qui génèrent $\underline{a}$.*
3. *Si $\underline{b}$ et $\underline{c}$ sont strictement périodiques, alors $\mathcal{L} = (\mathbb{F}_{p^n}, \deg(q_1) + \deg(q_2), q_1 q_2)$.*

*Démonstration.*

$$a(X) = \alpha b(X) + \beta c(X) = \frac{\alpha q_2(X) f_1(X) + \beta q_1(X) f_2(X)}{q_1(X) q_2(X)}.$$

D'après l'algorithme 5.6.1, le LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q_1 q_2)$ avec $r = \max(\max(\deg(f_2) + \deg(q_1), \deg(f_1) + \deg(q_2)), \deg(q_1) + \deg(q_2))$ génère $\underline{a}$. Si $\underline{b}$ et $\underline{c}$ sont strictement périodiques alors $\deg(f_1) < \deg(q_1)$ et $\deg(f_2) < \deg(q_2)$. Donc $\max(\deg(f_2)+\deg(q_1), \deg(f_1)+\deg(q_2)) < \deg(q_1)+\deg(q_2)$. La taille de $\mathcal{L}$ est alors $r = \deg(q_1)+\deg(q_2) = r_1 + r_2$. □

Inversement, soit $\underline{a}$ une séquence ultimement périodique. C'est une LFSR séquence. Supposons que le LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$ génère $\underline{a}$ et posons $a(X) = \frac{f(X)}{q(X)}$. Si $q = q_1 q_2$ avec $q_1$ et $q_2$ premiers entre eux dans $\mathbb{F}_{p^n}[X]$, alors $\underline{a}$ peut sécrire comme la somme de deux LFSR séquences générées par des LFSRs de polynôme de connexion $q_1$ et $q_2$.

**Proposition 5.10.2.** *Soient $\underline{a}$ une LFSR séquence générée par $\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$ et $a(X) = \frac{f(X)}{q(X)}$ sa fonction génératrice. Supposons que $q = q_1 q_2$ avec $q_1$ et $q_2$ premiers entre eux. Alors :*

1. *$\underline{a}$ est la somme de deux LFSRs séquences générées par deux LFSRs respectivement de polynômes de connexion $q_1$ et $q_2$.*
2. *Si $\underline{a}$ est strictement périodique, alors $\underline{b}$ et $\underline{c}$ sont deux séquences strictement périodiques.*
3. *Si $\deg(q) = r$, alors $\underline{b}$ et $\underline{c}$ sont générées par deux LFSRs dont la taille est respectivement $\deg(q_1)$ et $\deg(q_2)$.*

*Démonstration.* $q_1$ et $q_2$ sont premiers entre eux dans $\mathbb{F}_{p^n}[X]$. Comme $\mathbb{F}_{p^n}$ est un corps, alors $\mathbb{F}_{p^n}$ est un anneau euclidien. D'après le théorème de Bézout, il existe $u_1$ et $u_2$ tels que $fu_1q_1 + fu_2q_2 = f$.

$$a(X) = \frac{f}{q} = \frac{fu_1q_1 + fu_2q_2}{q_1q_2} = \frac{fu_2}{q_1} + \frac{fu_1}{q_2}.$$

Posons $\underline{b} = \mathtt{seq}_{p^n} \frac{fu_2}{q_1}$ et $\underline{c} = \mathtt{seq}_{p^n} \frac{fu_1}{q_2}$. D'après l'algorithme 5.6.1, il existe deux LFSRs $\mathcal{L}_1$ et $\mathcal{L}_2$ de polynômes de connexion $q_1$ et $q_2$ générant respectivement $\underline{b}$ et $\underline{c}$. La taille de $\mathcal{L}_1$ est $r_1 = \max(\deg(f) + \deg(u_2) + 1, \deg(q_1))$ et celle de $\mathcal{L}_2$ est $r_2 = \max(\deg(f) + \deg(u_1) + 1, \deg(q_2))$. Les états initiaux sont respectivement déterminés par $fu_2$ et $fu_1$. Donc par la correspondance entre les séries formelles et les séquences infinies, $\underline{a} = \underline{b} + \underline{c}$. Si en plus $\underline{a}$ est strictement périodique, alors $\deg(f) < \deg(q)$. Il faut décomposer la fraction $a(X)$ en deux fractions dont le degré du numérateur est strictement inférieur au degré du dénominateur. Grâce aux divisions euclidiennes suivantes

$$\begin{array}{rll} fu_2 = & q_1g_1 + h_1 & \text{avec } \deg(h_1) < \deg(q_1) \\ fu_1 = & q_2g_2 + h_2 & \text{avec } \deg(h_2) < \deg(q_2) \end{array},$$

nous avons $f = (g_1+g_2)q_1q_2+q_2h_1+q_1h_2$. Si $g_1+g_2 \neq 0$, alors $\deg(f) \geq \deg(g_1+g_2)q_1q_2 \geq \deg(q)$. C'est impossible, donc $g_1 + g_2 = 0$. Alors

$$\frac{f}{q} = \frac{h_1}{q_1} + \frac{h_2}{q_2}.$$

Comme $\deg(h_1) < \deg(q_1)$ et $\deg(h_2) < \deg(q_2)$, alors $\mathtt{seq}_{p^n} \frac{h_1}{q_1}$ et $\mathtt{seq}_{p^n} \frac{h_2}{q_2}$ sont strictement périodiques.
Si $\deg(q) = r$, alors d'après l'algorithme 5.6.1, on trouve deux LFSRs de taille respectivement $r_1 = \deg(q_1)$ et $r_2 = \deg(q_2)$ et $r = r_1 + r_2$. □

On peut poser le problème différemment, en fixant trois LFSRs $\mathcal{L} = (\mathbb{F}_{p^n}, \deg(q), q)$, $\mathcal{L}_1 = (\mathbb{F}_{p^n}, \deg(q_1), q_1)$ et $\mathcal{L}_2 = (\mathbb{F}_{p^n}, \deg(q_2), q_2)$ avec $q = q_1 q_2$ et $q_1$ et $q_2$ premiers entre eux. Toute séquence de sorties de $\mathcal{L}$ est-elle la somme de deux séquences de sorties de $\mathcal{L}_1$ et $\mathcal{L}_2$ ? Inversement, la somme de deux séquences générées par $\mathcal{L}_1$ et $\mathcal{L}_2$ est-elle une séquence de sorties de $\mathcal{L}$ ?

**Théorème 5.10.1.** *Pour tout état initial de $\mathcal{L}$, il existe deux uniques états initiaux de $\mathcal{L}_1$ et $\mathcal{L}_2$ tels que la somme de leur séquence de sorties soit la séquence de sorties de $\mathcal{L}$ . Inversement, pour tout couple d'états initiaux de $\mathcal{L}_1$ et $\mathcal{L}_2$, il existe un unique état initial de $\mathcal{L}$ tel que sa séquence de sorties soit la somme des séquences de sorties de $\mathcal{L}_1$ et $\mathcal{L}_2$.*

*Démonstration.* Les séquences de sorties de ces LFSRs sont strictement périodiques car la taille du registre est égale au degré du polynôme de connexion respectif.
Soit un état initial de $\mathcal{L}$, la séquence de sorties notée $\underline{a}$ a pour fonction génératrice $\frac{f(X)}{q(X)}$ avec $\deg(f) \leq \deg(q) - 1$. La proposition 5.10.2 prouve l'existence de deux états initiaux qui génèrent deux séquences $\underline{b}$ et $\underline{c}$ à partir de $\mathcal{L}_1$ et $\mathcal{L}_2$. Il reste à prouver l'unicité. Dans la démonstration de cette proposition, la division euclidienne $fu_2 = q_1 g_1 + h_1$ avec $\deg(h_1) < \deg(q_1)$ est unique. De plus, si on suppose l'existence de deux couples d'états initiaux, alors il existe deux couples $(h_1, h_2)$ et $(h_1^{'}, h_2^{'})$ tels que

$$\frac{f}{q} = \frac{h_1^{'}}{q_1^{'}} + \frac{h_2^{'}}{q_2^{'}}$$

avec $\deg(h_1^{'}) < \deg(q_1)$ et $\deg(h_2^{'}) < \deg(q_2)$.

$$h_1 q_2 + h_2 q_1 = h_1^{'} q_2 + h_2^{'} q_1 \Rightarrow (h_1 - h_1^{'}) q_2 = (h_2^{'} - h_2) q_1.$$

$q_1$ et $q_2$ étant premiers entre eux, alors $q_1$ divise $h_1 - h_1^{'}$ et $q_2$ divise $h_2 - h_2^{'}$. Cela est possible seulement si $h_1 - h_1^{'} = h_2 - h_2^{'} = 0$ par comparaison des degrés. Donc l'unicité est démontrée. Réciproquement, soit deux états initiaux de $\mathcal{L}_1$ et $\mathcal{L}_2$. D'après la proposition 5.10.1, la somme de leur séquences de sorties est une séquence générée par $\mathcal{L}$. D'après la proposition 5.4.1, il existe un unique état initial qui génère cette séquence à partir de $\mathcal{L}$. □

### 5.10.2 Facteur d'ordre multiple

Dans la suite, nous étudions le cas où un facteur est multiple. Soit $\mathcal{L} = (\mathbb{F}_{p^n}, \deg(q), q)$ avec $q(X) = (-1)^{j+1} q_0(X)$ et $q(0) = -1$ et $q_0$ irréductible. La plus petite puissance de $p$ plus grande que $t$ est $e = p^{[\log_p(t)]}$. Toute séquence de sorties de $\mathcal{L}$ est une somme de $e$ LFSR séquences générées par le même LFSR $\mathcal{L}_0 = (\mathbb{F}_{p^n}, e \deg(q_0), q_0(x^e))$.

**Théorème 5.10.2.** *Soit $q_0(X)$ un polynôme irréductible tel que $q(0) = -1$. Soit $\mathcal{L} = (\mathbb{F}_{p^n}, \deg(q), q)$ avec $q(X) = (-1)^{t+1} q_0(X)^t$. Posons $e = p^{[\log_p(t)]}$. Alors toute séquence de sorties de $\mathcal{L}$ est une somme de $e$ séquences générées par le LFSR $\mathcal{L}_0 = (\mathbb{F}_{p^n}, e \deg(q_0), q_0(x^e))$.*

*Démonstration.* Soit $\underline{a}$ une séquence de sorties. Alors $a(X)$ est de la forme $\frac{f(X)}{(-1)^{t+1}q_0(X)^t}$.

$$a(X) = \frac{f(X)}{(-1)^{t+1}q(X)^t} = \frac{(-1)^{t+1}f(X)q_0(X)^{e-t}}{q_0(X)^e}.$$

$\mathbb{F}_{p^n}[X]$ est de caractéristique $p$, donc $q_0(X)^e = q_0(X^e)$. Posons

$$h(X) = (-1)^{t+1}f(X)q_0(X)^{e-t} = \sum_{i=0}^{i=\deg(h)} h_i X^i.$$

Comme le LFSR est de taille le degré du polynôme de connexion, $\underline{a}$ est strictement périodique et $\deg(h) < e\deg(q_0)$. Rassemblons les $e^{\text{ième}}$ termes de $h$ :

$$h(X) = h_0 + h_e X^e + \ldots + h_1 X + h_{e+1}X^{e+1} + \ldots + h_{e-1}X^{e-1} + h_{2e-1}X^{2e-1} + \ldots.$$

Posons $x^i H_i(X^e) = h_i X^i + h_{i+e}X^{i+e} + \ldots$, donc $h(X) = H_0(X) + XH_1(X^e) + \ldots + X^{e-1}H_{e-1}(X^e)$.

$$a(X) = \sum_{i=0}^{i=e-1} X^i \frac{H_i(X^e)}{q_0(X^e)}.$$

Notons $a_i(X) = \frac{H_i(X)}{q_0(X)}$. Rappelons que

$$\begin{array}{rcl} \deg(X^i H_i(X^e)) = i + e\deg(H_i) & \leq & \deg(h) \\ & < & e\deg(q_0) \\ e\deg(H_i) & < & e\deg(q_0) \\ \deg(H_i) & < & \deg(q_0). \end{array}$$

Autrement dit, $\mathtt{seq}_{p_n} a_i(X)$ est strictement périodique. La séquence $\mathtt{seq}_{p^n} a_i(X^e)$ est générée par $\mathcal{L}_0$ et est obtenue en insérant $e-1$ zéros entre chaque coefficient de $\mathtt{seq}_{p^n} a_i(X)$ . En effet, on a

$$a_i(X) = \sum_{j=0}^{j=+\infty} a_j^i X^j \Rightarrow a_i(X^e) = \sum_{j=0}^{j=+\infty} a_j^i X^{ej} \Rightarrow \mathtt{seq}_{p^n} a_i(X^e) = (\underbrace{a_0^i, 0, \ldots, 0}_{e}, a_1^i, \ldots).$$

En multipliant cette fonction génératrice par $X^i$ la séquence obtenue est décalée $i$ fois vers la droite. Cette séquence est aussi générée par $\mathcal{L}_0$ car elle a pour polynôme de connexion $q_0(X^e)$ et le degré du numérateur est strictement inférieur à $e\deg(q_0)$.

$$\mathtt{seq}_{p^n}(X^i a_i(X^e)) = (\underbrace{0, \ldots, 0}_{i}, \underbrace{a_0^i, 0, \ldots, 0}_{e}, a_1^i, \ldots).$$

On déduit de $a(X) = \sum_{i=0}^{i=e-1} X^i a_i(X^e)$ que la séquence $\underline{a}$ est une somme de $e$ séquences générées par le même LFSR $\mathcal{L}_0$ avec la particularité que les séquences forment un "en-

trelacement".

$$\begin{array}{rccccccc} \underline{a} = (a_0^0, & 0, & 0, & \ldots, & 0, & a_1^0, & \ldots)+ & \\ (a_0^1, & 0, & \ldots, & 0, & 0, & a_1^1, & \ldots)+ & \\ \ddots & & & & & & & \\ & \ddots & & & & & & \\ & & & & (a_0^{e-1}, & 0, & \ldots, & 0, \quad a_1^{e-1}, \quad \ldots). \end{array}$$

□

## 5.11 Opérateur de décalage et Polynôme caractéristique d'un LFSR

### 5.11.1 Définitions et Généralités

**Définition 5.11.1.** *Définissons $L$ comme l'opérateur de décalage à gauche. Pour toute séquence $\underline{a} = (a_0, a_1, \ldots)$ infinie dans $\mathbb{F}_{p^n}$, $L(\underline{a}) = (a_1, a_2, \ldots)$. Pour tout $i \in \mathbb{N}$, posons $L^i(\underline{a}) = (a_i, a_{i+1}, \ldots)$. Pour tout polynôme $P(X) = p_k X^k + \ldots + p_1 X + p_0$ dans $\mathbb{F}_{p^n}[X]$, on définit $P(L) = p_k L^k + \ldots + p_1 L + p_0$.*

**Proposition 5.11.1.** *$\underline{a}$ est une séquence récurrente linéaire dans $\mathbb{F}_{p^n}$ si et seulement s'il existe un polynôme unitaire $P(X) \in \mathbb{F}_{p^n}[X]$ tel que*

$$P(L)(\underline{a}) = 0.$$

*Démonstration.* $\underline{a}$ est une séquence récurrente linéaire (ou une LFSR séquence) si et seulement s'il existe $q_1, \ldots, q_r$ dans $\mathbb{F}_{p^n}$ tels que $a_r = \sum_{i=1}^{i=r} q_i a_{r-i}$. Soit le polynôme $q^*(X) = X^r - \sum_{i=1}^{i=r} q_i X^{r-i}$. Alors

$$\begin{aligned} q^*(L)(\underline{a}) &= L^r(\underline{a}) - \sum_{i=1}^{i=r} q_i L^{r-i}(\underline{a}) \\ &= (a_r - \sum_{i=1}^{i=r} q_i a_{r-i}, a_{r+1} - \sum_{i=1}^{i=r} q_i a_{r+1-i}, \ldots) \\ &= (0, 0, \ldots). \end{aligned}$$

Inversement, si la séquence vérifie $P(L)(\underline{a}) = 0$ alors on peut générer $\underline{a}$ par le LFSR défini par $\mathcal{L} = (\mathbb{F}_{p^n}, \deg(P), (q_1, \ldots, q_r))$ où $P(X) = X^r - q_1 X^{r-1} - \ldots - q_r$. C'est une LFSR séquence, donc une séquence récurrente linéaire. □

La proposition 5.11.1 est en fait une définition équivalente des LFSRs séquences.

**Définition 5.11.2.** *Pour tout LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$, le polynôme*

$$q^*(X) = X^r - q_1 X^{r-1} - \ldots - q_{r-1} X - q_r$$

*est appelé polynôme caractéristique de $\mathcal{L}$.*

### 5.11.2 Période et ordre du Polynôme caractéristique

Dans cette sous-section, nous regardons les propriétés de périodicité d'une LFSR séquences par rapport au polynôme caractéristique du LFSR qui l'engendre (choisi arbitrairement). Dans la sous-section suivante, on verra que ces propriétés se déduisent directement des liens entre polynôme caractéristique et polynôme de connexion. Rappelons que dans la section 2, nous avons déterminés la période d'une séquence par rapport à un polynôme de connexion.

**Théorème 5.11.1.** *Soit un LFSR* $\mathcal{L} = (\mathbb{F}_{p^n}, q^*)$.

1. *Toute séquence de sorties est bien évidemment périodique.*
2. *La période divise l'ordre de* $q^*$.
3. *Si* $q_r \neq 0$, *la séquence est strictement périodique.*
4. *Si* $q_r = 0$, *alors la séquence est (ultimement ou strictement) périodique.*

*Démonstration.* Soit $T = \mathtt{ord}(q^*)$. Si $q^*(0) \neq 0$, alors $q^*(X)/X^T - 1$. Donc $(L^T - I)(\underline{a}) = 0$. On en déduit que $a_{i+T} = a_i$ pour tout $i$. Donc la séquence est strictement périodique et la période divise $T$.
Si $q^*(0) = 0$, alors il existe un entier non nul $k$ tel que $q^*(X) = X^k q_0^*(X)$ et $q_0^*(0) \neq 0$. L'ordre de $q^*$ est par définition celui de $q_0^*$. On a $q_0^*(X)/(X^T - 1)$. Donc $(L^{k+T} - L^k)(\underline{a}) = 0$. Ainsi pour $i$, $a_{i+k+T} = a_{i+k}$. La séquence peut être ultimement périodique ou strictement périodique. La période divise toujours $T$. De plus la pré-période est inférieure ou égale à $k$. □

On redémontre grâce à ce résultat celui énoncé en tout début, à savoir que la période a pour borne supérieur $p^{nr} - 1$.

**Lemme 5.11.1.** *L'ordre de* $q^*$ *est inférieur ou égal à* $p^{nr} - 1$. *Si* $q_r \neq 0$, *alors l'ordre de* $q^*$ *divise* $|(\mathbb{F}_{p^n}[X]/(q^*))^*|$. *Si* $q^*$ *est irréductible alors son ordre divise* $|(\mathbb{F}_{p^n}[X]/(q^*))^*| = p^{nr} - 1$. *Si* $q^*$ *est primitif alors son ordre est exactement* $p^{nr} - 1$.

*Démonstration.* $\mathbb{F}_{p^n}[X]$ est euclidien. Posons $q^*(X) = X^k h(X)$ tel que $h(0) \neq 0$. L'ordre de $h$ est par définition celui de $q^*$. Il existe donc un plus petit $T$ tel que $q^*$ divise $X^{k+T} - X^k$. Dans l'anneau quotient $\mathbb{F}_{p^n}[X]/(h)$, $X^T \equiv 1 \mod h$. La classe de $X$ appartient donc au sous-groupe multiplicatif des éléments inversibles modulo $h$ noté $(\mathbb{F}_{p^n}[X]/(h))^*$. $T$ est l'ordre de la classe de $X$. Autrement dit $T = \mathtt{ord}_h(X)$. Il divise l'ordre du groupe qui est inférieur ou égal à $p^{n\deg(h)} - 1$. Or $\deg(h) \leq \deg(q^*)$, donc $T \leq p^{nr} - 1$.
Si $q_r \neq 0$, alors $k = 0$ et $h = q^*$, donc $T$ divise $|(\mathbb{F}_{p^n}[X]/(q^*))^*|$.
Si $q^*$ est irréductible alors $k = 0$ et $h = q^*$. De plus $\mathbb{F}_{p^n}[X]/(q^*)$ est un corps et son sous-groupe multiplicatif est $\mathbb{F}_{p^n}[X]/(q^*) - \{0\}$. Donc l'ordre de la classe de $X$ divise $p^{nr} - 1$.
Si en plus, il est primitif, $q^*$ a une racine primitive $\alpha$, c'est à dire qu'il existe un élément d'ordre $p^{nr} - 1$ dans $\mathbb{F}_{p^n}[X]/(q^*)$. Donc il existe $k$ tel que $\alpha^k = \bar{X}$ où $\bar{X}$ est la classe de $X$ modulo $q^*$.

$$1 = (\bar{X}^T)^k = \bar{X}^{kT} = \alpha^T.$$

Donc $p^{nr} - 1 = T$. □

**Corollaire 5.11.1.** *La période de toute séquence de sorties de $\mathcal{L} = (\mathbb{F}_{p^n}, q^*)$ est inférieure ou égale à $p^{nr} - 1$.*

*Démonstration.* D'après le théorème 5.11.1, la période divise $T$. Le reste suit. □

### 5.11.3 Relation entre Polynôme caractéristique et Polynôme de connexion

Nous allons étudier la relation entre le polynôme de connexion et le polynôme caractéristique d'un LFSR ainsi que l'analyse de ce LFSR via le polynôme caractéristique. L'utilisation du polynôme caractéristique peut grandement faciliter l'analyse des LFSRs, cependant nous verrons dans la suite que les autres AFSRs comme les FCSRs ne disposent pas de notion équivalente au polynôme caractéristique, alors qu'elles possédent une notion équivalente au polynôme de connexion. Pour faire resortir les similitudes entre les différents AFSRs, il est préférable d'étudier les LFSRs via leur polynôme de connexion.

**Proposition 5.11.2.** *Pour tout LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$, $q^*(X) = -X^r q(\frac{1}{X})$.*

*Démonstration.* La preuve est un calcul direct. □

**Exemple 5.11.1.** *Le LFSR $(\mathbb{F}_{p^n}, r, -1)$ a pour polynôme caractéristique $X^r$.*

**Lemme 5.11.2.** *Soit un LFSR. Soit $q$ son polynôme de connexion et $q^*$ son polynôme caractéristique. Alors*

1. *$q$ et $q^*$ ont même degré si et seulement si $q_r \neq 0$.*
2. *$q$ et $q^*$ sont de même ordre.*
3. *$q$ est irréductible si et seulement si $q^*$ l'est aussi.*
4. *$q$ est un polynôme primitif si et seulement si $q^*$ l'est aussi.*
5. *$\alpha$ est racine de $q^*$ si et seulement si $\alpha^{-1}$ est racine de $q$.*

*Démonstration.*

1. $q^*$ est de degré $r$. L'entier $q$ est de degré $r$ si et seulement si $q_r \neq 0$.
2. Soit $N$ l'ordre de $q$. Alors il existe $h$ tel que $q(X)h(X) = X^N - 1$.

$$\begin{aligned} q(X)h(X) &= X^N - 1 \\ q(\tfrac{1}{X})h(\tfrac{1}{X}) &= \tfrac{1}{X^N} - 1 \\ -X^r q(\tfrac{1}{X})X^N h(\tfrac{1}{X}) &= -X^r(1 - X^N) \\ q^*(X)X^N h(\tfrac{1}{X}) &= X^r(X^N - 1) \end{aligned}$$

Le degré de $h$ est inférieur ou égal à $N$. Donc $X^N h(\frac{1}{X}) \in \mathbb{F}_{p^n}[X]$. On en déduit que $q^*$ divise $X^r(X^N - 1)$. Si $q^*(0) \neq 0$, alors $q^*$ divise $X^N - 1$. On en déduit que l'ordre de $q^*$ divise celui de $q$. Si $q^*(0) = 0$, alors il existe $d$ tel que $q^*(X) = X^d g(X)$.

$$X^d g(X) X^N h(\frac{1}{X}) = X^r(X^N - 1).$$

Donc $g$ divise $X^N - 1$. L'ordre de $g$ divise celui de $q$. Or par définition, l'ordre de $g$ est l'ordre de $q^*$.

Montrons que l'ordre de $q$ divise celui de $q^*$.
Si $q_r \neq 0$, l'ordre de $q^*$ existe et par symétrie, on en conclut qu'ils possédent le même ordre.
Si $q_r = 0$, alors $q^*(X) = X^d g(X)$ avec $g(0) \neq 0$ et l'ordre de $q^*$ est défini par l'ordre de $g$. Supposons que $g(X)m(X) = X^N - 1$.

$$\begin{aligned} X^d g(X)m(X) &= X^d(X^N - 1) \\ q^*(X)m(X) &= X^d(X^N - 1) \\ q^*(\tfrac{1}{X})m(\tfrac{1}{X}) &= \tfrac{1}{X^d}(\tfrac{1}{X^N} - 1) \\ -X^r q^*(\tfrac{1}{X})m(\tfrac{1}{X}) &= -\tfrac{X^r}{X^d}(\tfrac{1}{X^N} - 1) \\ q(X)X^N m(\tfrac{1}{X}) &= -\tfrac{X^r}{X^d}(1 - X^N) \\ q(X)X^N m(\tfrac{1}{X}) &= X^{r-d}(X^N - 1) \end{aligned}$$

$d$ est inférieur ou égal au degré de $q^*$, donc $d \leq r$. Le degré de $m$ est inférieur ou égal à $N$. Donc $X^N m(\frac{1}{X}) \in \mathbb{F}_{p^n}[X]$. On en déduit que $q(X)$ divise $X^{r-d}(X^N - 1)$, or $q(0) \neq 0$, donc $q(X)$ divise $X^N - 1$. L'ordre de $q$ divise l'ordre de $q^*$. On en conclut qu'ils sont égaux.

3. Si $q$ est réductible, alors il existe deux polynômes $f$ et $g$ de degré non nul tels que $q(X) = f(X)g(X)$. Donc

$$q^*(X) = -X^r f(\frac{1}{X})g(\frac{1}{X}) = -X^{r-\deg(fg)}X^{\deg(f)}f(\frac{1}{X})X^{\deg(g)}g(\frac{1}{X}) = X^{r-\deg(fg)}f^*(X)g^*(X).$$

   Ici $f^*$ et $g^*$ sont de même degré que $f$ et $g$ de manière respective, donc ils sont de degré non nuls. Donc $q^*$ est réductible. De même on démontre que la réductibilité de $q^*$ implique celle de $q$.

4. Soit $\alpha$ une racine primitive de $q$, $q(\alpha) = 0$. Si $\alpha$ est primitif dans $\mathbb{F}_{p^n}$, alors $\frac{1}{\alpha}$ l'est aussi. Or $q^*(\frac{1}{\alpha}) = -\frac{1}{\alpha^r}q(\alpha) = 0$. On en conclut que $q^*$ est primitif. Par symétrie, on démontre l'inverse.

5. Toute racine de $q^*$ est non nulle. Elle est donc inversible dans le corps de décomposition de $q^*$.

$$q^*(\alpha) = 0 \Leftrightarrow -\alpha^r q(\alpha^{-1}) = 0 \Leftrightarrow q(\alpha^-) = 0.$$

□

Une remarque s'impose. Le polynôme de connexion n'identifie pas un LFSR, car deux LFSRs de taille différente peuvent avoir le même polynôme de connexion. En effet, il suffit d'ajouter des zéros comme coefficients de monômes de degré supérieur à celui de $q$ pour augmenter la taille. Par contre, le polynôme caractéristique caractérise, comme son nom l'indique, un LFSR. En effet le degré de $q^*$ est la taille de $\mathcal{L}$ et ses coefficients de connexion sont les coefficients de $q^*$. Donc on peut définir $\mathcal{L}$ par le couple $(\mathbb{F}_{p^n}, q^*(X))$. Il y a une correspondance entre les polynômes sur $\mathbb{F}_{p^n}$ et les LFSRs construits sur $\mathbb{F}_{p^n}$.

D'autre part, nous avons caractérisé les séquences de sorties d'un LFSR avec la méthode utilisant la fonction génératrice et donc le polynôme de connexion. Ici, nous allons étudier l'ensemble des séquences générées par un LFSR en utilisant le polynôme caractéristique.

### 5.11.4 Structure de $G^*(q^*)$

Munissons l'espace de ${\mathbb{F}_{p^n}}^{\mathbb{N}}$ de la structure vectorielle produit direct. On définit l'addition par $\underline{a} \oplus \underline{b} = (a_0 + b_0, a_1 + b_1, \ldots)$ et la multiplication par un scalaire $\lambda.\underline{a} = (\lambda a_0, \lambda a_1, \ldots)$.

**Définition 5.11.3.** *Pour tout polynôme $q^*(X)$ de $\mathbb{F}_{p^n}[X]$, on définit l'ensemble suivant*

$$G^* = G^*(q^*) = \left\{ \underline{a} \in {\mathbb{F}_{p^n}}^{\mathbb{N}} \text{ telle que } q^*(L)(\underline{a}) = 0 \right\}.$$

*Si $q^*$ est unitaire, cet ensemble n'est autre que l'ensemble des séquences de sorties de $\mathcal{L} = (\mathbb{F}_{p^n}, q^*)$.*

$$G^* = S(\mathcal{L}).$$

*Sinon, $q^*$ peut s'écrire $-q_0X^r - q_1X^{r-1} - \ldots - q_r$. Le polynôme $-q_0^{-1}q^*(X)$ est unitaire. On a l'équivalence $q^*(L)(\underline{a}) = 0 \Leftrightarrow -q_0^{-1}q^*(L)(\underline{a}) = 0$. Donc $G^*(q^*) = G^*(-q_0^{-1}q^*)$ et $-q_0^{-1}q(X)$ est polynôme caractéristique d'un LFSR. Donc $G^*(q^*) = S(\mathcal{L})$ pour $\mathcal{L} = (\mathbb{F}_{p^n}, -q(0)^{-1}q^*(X))$.*

**Proposition 5.11.3.** *$G^*(q^*)$ est un sous espace vectoriel non-vide de ${\mathbb{F}_{p^n}}^{\mathbb{N}}$ de dimension $r = \deg(q^*)$ sur $\mathbb{F}_{p^n}$. Il contient $p^{nr}$ séquences différentes.*

*Démonstration.* La séquence nulle appartient à $G^*(q^*)$ car $q^*(L)(\underline{0}) = 0$. Soit deux séquences $\underline{a}$ et $\underline{b}$ dans $G^*(q^*)$. L'application $L$ est linéaire.

$$L(\underline{a} \oplus \underline{b}) = (a_1 + b_1, a_2 + b_2, \ldots) = (a_1, a_2, \ldots) \oplus (b_1 b_2, \ldots) = L(\underline{a}) \oplus L(\underline{b}),$$

$$L(\lambda.\underline{a}) = L(\lambda a_0, \lambda a_1, \ldots) = (\lambda a_1, \lambda a_2, \ldots) = \lambda.(a_1, a_2, \ldots) = \lambda.L(\underline{a}).$$

Par récurrence, on démontre que $L^k$ est aussi linéaire. En effet

$$L^2(\underline{a} \oplus \underline{b}) = L(L(\underline{a}) \oplus L(\underline{b})) = L^2(\underline{a}) \oplus L^2(\underline{b}).$$

$$L^2(\lambda.\underline{a}) = L(\lambda.L(\underline{a}) = \lambda.L^2(\underline{a}).$$

On en déduit que $q^*(L)(\lambda.\underline{a} + \mu.\underline{b}) = \lambda.q^*(L)(\underline{a}) + \mu.q^*(L)(\underline{b}) = \underline{0}$. Toute séquence générée par $\mathcal{L} = (\mathbb{F}_{p^n}, q^*)$ est déterminée par son état initial de taille $r$ et à coefficients dans $\mathbb{F}_{p^n}$. Or il existe $p^{nr}$ états possibles, donc il y a $p^{nr}$ séquences différentes dans $G^*(q^*)$. □

Nous étudions dans la suite le cas ou $q^*$ est irréductible sur $\mathbb{F}_{p^n}$, puis le cas où $q^*$ est le produit de polynômes irréductibles distincts deux à deux. Mais avant tout, il faut traiter la question inverse, c'est à dire quels sont tous les polynômes caractéristiques des LFSRs générant une séquence périodique donnée ?

## 5.12 Polynôme minimal d'une séquence

Dans les sections précédentes, nous avons introduit le polynôme de connexion et le polynôme caractéristique d'un LFSR fixé. Ces deux polynômes sont réciproques et ont donc le même ordre. Inversement, nous avons vu que pour une séquence périodique fixée, il existait un plus petit LFSR qui génère cette séquence, le polynôme de connexion de cet LFSR peut être appelé *"polynôme de connexion minimal"*. Les polynômes de connexion de tous les autres LFSRs générant la séquence en question sont des multiples du "polynôme minimal de connexion". Dans cette section, nous étudions la question inverse à travers le polynôme caractéristique en fixant une séquence périodique et en cherchant *"le polynôme caractéristique minimal"*.

**Définition 5.12.1.** *Soit $\underline{a}$ une séquence périodique. Définissons l'ensemble suivant*

$$A^*(\underline{a}) = \{Q(X) \in \mathbb{F}_{p^n}[X] \text{ tel que } Q(L)(\underline{a}) = 0\}.$$

*C'est l'ensemble des polynômes qui sont à un inversible près polynômes caractéristiques des LFSRs qui génèrent la séquence $\underline{a}$ plus le polynôme nul. En effet $0(L)(\underline{a}) = 0(\underline{a}) = \underline{0}$. On peut aussi définir cet ensemble comme suit*

$$A^*(\underline{a}) = \{Q(X) \in \mathbb{F}_{p^n}[X] \text{ tel que } \underline{a} \in G^*(Q)\}.$$

**Proposition 5.12.1.** *Pour toute séquence périodique $\underline{a}$,*

1. $A^*(\underline{a}) \neq \{0\}$.
2. *C'est un idéal de l'anneau $\mathbb{F}_{p^n}[X]$ qui contient une infinité de polynômes.*
3. $\underline{a} = \underline{0}$ *si et seulement si* $A^*(\underline{a}) = \mathbb{F}_{p^n}[X]$.

*Démonstration.* Soit $r$ la période de $\underline{a}$. Alors d'après le théorème 5.7.2, il existe un LFSR naturel de polynôme de connexion $X^r - 1$ qui génère $\underline{a}$. Cet LFSR a la particularité d'avoir un polynôme de connexion identique au polynôme caractéristique, en l'occurrence $X^r - 1$. Donc $X^{\mathtt{per}(\underline{a})} - 1 \in A^*(\underline{a})$.
Soient $P$ et $Q$ deux polynômes de $A^*(\underline{a})$. Soit $R$ un polynôme quelconque de $\mathbb{F}_{p^n}[X]$.

$$(P - Q)(L)(\underline{a}) = (P(L) - Q(L))(\underline{a}) = P(L)(\underline{a}) - Q(L)(\underline{a}) = \underline{0} - \underline{0} = \underline{0}.$$

$$(RQ)(L)(\underline{a}) = (R(L)Q(L))(\underline{a}) = R(L)Q(L)(\underline{a}) = R(L)(\underline{0}) = \underline{0}.$$

C'est bel et bien un idéal de $\mathbb{F}_{p^n}[X]$. Il contient l'idéal engendré par $X^r - 1$, donc une infinité de polynômes. Tout polynôme $Q$ dans $\mathbb{F}_{p^n}$ vérifie $Q(L)(\underline{0}) = \underline{0}$. Inversement, si tout polynôme dans $\mathbb{F}_{p^n}[X]$ vérifie cette relation, alors c'est valable pour le polynôme constant 1. Donc

$$1(L)(\underline{a}) = \underline{0} \Rightarrow \underline{a} = \underline{0}.$$

□

**Remarque 5.12.1.** *On aurait pu définir $A^*$ pour toute séquence définie sur $\mathbb{F}_{p^n}$ en imposant la condition qu'elle soit périodique. Mais cette condition est évidente. En effet, les LFSR séquences, les séquences récurrentes linéaires et les séquences périodiques sont les mêmes. Une séquence quelconque vérifie toujours $0(L)(\underline{a}) = \underline{0}$. Donc $0 \in A^*$ pour toute séquence. S'il est un ensemble non-nul, alors il existe un polynôme $q^* \neq 0$ tel que $q^*(L)(\underline{a}) = 0$, d'après le théroème 5.11.1, $\underline{a}$ est périodique. D'une autre manière, en divisant $q^*$ par son coefficient dominant, on a un polynôme unitaire appartenant à $A^*$. Ce polynôme définit un LFSR, donc $\underline{a}$ est une LFSR séquence, donc une séquence périodique. En bref, $A^*$ est non-nul équivaut à $\underline{a}$ est périodique. C'est donc le seul cas où l'étude de $A^*$ est intéressante.*

**Proposition 5.12.2.** *Il existe un unique polynôme unitaire non-nul de plus bas degré dans $A^*(\underline{a})$.*

*Démonstration.* Pour l'unicité, soient deux polynômes $Q_1$ et $Q_2$ unitaires non-nuls de plus bas degré. Comme $\mathbb{F}_{p^n}[X]$ est euclidien, on peut faire la division euclidienne de $Q_1$ par $Q_2$. Il existe donc $P$ et $R$ tels que $Q_1(X) = Q_2(X)P(X) + R(X)$ tel que $\deg(R) < \deg(Q_2)$. On a alors

$$\begin{aligned} Q_1(L)(\underline{a}) &= Q_2(L)(\underline{a})P(L)(\underline{a}) + R(L)(\underline{a}) \\ \underline{0} &= \underline{0} + R(L)(\underline{a}) \\ R(L)(\underline{a}) &= \underline{0} \end{aligned}$$

Donc $R$ est un polynôme de $A^*(\underline{a})$ de degré strictement inférieur au plus bas des degrés des polynômes de $A^*(\underline{a})$. On en déduit que $R = 0$ et donc $Q_2$ divise $Q_1$. Par symétrie, on en conclut que $Q_1$ divise $Q_2$, donc $Q_1 = Q_2$.
Pour l'existence, comme $A^*(\underline{a})$ contient $X^r - 1$, ou bien $X^r - 1$ est de plus bas degré ou bien c'est un autre polynôme de degré strictement inférieur à $r$. □

**Définition 5.12.2.** *L'unique polynôme unitaire de plus bas degré de $A^*(\underline{a})$ est appelé polynôme minimal de $\underline{a}$.*

**Exemple 5.12.1.** *Le polynôme minimal de la séquence nulle est le polynôme constant 1. C'est le polynôme caractéristique du registre de taille $r = 0$, c'est à dire le registre nul $(\mathbb{F}_{p^n}, 0, -1)$. Dans ce cas le polynôme de connexion est $-1$.*
*Le polynôme minimal d'une séquence périodique non-nulle de période 1 est $X - 1$. En effet, pour tout séquence de la forme $\underline{a} = (a, a, \ldots)$ avec $a \neq 0$, $X - 1$ vérifie*

$$(X-1)(L)(\underline{a}) = (L - I)(\underline{a}) = (a - a, a - a, \ldots) = (0, 0, \ldots).$$

*Donc $X - 1 \in A^*(a, a, \ldots)$. Si $X - 1$ n'est pas le polynôme minimal de $(a, a, \ldots)$, alors c'est un polynôme constant, unitaire, donc c'est la constante 1 ce qui impliquerait que $\underline{a} = \underline{0}$. On en déduit que $X - 1$ est le polynôme minimal. Le polynôme $X - 1$ est le polynôme caractéristique de $\mathcal{L} = (\mathbb{F}_{p^n}, 1, X - 1)$ dont le polynôme de connexion coincide avec le polynôme minimal.*

**Théorème 5.12.1.** *Soit $\underline{a}$ une séquence périodique, alors l'idéal $A^*(\underline{a})$ est un idéal principal généré par le polynôme minimal de $\underline{a}$.*

*Démonstration.* Pour la séquence nulle, $A^*(\underline{a})$ est $\mathbb{F}_{p^n}[X]$ qui peut être vu comme l'idéal engendré par 1. Sinon $\mathbb{F}_{p^n}[X]$ est un anneau euclidien donc principal. Tout idéal de $\mathbb{F}_{p^n}[X]$ est principal, donc pour toute séquence périodique non-nulle dans $\mathbb{F}_{p^n}$, il existe un polynôme $m^*(X) \neq 0$ tel que $A^*(\underline{a}) = m^*(X).\mathbb{F}_{p^n}[X]$. On en déduit que $m^*(X)$ divise le polynôme minimal de $\underline{a}$, donc il est de degré inférieur ou égal au plus bas degré des polynômes de $A^*(\underline{a})$. On en déduit alors qu'il est de plus bas degré. Ainsi $m^*(X)$ est le polynôme minimal de $\underline{a}$ à un inversible près. L'idéal $A^*(\underline{a})$ est généré par le polynôme minimal de $\underline{a}$.
D'une autre manière, soit un polynôme $Q(X) \in A^*(\underline{a})$. Notons $m^*_{\underline{a}}(X)$ le polynôme minimal de $\underline{a}$. On fait la division euclidienne de $Q$ par $m^*_{\underline{a}}$.

$$Q(X) = P(X)m^*_{\underline{a}}(X) + R(X) \text{ tel que } \deg(R) < \deg(m^*_{\underline{a}}).$$

On en déduit que $R(L)(\underline{a}) = \underline{0}$, donc que $R \in A^*(\underline{a})$. Or $R$ est de degré strictement inférieur à au degré le plus bas, donc $R = 0$. On vient de démontrer que $A^*(\underline{a}) \subseteq m^*_{\underline{a}}.\mathbb{F}_{p^n}$. Comme $A^*(\underline{a})$ est un idéal, alors $m^*_{\underline{a}}(X).\mathbb{F}_{p^n}[X] \subseteq A^*(\underline{a})$. □

**Notation 5.12.1.** *Le polynôme minimal d'une séquence périodique $\underline{a}$ sera noté $m^*_{\underline{a}}(X)$.*

**Corollaire 5.12.1.** *Soit $q^*$ un polynôme unitaire non nul. Soit le LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, q^*)$. Alors*

$$\underline{a} \in G^*(q^*) \Leftrightarrow \underline{a} \in S(\mathcal{L}) \Leftrightarrow \mathcal{L} \in R(\underline{a}) \Leftrightarrow q^* \in A^*(\underline{a}) \Leftrightarrow m^*_{\underline{a}} \mid q^*.$$

*Démonstration.* La preuve est évidente. □

**Corollaire 5.12.2.** *Soit $q^*$ un polynôme caractéristique d'un LFSR $\mathcal{L}$. Supposons que $q^*$ soit irréductible sur $\mathbb{F}_{p^n}$. Alors pour toute séquence de sorties $\underline{a}$ non-nulle de $\mathcal{L}$, $q^*$ est le polynôme minimal de $\underline{a}$.*

*Démonstration.* Le polynôme minimal de toute séquence non-nulle de sorties divise $q^*$ qui est irréductible et unitaire (par définition). Alors soit ils sont égaux, soit le polynôme minimal est 1. La dernière assertion est impossible puisque la séquence est non-nulle. □

## 5.13 Période et ordre du Polynôme minimal

Dans cette section, nous étudions le rapport entre la période d'une séquence donnée et son polynôme minimal.

**Théorème 5.13.1.** *Soit $\underline{a}$ une séquence périodique. Soit $m^*_{\underline{a}}$ son polynôme minimal.*

1. *Si $m^*_{\underline{a}}(X) = X^k m(X)$ avec $m(0) \neq 0$ et $k \geq 1$, alors la séquence est ultimement périodique de pré-période $k$ et de période $\texttt{ord}(m^*_{\underline{a}})$.*
2. *Si $m^*_{\underline{a}}(0) \neq 0$, alors $\underline{a}$ est strictement périodique de période $\texttt{ord}(m^*_{\underline{a}})$.*

*Démonstration.* D'après le théorème 5.11.1, la période de $\underline{a}$ divise l'ordre de $m^*_{\underline{a}}$. Inversement $X^r(X^{\mathtt{per}(\underline{a})}-1) \in A^*(\underline{a})$ où $r$ désigne la pré-période. Donc $m^*_{\underline{a}}$ divise $X^r(X^{\mathtt{per}(\underline{a})}-1)$.

$$m^*_{\underline{a}}(X) = X^k m(X) \text{ tel que } m(0) \neq 0.$$

$m$ divise $X^r(X^{\mathtt{per}(\underline{a})}-1)$ et est premier à $X$, donc $m$ divise $X^{\mathtt{per}(\underline{a})}-1$. Alors son ordre divise $\mathtt{per}\underline{a}$. Donc la période de $\underline{a}$ est l'ordre de $m^*_{\underline{a}}$.
De plus, d'après le théorème 5.11.1, la pré-période $r$ est inférieure à $k$. Ici $X^k$ divise$X^r(X^{\mathtt{per}(\underline{a})}-1)$ et est premier à $X^{\mathtt{per}(\underline{a})}-1$, donc $X^k$ divise $X^r$, ce qui signifie que $k$ est inférieur à la pré-période. On en déduit que la pré-période est $k$.

Si $m^*_{\underline{a}}(0) \neq 0$, d'après le même théorème, $\underline{a}$ est strictement périodique. Si $m^*_{\underline{a}}(0) = 0$, elle est soit ultimement périodique, soit strictement périodique. Supposons que $\underline{a}$ soit strictement périodique. Alors $X^{\mathtt{per}\underline{a}}-1 \in A^*(\underline{a})$. Donc $m^*_{\underline{a}}$ divise $X^{\mathtt{per}\underline{a}}-1$.

$$m^*_{\underline{a}}(0) = 0 \Rightarrow 0^{\mathtt{per}\underline{a}} - 1 = 0 \Rightarrow -1 = 0.$$

C'est absurde. La séquence $\underline{a}$ est ultimement périodique. □

**Corollaire 5.13.1.** *Soit $q^*$ un polynôme caractéristique d'un LFSR $\mathcal{L}$. Supposons que $q^*$ soit irréductible sur $\mathbb{F}_{p^n}$. Alors toute séquence de sorties $\underline{a}$ non-nulle de $\mathcal{L}$ est de période* $\mathtt{ord}(q^*)$ .

*Démonstration.* D'après le corollaire 5.12.2, $q^*$ est polynôme minimal des séquences de sorties. D'après le théorème 5.13.1, la période est donc $\mathtt{ord}(q^*)$. □

**Théorème 5.13.2.** *Soit $\underline{a}$ une séquence périodique. Soit $m^*_{\underline{a}}$ son polynôme minimal de degré $r$. Supposons que $m^*_{\underline{a}}$ soit irréductible sur $\mathbb{F}_{p^n}$ et $\alpha$ soit une racine dans l'extension de $\mathbb{F}_{p^{nr}}$. Alors la période de $\underline{a}$ est l'ordre de $\alpha$.*

*Démonstration.* Le degré de l'extension $\mathbb{F}_{p^n}[\alpha] \supseteq \mathbb{F}_{p^n}$ est le degré du polynôme minimal de $\alpha$ sur $\mathbb{F}_{p^n}$. Comme $m$ est irréductible, alors c'est le polynôme minimal de $\alpha$ et cette extension est de degré $r$. Le corps $\mathbb{F}_{p^n}[\alpha]$ est isomorphe à $\mathbb{F}_{p^{nr}}$. L'élément $\alpha$ appartient au sous-groupe multiplicatif des éléments non nuls de ce corps, donc $\alpha^{p^{nr}}-1=0$. L'ordre de $\alpha$ existe et le polynôme $X^{\mathtt{ord}(\alpha)}-1$ annule $\alpha$ sur $\mathbb{F}_{p^n}$. Donc $m$ divise ce polynôme ce qui implique que l'ordre de $m$ divise l'ordre de $\alpha$. Inversement $m$ divise $X^{\mathtt{ord}(m)}-1$ et $m(\alpha)=0$ donc $\alpha^{\mathtt{ord}(m)}-1=0$. On en déduit que l'ordre de $\alpha$ divise l'ordre de $m$. On en conclut que $m$ et $\alpha$ ont même ordre. Le reste du théorème suit. □

## 5.14 Polynôme caractéristique et Factorisation

### 5.14.1 Polynôme caractéristique irréductible

Supposons que le polynôme caractéristique du LFSR soit irréductible sur $\mathbb{F}_{p^n}$.

**Définition 5.14.1.** *Soient $\underline{a}$ et $\underline{b}$ deux séquences ultimement périodiques. On définit la relation suivante : $\underline{a} \sim \underline{b}$ si et seulement s'il existe $k \in \mathbb{N}$ tel que $\underline{b} = L^k(\underline{a})$. Si $\underline{a}$ et $\underline{b}$ vérifient cette relation, on dit qu'elles sont cycliquement identiques ou équivalentes. Sinon, on dit qu'elles sont cycliquement distinctes.*

**Proposition 5.14.1.** *$\sim$ est une relation d'équivalence.*

*Démonstration.*

- $\underline{a} = L^0(\underline{a})$
- $\underline{a} \sim \underline{b} \Leftrightarrow \underline{b} = L^k(\underline{a}) \Leftrightarrow \underline{a} = L^{N-k}(\underline{b}) \Leftrightarrow \underline{b} \sim \underline{a}$.
- $\left.\begin{array}{c} \underline{a} \sim \underline{b} \\ \underline{b} \sim \underline{c} \end{array}\right\} \Rightarrow \left.\begin{array}{c} \underline{b} = L^k(\underline{a}) \\ \underline{c} = L^j(\underline{b}) \end{array}\right\} \Rightarrow \underline{c} = L^{k+j}(\underline{a})$.

□

Les classes d'équivalence de séquences cycliquement équivalentes forment une partition de l'ensemble des séquences périodiques sur $\mathbb{F}_{p^n}$.

**Théorème 5.14.1.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, q^*)$. Supposons que $q^*$ soit un polynôme irréductible de degré $r$ sur $\mathbb{F}_{p^n}$ tel que $q^*(0) \neq 0$. Alors il y a $\frac{p^{nr}-1}{\mathtt{ord}(q^*)}$ classes d'équivalence non nulle dans $G^*(q^*)$.*

*Démonstration.* $q^*$ étant irréductible, il est le polynôme minimal de toute séquence dans $G^*$. D'après le théorème 5.13.1, $q^*(0) \neq 0$, alors toute séquence dans $G^*$ est strictement périodique. D'après le même théorème, les séquences non-nulles sont de période $\mathtt{ord}(q^*)$. Donc dans une classe d'équivalence non-nulle, il y a $\mathtt{ord}(q^*)$ séquences différentes. Soit $c$ le nombre de classes d'équivalence non-nulles. Alors $\mathtt{ord}(q^*) \times c + 1 = p^{nr}$. □

**Corollaire 5.14.1.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, q^*)$ dont le polynôme caractéristique est un polynôme irréductible de degré $r$ sur $\mathbb{F}_{p^n}$ ( donc $q^*(0) \neq 0$). Supposons en plus que $q^*$ soit primitif, alors il y a une seule classe d'équivalence non nulle et toute séquence non-nulle est de période $p^{nr} - 1$. Pour toute séquence $\underline{a}$ non-nulle,*

$$G^*(q^*) = \left\{L^i(\underline{a}) \text{ tel que } 0 \leq i \leq p^{nr} - 2\right\} \cup \{0\}.$$

**Remarque 5.14.1.** *En travaillant avec les polynômes de connexion $q$, on a vu que la période atteignait son maximum, $p^{n \deg(q)} - 1$, quand $q$ est primitif. Or $\deg(q)$ n'est pas forcément la taille du LFSR en question donc la période n'atteint pas la valeur maximale théorique $p^{nr} - 1$ sauf si $\deg(q) = r$. Par contre quand $q^*$ est primitif, il est irréductible, donc ne peut être divisé par $X$, ce qui implique que le coefficient constant $q_r \neq 0$ et dans ce cas la taille du registre est $r$ le degré de $q^*$. C'est un point essentiel pour éviter toute ambiguité.*

*Démonstration.* Si $q^*$ est primitif, alors il admet pour racine un élément primitif de $\mathbb{F}_{p^{nr}}$. Il existe $\alpha$ qui engendre $\mathbb{F}^*_{p^{nr}}$. Donc l'ordre de $\alpha$ est $p^{nr} - 1$. L'ordre de $q^*$ dans $\mathbb{F}_{p^n}[X]$ est aussi $p^{nr} - 1$. On en déduit, d'après le théorème précédent qu'il y a une seule classe

d'équivalence non nulle et que les séquences non nulles sont de période $p^{nr}-1$. En fait, on peut prendre une séquence non nulle arbitrairement, et obtenir toutes les autres par des décalages à gauche. □

Ce dernier corollaire donne une méthode pour générer des séquences de période maximale. En effet, c'est la période maximale puisque d'après la proposition 5.3.1, la période ne dépasse jamais $p^{nr}-1$. Il suffit de prendre pour polynôme caractéristique un polynôme primitif sur $\mathbb{F}_{p^n}$. Ces séquences occupent une place centrale dans la théorie des LFSR séquences.

### 5.14.2 $m$-séquences ou séquences maximales

**Définition 5.14.2.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$. Toute séquence de sorties de période $p^{nr}-1$ est appelée m-séquences ou séquences maximales. Dans la littérature anglaise, on parle de maximal sequences.*

**Théorème 5.14.2.** *Soit un LFSR $(\mathbb{F}_{p^n}, q^*)$. Considérons $\underline{a}$ une séquence de sorties. Si $\underline{a}$ est une m-séquence, alors $q^*$ est primitif.*

*Démonstration.* D'après le théorème 5.11.1, la période de toute séquence de sorties divise l'ordre de $q^*$. Ici $p^{nr}-1$ divise $\mathtt{ord}(q^*)$. D'après le même théorème, $\mathtt{ord}(q^*) \leq p^{nr}-1$, donc ici $\mathtt{ord}(q^*) = p^{nr}-1$. Or $\mathtt{ord}(q^*)$ n'est autre que $\mathtt{ord}_{q^*}(X)$, donc $\mathtt{ord}_{q^*}(X) = p^{nr}-1$ ce qui signifie que la classe de $X$ est primitive dans $\mathbb{F}_{p^{nr}} \cong \mathbb{F}_{p^n}[X]/(q^*)$ qui est le corps de décomposition de $q^*$. Rappelons que la classe de $X$ est une racine de $q$ dans ce corps de décomposition. Autrement dit $q^*$ a une racine primitive donc il est primitif. □

**Proposition 5.14.2.** *La complexité linéaire d'une m-séquence de période $p^{nr}-1$ est $r$.*

*Démonstration.* En effet, une $m$-séquence de période $p^{nr}-1$ est générée par un LFSR de polynôme caractéristique primitif de degré $r$. D'après le lemme 5.11.2, le polynôme de connexion est aussi primitif et irréductible. C'est donc le polynôme de connexion minimal $m_{\underline{a}}$. La complexité linéaire est le degré de $m_{\underline{a}}$. Or comme $q^*$ est irréductible alors $q^*(0) \neq 0$, donc $q_r \neq 0$. Donc $r$ est de degré. C'est ce qu'il fallait démontrer. □

Les $m$-séquences sont générées grâce à un polynôme caractéristique primitif sur $\mathbb{F}_{p^n}$. L'existence des $m$-séquences dépend donc de l'existence de tels polynômes. On dispose d'une conjecture sur l'existence de trinôme primitif sur $\mathbb{F}_2$.

**Conjecture 5.14.1** (Golomb)**.** *Il existe une infinité d'entiers $r$ pour lesquels il existe un entier $k$ compris entre 1 et $r$ strictement tel que le trinôme $X^r - X^k - 1$ est primitif.*

Cette conjecture a été vérifiée jusqu'à $r = 1000$. Ces trinômes définissent des LFSRs de taille $r$ avec 2 connexions en binaire. Donc l'implémentation de ces registres linéaires est très simple. En sortie, on obtient des séquences de période $2^r - 1$. Plus tard, nous verrons les propriétés remarquables de ces dites $m$-séquences.

Dans la sous-section suivante, nous traitons le cas des polynômes de connexion produits de polynômes irréductibles distincts deux à deux.

### 5.14.3 Produit de polynômes irréductibles distincts deux à deux

L'anneau $\mathbb{F}_{p^n}[X]$ est factoriel, donc tout polynôme admet une décomposition en facteurs irréductibles. Étudions le cas où le polynôme caractéristique est produit de polynômes irréductibles premiers entre eux. Nous développons tout d'abord des résultats intermédiaires tout aussi important.

**Proposition 5.14.3.** *Soit un polynôme $q^*(X) = X^r - q_1X^{r-1} - \ldots - q_r$. Il existe une séquence $\underline{a} \in G^*(q^*)$ telle que $m^*_{\underline{a}} = q^*$.*

*Démonstration.* Construisons une séquence telle que $q^*$ soit son polynôme minimal. Autrement dit cherchons une séquence telle que le LFSR défini par $q^*$ soit le plus petit générant cette séquence. Ici, $\mathcal{L}$ est de taille $r$. Prenons l'état initial $(0, \ldots, 0, 1)$. La séquence de sorties de $\mathcal{L}$ est $\underline{a} = (0, \ldots, 0, 1, q_1, \ldots)$. Soit un LFSR de taille plus petite que $r$. Supposons que ce LFSR génère $\underline{a}$. L'état initial est forcément l'état nul. Or dans ce cas, par linéarité, les coefficients de sorties sont tous nuls. Donc la séquence de sorties est nulle et n'est pas $\underline{a}$. C'est absurde, donc le LFSR de plus petite taille est bien $\mathcal{L}$. □

**Lemme 5.14.1.** *Soient $f(X)$ et $g(X)$ deux polynômes non-nuls de $\mathbb{F}_{p^n}[X]$ , alors :*

1. *$G^*(f) \subseteq G^*(g)$ si et seulement si $f(X)$ divise $g(X)$.*
2. *$G^*(f) \cap G^*(g) = G^*(d)$ où $d = PGCD(f, g)$.*
3. *$G^*(f) + G^*(g) = G^*(h)$ où $h = PPCM(f, g)$.*

*Démonstration.*

1. Si $f$ divise $g$, alors il existe $u$ tel que $g = fu$.

$$\underline{a} \in G^*(f) \Leftrightarrow f(L)(\underline{a}) = 0 \Rightarrow u(f(L))(\underline{a}) = 0 \Leftrightarrow g(L)(\underline{a}) = 0 \Leftrightarrow \underline{a} \in G^*(g).$$

   Supposons que $G^*(f) \subseteq G^*(g)$ et notons $f_0$ le coefficient dominant de $f$. D'après la proposition 5.3.1, il existe une séquence dans $G^*(-f_0^{-1}f)$ telle que $-f_0^{-1}f$ soit son polynôme minimal. Or $\underline{a} \in G^*(g)$, donc d'après le corollaire 5.7.1, $-f_0^{-1}f$ divise $g$.

2. Soit $\underline{a} \in G^*(f) \cap G^*(g)$. Donc on a $f(L)(\underline{a}) = 0$ et $g(L)(\underline{a}) = 0$. Comme $d$ est le $PGCD$ de $f$ et $g$, alors il existe $u$ et $v \in \mathbb{F}_q[X]$ tels que $u(X)f(X) + v(X)g(X) = d(X)$. Ainsi $d(L)(\underline{a}) = (u(L)f(L)+v(L)g(L))(\underline{a}) = u(L)f(L)(\underline{a})+v(L)g(L)(\underline{a}) = 0$. Donc $\underline{a} \in G^*(d)$. On a montré que $G^*(f) \cap G^*(g) \subseteq G^*(d)$.
   Soit $\underline{a} \in G^*(d)$. Or $d \mid f$ et $d \mid g$. Donc $f(L)(\underline{a}) = 0$ et $g(L)(\underline{a}) = 0$. Ainsi $\underline{a} \in G^*(f) \cap G^*(g)$. On a montré que $G^*(f) \cap G^*(g) = G^*(d)$.

3. Soit $\underline{a} \in G^*(f) + G^*(g)$.

$$\left\{ \begin{array}{rcl} f & | & PPCM(f,g) \\ g & | & PPCM(f,g) \end{array} \right. \Rightarrow \left\{ \begin{array}{rcl} G^*(f) & \subseteq & G^*(PPCM(f,g)) \\ G^*(g) & \subseteq & G^*(PPCM(f,g)) \end{array} \right.$$

$G^*(PPCM(f,g))$ étant un $\mathbb{F}_{p^n}$-espace vectoriel, on a : $G^*(f)+G^*(g) \subseteq G^*(PPCM(f,g))$. De plus, d'après la proposotion 5.11.3,

$$\begin{array}{rcl} \dim(G^*(f)+G^*(g)) & = & \dim G^*(f) + \dim G^*(g) - \dim(G^*(f) \cap G^*(g)) \\ & = & \dim G^*(f) + \dim G^*(g) - \dim G^*(d) \\ & = & \deg(f) + \deg(g) - \deg(d) \\ & = & \deg(h) \\ \dim(G^*(f)+G^*(g)) & = & \dim G^*(h) \end{array}$$

Donc $G^*(f) + G^*(g) = G^*(h)$.

□

**Théorème 5.14.3.** *Soit un polynôme $f(X) = f_1(X)\dots f_s(X)$ où les $f_i$ sont des polynômes irréductibles distincts sur $\mathbb{F}_{p^n}$ et $s$ un entier strictement positif. Alors $G^*(f)$ peut etre décomposé en somme directe des sous-espaces $G^*(f_i)$, c'est à dire que*

$$G^*(f) = G^*(f_1) \oplus \dots \oplus G^*(f_s).$$

*Démonstration.* Nous avons que $G^*(f_1)+G^*(f_2) = G^*(PPCM(f_1,f_2))$. Or $f_1$ et $f_2$ étant irréductibles et distincts alors $PPCM(f_1,f_2) = f_1 f_2$ et $PGCD(f_1,f_2) = 1$. Donc :

$$\begin{array}{rcl} G^*(f_1) + G^*(f_2) & = & G^*(f_1 f_2) \\ G^*(f_1) \cap (f_2) & = & \{0\} \end{array}$$

Ainsi on a $G^*(f_1) \oplus G^*(f_2) = G^*(f_1 f_2)$.
Par récurrence, on en déduit que $\bigoplus_{i=1}^{i=s} G^*(f_i) = G^*(\prod_{i=1}^{i=s} f_i) = G^*(f)$. □

## 5.15 Représentation Matricielle

Un LFSR peut être représenté par une matrice particulière. Soit $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$. Considérons un état initial $(a_0, \dots, a_{r-1})$ comme un vecteur ligne. On obtient l'état suivant par la multiplication matricielle :

$$(a_1, \dots, a_{r-1}, a_r) = (a_0, \dots, a_{r-1}) \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & q_r \\ 1 & 0 & \cdots & 0 & 0 & q_{r-1} \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 & q_2 \\ 0 & 0 & \cdots & 0 & 1 & q_1 \end{pmatrix}.$$

C'est une matrice de dimension $r \times r$ et dont les coefficients sont entièrement déterminés par les coefficients de connexion du LFSR de la forme

$$\begin{pmatrix} 0 & \cdots & 0 & q_r \\ & & & q_{r-1} \\ & I_{r-1} & & \vdots \\ & & & q_1 \end{pmatrix}$$

où $I_{r-1}$ représente la matrice identité de taille $r-1$. Il y a donc correspondance entre les LFSRs sur $\mathbb{F}_{p^n}$ et les matrices de cette forme à coefficients dans $\mathbb{F}_{p^n}$.

**Définition 5.15.1.** *On appelle cette matrice la matrice compagnon de $\mathcal{L}$.*

La matrice compagnon caractérise le LFSR. En effet, elle définit les coefficients de connexion, mais aussi la taille du registre par sa propre dimension. Donc, on peut définir $\mathcal{L}$ par un couple $(\mathbb{F}_{p^n}, \mathcal{M})$.

**Exemple 5.15.1.** *La matrice compagnon de $\mathcal{L} = (\mathbb{F}_{p^n}, 3, X^3 + X^2 - 1)$ est*

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

**Théorème 5.15.1.** *Soit $\mathcal{L}$ un LFSR de matrice compagnon $\mathcal{M}$. Le polynôme caractéristique de $\mathcal{M}$ est $(-1)^r q^*(X)$.*

*Démonstration.*

$$\det(\mathcal{M} - XI_r) = \det \begin{pmatrix} -X & 0 & \cdots & 0 & 0 & q_r \\ 1 & -X & \cdots & 0 & 0 & q_{r-1} \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & \cdots & 1 & -X & q_2 \\ 0 & 0 & \cdots & 0 & 1 & q_1 - X \end{pmatrix}$$

Montrons par récurrence sur $r$ que $\det(\mathcal{M} - XI_r) = (-1)^r q^*(X)$.
Pour $r = 1$, $\mathcal{L} = (\mathbb{F}_{p^n}, 1, q_1X - 1)$ et $\mathcal{M} = (q_1)$.

$$\det(q_1 - X) = q_1 - X = -q^*(X).$$

Pour $r = 2$, $\mathcal{L} = (\mathbb{F}_{p^n}, 1, q_2X^2 + q_1X - 1)$ et $\mathcal{M} = \begin{pmatrix} 0 & q_2 \\ 1 & q_1 \end{pmatrix}$.

$$\det(\mathcal{M} - XI_2) = \det \begin{pmatrix} -X & q_2 \\ 1 & q_1 - X \end{pmatrix} = X^2 - q_1X - q_2 = q^*(X).$$

Supposons que ce soit vérifié pour un $r-1$ fixé quelconque, montrons que c'est vrai pour $r$. En développant par rapport à la première colonne, on trouve :

$$\det(\mathcal{M}-XI) = (-X)\det \begin{pmatrix} -X & 0 & \cdots & 0 & q_{r-1} \\ 1 & 0 & \cdots & 0 & q_{r-2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & -X & q_2 \\ 0 & 0 & \cdots & 1 & q_1 - X \end{pmatrix} - \det \begin{pmatrix} 0 & 0 & \cdots & 0 & q_r \\ 1 & -X & \cdots & 0 & q_{r-2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & -X & q_2 \\ 0 & 0 & \cdots & 1 & q_1 - X \end{pmatrix}$$

Par hypothèse de récurrence, le premier déterminant est $(-1)^{r-1}(X^{r-1} - q_1X^{r-2} - \ldots - q_{r-2}X - q_{r-1})$. En développant par rapport à la première ligne, le deuxième déterminant est $(-1)^r q_r$.

$$\begin{aligned}\det(\mathcal{M} - XI) &= (-X)(-1)^{r-1}(X^{r-1} - q_1X^{r-2} - \ldots - q_{r-2}X - q_{r-1}) - (-1)^r q_r \\ &= (-1)^r q^*(X)\end{aligned}$$

□

**Corollaire 5.15.1.** *Soit $\mathcal{L}$ un LFSR de matrice compagnon $\mathcal{M}$. Alors*

1. $\det(X\mathcal{M} - I_r) = (-1)^{r+1}q(X)$.
2. *$\mathcal{M}$ est inversible si et seulement si $q_r \neq 0$.*
3. *Les valeurs propres de $\mathcal{M}$ sont les racines de $q(X)$.*
4. $q^*(\mathcal{M}) = 0$.
5. *$q^*$ est le polynôme minimal de $\mathcal{M}$. Si $Q(X) \in \mathbb{F}_{p^n}$ tel que $Q(\mathcal{M}) = 0$ et $\deg(Q) < r$, alors $Q(X) = 0$.*
6. *L'ensemble des polynômes annulateurs de $\mathcal{M}$ est un idéal principal engendré par $q^*(X)$ dans l'anneau $\mathbb{F}_{p^n}[X]$.*
7. *l'ordre de $q^*$ est fini si et seulement si l'ordre de $\mathcal{M}$ est fini. Dans ces cas, l'ordre de $q^*$ est l'ordre de $\mathcal{M}$, qui équivaut à $\mathcal{M}$ est inversible*

*Démonstration.* 1. $\det(X\mathcal{M}-I_r) = \det(X(\mathcal{M}-\frac{1}{X}I_r)) = X^r(-1)^r q^*(\frac{1}{X}) = (-1)^{r+1}q(X)$.

2. $\mathcal{M}$ es inversible si et seulement si $\det\mathcal{M} \neq 0$. Or $\det\mathcal{M} = (-1)^r \det q^*(0) = (-1)^r q_r$. Alors $\mathcal{M}$ est inversible si et seulement si $q_r \neq 0$.
3. les valeurs propres de $\mathcal{M}$ sont les racines de son polynôme caractéristique, donc les racines de $q(X)$.
4. D'après, les résultats classiques de l'algèbre linéaire, le polynôme caractéristique d'une matrice l'annule. Ici nous avons un argument indépendamment de ce résultat.

$$\forall s \in (\mathbb{F}_{p^n})^r, s.q^*(\mathcal{M}) = s.\mathcal{M}^r - \sum_{i=1}^{i=r} q_i s.\mathcal{M}^{r-i}$$

Avec $s = (a_0, \ldots, a_{r-1})$, on trouve que

$$\begin{aligned}s.\mathcal{M}^r &= (\sum_{i=1}^{i=r} q_i a_{r-i}, \sum_{i=1}^{i=r} q_i a_{r+1-i}, \ldots) \\ s.\mathcal{M}^{r-i} &= (a_{r-i}, \ldots, a_{r-1}, \sum_{i=1}^{i=r} q_i a_{r-i}, \ldots).\end{aligned}$$

Par exemple, pour le premier coefficient, on obtient $\sum_{i=1}^{i=r} q_i a_{r-i} - \sum_{i=1}^{i=r} q_i a_{r-i} = 0$. De même, on trouve 0 pour tous les autres coefficients.

5. Soit $Q(X) = \sum_{i=0}^{i=k} Q_i X^i$ vérifiant les hypothèses du théorème et $Q_k \neq 0$. Donc pour tout vecteur $s \in (\mathbb{F}_{p^n})^r$, $s.Q(\mathcal{M}) = 0$, en particulier pour $s = (0, \ldots, 0, 1)$. Pour tout $0 \leq i \leq k$, $Q_i s.\mathcal{M}^i = (\underbrace{0, \ldots, 0, Q_i}_{r-i}, \underbrace{*, \ldots, *}_{i})$.

   Donc $0 = s.Q(\mathcal{M}) = (\underbrace{0, \ldots, 0, Q_k}_{r-k}, \underbrace{*, \ldots, *}_{k})$. On en déduit que $Q_k = 0$ car $Q_k$ apparait puisque que $k < r$. C'est absurde, donc un tel $Q$ n'existe pas.

6. $\mathbb{F}_{p^n}$ est un corps, donc $\mathbb{F}_{p^n}[X]$ est un anneau euclidien. La différence entre deux polynômes annulateurs de $\mathcal{M}$ est encore un polynôme annulateur de $\mathcal{M}$. Le produit d'un polynôme annulateur et d'un polynôme quelconque est encore un polynôme annulateur. Soit $Q(X)$ un polynôme annulateur de $\mathcal{M}$. Considérons sa division euclidienne par $q^* : Q(X) = q^*(X)P(X) + R(X)$ avec $\deg R < r$. Alors $Q(\mathcal{M}) = 0$ implique que $R(\mathcal{M}) = 0$. D'après le point précédent, $R = 0$. Donc l'idéal des polynômes annulateurs de $\mathcal{M}$ est généré par $q^*(X)$.

7. Si $\mathtt{ord}(\mathcal{M}) = N < +\infty$, alors il existe $m$ et $N$ tels que $\mathcal{M}^m(\mathcal{M}^N - 1) = 0$. Donc $X^m(X^N - 1)$ annule $\mathcal{M}$ et $q^*$ divise $X^m(X^N - 1)$. L'ordre de $q^*$ divise celui de $\mathcal{M}$. Inversement si $q^*(X) = X^m(X^N - 1)$, alors $\mathcal{M}^m(\mathcal{M}^N - 1) = 0$. Donc l'ordre de $\mathcal{M}$ divise celui de $q^*$.

□

## 5.16 Représentation par la Trace

Soit $q^*(X) = X^r - q_1 X^{r-1} - \ldots - q^r$ un polynôme sur $\mathbb{F}_{p^r}$ de degré $r$. Soit $\alpha$ une racine de $q^*$. Soit la fonction trace : $\mathtt{Tr} : \mathbb{F}_{p^{nr}} \to \mathbb{F}_{p^n}$.

**Lemme 5.16.1.** *Pour tout* $\beta \in \mathbb{F}_{p^{nr}}$, $\underline{a} = (\mathtt{Tr}(\beta), \mathtt{Tr}(\beta\alpha), \mathtt{Tr}(\beta\alpha^2), \ldots) \in G^*(q^*)$.

*Démonstration.* Si $\beta = 0$, alors $\underline{a} = 0$. Or $0 \in G^*(q^*)$. Si $\beta \neq 0$, alors

$$\begin{aligned}
q^*(L)(\underline{a}) &= L^r(\underline{a}) - q_1 L^{r-1}(\underline{a}) - \ldots - q_r \underline{a} \\
&= \Big(a_{r+i} - q_{r-1} a_{r-1+i} - \ldots - q_r a_i\Big)_{i \geq 0} \\
&= \Big(Tr(\beta\alpha^{r+i}) - q_{r-1} Tr(\beta\alpha^{r-1+i}) - \ldots - q_r Tr(\beta\alpha^i)\Big)_{i \geq 0} \\
&= \Big(Tr(\beta(\alpha^{r+i} - q_1\alpha^{r-1+i} - \ldots - q_r\alpha^i))\Big)_{i \geq 0} \\
&= \Big(Tr(\beta\alpha^i q^*(\alpha))\Big)_{i \geq 0} \\
q^*(L)(\underline{a}) &= \underline{0}
\end{aligned}$$

Donc $\underline{a} \in G^*(q^*)$. □

On peut aussi reformuler ce lemme en utilisant le polynôme de connexion d'un LFSR. C'est le polynôme réciproque du polynôme caractéristique.

$$q(X) = -X^r q^*(\frac{1}{X}).$$

D'après le lemme 5.11.2, $\alpha$ est racine de $q^*$ si et seulement si $\alpha^{-1}$ est racine de $q$. On en déduit que si pour tout racine $\alpha$ de $q$, pour tout $\beta \in \mathbb{F}_{p^{n\deg(q)}}$, la séquence

$$\underline{a} = (\mathtt{Tr}(\beta), \mathtt{Tr}(\beta\alpha^{-1}), \mathtt{Tr}(\beta\alpha^{-2}), \ldots) \in G(q).$$

**Théorème 5.16.1.** *Supposons que $q^*$ soit irréductible. Pour toute séquence $\underline{a} = \{a_i\}_{i\in\mathbb{N}}$ de $G^*(q^*)$, il existe $\beta \in \mathbb{F}_{p^{nr}}$ tel que $a_i = \mathtt{Tr}(\beta\alpha^i)$ pour tout $i \geq 0$.*

*Démonstration.* $G^*(q^*)$ est un $\mathbb{F}_{p^{nr}}$-espace vectoriel à $p^{nr}$ éléments. On a montré que pour tout $\beta \in \mathbb{F}_{p^{nr}}$, $(\mathtt{Tr}(\beta\alpha^i))_{i\in\mathbb{N}} \in G^*(q^*)$. Donc l'application

$$\phi : \left\{ \begin{array}{ccc} \mathbb{F}_{p^{nr}} & \to & G^*(q^*) \\ \beta & \mapsto & (\mathtt{Tr}(\beta\alpha^i))_{i\in\mathbb{N}} \end{array} \right.$$

est bien définie. Maintenant, on cherche à montrer qu'elle est injective. La Trace est une application $\mathbb{F}_{p^n}$-linéaire. Donc $\phi$ est $\mathbb{F}_{p^n}$-linéaire. Montrons que $\phi(\beta) = 0$ implique que $\beta = 0$. Soit $\beta \in \mathbb{F}_{q^n}$ :

$$\begin{array}{rcl} \phi(\beta) = 0 & \Leftrightarrow & (\mathtt{Tr}(\beta\alpha^i))_{i\in\mathbb{N}} = 0 \\ \phi(\beta) = 0 & \Leftrightarrow & \forall i \in \mathbb{N}, \mathtt{Tr}(\beta\alpha^i) = 0 \end{array}$$

Or $\mathtt{Tr}(X) = X + X^{p^n} + \ldots + X^{p^{n(r-1)}}$. Donc :

$$
\begin{aligned}
\phi(\beta)=0 \quad &\Leftrightarrow \quad \forall i\in\mathbb{N},\ (\beta\alpha^i)+(\beta\alpha^i)^{p^n}+\ldots+(\beta\alpha^i)^{p^{n(r-1)}}=0\\
&\Leftrightarrow \quad \left\{\begin{array}{ccccccccc}
\beta & + & \beta^{p^n} & + & \ldots & + & \beta^{p^{n(r-1)}} & = & 0\\
\beta\alpha & + & \beta^{p^n}\alpha^{p^n} & + & \ldots & + & \beta^{p^{n(r-1)}}\alpha^{p^{n(r-1)}} & = & 0\\
\vdots & & \vdots & & & & \vdots & & \vdots\\
\beta\alpha^{r-1} & + & \beta^{p^n}\alpha^{p^{n(r-1)}} & + & \ldots & + & \beta^{p^{n(r-1)}}\alpha^{(r-1)p^{n(r-1)}} & = & 0\\
\vdots & & \vdots & & & & \vdots & & \vdots
\end{array}\right.\\
&\Leftrightarrow \quad \begin{pmatrix}
1 & 1 & \cdots & 1\\
\alpha & \alpha^{p^n} & \cdots & \alpha^{p^{n(r-1)}}\\
\vdots & \vdots & & \vdots\\
\alpha^{r-1} & \alpha^{(r-1)p^n} & \cdots & \alpha^{(r-1)p^{n(r-1)}}\\
\vdots & \vdots & & \vdots
\end{pmatrix}.\begin{pmatrix}
\beta\\ \beta^{p^n}\\ \vdots\\ \beta^{p^{n(r-1)}}\\ \vdots
\end{pmatrix}=0\\
&\Leftrightarrow \quad \begin{pmatrix}
1 & 1 & \cdots & 1\\
\alpha & \alpha^{p^n} & \cdots & \alpha^{p^{n(r-1)}}\\
\vdots & \vdots & & \vdots\\
\alpha^{r-1} & (\alpha^{p^n})^{r-1} & \cdots & (\alpha^{p^{n(r-1)}})^{r-1}\\
\vdots & \vdots & & \vdots
\end{pmatrix}.\begin{pmatrix}
\beta\\ \beta^{p^n}\\ \vdots\\ \beta^{p^{n(r-1)}}\\ \vdots
\end{pmatrix}=0\\
&\Leftrightarrow \quad \mathfrak{V}(\alpha,\alpha^{p^n},\ldots,\alpha^{p^{n(r-1)}}).\begin{pmatrix}
\beta\\ \beta^{p^n}\\ \vdots\\ \beta^{p^{n(r-1)}}\\ \vdots
\end{pmatrix}=0
\end{aligned}
$$

En effet $\mathfrak{V}(\alpha,\alpha^{p^n},\ldots,\alpha^{p^{n(r-1)}})$ est la matrice de Vandermonde de coefficient $\alpha$. Son déterminant est un produit de différence des racines de $q^*$. Les $r$ racines de $q^*$, $\alpha$, $\alpha^{p^n}$,... et $\alpha^{p^{n(r-1)}}$, sont conjuguées entre elles et $q^*$ est irréductible. Donc elles sont distinctes. Ainsi le déterminant de Vandermonde est non nul ce qui implique que la matrice est inversible.

$$
\phi(\beta)=0\Leftrightarrow\begin{pmatrix}
\beta\\ \beta^{p^n}\\ \vdots\\ \beta^{p^{n(r-1)}}\\ \vdots
\end{pmatrix}=0\Leftrightarrow\beta=0.
$$

Donc $\phi$ est injective. Or $\mathbb{F}_{p^{nr}}$ est un $\mathbb{F}_{p^n}$-espace vectoriel de dimension $r$ de même que $G^*(q^*)$. Donc par le théorème du rang, $\phi$ est un isomorphisme. On en conclut que pour toute séquence $\underline{a}$ de $G^*(q^*)$, il existe $\beta\in\mathbb{F}_{p^{nr}}$, tel que $\underline{a}=(\mathtt{Tr}(\beta\alpha^i))_{i\in\mathbb{N}}$.
D'une autre manière toute séquence de $G^*(q^*)$ est uniquement déterminée par son état

initial de taille $r$. On construit l'application

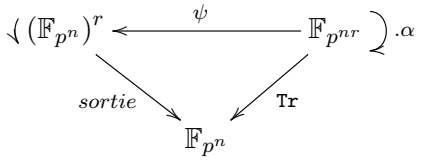
$$\psi : \begin{cases} \mathbb{F}_{p^{nr}} & \to & (\mathbb{F}_{p^n})^r \\ \beta & \mapsto & (\mathtt{Tr}(\beta), \mathtt{Tr}(\beta\alpha), \ldots, \mathtt{Tr}(\beta\alpha^{r-1})) \end{cases}$$

C'est une application linéaire entre deux $\mathbb{F}_{p^n}$-espaces vectoriels de même dimension. Il suffit de montrer son injectivité.

$$\psi(\beta) = 0 \Leftrightarrow \forall 0 \leq i \leq r-1,\ \mathtt{Tr}(\beta\alpha^i).$$

Comme $q^*$ est irréductible, $\{1, \alpha, \ldots, \alpha^{r-1}\}$ forment une base de $\mathbb{F}_{p^{nr}}$ en tant que $\mathbb{F}_{p^n}$-espace vectoriel. Donc tout élément est combinaison linéaire de cette base. Par linéarité de la trace, cela implique que pour tout $\xi \in \mathbb{F}_{p^{nr}}$, $\mathtt{Tr}(\beta\xi) = 0$. Donc $\beta = 0$, $\psi$ est donc un isomorphisme. □

**Théorème 5.16.2.** *Le modèle d'automate suivant est projectif et injectif.*




*Démonstration.* Comme $\psi$ est un isomorphisme, alors on a un modèle avec une fléche dans les deux sens. C'est à la fois un modèle injectif et un modéle surjectif. □

**Définition 5.16.1** (Représentation par la Trace)**.** *Si $q^*$ est le polynôme caractéristique d'un LFSR et est irréductible, alors, pour toute séquence de sorties, on appelle l'écriture $\underline{a} = (\mathtt{Tr}(\beta\alpha^i)_{i\in\mathbb{N}}$ la représentation par la trace de $\underline{a}$.*

## 5.17 Représentation Exponentielle

Les LFSRs séquences possédent une autre représentation plus abstraite appelée représentation exponentielle. Elle utilise le corps quotient $\mathbb{F}_{p^n}[X]/(q)$ où $q$ est le polynôme de connexion.

**Proposition 5.17.1.** *Soit un polynôme $q(X) = q_r X^r + \ldots + q_1 X - 1$ à coefficients dans $\mathbb{F}_{p^n}[X]$. Alors $q$ est inversible dans l'anneau des séries formelles $\mathbb{F}_{p^n}[[X]]$. Soit $h(X) \in \mathbb{F}_{p^n}[X]$ tel que $\deg(h) < \deg(q)$. Considérons le développement en série formelle de $\frac{h}{q}$ :*

$$\frac{h(X)}{q(X)} = a_0 + a_1 X + a_2 X^2 + \ldots$$

*Alors pour tout $i \geq 0$, $a_i = (-h(X)X^{-i}) \pmod q \pmod X$.*

*Démonstration.* $\mathbb{F}_{p^n}[[X]]$ est l'unique anneau de valuation discrète complet de corps résiduel $\mathbb{F}_{p^n}$ à isomorphisme prés. Son unique idéal premier est $(X) = X\mathbb{F}_{p^n}[[X]]$. L'ensemble $\mathbb{F}_{p^n}[[X]] \setminus (X)$ est l'ensemble des éléments inversibles de cet anneau. Le polynôme $q(X)$ n'étant pas un multiple de $X$, il est donc inversible dans $\mathbb{F}_{p^n}[[X]]$. La fraction $\frac{h(X)}{q(X)}$ admet donc un unique développement en série formelle dans $\mathbb{F}_{p^n}[[X]]$.

$$\begin{aligned}
\tfrac{h(X)}{q(X)} = a_0 + a_1X + a_2X^2 + \ldots \quad &\Rightarrow \quad h(X) = q(X)a_0 + q(X)a_1X + q(X)a_2X^2 + \ldots \\
&\Rightarrow \quad h(X) \equiv q(X)a_0 \mod X \\
&\Rightarrow \quad h(X) \equiv (q^rX^r + \ldots + q_1X - 1)a_0 \mod X \\
&\Rightarrow \quad h(X) \equiv -a_0 \mod X \\
&\Rightarrow \quad a_0 \equiv -h(X) \mod X \\
&\Rightarrow \quad a_0 = (-h(X)) \pmod X \\
\deg(h) < \deg(q) \quad &\Rightarrow \quad -h(X) = (-h(X)) \pmod q \\
&\Rightarrow \quad a_0 = (-h(X)) \pmod q \pmod X.
\end{aligned}$$

Comme $h(X) \equiv q(X)a_0 \mod X$, alors $\frac{1}{X}(h(X) - q(X)a_0) \in \mathbb{F}_{p^n}[X]$. On a de même :

$$\begin{aligned}
\tfrac{\frac{1}{X}(h(X)-q(X)a_0)}{q(X)} = a_1 + a_2X + \ldots \quad &\Rightarrow \quad a_1 = -\tfrac{1}{X}(h(X) - q(X)a_0) \pmod X \\
\deg(h) < \deg(q) \quad &\Rightarrow \quad \deg(h - a_0q) \leq \deg(q) \\
&\Rightarrow \quad \deg(-\tfrac{1}{X}(h(X) - q(X)a_0)) < \deg(q)
\end{aligned}$$

$X$ et $q$ sont premiers entre eux, donc $X$ est inversible dans $\mathbb{F}_{p^n}[X]/(q)$. Il existe alors un polynôme $\mu(X)$ et un polynôme $k(X)$ tels que $X\mu(X) = q(X)k(X) + 1$.

$$\begin{aligned}
-\mu(X)h(X) + \tfrac{h(X)-a_0q(X)}{X} &= \tfrac{-\mu(X)Xh(X)+h(X)-a_0q(X)}{X} = \tfrac{-(q(X)k(X)+1)h(X)+h(X)-a_0q(X)}{X} \\
&= \tfrac{q(X)(-k(X)h(X)-a_0)}{X}.
\end{aligned}$$

Donc $\frac{q(X)(-k(X)h(X)-a_0)}{X} \in \mathbb{F}_{p^n}[X]$. Or $X$ et $q$ étant premiers entre eux, alors $X \mid (-k(X)h(X) - a_0)$. Ainsi $-\mu(X)h(X) + \frac{h(X)-a_0q(X)}{X} \in q(X)\mathbb{F}_{p^n}[X]$.

$$-\mu(X)h(X) \equiv -\frac{h(X) - a_0q(X)}{X} \mod q.$$

$$\deg(-\frac{1}{X}(h(X) - q(X)a_0)) < \deg(q) \Rightarrow \frac{h(X) - a_0q(X)}{X} = (-\mu(X)h(X)) \pmod q.$$

On en conclut que $a_1 = (-\mu h) \pmod q \pmod X$. On notera $\mu$ par $X^{-1}$ l'inverse de $X$ modulo $q(X)$ et on a par récurrence pour tout $i$, $a_i = (-h(X)X^{-i}) \pmod q \pmod X$. □

**Théorème 5.17.1.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$. Considérons $\underline{a}$ une séquence de sorties et $a(X) = \frac{f(X)}{q(X)}$ sa fonction génératrice. Alors pour tout $i \in \mathbb{N}$,*

$$a_i = (-f(X)X^{-i}) \pmod q \pmod X.$$

*Démonstration.* La proposition 5.17.1 et le théorème 5.4.1 implique ce théorème. □

**Définition 5.17.1** (Représentation exponentielle d'une LFSR séquence)**.** *Cette représentation est appelée représentation exponentielle.*

## 5.18 Suite de Fibonacci

Ce mode de registre est appelé mode de Fibonacci car il permet de générer la suite de Fibonacci. Cependant, on ne construit pas la séquence sur $\mathbb{F}_{p^n}$ mais sur $\mathbb{Z}$ et la fonction de retour est une addition dans $\mathbb{Z}$ sans fonction modulo. La suite de Fibonacci est définie par la relation de récurrence

$$a_r = a_{r-1} + a_{r-2}.$$

On construit donc le LFSR de taille 2 et d'entier de connexion $q_1 = 1, q_2 = 1$. La figure 5.8 représente le registre obtenu. Avec l'état initial $(1, 1)$, on obtient en sortie la séquence suivante

$$(1, 1, 2, 3, 5, 8, 13, \ldots).$$

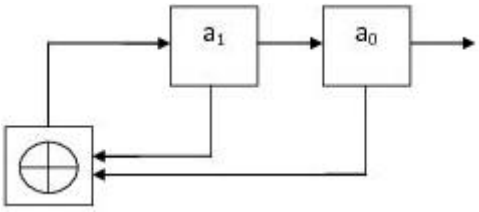



FIGURE 5.8 – Suite de Fibonacci et Mode de Fibonacci

## 5.19 Décimations

Dans cette section, nous définissons les décimations d'une séquence ainsi que les propriétés de base dans le cas d'une $m$-séquence. On désignera dans la suite par $q^*$ un polynôme sous la forme d'un polynôme caractéristique d'un LFSR.

**Définition 5.19.1** (décimations). *Considérons une séquence $\underline{a}$. Construisons la séquence $\underline{b}$ définie par $b_i = a_{si}$ pour tout $i \geq 0$ :*

$$\underline{b} = (a_0, a_s, a_{2s}, \ldots).$$

*Alors $\underline{b}$ est appelé la $s$-décimation de $\underline{a}$, notée $\underline{a}^{(s)}$.*

**Théorème 5.19.1.** *Soient $q^*$ un polynôme irréductible sur $\mathbb{F}_{p^n}$ de degré $r$ et $s$ un entier. Soit $\alpha$ une racine de $q^*$ dans une extension $\mathbb{F}_{p^{nr}}$. Considérons une séquence $\underline{a} \in G^*(q^*)$ et une $s$-décimation $\underline{a}^{(s)} \neq \underline{0}$. Le polynôme minimal de $\underline{a}^{(s)}$ est le polynôme minimal de $\alpha^s$ sur $\mathbb{F}_{p^n}$.*

*Démonstration.* Comme $\underline{a} \in G(q^*)$ avec $q^*$ irréductible alors $\underline{a}$ a une représentation par la trace. Il existe $\beta \in \mathbb{F}_{p^{nr}}$ tel que $a_i = \mathtt{Tr}(\beta\alpha^i)$ pour tout $i \geq 0$. On a alors :

$$\underline{a}^{(s)} = (a_{si})_{i\in\mathbb{N}} = (\mathtt{Tr}(\beta\alpha^{si}))_{i\in\mathbb{N}} = (\mathtt{Tr}(\beta(\alpha^s))^i)_{i\in\mathbb{N}}.$$

Soit $g$ le polynôme minimal de $\alpha^s$ sur $\mathbb{F}_{p^n}$.

$$g(L)(\underline{a}^{(s)}) = (\mathtt{Tr}(\beta(g(\alpha^s))\alpha^i))_{i\geq 0} = 0.$$

Donc $\underline{a}^{(s)} \in G^*(g)$. De plus $g$ étant le polynôme minimal de $\alpha^s$ sur $\mathbb{F}_{p^n}$, il est irréductible sur $\mathbb{F}_{p^n}$. Alors $g$ est aussi le polynôme minimal de $\underline{a}^{(s)}$. □

**Théorème 5.19.2.** *Soient $q^*$ un polynôme irréductible sur $\mathbb{F}_{p^n}$ et une séquence $\underline{a} \in G^*(q^*)$. Alors*

$$\mathtt{per}(\underline{a}^{(s)}) = \frac{\mathtt{per}(\underline{a})}{\mathtt{PGCD}(s, \mathtt{per}(\underline{a}))}.$$

*Démonstration.* D'après le corollaire 5.13.1 et le théorème 5.13.2, $q^*$ étant irréductble, alors $\mathtt{per}(\underline{a}) = \mathtt{ord}(q^*) = \mathtt{ord}(\alpha)$. D'autre part $g$ le polynôme minimal de $\alpha^s$ est le polynôme minimal de $\underline{a}^{(s)}$. Donc d'après ce même théorème, $\mathtt{per}(\underline{a}^{(s)}) = \mathtt{ord}(g) = \mathtt{ord}(\alpha^{(s)})$. Or $\mathtt{ord}(\alpha^{(s)}) = \frac{\mathtt{ord}(\alpha)}{\mathtt{PGCD}(s,\mathtt{ord}(\alpha))}$. Donc $\mathtt{per}(\underline{a}^{(s)}) = \frac{\mathtt{per}(\underline{a})}{\mathtt{PGCD}(s,\mathtt{per}(\underline{a}))}$. □

**Corollaire 5.19.1.** *Soient $q^*$ un polynôme primitif sur $\mathbb{F}_{p^n}$ et $\underline{a} \in G^*(q^*)$ une séquence. Alors $\underline{a}$ est une m-séquence. Toute s-décimation $\underline{a}^{(s)}$ est une m-séquence si*

$$PGCD(s, p^{nr} - 1) = 1.$$

*Démonstration.* D'après le corollaire 5.14.1, $\underline{a}$ est une $m$-séquence. En utilisant la formule sur la période de $\underline{a}^s$, on trouve que $\underline{a}^s$ est de période $p^{nr}-1$ si et seulement si $\mathtt{PGCD}(s, p^{nr}-1) = 1$. □

**Corollaire 5.19.2.** *Le nombre de m-séquences dans $\mathbb{F}_{p^n}$ de période $p^{nr}-1$ cycliquement distinctes est $\frac{\phi(p^{nr}-1)}{r}$.*

*Démonstration.* Soit une $m$-séquence de période $p^{nr} - 1$, elle est engendrée par un polynôme minimal irréductible primitif de degré $r$. Toutes les séquences qui en sont un décalage sont engendrées par le même polynôme primitif. Donc, il s'agit en fait de dénombrer les polynômes irréductibles et primitifs sur $\mathbb{F}_{p^n}$ de degré $r$. Soit $P$ un polynôme irréducitble et primitif de degré $r$ sur $\mathbb{F}_{p^n}$. Soit $\alpha$ une racine de $P$, alors elle est primitive, c'est-à dire qu'elle génère toutes ses racines et $P$ est de la forme $P(X) = (X-\alpha)(X-\alpha^{p^n})\dots(X-\alpha^{p^{(r-1)n}})$. Si $\alpha$ est primitif dans $\mathbb{F}_{p^n}$, alors les conjugués de $\alpha$ le sont aussi et ils sont distintcs deux à deux. Donc $P$ possède $r$ éléments primitifs distincts deux à deux comme racines. Donc à chaque polynôme irréductible et primitif correspond $r$ éléments primitifs de $\mathbb{F}_{p^n}$. Alors il y a $\frac{\phi(p^{nr}-1)}{r}$ polynômes irréductibles primitifs sur $\mathbb{F}_{p^n}$, donc il y a $\frac{\phi(p^{nr}-1)}{r}$ $m$-séquences de période $p^{nr}-1$ cycliquement distinctes. □

**Exemple 5.19.1.** *Soient $q^*(X) = X^4 + X + 1 \in \mathbb{F}_2[X]$ et $\alpha$ une racine de $q^*$. Le polynôme $q^*$ étant irréductible, $q^*$ est donc le polynôme minimal de $\alpha$. De plus $\alpha^{15} = 1$, donc l'ordre de $\alpha$ divise 15. Il est donc égal à 1,3,5 ou 15. On a $\alpha \neq 1$, $\alpha^3 \neq 1$ et $\alpha^5 = \alpha^2 + \alpha \neq 1$. Donc $\alpha$ est d'ordre 15, c'est un élément primitif de $\mathbb{F}_2$. Donc $q^*$ est*

*primitif.*
*Toute séquence* $\underline{a} \in G^*(X^4+X+1)$ *est une m-séquence de période* $15 = 2^4 - 1$.

$$\underline{a}^3 = (1000110001\ldots) \text{ et } \mathtt{per}(\underline{a}^3) = \frac{15}{3} = 5,$$

$$\underline{a}^5 = (101101\ldots) \text{ et } \mathtt{per}(\underline{a}^3) = \frac{15}{5} = 3,$$

$$\underline{a}^7 = (111010\ldots) \text{ et } \mathtt{per}(\underline{a}^3) = \frac{15}{1} = 15.$$

Ce corollaire prouve qu'existent des $m$-séquences cycliquement distinctes. Cependant, en considérant les décimations des $m$-séquences, on prouve que deux $m$ séquences de même période $p^{nr}-1$ sont cycliquement identiques par décimation.

**Proposition 5.19.1.** *Considérons* $\underline{a}$ *et* $\underline{b}$ *deux m-séquences de même période* $p^{nr}-1$, *alors* $\underline{b}$ *est cycliquement identique à une décimation de* $\underline{a}$.

*Démonstration.* $\underline{a}$ est générée par un LFSR $(\mathbb{F}_{p^n}, q^*)$ et $\underline{b}$ est générée par un LFSR $(\mathbb{F}_{p^n}, Q^*)$ tel que $q^*$ et $Q^*$ soient primitifs. Soient $\alpha$ et $\mu$ deux racines primitives respectives de $q^*$ et $Q^*$. D'après le théorème 5.16.1, $\underline{a}$ et $\underline{b}$ admettent une représentation par la trace. Il existe $\beta$ et $\theta$ tels que

$$\begin{aligned} a_i &= \mathtt{Tr}(\beta\alpha^i) \text{ et} \\ b_i &= \mathtt{Tr}(\theta\mu^i). \end{aligned}$$

$\alpha$ étant primitive, il existe un $s$ tel que $\mu = \alpha^s$. Comme $\underline{a}$ et $\underline{b}$ sont deux $m$-séquences, alors $\beta \neq 0$ et $\theta \neq 0$. Donc $\frac{\theta}{\beta} \in \mathbb{F}^*_{p^{nr}}$. L'élément $\mu$ étant primitif, donc il existe un $t$ tel que $\frac{\theta}{\beta} = \mu^t$. On en déduit que :

$$b_i = \mathtt{Tr}(\beta\mu^t\alpha^{si}) = \mathtt{Tr}(\beta\alpha^{st}\alpha^{si} = \mathtt{Tr}(\beta\alpha^{s(t+i)}) = a_{s(i+t)}.$$

□

Inversement, d'après le corollaire 5.19.1, une décimation d'une $m$-séquence n'est pas forcément une $m$-séquence sauf si le degré de décimation est premier avec la période. Une décimation d'une $m$-séquence $\underline{a}$ est cycliquement identique à $\underline{a}$ si et seulement si le degré de décimation est une puissance de $p^n$.

## 5.20 Propriétés de distribution des $m$-séquences

Dans cette section, nous étudions la distribution des états des $m$-séquences, c'est à dire le nombre d'apparition des différents bits constituant la séquence et leur disposition.

Une séquence pseudo-aléatoire doit à la fois paraître aléatoire tout en obéissant à des propriétés très fortes sur la distribution de ses bits. C'est un paradoxe exigé par les applications des séquences aux différents domaines scientifiques et techniques (simulation informatique, intégration de Monte carlo, radar, cryptographie...). Golomb a posé trois grands postulats d'aléarité :

1. la propriété de l'équilibre (balanced property),
2. la propriété des séries (run properties) et
3. une auto-corrélation idéale.

Ces trois postulats paraissent minimes et pourtant il est étonnant de constater que rares sont les familles de séquences vérifiant ces trois postulats. Les $m$-séquences font parties des familles de séquences vérifiant les trois grands postulats de Golomb.

### 5.20.1 Critères de pseudo-alé de Golomb

Nous énonçons les trois grands postulats de Golomb dans cette sous-section. Nous les énonçons tout d'abord pour une séquence binaire puis ensuite nous discutons de ces notions pour une séquence dite $p^n$-aire ou quelconques.

#### Séquence périodique binaire

Soit $\underline{a}$ une séquence binaire de période $N$.

**Définition 5.20.1** (série). *$k$ zéros (ou uns) consécutifs sont appelés une série de zéros (ou de uns) de longueur $k$.*

**Définition 5.20.2** (auto-corrélation). *L'autocorrélation de $\underline{a}$ est la fonction :*

$$\begin{array}{rcl} \mathcal{C}_{\underline{a}} : \mathbb{N} & \to & \mathbb{N} \\ \tau & \mapsto & \mathcal{C}_{\underline{a}}(\tau) = \sum_{i=0}^{N-1} (-1)^{a_i + a_{i+\tau}}. \end{array}$$

*On la note aussi $\mathcal{C}(\tau)$ dans un contexte clair.*

Pour toute séquence binaire de période $N$, on trouve que $\mathcal{C}_{\underline{a}}(0) = \sum_{i=0}^{N-1} (-1)^{2a_i} = N$.

Si $\underline{a}$ est de période $N$, alors $\underline{a}$ est déterminée et est représentée par $(a_0, a_1, \ldots, a_{N-1})$. Golomb propose 3 postulats pour la mesure de la qualité aléatoire d'une séquence binaire périodique.

**R1** : Pour toute période, le nombre de zéros est presque égal au nombre de uns. Plus précisement, la différence n'excède pas 1. En d'autres termes :

$$\sum_{i=0}^{N-1} (-1)^{a_i} = \sum_{a_i=0}^{1 \le i \le N-1} 1 + \sum_{a_i=1}^{1 \le i \le N-1} (-1) = \pm 1$$

$$\left| \sum_{i=0}^{N-1} (-1)^{a_i} \right| = 1$$

**R2** : Dans une période, la moitié des séries sont de longueurs 1, le quart de longueur 2, le huitième de longueur 3, etc... tant que le nombre de séries est supérieur à 1. Pour chaque longueur, le nombre de séries composées de zéros est égale au nombre de séries composées de uns.

**R3** : L'auto-corrélation de la séquence doit être à deux niveaux, c'est à dire prendre deux valeurs. Explicitement, il doit exister une constante $K$ telle que :

$$\mathcal{C}(\tau) = \begin{cases} N & \text{si} \quad \tau \equiv 0 \mod N \\ K & \text{si} \quad \tau \not\equiv 0 \mod N \end{cases}$$

Si $N = 2^n - 1$, alors nous redéfinissons les postulats de la manière suivante.

**R1** : Dans toute période, il y a $2^{n-1} - 1$ zéros et $2^{n-1}$ uns, ou $2^{n-1}$ zéros et $2^{n-1} - 1$ uns. Cette propriété est appelée *la propriété de l'équilibre.*

**R2** : Dans toute période, les séries de zéros (ou de uns) de longueur $k$ apparaissent $2^{n-k-2}$, pour tout $1 \leq k \leq n-2$. La série de zéros de longueur $n-1$ apparait une fois. La série de uns de longueur $n$ apparait une fois. Cette propriété est appelée *la propriété des séries.*

**R3** : L'auto-corrélation prend 2 valeurs avec $K = -1$.

$$\mathcal{C}(\tau) = \begin{cases} N & \text{si } \tau \equiv 0 \text{ mod } N \\ -1 & \text{sinon} \end{cases}$$

**Exemple 5.20.1.** *Soit la séquence* $\underline{a} = (1110010\ldots)$ *avec pour période* $7 = 2^3 - 1$ *minimal* $q^*(x) = x^3 + x + 1$. *C'est une m-séquence. Elle vérifie les 3 postulats aléatoires de Golomb.*

- *Il y a* $4 = 2^2$ *zéros et* $3 = 2^2 - 1$ *uns. Donc le postulat 1 est vérifié.*
- *Les séries de zéros de longueur 1 sont au nombre de 1. Les séries de zéros de longueur 2 sont au nombre de 1. Les séries de uns de longueur 1 sont au nombre de 1. Les séries de uns de longueur 3 sont au nombre de 1.*
- *En calculant l'auto-corrélation pour les différentes valeurs de* $\tau$, *on trouve :*

$$\mathcal{C}(0) = 7 \text{ et } \mathcal{C}(1) = \mathcal{C}(2) = \mathcal{C}(3) = \mathcal{C}(4) = \mathcal{C}(5) = \mathcal{C}(6) = -1$$

### Séquence périodique non-binaire

On se place sur $\mathbb{F}_{p^n}$ pour $p$ premier et $n = 1$. Soit $\underline{a}$ une séquence sur $\mathbb{F}_{p^n}$ de période $p^{nr} - 1$. Nous allons généraliser les postulats de Golomb pour ces séquences.

**Définition 5.20.3** (séries)**.** *Soit* $\mu$, $\lambda$ *et* $\xi \in \mathbb{F}_{p^n}$ *tels que* $\mu \neq \lambda$ *et* $\xi \neq \lambda$. *Si la série* $(\mu, \lambda, \ldots, \lambda, \xi)$ *apparait dans la séquence, alors nous disons que* $(\lambda, \ldots, \lambda)$ *est une série de* $\lambda$ *de longueur* $k$.

Pour définir l'auto-corrélation d'une séquence non-binaire, nous devons introduire les caractères additifs.

**Définition 5.20.4** (caractére additif)**.** *On appelle caractère canonique additif de* $\mathbb{F}_{p^n}$ *la fonction définie par :*

$$\forall x \in \mathbb{F}_{p^n},\ \chi(x) = e^{2i\pi \frac{\mathtt{Tr}(x))}{p}}$$

*avec* $\mathtt{Tr}(x) = x + x^p + \ldots + x^{p^{n-1}}$.

**Définition 5.20.5** (auto-corrélation). *L'auto-corrélation relative à $\chi$ de $\underline{a}$ est définie par :*

$$\forall\, 0 \leq \tau \leq p^{nr} - 2,\ \mathcal{C}_{\underline{a}}(\tau) = \sum_{i=0}^{p^{nr}-2} \chi(a_i)\overline{\chi(a_{i+\tau})}$$

**Remarque 5.20.1.** *Si $p = 2$, alors $\chi(x) = e^{\frac{2i\pi \mathrm{Tr}(x)}{2}} = e^{i\pi x}$. On a alors $\chi(0) = 1$ et $\chi(1) = -1$, donc $\chi(x) = (-1)^x$. L'autocorrélation telle qu'elle est définie sur $\mathbb{F}_2$ est un cas particulier.*

**R1 :** Pour toute période, tout élément non nul apparait $p^{n(r-1)}$ fois. le 0 apparait $p^{n(r-1)} - 1$. Cette propriété est équivalente à la propriété d'équilibre (balanced property) d'une séquence non binaire.

**R2 :** Pour toute période :

- Pour $1 \leq k \leq n-2$, les séries de tout élément dans $\mathbb{F}_{p^n}$ de longueur $k$ apparaissent $(p^n - 1)^2 p^{n(r-k-2)}$ fois.
- La série de tout élément non-nul de longueur $r - 1$ apparait $p^n - 2$ fois.
- La série de l'élément nul apparait $p^n - 1$ fois.
- La série de n'importe quel élément non-nul de longueur $r$ apparait une fois.

**R3 :** L'auto-corrélation $\mathcal{C}_{\underline{a}}(\tau) = \begin{cases} p^{nr} - 1 & \text{si} \tau \equiv 0 \mod p^{nr} - 1 \\ -1 & \text{sinon} \end{cases}$

### Séquences vectorielles

Dans le cas où $n \geq 2$, on a des séquences périodiques qui se décomposent en séquences à coefficients dans $\mathbb{F}_p$.

**Définition 5.20.6** (séquences composantes). *On appelle séquences composantes les séquences composées des coordonnées vectorielles d'une séquence à coefficient dans $\mathbb{F}_{p^n}$. Soit $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ une base de $\mathbb{F}_{p^n}$. Alors pour tout $i$, il existe $a_{i,j} \in \mathbb{F}_p$ tels que*

$$a_i = \sum_{j=0}^{j=n-1} a_{i,j}\alpha_j.$$

*On notera les séquences composantes par $\underline{a}_j = (a_{0,j}, a_{1,j}, \ldots)$.*

On peut redéfinir l'auto-corrélation d'une séquence périodique à coefficients dans $\mathbb{F}_{p^n}$ par l'auto-corrélation de ses séquences composantes :

**Définition 5.20.7** (auto-correlation composante). *On définit la fonction :*

$$\mathcal{D}_{\underline{a}}(\tau) = \sum_{j=0}^{j=m-1} \mathcal{C}_{\underline{a}_j}(\tau).$$

On redéfinit alors le troisième postulat de Golomb par

**R3́** L'auto-correlation composante doit être à deux niveaux :

$$\mathcal{D}(\tau) = \begin{cases} n(p^{nr} - 1) & \text{si } \tau \equiv 0 \mod p^{nr} - 1 \\ -n & \text{sinon.} \end{cases}$$

### 5.20.2 Propriétés aléatoires des $m$-séquences

Dans cette section, nous démontrons que les $m$-séquences vérifient les 3 postulats de Golomb. Dans un premier temps, on démontre qu'elles vérifient les postulats **R1** et **R2**. Ensuite on vérifie le postulat **R3**.

#### Les deux premiers Postulats

On pose une nouvelle propriété d'aléarité pour une séquences à coefficients dans $\mathbb{F}_{p^n}$ et de période $p^{nr}-1$ :

- **R4 :** Dans toute période de $\underline{a}$, tout $r$-uplet non-nul $(\lambda_1, \lambda_2, \ldots, \lambda_r) \in (\mathbb{F}_{p^n})^r$ apparait une seule fois.

**Définition 5.20.8** (distribution idéal de $k$-uplet)**.** *Dans toute période de $\underline{a}$, si pour tout $1 \leq k \leq r$, tout $k$-uplet non-nul $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{F}_q^{(k)}$ apparait $p^{n(r-k)}$ fois et le $k$-uplet nul apparait $p^{n(r-k)}-1$ fois, alors on dit que $\underline{a}$ a une distribution idéale des $k$-uplets.*

**Remarque 5.20.2.** *Si $\underline{a}$ a une distribution idéale des $k$-uplets alors tout $r$-uplet non-nul apparait $p^{n(r-r)}$ fois, soit une seule fois. Donc la distribution idéale des $k$-uplets implique la propriété **R4**.*

**Proposition 5.20.1.** *Si $\underline{a}$ vérifie la propriété **R4** alors $\underline{a}$ a une distribution idéale des $k$-uplets pour $1 \leq k \leq r$.*

*Démonstration.* Soit le $k$-uplet non-nul $(\lambda_1, \lambda_2, \ldots, \lambda_k)$. Si $k = r$, alors il apparait une seule fois. Si $k < r$, alors tout $r$-uplet $(\lambda_1, \lambda_2, \ldots, \lambda_r)$ apparait une seule fois. Comme le $k$-uplet $\lambda_1, \lambda_2, \ldots, \lambda_k$ est fixé, il apparait dans $p^{n(r-k)}$ $r$-uplets différents de cette forme :

$$(\lambda_1, \lambda_2, \ldots, \lambda_k, \underbrace{\lambda_{k+1}, \ldots, \lambda_r}_{r-k})$$

Donc le $k$-uplet apparait $p^{n(r-k)}$ fois. □

**Propriété 5.20.1.** *Toute $m$-séquence vérifie la propriété **R4**.*

*Démonstration.* Soit $\underline{a}$ une $m$-séquence sur $\mathbb{F}_{p^n}$ de période $p^{nr}-1$. La séquence $\underline{a}$ est une LFSR séquence de complexité linéaire $r$. Nous allons prouver que tout $r$-uplet non-nul apparait dans toute période exactement une fois. C'est équivalent à montrer que :

$$\forall\, i \neq j,\ \forall\, 0 \leq i, j \leq q^n - 2,\ (a_i, \ldots, a_{i+n-1}) \neq (a_j, \ldots, a_{j+n-1}).$$

Soit $m_{\underline{a}}^*$ le polynôme minimal de $\underline{a}$ sur $\mathbb{F}_{p^n}$ et soit $\alpha$ une racine de $m_{\underline{a}}^*$ dans l'extension $\mathbb{F}_{p^{nr}}$. D'après le théorème 5.14.2, $m_{\underline{a}}^*$ est irréductible, primitif de degré $r$ et $\alpha$ est un élément primitif de $\mathbb{F}_{p^{nr}}$. D'après le corollaire 5.14.1, $G^*(q^*)$ est de cardinal $p^{nr}$ et

$$G^*(q^*) = \left\{L^i(\underline{a}); 0 \leq i \leq q^n - 2\right\} \cup \{0\}$$

Une séquence de $G^*(q^*)$ est déterminée par son état initial de taille $r$. Il y en a $p^{nr}-1$ possibles non-nuls distincts. Donc chaque séquence de $G^*(q^*)$ correspond à un état initial. Supposons qu'il existe $i \neq j$ tels que $(a_i, \ldots, a_{i+r-1}) = (a_j, \ldots, a_{j+r-1})$. Or la séquence $L^i(\underline{a})$ a pour état initial $(a_i, \ldots, a_{i+r-1})$ et $L^j(\underline{a})$ a pour état initial $(a_j, \ldots, a_{j+r-1})$. Comme les états initiaux sont égaux, alors $L^i(\underline{a}) = L^j(\underline{a})$. Donc l'ensemble $G^*(q^*) = \left\{L^i(\underline{a}); 0 \leq i \leq p^{nr}-2\right\} \cup \{0\}$ a un cardinal inférieur ou égal à $p^{nr}-1$. Or le cardinal de $G^*(q^*)$ est égal à $p^{nr}$. C'est absurde. On en conclut que toute $m$-séquence vérifie la propriété **R4**. □

**Proposition 5.20.2.** *Toute $m$-séquence a une distribution idéale de $k$-uplet pour $1 \leq k \leq r$.*

*Démonstration.* Toute $m$-séquence vérifie la propriété **R4** qui est équivalente à la propriété de l'idéale distribution. □

**Proposition 5.20.3.** *Toute $m$-séquence vérifie la propriété **R1**.*

*Démonstration.* On sait que toute $m$-séquence est une idéale distribution pour tout $k$-uplet pour $1 \leq k \leq r$. Si on prend $k = 1$, on trouve que tout élément non-nul apparait $p^{n(r-1)}$ fois et l'élément nul apparait $p^{n(r-1)} - 1$ fois. Ainsi toute $m$-séquence vérifie la propriété de **R1**, propriété de la balance. □

En utilisant cette propriété des $m$-séquences et leur représentation par la trace, on obtient un résultat sur la trace.

**Corollaire 5.20.1.** *Pour tout $c \in \mathbb{F}_{p^n}^*$ et pour tout $\beta \in \mathbb{F}_{p^{nr}}^*$, l'équation $\mathtt{Tr}(\beta x) = c$ a $p^{n(r-1)}$ solutions dans $\mathbb{F}_{p^{nr}}$.*

*Démonstration.* Soit $\underline{a}$ une $m$-séquence de période $p^{nr}-1$. Elle admet une représentation par la trace. Soit $\alpha$ un élément primitif de $\mathbb{F}_{p^{nr}}$. Il existe $\beta \in \mathbb{F}_{p^{nr}}$ non nul tel que pour tout $0 \leq i \leq p^{nr}-2$, $a_i = \mathtt{Tr}(\beta\alpha^i)$. D'après la propriété **R1**, tout élément non-nul de $\mathbb{F}_{p^n}$ apparait $p^{n(r-1)}$ fois dans une période de la séquence $\underline{a}$ et l'élément nul apparait $p^{n(r-1)} - 1$. Donc il y a exactement $p^{n(r-1)}$ éléments $i \in \mathbb{F}_{p^{nr}}$ tels que $a_i = \mathtt{Tr}(\beta\alpha^i) = c$, pour $c$ non-nul et il y a exactement $p^{n(r-1)}-1$ éléments $i \in \mathbb{F}_{p^{nr}}$ tels que $a_i = \mathtt{Tr}(\beta\alpha^i) = 0$. Or $\alpha$ est primitif, donc $\mathbb{F}_{p^{nr}} = \mathbb{F}_{p^n}[\alpha]$. Donc l'équation $\mathtt{Tr}(\beta x) = c$ a $p^{n(r-1)}$ solutions dans le cas ou $c \neq 0$ et l'équation $\mathtt{Tr}(\beta x) = 0$ a $p^{n(r-1)} - 1$ solutions non-nulles plus la solution nulle, donc $p^{n(r-1)}$ solutions au total. □

**Proposition 5.20.4.** *Une $m$-séquence vérifie la propriété **R2**.*

*Démonstration.* Démontrons que toute série de tout élément de longueur $k$ pour $1 \leq k \leq r-2$ apparait $(p^n-1)^2 p^{n(r-k-2)}$ fois. Soit $(\lambda, \lambda, \ldots, \lambda)$ une série de longueur $k$ avec $1 \leq k \leq r-2$. Elle est forcément incluse dans un $r$-uplet de la forme suivante :

$$(\mu_1, \underbrace{\lambda, \ldots, \lambda}_{k}, \mu_{k+1}, \underbrace{\mu_{k+2}, \ldots, \mu_{r-1}}_{r-k-2}).$$

En effet, les deux coefficients les plus proches sont forcément différents de $\lambda$ afin que ce soit une série de longueur $k$. Comme une $m$-séquence vérifie la propriété **R4**, ce $r$-uplet apparait exactement une seule fois dans une période. Il est déterminé par le choix des $\mu_i$ avec $i \in \{1, k+1, \ldots, r-1\}$. Les éléments $\mu_1$ et $\mu_{k+1}$ appartiennent à $\mathbb{F}_{p^n} \setminus \{\lambda\}$, donc il existe $(p^n-1)^2$ couples dinstincts de $(\mu_1, \mu_{k+1})$. Quant aux $(r-k-2)$-uplets $(\mu_{k+2}, \ldots, \mu_{r-1})$, il en existe $p^{n(r-k-2)}$ car les $\mu_i$ parcourent $\mathbb{F}_{p^n}$. Donc il y a exactement $(p^n-1)^2 p^{n(r-k-2)}$ $r$-uplets de la forme $(\mu_1, \underbrace{\lambda, \ldots, \lambda}_{k}, \mu_{k+1}, \underbrace{\mu_{k+2}, \ldots, \mu_{r-1}}_{n-k-2})$ qui apparaissent une seule fois dans chaque période de la $m$-séquence. D'où le fait que la série $(\lambda, \ldots, \lambda)$ de longueur $k$ apparait $(p^n-1)^2 p^{n(r-k-2)}$ fois dans une seule période.

Montrons maintenant que toute série de n'importe quel élément non-nul de longueur $r-1$ apparait $p^n-2$ fois. Soit la série $\underbrace{(\lambda, \ldots, \lambda)}_{r-1}$ avec $\lambda \neq 0$. Cette série peut se localiser dans un $r$-uplet de la forme $(\mu, \lambda, \ldots, \lambda)$, avec $\mu \neq \lambda$. Par la propriété **R4**, ce $r$-uplet apparait exactement une fois dans une seule période et il existe $p^n - 1$ $r$-uplets de cette forme. Donc la série apparait $p^n - 1$ fois dans une seule période de la $m$-séquence.

Enfin la série de tout élément non-nul de longueur $r$ apparait une seule fois. C'est un $r$-uplet, d'après la propriété **R4**, il apparait une seule fois. □

Pour le postulat concernant l'auto-corrélation d'une $m$-séquence, on doit d'abord introduire des résultats intermédiaires sur les sommes exponentielles.

### Propriété basique des sommes exponentielles

**Lemme 5.20.1.** *Soit le caractère additif $\chi$ défini par $\chi : \mathbb{F}_{p^{nr}} \to \mathbb{F}_p$, $x \mapsto \chi(x) = e^{2i\pi \frac{\mathtt{Tr}(x)}{p}}$. Alors on a :*

$$\forall \beta \in \mathbb{F}_{p^{nr}}, \sum_{x \in \mathbb{F}_{p^{nr}}} \chi(\beta x) = \begin{cases} p^{nr} & si\ \beta = 0 \\ 0 & sinon \end{cases} .$$

*Démonstration.* Posons $w = e^{\frac{2i\pi}{p}}$, donc $\chi(x) = w^{\mathtt{Tr}(x)}$. Le nombre complexe $\omega$ est une racine $p$-ième primitive de l'unité, $\omega^p - 1 = 0$ et elle est aussi racine du polynôme cyclotomique $\Phi_p(x)$. L'entier $p$ étant premier, on a :

$$x^p - 1 = \Phi_p(x)\Phi_1(x) = (x-1)\Phi_p(x) \Leftrightarrow \frac{x^p-1}{x-1} = x^{p-1} + \ldots + x + 1.$$

Donc $\sum_{i=0}^{p-1} \omega^i = 0$. Si $\beta \neq 0$ alors d'après le corollaire 5.20.1, l'équation $\mathtt{Tr}(\beta x) = z$ admet $p^{n(r-1)}$ solutions pour tout $z \in \mathbb{F}_{p^n}$ et l'équation $\mathtt{Tr}(z) = y$ admet $p^{n-1}$ solutions pour tout $y \in \mathbb{F}_p$. Donc l'équation

$$\mathtt{Tr}(\beta x) = y \Leftrightarrow \mathtt{Tr}(\mathtt{Tr}(\beta x)) = \mathtt{Tr}(z) = y$$

admet $p^{n(r-1)}p^{n-1} = p^{nr-1}$ solutions. Donc :

$$\sum_{x\in\mathbb{F}_{p^{nr}}} \chi(\beta x) = \sum_{x\in\mathbb{F}_{p^{nr}}} \omega^{Tr(\beta x)} = p^{nr-1}\sum_{y\in\mathbb{F}_p} \omega^y = p^{nr-1}\sum_{y=0}^{p-1}\omega^y = p^{nr-1}.0 = 0.$$

Donc pour tout $\beta \neq 0$, $\sum_{x\in\mathbb{F}_{p^{nr}}} \chi(\beta x) = 0$. Et si $\beta = 0$, alors

$$\sum_{x\in\mathbb{F}_{p^{nr}}} \chi(\beta x) = \sum_{x\in\mathbb{F}_{p^{nr}}} \omega^0 = \sum_{x\in\mathbb{F}_{p^{nr}}} 1 = p^{nr}.$$

□

**Lemme 5.20.2.** *Soit le caractère additif $\chi$ définie par $\chi : \mathbb{F}_{p^{nr}} \to \mathbb{F}_p$, $x \mapsto \chi(x) = e^{2i\pi\frac{\mathrm{Tr}(x)}{p}}$, alors $\forall x, y \in \mathbb{F}_{p^{nr}}$, $\chi(x)\overline{\chi(y)} = \chi(x-y)$.*

*Démonstration.* Il s'agit d'un calcul direct :

$$\chi(x)\overline{\chi(y)} = \omega^{Tr(x)}\overline{\omega^{Tr(y)}} = \omega^{Tr(x)}\overline{\omega}^{Tr(y)} = \omega^{Tr(x)}\omega^{-Tr(y)} = \omega^{Tr(x)-Tr(y)} = \omega^{Tr(x-y)} = \chi(x-y).$$

□

**Le troisième postulat**

En utilisant ces deux lemmes, démontrons qu'une $m$-séquence vérifie la propriété **R3**.

**Proposition 5.20.5.** *Toute $m$-séquence vérifie la propriété **R3**.*

*Démonstration.* $\underline{a}$ étant une $m$-séquence, elle admet une représentation par la trace avec

$\alpha$ élément primitif de $\mathbb{F}_{p^{nr}}$.

$$\begin{aligned}
\mathcal{C}_{\underline{a}}(\tau) &= \sum_{i=0}^{p^{nr}-2} \chi(a_i)\overline{\chi(a_{i+\tau})} \\
&= \sum_{i=0}^{p^{nr}-2} e^{\frac{2i\pi}{p}\mathtt{Tr}(a_i)}\overline{e^{\frac{2i\pi}{p}\mathtt{Tr}(a_{i+\tau})}} \\
&= \sum_{i=0}^{p^{nr}-2} e^{\frac{2i\pi}{p}\mathtt{Tr}(a_i)}e^{-\frac{2i\pi}{p}\mathtt{Tr}(a_{i+\tau})} \\
&= \sum_{i=0}^{p^{nr}-2} w^{\mathtt{Tr}(a_i-a_{i+\tau})} \\
&= \sum_{i=0}^{p^{nr}-2} w^{\mathtt{Tr}(\mathtt{Tr}(\beta\alpha^i-\beta\alpha^{i+\tau}))} \\
&= \sum_{i=0}^{p^{nr}-2} w^{\mathtt{Tr}(\beta\alpha^i-\beta\alpha^{i+\tau})} \\
&= \sum_{i=0}^{p^{nr}-2} w^{\mathtt{Tr}(\beta\alpha^i(1-\alpha^\tau))} \\
&= \sum_{x\in\mathbb{F}_{p^{nr}}} w^{\mathtt{Tr}(\beta x(1-\alpha^\tau))} - 1 \\
&= \sum_{x\in\mathbb{F}_{p^{nr}}} w^{\mathtt{Tr}(\mu x)} - 1 \text{ avec } \mu = \beta(1-\alpha^\tau) \\
&= \sum_{x\in\mathbb{F}_{p^{nr}}} \chi(\mu x) - 1.
\end{aligned}$$

D'après le lemme 5.20.1 :

$$\mathcal{C}_{\underline{a}}(\tau) = \begin{cases} p^{nr}-1 \text{ si } \mu = 0 \\ -1 \text{ si } \mu \neq 0 \end{cases}$$

D'autre part $\mu = 0 \Leftrightarrow \beta(1-\alpha^\tau) = 0 \Leftrightarrow \alpha^\tau = 1 \Leftrightarrow \tau \equiv 0 \mod \mathtt{ord}(\alpha)$ et $\mathtt{ord}(\alpha) = p^{nr}-1$. □

On en conclut que les $m$-séquences vérifient les propriétés aléatoires de Golomb : **R1**, **R2**, **R3** et **R4**. La question est de savoir s'il existe d'autres séquences vérifiant ces trois postulats. Golomb a énoncé la conjecture suivante :

**Conjecture 5.20.1.** *Les seules séquences binaires satisfaisant les trois postulats de Golomb sont les m-séquences.*

### 5.20.3 Propriété Trinomiale

Dans cette sous-section, on démontre la propriété trinomiale ou dite *shift-and-add* des $m$-séquences. C'est une propriété très importantes.

**R5** Une séquences périodique $\underline{a}$ de période $T$ vérifie la propriété trinomiale si pour tout décalage $\tau < T$, on a $\underline{a} + L^\tau(\underline{a}) = \underline{0}$ ou s'il existe un autre décalage $\tau' < T$ tel que $\underline{a} + L^\tau(\underline{a}) = L^{\tau'}(\underline{a})$.

**Définition 5.20.9** (shift-and-add). *Une séquence vérifiant la propriété trinomiale est aussi appelée shift-and-add.*

**Théorème 5.20.1** (la propriété shift-and-add des séquences binaires). *Soit $\underline{a}$ une séquence binaire périodique de période $N$ telle que $\forall i, j \in \mathbb{N}$, il existe $k \in \mathbb{N}$ tel que*

$$L^i(\underline{a}) + L^j(\underline{a}) = L^k(\underline{a}) \text{ ou } L^i(\underline{a}) + L^j(\underline{a}) = \underline{0},$$

*alors il existe $r \in \mathbb{N}$ tel que $N = 2^r - 1$ et $\underline{a}$ une m-séquence. Inversement si $\underline{a}$ est une m-séquence alors $\forall i, j \in \{0, 1, \ldots, 2^r - 1\}$, il existe un $0 \leq k \leq 2^r - 2$ tel que $L^i(\underline{a}) + L^j(\underline{a}) = L^k(\underline{a})$ ou $L^i(\underline{a}) + L^j(\underline{a}) = \underline{0}$.*

*Démonstration.* Montrons la première implication. Soit $S = \left\{L^i(\underline{a}); 0 \leq i \leq N-1\right\} \cup \{0\}$. Donc $S$ est un ensemble à $N+1$ éléments. Par hypothèse, il est stable par addition et il est stable par multiplication d'un scalaire de $\mathbb{F}_2$, donc $S$ est un $\mathbb{F}_2$-espace vectoriel à $N+1$ éléments. Si $r$ sa dimension, il possède $2^r$ éléments, $N + 1 = 2^r \Rightarrow N = 2^r - 1$. Donc $\underline{a}$ est de période $2^r - 1$. Montrons que $\underline{a}$ peut être généré par un LFSR de taille $r$ pour conclure que c'est une $m$-séquence. Soit $m^*_{\underline{a}}$ le polynôme minimal de $\underline{a}$ sur $\mathbb{F}_2$ de degré $k$. Donc $G^*(m^*)$ est de cardinal $2^k$, d'autre part

$$m^*(L)(L^i(\underline{a})) = L^i.m^*(L)(\underline{a}) = \underline{0} \Rightarrow S \subseteq G^*(m^*) \Rightarrow 2^r \leq 2^k \Rightarrow r \leq k.$$

Montrons que $k \leq r$. Le polynôme minimal de $\underline{a}$ est de degré $k$, donc la famille

$$\left\{\underline{a}, L(\underline{a}), L^2(\underline{a}), \ldots, L^{k-1}(\underline{a})\right\}$$

est une famille libre sur $\mathbb{F}_2$. Donc l'espace vectoriel engendré par cette famille est de dimension $k$ et cet espace est inclus dans $S$, donc $k \leq r$. On a donc démontré que le polynôme minimal de $\underline{a}$ est de degré $r$. C'est donc une $m$-séquence.

Inversement si $\underline{a}$ est une $m$-séquence, $\underline{a}$ est de période $2^r - 1$ et d'après la proposition 5.14.2, son polynôme minimal $m^*$ est de degré $r$. Comme la période de $\underline{a}$ est $2^r - 1$, alors $\left\{L^i(\underline{a}); 0 \leq i \leq 2^r - 2\right\} \cup \{0\}$ est de cardinal $2^r$. Comme le degré du polynôme minimal de $\underline{a}$ est $r$, alors $G(m^*)$ est de cardinal $2^r$. Or $\left\{L^i(\underline{a}); 0 \leq i \leq 2^n - 2\right\} \cup \{0\} \subseteq G^*(m^*)$, donc $G^*(m^*) = \left\{L^i(\underline{a}); 0 \leq i \leq 2^r - 2\right\} \cup \{0\}$. L'espace $G^*(m^*)$ étant un $\mathbb{F}_2$-espace vectoriel, alors pour tout $0 \leq j \leq 2^r - 2$, $\underline{a} + L^j(\underline{a}) \in G^*(m^*)$, donc il existe $0 \leq k \leq 2^r - 2$ tel que $\underline{a} + L^j(\underline{a}) = L^k(\underline{a})$ ou $\underline{a} + L^j(\underline{a}) = 0$. En appliquant l'opérateur de décalage $L^i$, on obtient $L^i(\underline{a}) + L^{i+j}(\underline{a}) = L^{i+k}(\underline{a})$ ou $L^i(\underline{a}) + L^{i+j}(\underline{a}) = \underline{0}$. Ceci étant vrai pour tout $i$ et $j$, c'est équivalent à dire que pour tout $i$ et $j$ appartenant à $\{0, 1, \ldots, 2^r - 2\}$, $L^i(\underline{a}) + L^j(\underline{a}) = L^k(\underline{a})$ ou $\underline{0}$. □

**Théorème 5.20.2.** *Soit $\underline{a}$ une m-séquence sur $\mathbb{F}_{p^n}$. Alors $\forall 0 \leq i, j \leq p^{nr} - 1$, il existe un $0 \leq k \leq p^{nr} - 2$ tel que $L^i(\underline{a}) + L^j(\underline{a}) = L^k(\underline{a})$ ou $\underline{0}$.*

*Démonstration.* Considérons $m^*$ le polynôme minimal de $\underline{a}$ de degré $r$. Donc $G^*(m^*) = \left\{L^i(\underline{a}); 0 \leq i \leq p^{nr} - 2\right\} \cup \{0\}$. On trouve que : $L^i(\underline{a}) + L^j(\underline{a}) = L^i(\underline{a} + L^{j-i}(\underline{a}))$. Or $G^*$ est un $\mathbb{F}_{p^n}$-espace vectoriel, donc il existe un $k$ tel que $\underline{a} + L^{j-i}(\underline{a}) = L^k(\underline{a})$ ou $\underline{0}$. On en déduit que $L^i(\underline{a}) + L^j(\underline{a}) = L^{i+k}(\underline{a})$ ou $\underline{0}$. □

**Théorème 5.20.3.** *Soit une séquence périodique à coefficient dans $\mathbb{F}_{p^n}$ vérifiant la propriété trinomiale, alors c'est une m-séquence.*

*Démonstration.* Considérons $S$ l'ensemble des décalages de $\underline{a}$ et de la séquence nulle. Par la propriété trinomiale, c'est un $\mathbb{F}_{p^n}$-espace vectoriel fini. Notons $r$ sa dimension. Il contient $p^{nr}$ éléments. Donc la période de $\underline{a}$ est $p^{nr}-1$. La séquence $\underline{a}$ est périodique, c'est donc une LFSR-séquence. Soit $m^*$ son polynôme minimal. L'ensemble $S$ est inclu dans $G^*(m^*)$. L'ensemble $G^*$ a $p^{n\deg(m^*)}$ éléments. Donc $r \leq \deg(m^*)$. La famille $\left\{\underline{a}, L(\underline{a}), \ldots, L^{\deg(m^*)-1}(\underline{a})\right\}$ est libre sur $\mathbb{F}_{p^n}$, donc $S$ est au moins de dimension $\deg(m^*)$, ce qui achève la démonstration. □

La propriété shift-and-add caractérise les $m$-séquences. Ce n'est pas le cas des séquences non-linéaires ou NLFSR séquences. En effet dans certaines conditions, une séquence binaire, non linéaire et périodique de période $2^r-1$ ne vérifie pas cette propriété.

**Conjecture 5.20.2.** *(Conjecture de Golomb-Gong) Toute séquence binaire non-linéaire de période $2^r-1$ n'a pas de paire trinomiale si n est premier.*

Cette conjecture est vérifiée jusqu'à $n = 17$.

## 5.21 Transformée de Fourier et complexité linéaire

Dans cette section , nous étudions la transformée discrète de Fourier d'une séquence périodique. Elle se divise en trois sous-sections : la première concerne les définitions, la deuxième la représentation par la trace et la troisième fait le lien entre la complexité linéaire et la transformée de Fourier.

### 5.21.1 Spectre de Fourier d'une séquence périodique

**Définition 5.21.1.** *Soit $\underline{a}$ une séquence à coefficient dans $\mathbb{F}_{p^n}$ de période $N > 1$ où $N$ divise $p^{nr}-1$ pour un certain $n \geq 1$. On identifie $\underline{a}$ par sa période $\underline{a} = (a_0, a_1, \ldots, a_{N-1})$. Considérons $\alpha$ un élément de $\mathbb{F}_{p^{nr}}$ d'ordre $N$. On définit la transformée discrète de Fourier de $\underline{a}$ par :*

$$\underline{A} = (A_k)_{0\leq k\leq N-1} \text{ avec } A_k = \sum_{t=0}^{N-1} a_t \alpha^{tk}.$$

La transformée discrète de Fourier peut être repésentée par une forme matricielle :

$$\underline{A} = (a_0, a_1, \ldots, a_{N-1}) \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{N-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{N-1} & \cdots & (\alpha^{N-1})^{N-1} \end{pmatrix}.$$

**Lemme 5.21.1.** *La formule inverse de la transformée discrète de Fourier est*

$$\forall\, 0 \leq t \leq N-1,\, a_t = \frac{1}{N}\sum_{k=0}^{N-1} A_k \alpha^{-kt}.$$

Pour démontrer cette formule, nous avons besoin d'énoncer un lemme.

**Lemme 5.21.2.**

$$\sum_{i=0}^{N-1} \alpha^{di} = \begin{cases} N & \Leftrightarrow \quad d \equiv 0(N) \\ 0 & sinon \end{cases}$$

*Démonstration.* Si $N$ divise $d$, alors :

$$d \equiv 0 \mod N \Rightarrow \alpha^d = 1 \Rightarrow \forall 0 \leq i \leq N-1,\, \alpha^{di} = 1 \Rightarrow \sum_{i=0}^{N-1} \alpha^{di} = N.$$

Sinon $\alpha^d \neq 1$ car $\alpha$ est d'ordre $N$. On pose $s = \texttt{ord}(\alpha^d)$

$$\begin{array}{rcl} (\alpha^d)^s = 1 & \Rightarrow & (\alpha^d)^s - 1 = 0 \Rightarrow (\alpha^d - 1)((\alpha^d)^{s-1} + \cdots + \alpha^d + 1) = 0 \\ & \Rightarrow & (\alpha^d)^{s-1} + \cdots + \alpha^d + 1 = 0 \end{array}.$$

Comme $d \not\equiv 0 \mod N$, alors $d > 1$ et comme $N > 1$ alors $\texttt{PGCD}(d, N) \geq 1$. Si $\texttt{PGCD}(d, N) = N \Rightarrow N \mid d \Rightarrow d \equiv 0(N)$, donc

$$\texttt{PGCD}(d, N) \neq N \Rightarrow 1 \leq \texttt{PGCD}(d, N) < N \Rightarrow 1 < \frac{N}{\texttt{PGCD}(d, N)}.$$

Or $\texttt{ord}(\alpha^d) = \frac{N}{\texttt{PGCD}(d,N)}$, donc $\texttt{ord}(\alpha^d) > 1$. Posons $v = \texttt{PGCD}(d, N)$ et $e = \frac{N}{v}$. Pour tout $0 \leq k \leq N-1$, il existe $i$ et $j$ tels que $k = ie + j$ et $0 \leq j < e$. Donc $\frac{k}{e} = i + \frac{j}{e}$ et $0 \leq \frac{j}{e} < 1$. Alors

$$i < \frac{k}{e} \leq \frac{N-1}{e} < \frac{N}{e} = v.$$

$$e = \texttt{ord}(\alpha^d) \Rightarrow \begin{cases} \sum_{j=0}^{e-1} (\alpha^d)^j &=& 0 \\ (\alpha^d)^e &=& 1 \end{cases} \Rightarrow \begin{cases} \sum_{j=0}^{e-1} (\alpha^d)^j &=& 0 \\ \forall i,\, (\alpha^d)^{ei} &=& 1 \end{cases}$$

$$\sum_{k=0}^{N-1} \alpha^{dk} = \sum_{k=0}^{N-1} (\alpha^d)^k = \sum_{i=0}^{v-1}\sum_{j=0}^{e-1} (\alpha^d)^{ie+j} = \sum_{i=0}^{v-1} ((\alpha^d)^e)^i \sum_{j=0}^{e-1} (\alpha^d)^j.$$

En effet $0 \leq ie + j \leq (v-1)e + e - 1 = ve - e + e - 1 = N - 1$. Donc il y a une bijection entre les couples $(i, j) \in \{0, \ldots, e-1\} \times \{0, \ldots, v-1\}$ et les éléments de $\{0, \ldots, N-1\}$.

$$\sum_{k=0}^{N-1} (\alpha^d)^k = \sum_{i=0}^{v-1} 1 \sum_{j=0}^{e-1} (\alpha^d)^j = v \cdot 0 = 0.$$

Le lemme est démontré. □

Maintenant, nous pouvons passer à la démonstration de la formule inverse.

*Démonstration du lemme 5.21.1.*

$$\begin{aligned}
\tfrac{1}{N}\sum_{k=0}^{N-1}(\sum_{i=0}^{N-1} a_i\alpha^{ik})\alpha^{-kt} &= \tfrac{1}{N}\sum_{k=0}^{N-1}\sum_{i=0}^{N-1} a_i\alpha^{(i-t)k} \\
&= \tfrac{1}{N}\sum_{k=0}^{N-1}\sum_{i=0}^{N-1} a_i\alpha^{(i-t)k} \\
&= \tfrac{1}{N}\sum_{i=0}^{N-1} a_i \sum_{k=0}^{N-1}\alpha^{(i-t)k} \\
&= \tfrac{1}{N}\sum_{0\le i\le N-1;N|(i-t)} a_i \times N + \tfrac{1}{N}\sum_{0\le i\le N-1;N\nmid(i-t)} a_i \times 0 \\
&= \tfrac{1}{N}N\sum_{0\le i\le N-1;N|(i-t)} a_i \\
&= a_t + \sum_{0\le i\le N-1;i\equiv t(N);i\neq t} a_i \\
\tfrac{1}{N}\sum_{k=0}^{N-1}(\sum_{i=0}^{N-1} a_i\alpha^{ik})\alpha^{-kt} &= a_t
\end{aligned}$$

En effet, l'ensemble suivant est vide :

$$\{0 \le i \le N-1 \text{ tels que } i \equiv t \mod N \text{ et } i \neq t\} = \{0 \le i \le N-1\} \cap \{t+N, t+2N, \ldots\} = \emptyset.$$

□

**Définition 5.21.2** (séquence spectrale)**.** *$A_k$ est appelé spectre de Fourier de la séquence. La séquence $\underline{A}$ est aussi de période $N$ que l'on note $\underline{A} = (A_0, A_1, \ldots, A_{N-1})$. On l'appelle la séquence spectrale de $\underline{a}$. La séquence spectrale est à valeurs dans $\mathbb{F}_{p^{nr}}$.*

**Exemple 5.21.1.** *Plaçons nous dans $\mathbb{F}_2$. Posons $r = 3$. Considérons $q^*(x) = X^3+X+1$ irréductible sur $\mathbb{F}_2$ et $\alpha = \bar{X}$ racine de $q^*$ dans $\mathbb{F}_2[X]/(X^3+X+1)$. Soit la séquence $\underline{a} = (0100010)$ de période $7 = 2^3 - 1$. L'élément $\alpha$ est racine de $q^*$ donc $ord(\alpha)$ divise 7. Le nombre 7 étant premier, alors $ord(\alpha) = 1$ ou 7. 1 n'étant pas racine de $q^*$, alors $ord(\alpha) = 7$. La séquence spectrale est donnée par*

$$A_k = \sum_{t=0}^{N-1} a_t\alpha^{tk} = \sum_{t=0}^{6} a_t\alpha^{tk} = \alpha^k + \alpha^{5k}.$$

*D'où*

$$\underline{A} = (0, \alpha^6, \alpha^5, 1, \alpha^3, 1, 1).$$

*La transformée inverse donne*

$$\begin{aligned}
a_t &= \textstyle\sum_{k=0}^{6} A_k\alpha^{-tk} = \sum_{k=0}^{6} A_k\alpha^{-tk} \\
a_0 &= \alpha^6 + \alpha^5 + 1 + \alpha^3 + 1 + 1 &&= 0 \\
a_1 &= \alpha^5 + \alpha^3 + \alpha^4 + \alpha^6 + \alpha^2 + \alpha &&= 1 \\
&\vdots
\end{aligned}$$

*On retrouve $\underline{a} = (0100010)$.*

### 5.21.2 Représentation par la Trace d'une séquence périodique

**Sous-ensemble cyclotomique de $p^n$ modulo $N$**

**Définition 5.21.3** (sous-ensemble cyclotomique)**.** *Soit $N$ un diviseur de $p^{nr}-1$. Définissons l'ensemble suivant*

$$\mathcal{C}_s = \left\{ s, sp^n, sp^{2n}, \ldots, sp^{n(n_s-1)} \right\}$$

*où*

$$n_s = \inf \{ m \in \mathbb{N} \text{ tels que } sp^{nm} \equiv s \mod N \}.$$

*On appelle $\mathcal{C}_s$ un sous-ensemble cyclotomique de $p^n$ modulo $N$. L'entier $s$ est appelé représentant de $\mathcal{C}_s$ et $n_s$ est appelé ordre de $s$ ou ordre de $\mathcal{C}_s$.*

**Remarque 5.21.1.** *Les sous-ensembles cyclotomiques forment une partition de $\mathbb{Z}/N\mathbb{Z}$.*

$$\mathbb{Z}/N\mathbb{Z} = \cup_{j \in I} \mathcal{C}_j$$

*où $I$ est l'ensemble des représentants des sous-ensembles cyclotomiques.*

**Exemple 5.21.2.** *Soient $p=2$, $n=1$, $r=6$ et $N=21$. On a $2^6-1=63$ et $21 \mid 63$.*

$$\begin{array}{lcl}
\mathcal{C}_0 & = & \{0\} \\
\mathcal{C}_1 & = & \{1,2,4,8,16,11\} \text{ car } 32 = 21+11 \text{ et } 64 = 1+3\times 21 \\
\mathcal{C}_3 & = & \{3,6,12\} \text{ car } 24 = 21+3 \\
\mathcal{C}_5 & = & \{5,10,20,19,17,13\} \text{ car } 5\times 8 = 40 = 19+21 \\
 & & 5\times 16 = 80 = 3\times 21+17,\ 5\times 32 = 160 = 7\times 21+13 \text{ et } 5\times 64 = 320 = 15\times 21+5 \\
\mathcal{C}_7 & = & \{7,14\} \\
\mathcal{C}_9 & = & \{9,18,15\}
\end{array}$$

*L'union de ces sous-ensemble forme $\mathbb{Z}/21\mathbb{Z}$.*

**Propriété de conjugaison de la séquence spectrale**

**Lemme 5.21.3.** *Pour tout $1 \leq k \leq N-1$ et pour tout $0 \leq j < n$ :*

$$A_{kp^{nj}} = (A_k)^{p^{nj}}.$$

*Démonstration.*

$$A_{kp^{nj}} = \sum_{t=0}^{N-1} a_t \alpha^{tkp^{nj}} = \sum_{t=0}^{N-1} a_t (\alpha^{tk})^{p^{nj}}.$$

$$a_t \in \mathbb{F}_{p^n} \Rightarrow a_t^{p^n} = a_t \Rightarrow (a_t^{p^n})^{p^n} = a_t = a_t^{p^{2n}} \Rightarrow (a_t)^{p^{nj}} = a_t.$$

$$A_k p^{nj} = \sum_{t=0}^{N-1} a_t^{p^{nj}} (\alpha^{tk})^{p^{nj}} = \sum_{t=0}^{N-1} (a_t \alpha^{tk})^{p^{nj}} = (\sum_{t=0}^{N-1} a_t \alpha^{tk})^{p^{nj}} = (A_k)^{p^{nj}}.$$

□

Cette propriété de conjugaison permet de restreindre les calculs du spectre.

**Exemple 5.21.3.** $\underline{a} = (0100010)$ *a pour séquence spectrale* $\underline{A} = (0, \alpha^6, \alpha^5, 1, \alpha^3, 1, 1)$.

$$\begin{array}{lllllll} A_1 & = & \alpha^6 & & & & \\ A_1^2 & = & \alpha^{12} & = & \alpha^5 & = & A_2 \\ A_1^4 & = & \alpha^{24} & = & \alpha^3 & = & A_4 \\ A_3 & = & 1 & & & & \\ A_3^2 & = & 1 & = & A_6 & & \\ A_3^4 & = & 1 & = & A_{12} & = & A_5 \end{array}$$

**Exemple 5.21.4.** *Soient* $p = 2$, $n = 1$, $r = 6$ *et* $\mathbb{F}_{2^6} = \mathbb{F}_2[X]/(X^6 + X + 1) = \mathbb{F}_2[\alpha]$ *où* $\alpha = \bar{X}$. *On a* $|(\mathbb{F}_2[\alpha])^*| = 63$ *donc* $\alpha^{63} = 1$. *On cherche son ordre, il divise* $63 = 3^2 \times 7$.

$$\begin{array}{rcl} \alpha^9 & = & \alpha^4 + \alpha^3 \neq 1 \\ \alpha^7 & = & \alpha^2 + \alpha \neq 1 \\ \alpha^{21} & = & \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1 \neq 1. \end{array}$$

*Donc* $\alpha$ *est d'ordre 63 et* $\alpha^3$ *est d'ordre 21. Soit* $\underline{a}$ *une séquence de période 21.*

$$\underline{a} = (010000001010000010000).$$

*Les représentants des sous-ensembles cyclotomiques modulo 21 de 2 sont* $\{0, 1, 3, 5, 7, 9\}$.
*On a d'abord la formule* $A_k = \sum_{t=0}^{20} a_t(\alpha^3)^{tk} = \alpha^{3k} + \alpha^{24k} + \alpha^{30k} + \alpha^{48k}$.
*On détermine d'abord* $A_0, A_1, A_3, A_5, A_7$ *et* $A_9$.

$$A_0 = 0, A_1 = \alpha^{47}, A_3 = 1, A_5 = \alpha^{37}, A_7 = 1, A_9 = \alpha^9.$$

*Grâce à la propriété de conjugaison, nous pouvons déterminer tous les conjugués.*

$$\begin{array}{rlllllllll} A_2 & = & A_1^2 & = & (\alpha^{47})^2 & = & \alpha^{94} & = & \alpha^{63} & = & \alpha^{31} \\ A_4 & = & A_1^4 & = & \alpha_2^2 & = & \alpha^{62} & & & & \\ A_8 & = & A_4^2 & = & (\alpha^{62})^2 & = & \alpha^{124} & = & \alpha^{61} & & \\ A_{16} & = & A_8^2 & = & (\alpha^{61})^2 & = & \alpha^{122} & = & \alpha^{59} & & \\ A_{32} & = & A_{21+11} & = & A_{11} & = & (A_1)^{11} & = & (\alpha^{47})^{11} & = & \alpha^{55} \\ A_6 & = & (A_3)^2 & = & 1 & & & & & & \\ A_{12} & = & (A_3)^4 & = & 1 & & & & & & \\ A_{10} & = & (\alpha^{37})^2 & = & \alpha^{74} & = & \alpha^{11} & & & & \\ A_{20} & = & (\alpha^{37})^4 & = & \alpha^{148} & = & \alpha^{22} & & & & \\ A_{19} & = & A_{40} & = & (A_5)^8 & = & \alpha^{296} & = & \alpha^{44} & & \\ A_{17} & = & A_{80} & = & (A_5)^{16} & = & \alpha^{592} & = & \alpha^{25} & & \\ A_{13} & = & A_{160} & = & (A_5)^{32} & = & \alpha^{1184} & = & \alpha^{50} & & \end{array}$$

*Ainsi de suite, on calcule tous les autres coefficients de cette manière et on détermine facilement la séquence spectrale sans utiliser à chaque fois la formule générale. On obtient la séquence finale :*

$$\underline{A} = (0, \alpha^{47}, \alpha^{31}, 1, \alpha^{62}, \alpha^{37}, 1, 1, \alpha^{61}, \alpha^9, \alpha^{11}, \alpha^{55}, 1, \alpha^{50}, 1, \alpha^{36}, \alpha^{59}, \alpha^{25}, \alpha^{18}, \alpha^{44}, \alpha^{22}).$$

**Représentation par la Trace**

**Théorème 5.21.1.** *[Représentation par la trace] Soit $I$ l'ensemble des représentants modulo $N$ respectivement à $p^n$. Soit $(a_i)_{i\in\mathbb{N}}$ une séquence sur $\mathbb{F}_{p^n}$ de période $N$ divisant $p^{nr}-1$ pour un certain $r>0$. Alors la formule inverse de la transformée discrète de Fourier de la séquence est donnée par :*

$$\forall\, t\in\mathbb{N},\ a_t=\frac{1}{N}\sum_{j\in I} Tr^{n_j}(A_j\alpha^{-jt})$$

*où $n_j=|C_j|=ord(j)$*

*Démonstration.* Par définition, on a $p^{n.n_j}j\equiv j \bmod N$ pour tout $j\neq 0$. Comme la séquence spectrale est de période $N$, on a que :

$$\forall j\neq 0,\ (A_j)^{p^{nn_j}}=A_{jp^{nn_j}}=A_j.$$

Donc pour tout $j\neq 0$, $A_j\in\mathbb{F}_{p^{nn_j}}$, ainsi on peut définir sa trace sur $\mathbb{F}_{p^{nn_j}}$.

$$\begin{aligned}\mathtt{Tr}^{n_j}(A_j\alpha^{-jt}) &= A_j\alpha^{-jt}+(A_j\alpha^{-jt})^{p^n}+\cdots+(A_j\alpha^{-jt})^{p^{n(n_j-1)}}\\ \mathtt{Tr}^{n_j}(A_j\alpha^{-jt}) &= A_j\alpha^{-jt}+A_j^q\alpha^{-jp^nt}+\cdots+A_j^{p^{n(n_j-1)}}\alpha^{-jp^{n(n_j-1)}t}.\end{aligned}$$

D'après la propriété de conjugaison de la séquence spectrale $\underline{A}$, on a :

$$\mathtt{Tr}^{n_j}(A_j\alpha^{-jt})=A_j\alpha^{-jt}+A_{jp^n}\alpha^{-jp^nt}+\cdots+A_{jp^{n(n_j-1)}}\alpha^{-jp^{n(n_j-1)}t}.$$

D'où :

$$\begin{aligned}\tfrac{1}{N}\sum_{j\in I}\mathtt{Tr}_{p^n}^{n_j}(A_j\alpha^{-jt}) &= \tfrac{1}{N}\sum_{j\in I}(A_j\alpha^{-jt}+A_{jq}\alpha^{-jqt}+\cdots+A_{jq^{n_j-1}}\alpha^{-jp^{n(n_j-1)}t})\\ &= \tfrac{1}{N}\sum_{j\in I}\sum_{k\in\mathcal{C}_j}A_k\alpha^{-kt}\\ &= \tfrac{1}{N}\sum_{j\in\mathbb{Z}/N\mathbb{Z}}A_j\alpha^{-jt}\\ &= \tfrac{1}{N}\sum_{j=0}^{N-1}A_j\alpha^{-jt}\\ &= a_t\end{aligned}$$

Donc nous avons démontré le résultat recherché à savoir la représentation par la trace :

$$a_t=\frac{1}{N}\sum_{j\in I}\mathtt{Tr}^{n_j}(A_j\alpha^{-jt}).$$

□

**Corollaire 5.21.1.** *Soit $\underline{a}$ une séquence de période $N=p^{nr}-1$, alors la formule inverse est :*

$$\forall\, t\in\mathbb{N},\ a_t=-\sum_{j\in I}\mathtt{Tr}^{n_j}(A_j\alpha^{-jt})$$

*où $n_j=|C_j|=ord(j)$*

*Démonstration.* $p^{nr}-1=-1$ dans $\mathbb{F}_{p^n}$. Donc $-(p^{nr}-1)=1$ dans $\mathbb{F}_{p^n}$ alors $\frac{1}{p^{nr}-1}=-1$ dans $\mathbb{F}_{p^n}$. □

**Exemple 5.21.5.** *Considérons la séquence* $\underline{a}=(0100010)$ *de période 7. Soit* $\alpha$ *un élément primitif dans* $\mathbb{F}_{2^3}=\mathbb{F}_2[X]/(X^3+X+1)=\mathbb{F}_2[\alpha]$. *On a :*

$$\begin{array}{rcl}\underline{A} & = & (0,\alpha^6,\alpha^5,1,\alpha^3,1,)\\ \mathcal{C}_0 & = & \{0\}\\ \mathcal{C}_1 & = & \{1,2,4\}\\ \mathcal{C}_3 & = & \{3,6,5\}.\end{array}$$

*On utilise ici la formule d'inversion de la représentation par la trace :*

$$\begin{array}{rcl}a_t & = & \sum\limits_{j\in\{0,1,3\}} \mathtt{Tr}_2^{n_j}(A_j\alpha^{-jt})\\ & = & \mathtt{Tr}_2(A_0\alpha^0)+\mathtt{Tr}_2^3(A_1\alpha^{-t})+\mathtt{Tr}_2^3(A_3\alpha^{-3t})\\ & = & \mathtt{Tr}_2^3(\alpha^6\alpha^{-t})+\mathtt{Tr}_2^3(\alpha^{-3t})\\ & = & \mathtt{Tr}_2^3(\alpha^6\alpha^{6t})+\mathtt{Tr}_2^3((\alpha^6)^{3t})\ car\ \alpha^{-1}=\alpha^6\\ a_t & = & \mathtt{Tr}_2^3(\alpha^{2(3+3t)})+\mathtt{Tr}_2^3(\alpha^{18t})\end{array}$$

*Or*

$$\begin{array}{rcl}\mathtt{Tr}_2(\beta) & = & \beta+\beta^2+\cdots+\beta^{2^{n-1}}\ et\\ \mathtt{Tr}_2(\beta^2) & = & \beta^2+\beta^{2^2}+\cdots+\beta^{2^n}=\beta^2+\cdots+\beta^{2^{n-1}}+\beta=\mathtt{Tr}_2(\beta).\end{array}$$

$$\alpha^{18t}=\alpha^{(7\times2+4)t}=\alpha^{7\times2}\alpha^{4t}=\alpha^{4t}.$$

*La représentation par la trace est donc*

$$\begin{array}{rcl}a_t & = & \mathtt{Tr}_2^3(\alpha^{3+3t})+\mathtt{Tr}_2^3(\alpha^{4t})\\ a_t & = & \mathtt{Tr}_2^3(\alpha^{3+3t})+\mathtt{Tr}_2^3(\alpha^{t})\end{array}$$

Dans cette représentation par la trace, il est possible qu'un $A_j$ soit nul, donc nous allons considérer seulement les $A_j$ non-nuls car les autres n'apparaissent pas dans l'écriture. On pose

$$s=\mathtt{card}\,\{j\in I \text{ tel que } A_j\neq 0\}.$$

On a réordonne les $j$ tels que $A_j$ non-nuls. Le polynôme minimal sur $\mathbb{F}_{p^n}$ de $\alpha^{-r_j}$ est noté $q_j^*$. Pour faciliter la notation des $n_{r_j}$, on va poser $n_j=n_{r_j}$ avec $1\leq j\leq s$.

**Théorème 5.21.2.** *Le polynôme minimal de* $\underline{a}$ *est le produit* $q_1^*(X)q_2^*(X)\ldots q_s^*(X)$ *où* $q_j^*(X)$ *est le polynôme minimal de* $\alpha^{-r_j}$ *sur* $\mathbb{F}_{p^n}$ *pour tout* $1\leq j\leq s$.

*Démonstration.* D'après le théorème 5.21.1, on a :

$$\forall 0\leq t\leq N-1, a_t=\frac{1}{N}\sum_{j\in I}\mathtt{Tr}_{p^n}^{n_j}(A_j\alpha^{-jt})=\frac{1}{N}\sum_{j\in I;A_j\neq 0}\mathtt{Tr}_{p^n}^{n_j}(A_j\alpha^{-jt})$$

On pose $f(X) = q_1^*(X)q_2^*(X)\cdots q_s^*(X)$.

$$\begin{aligned}
q^*(L)(\underline{a}) &= q_1^*(L)q_2^*(L)\cdots q_s^*(L)(\underline{a}) \\
&= q_1^*(L)q_2^*(L)\cdots q_{s-1}^*(L)(q_s^*(L)(\underline{a})) \\
&= q_1^*(L)q_2^*(L)\cdots q_{s-1}^*(L)(q_s^*(L)(\tfrac{1}{N}\sum_{j\in I; A_j\neq 0} \mathtt{Tr}_{p^n}^{n_j}(A_j\alpha^{-jt}))_{t\in\mathbb{N}}) \\
&= q_1^*(L)q_2^*(L)\cdots q_{s-1}^*(L)(q_s^*(L)(\tfrac{1}{N}\sum_{j=1}^{s} \mathtt{Tr}_{p^n}^{n_j}(A_{r_j}\alpha^{-r_jt}))_{t\in\mathbb{N}}) \\
&= \tfrac{1}{N}\sum_{j=1}^{s} q_1^*(L)\ldots q_{j-1}^*(L)q_{j+1}^*(L)\ldots q_s^*(L)(q_j^*(L)(\mathtt{Tr}_{p^n}^{n_j}(A_{r_j}\alpha^{-r_jt}))_{t\in\mathbb{N}}) \\
&= \tfrac{1}{N}\sum_{j=1}^{s} q_1^*(L)\ldots q_{j-1}^*(L)q_{j+1}^*(L)\ldots q_s^*(L)(\mathtt{Tr}_{p^n}^{n_j}(A_{r_j}q_j^*(\alpha^{-r_jt})))_{t\in\mathbb{N}} \\
&= \tfrac{1}{N}\sum_{j=1}^{s} q_1^*(L)\ldots q_{j-1}^*(L)q_{j+1}^*(L)\ldots q_s^*(L)(\mathtt{Tr}_{p^n}^{n_j}(A_{r_j}0))_{t\in\mathbb{N}} \\
&= \tfrac{1}{N}\sum_{j=1}^{s} q_1^*(L)\ldots q_{j-1}^*(L)q_{j+1}^*(L)\ldots q_s^*(L)(\underline{0}) \\
q^*(L)(\underline{a}) &= 0
\end{aligned}$$

Donc $q^*$ est un polynôme caractéristique de $\mathcal{L}$.
Grâce à la représentation par la trace, $\underline{a}$ s'écrit comme somme de sous-séquences :

$$\underline{a} = (a_t)_{t\in\mathbb{N}} = (\frac{1}{N}\sum_{j=1}^{s} \mathtt{Tr}_{p^n}^{n_j}(A_{r_j}\alpha^{-r_jt}))_{t\in\mathbb{N}} = \sum_{j=1}^{s}(\frac{1}{N}\mathtt{Tr}_{p^n}^{n_j}(A_{r_j}\alpha^{-r_jt}))_{t\in\mathbb{N}}$$

.

La séquence $(\frac{1}{N}\mathtt{Tr}_{p^n}^{n_j}(A_{r_j}\alpha^{-r_jt}))_{t\in\mathbb{N}}$ a pour polynôme minimal $q_j^*$. En effet, $q_j^*$ est polynôme minimal de $\alpha^{-r_j}$, donc $q_j^*$ est irréductible sur $\mathbb{F}_{p^n}$ . D'après le corollaire 5.12.2, $q_j^*$ est le polynôme minimal de cette séquence. $q^*$ est polynôme caractéristique, donc $m_{\underline{a}}^*$ le polynôme minimal de $\underline{a}$ divise $q^*$. Supposons qu'il soit différent de $q^*$, alors il existe $k$ tel que $m^*$ divise $q_1^*\ldots q_{k-1}^*q_{k+1}^*\ldots q_s^*$. Dans ce cas

$$m^*(L)(\underline{a}) = m^*(L)(\frac{1}{N}\mathtt{Tr}_{p^n}^{n_j}(A_{r_j}\alpha^{-r_jt}))_{t\in\mathbb{N}} \neq \underline{0}.$$

Donc $q^*$ est le polynôme minimal de $\underline{a}$. □

**Application 5.21.1** (Calcul du polynôme minimal). *On se place sur $\mathbb{F}_2$. Soit la séquence $\underline{a} = (111011000101001)$ de période 15. Soit $\alpha$ un élément primitif de $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4+X+1)$, il est donc d'ordre 15 et $\alpha^4 = \alpha+1$. On cherche à appliquer le théorème précédent pour calculer le polynôme minimal de $\underline{a}$. Les sous-ensembles cyclotomique d'ordre 15 sont :*

$$\begin{aligned}
\mathcal{C}_0 &= \{0\} \\
\mathcal{C}_1 &= \{1,2,4,8\} \\
\mathcal{C}_3 &= \{3,6,12,9\} \\
\mathcal{C}_5 &= \{5,10\} \\
\mathcal{C}_7 &= \{7,14,13,11\}\,.
\end{aligned}$$

*Grâce à la formule du théorème 5.21.1, on trouve :*

$$\begin{aligned} a_t &= \tfrac{1}{N}\sum_{j\in I} \mathtt{Tr}_2^{n_j}(A_j\alpha^{-jt}) \\ &= \sum_{j\in\{0,1,3,5,7\}} \mathtt{Tr}_2^{n_j}(A_j\alpha^{-jt}) \\ &= \mathtt{Tr}(0) + \mathtt{Tr}(\alpha^{-t}) + \mathtt{Tr}(\alpha^{1-3t}) + \mathtt{Tr}(\alpha^{6-7t}) \\ &= \mathtt{Tr}(\alpha^{-t}) + \mathtt{Tr}(\alpha^{1-3t}) + \mathtt{Tr}(\alpha^{6-7t}). \end{aligned}$$

*Cherchons les polynômes minimaux de* $\alpha^{-r_j} \in \{\alpha^{-1}, \alpha^{-3}, \alpha^{-7}\}$. *Nous avons les extensions de corps suivantes :*

$$\mathbb{F}_2 \subseteq \mathbb{F}_2[\alpha^{-r_j}] \subseteq \mathbb{F}_2[\alpha]$$

*Par le théorème de la base téléscopique, on a :*

$$\big[\mathbb{F}_2[\alpha^{-r_j}] : \mathbb{F}_2\big] \times \big[\mathbb{F}_2[\alpha] : \mathbb{F}_2[\alpha^{-r_j}]\big] = [\mathbb{F}_2[\alpha] : \mathbb{F}_2]$$

*Donc l'extension* $\mathbb{F}_2 \subseteq \mathbb{F}_2[\alpha^{-r_j}]$ *est de degré divisant 4, c'est à dire 1, 2 ou 4. Donc le polynôme minimal de* $\alpha^{-r_j}$ *est de degré 1, 2 ou 4. Il ne peut pas être de degré 1 car* $\alpha^{-r_j}$ *n'appartient pas à* $\mathbb{F}_2$. *Il ne peut être de degré 2, en effet le seul polynôme irréductible de degré 2 sur* $\mathbb{F}_2$ *est* $X^2+X+1$. *Or si* $\alpha^{-2}+\alpha^{-1}+1=0$ *alors on a :*

$$\begin{aligned} \alpha^{-2}+\alpha^{-1}+1=0 &\Rightarrow \alpha^2\alpha^{-2}+\alpha^2\alpha^{-1}+\alpha^2=0 \\ &\Rightarrow \quad 1+\alpha+\alpha^2=0. \end{aligned}$$

*Or le polynôme minimal de* $\alpha$ *est* $X^4+X+1$, *donc c'est absurde. On en conclut que le polynôme minimal de* $\alpha^{-1}$ *est de degré 4. Par le même raisonnement, on trouve que le polynôme de* $\alpha^{-3}$ *et celui de* $\alpha^{-7}$ *sont aussi de degré 4. On trouve de même que :*

$$\begin{aligned} (\alpha^{-1})^4+(\alpha^{-1})^3+1 &= 0 \\ (\alpha^{-3})^4+(\alpha^{-3})^3+(\alpha^{-3})^2+\alpha^{-3}+1 &= 0 \\ (\alpha^{-7})^4+\alpha^{-7}+1 &= 0 \end{aligned}$$

*Donc les polynômes minimaux sont* $X^4+X+1$, $X^4+X^3+X^2+X+1$ *et* $X^4+X+1$. *D'après le théorème 5.21.2, le polynôme minimal de* $\underline{a}$ *est*

$$(X^4+X+1)(X^4+X^3+X^2+X+1)(X^4+X+1).$$

### 5.21.3 Détermination de la complexité linéaire par la méthode spectrale

Dans la sous-section précédente, nous avons étudié une autre représentation par la trace d'une séquence périodique quelconque à l'aide de sa séquence spectrale, puis cette représentation nous a permis de décomposer la séquence périodique en plusieurs sous-séquences. Cette décomposition facilite le calcul du polynôme minimal de la séquence périodique en sachant que ce polynôme est le produit des polynômes minimaux des sous-séquences spectrales.

Dans cette section, nous donnons une méthode très simple qui permet de calculer la complexité linéaire (*linear complexity*) d'une séquence périodique.

**Définition 5.21.4** (Poids de Hamming). *Soit $\underline{b} = \{b_t\}_{t\in\mathbb{N}}$ une séquence sur $\mathbb{F}_{p^n}$ de période $R$, alors le poids de Hamming de $\underline{b}$, noté $w(\underline{b})$ est défini par*

$$w(\underline{b}) = \mathtt{card}\,\{t; b_t \neq 0, 0 \leq t < R\}\,.$$

*C'est le nombre de bits non-nuls de la séquence spectrale dans une seule période.*

**Théorème 5.21.3.** *Soit $\underline{a} = (a_i)_{i\in\mathbb{N}}$ une séquence sur $\mathbb{F}_{p^n}$ de période $N$ où $N$ divise $p^{nr}-1$ pour un certain entier naturel $r$. Soit $\underline{A} = (A_i)_{i\in\mathbb{N}}$ sa séquence spectrale. Alors la complexité linéaire de $\underline{a}$ est donnée par le poids de Hamming de $\underline{A}$.*

$$LS(\underline{a}) = w(\underline{A}).$$

*Démonstration.* Par définition, la complexité linéaire $LS(\underline{a})$ est le degré du polynôme minimal de $\underline{a}$ sur $\mathbb{F}_{p^n}$. Or d'après le théorème 5.21.1, on a :

$$a_t = \frac{1}{N}\sum_{j\in I; A_j\neq 0} \mathtt{Tr}(A_j\alpha^{-jt})$$

D'après le théorème 5.21.2, on a vu que : $m^*_{\underline{a}}$ le polynôme minimal de $\underline{a}$ est le produit des polynômes minimaux $q^*_j$ des sous-séquences $\frac{1}{N}\mathtt{Tr}(A_j\alpha^{-jt})_{t\in\mathbb{N}}$ qui sont en fait respectivement les polynômes minimaux des $\alpha^{-j}$ sur $\mathbb{F}_{p^n}$. Donc :

$$LS(\underline{a}) = \deg(m^*_{\underline{a}}) = \sum_{j=1}^{s}\deg(q^*_j)$$

Or

$$\begin{aligned} n_j &= \inf_{n\in\mathbb{N}}\{n\in\mathbb{N} \text{ tel que } jp^{nn_j} \equiv j \bmod N\} \\ &= \inf_{n\in\mathbb{N}}\left\{n\in\mathbb{N} \text{ tel que } \alpha^{jp^{nn_j}} = \alpha^j\right\}. \end{aligned}$$

$\alpha$ étant dans $\mathbb{F}_{p^{nr}}$, alors le polynôme minimal de $\alpha^j$ a pour racines tous les conjugués de $\alpha^j$ dans $\mathbb{F}_{p^{nr}}$.

$$q^*_j = \prod_{i=0}^{n_j-1}(X - (\alpha^j)^{p^{ni}}) \text{ et } \deg(m^*_{\underline{a}}) = \sum_{j=1}^{s} n_j.$$

D'autre part, $n_j$ est le cardinal du sous-ensemble cyclotomique modulo $N$, $C_{r_j}$. En utilisant le lemme 5.21.3, on obtient :

$$\begin{aligned} w(\underline{A}) &= \mathtt{card}\,\{0\leq j\leq N-1; A_j\neq 0\} = \mathtt{card}\bigcup_{j=1}^{j=s}\left\{A_k \text{ tel que } k\in\mathcal{C}_{r_j}\right\} \\ &= \sum_{j=1}^{s}\mathtt{card}\left\{A_{r_j}, A_{r_jp^n}, \ldots, A_{r_jp^{n(n_j-1)}}\right\} = \sum_{j=1}^{s} n_j = LS(\underline{a}). \end{aligned}$$

□

**Exemple 5.21.6.** *On considère sur* $\mathbb{F}_2$ *une séquence* $\underline{a}$ *de période* $2^5 - 1 = 31$.

$$\underline{a} = (11000101011111101010000010010011).$$

*Les sous-ensembles cyclotomiques modulo 31 sont :*

$$\begin{array}{rcl} \mathcal{C}_0 & = & \{0\} \\ \mathcal{C}_1 & = & \{1,2,4,8,16\} \\ \mathcal{C}_3 & = & \{3,6,12,24,16,17\} \\ \mathcal{C}_5 & = & \{5,10,20,9,18\} \\ \mathcal{C}_7 & = & \{7,14,28,25,19\} \\ \mathcal{C}_{11} & = & \{11,22,13,26,21\} \\ \mathcal{C}_{15} & = & \{15,30,29,27,23\} \end{array}$$

*Soit* $\alpha$ *un élément primitif du corps* $\mathbb{F}_2[X]/(X^5 + X^3 + 1)$. *La séquence spectrale* $\underline{A}$ *se calcule grâce à* $A_0$, $A_1$, $A_3$, $A_5$, $A_7$, $A_{11}$ *et* $A_{15}$ *et grâce à la propriété de conjugaison de la séquence spectrale.*

$$\begin{array}{rcl} A_0 = A_3 = A_{11} = A_{15} = 0 \\ A_1 = \alpha^{25} \\ A_5 = A_7 = 1 \end{array} .$$

*Donc* $w(\underline{A}) = 15$, *on en déduit que* $LS(\underline{a}) = 15$. *Inversement* $w(\underline{a}) = 16$, *donc* $LS(\underline{A}) = 16$.

Grâce à cette formule reliant le poids de Hamming de la séquence spectrale à la complexité linéaire de la séquence d'origine, on peut calculer rapidement le degré du polynôme minimal. L'algorithme de Berlekamp-Massey permet lui de calculer directement le polynôme minimal. Pour plus de détails, nous renvoyons le lecteur à [1] page 109 et à [40] page 395.

## 5.22 Inter-corrélation et Séquences de Gold

### 5.22.1 Inter-corrélation

Dans cette sous-section, nous rappelons la définition de l'inter-corrélation entre deux séquences binaires de période $2^r - 1$. Posons $N = 2^r - 1$ et considérons $\alpha$ un élémentprimitif de $\mathbb{F}_{p^r}$.

**Définition 5.22.1** (Inter-corrélation ou cross-correlation)**.** *Soient deux séquences binaires de période* $N$. *L'inter-corrélation entre* $\underline{a}$ *et* $\underline{b}$ *est la fonction définie sur* $\{0,1,\ldots,N-1\}$ *à valeurs dans* $\mathbb{Z}$ *qui à un* $\tau$ *associe*

$$\mathcal{C}_{\underline{a},\underline{b}}(\tau) = \sum_{i=0}^{i=N-1} (-1)^{a_i + b_{i+\tau}}.$$

L'auto-corrélation n'est autre que l'intercorrélation $\mathcal{C}_{\underline{a},\underline{a}}$.

**Lemme 5.22.1.** *Pour tout* $0 \leq k \leq N-1$, *on a :*

$$\mathcal{C}_{L^k(\underline{a}),L^k(\underline{b})}(\tau) = \mathcal{C}_{\underline{a},\underline{b}}(\tau).$$

*Pour tout couple* $0 \leq k, j \leq N-1$, *on a :*

$$\mathcal{C}_{L^k(\underline{a}),L^j(\underline{b})}(\tau) = \mathcal{C}_{\underline{a},\underline{b}}((\tau+j-k)(\mathtt{mod}N)).$$

*Démonstration.*

$$\begin{aligned}
\mathcal{C}_{L^k(\underline{a}),L^k(\underline{b})}(\tau) &= \sum_{i=0}^{i=N-1} (-1)^{a_{i+k}+b_{i+k+\tau}} \\
&= \sum_{i=k}^{i=N+k-1} (-1)^{a_i+b_{i+\tau}} \\
&= \sum_{i=k}^{i=N-1} (-1)^{a_i+b_{i+\tau}} + \sum_{i=N}^{i=N+k-1} (-1)^{a_i+b_{i+\tau}} \\
&= \sum_{i=k}^{i=N-1} (-1)^{a_i+b_{i+\tau}} + \sum_{i=0}^{i=k-1} (-1)^{a_{i+N}+b_{i+N+\tau}} \\
&= \sum_{i=k}^{i=N-1} (-1)^{a_i+b_{i+\tau}} + \sum_{i=0}^{i=k-1} (-1)^{a_i+b_{i+tau}}.
\end{aligned}$$

$$\begin{aligned}
\mathcal{C}_{L^k(\underline{a}),L^j(\underline{b})}(\tau) &= \sum_{i=0}^{i=N-1} (-1)^{a_{i+k}+b_{i+j+\tau}} \\
&= \sum_{i=0}^{i=N-1} (-1)^{a_{i+k}+b_{i+k+\tau+j-k}} \\
&= \sum_{i=0}^{i=N-1} (-1)^{a_{i+k}+b_{i+k+(\tau+j-k) \mod N}} \\
&= \mathcal{C}_{L^k(\underline{a}),L^k(\underline{b})}((\tau+j-k)(\mathtt{mod}N)) \\
&= \mathcal{C}_{\underline{a},\underline{b}}((\tau+j-k)(\mathtt{mod}N)).
\end{aligned}$$

□

**Proposition 5.22.1.** *Pour toute séquence binaire de période* $N$, *il existe une unique fonction* $f$ *définie sur* $\mathbb{F}_{2^r}$ *dans* $\mathbb{F}_2$ *par :*

$$f(x) = \sum_{j \in I} \mathtt{Tr}_2^{n_j}(\beta_j x^j) \text{ avec } \beta_j \in \mathbb{F}_{2^{n_j}},$$

*telle que*

$$\underline{a} = (f(1), f(\alpha), f(\alpha^2), \ldots).$$

*Démonstration.* C'est une conséquence directe du théorème 5.21.1. □

**Définition 5.22.2.** *Dans la suite, nous notons,* $f$ *cette unique fonction associée à* $\underline{a}$ *et* $g$ *l'unique fonction associée à* $\underline{b}$. *Notons pour tout couple* $(f,g)$ *la fonction suivante*

$$\forall\, y \in \mathbb{F}_2,\ \Delta_{f,g}(y) = \sum_{x \in \mathbb{F}_{2^r}} (-1)^{f(x)+g(xy)}.$$

**Lemme 5.22.2.** *Si $f(0) = g(0) = 0$, alors*

$$\Delta_{f,g}(\alpha^\tau) = \mathcal{C}_{\underline{a},\underline{b}}(\tau) + 1.$$

*Démonstration.*

$$\begin{aligned}
\mathcal{C}_{\underline{a},\underline{b}}(\tau) &= \sum_{i=0}^{i=N-1} (-1)^{a_i + b_{i+\tau}} \\
&= \sum_{i=0}^{i=2^r-2} (-1)^{f(\alpha^i) + g(\alpha^{i+\tau})} \\
&= \sum_{i=0}^{i=2^r-2} (-1)^{f(\alpha^i) + g(\alpha^i \alpha^\tau)} \\
&= \sum_{x \in \mathbb{F}_{2^r}} (-1)^{f(x) + g(x\alpha^\tau)} - (-1)^{f(0)+g(0)} \\
&= \Delta_{f,g}(\alpha^\tau) - 1.
\end{aligned}$$

□

### 5.22.2 Paire de Séquences de Gold

Dans cette sous-section, nous introduisons les paires de séquences de Gold. C'est une famille de séquences ayant une inter-corrélation de niveaux 3. Les familles de séquences ayant de bonnes propriétés d'inter-corrélation ont d'importantes applications au CDMA (code design multiple access). Les paires de séquences de Gold ont été introduites par Gold en 1967.

#### Construction des Gold-pair séquences

Considérons $\underline{a}$ et $\underline{b}$ deux $m$-séquences de période $N = 2^r - 1$. D'après la proposition 5.19.1, $\underline{b}$ est un décalage d'une décimation de $\underline{a}$. C'est même une décimation dite première, c'est-à-dire que le degré de décimation est premier avec $N$. Ceci se déduit du corollaire 5.19.1. D'après le théorème 5.16.1, il existe $\alpha$ un élément primitif de $\mathbb{F}_{2^r}$ et un élément $\beta \neq 0$ tels que

$$a_i = \mathtt{Tr}(\beta \alpha^i).$$

Donc il existe $s$ et $\tau$ tels que $b_i = \mathtt{Tr}(\beta \alpha^{s\tau} \alpha^{si})$. De plus, d'après le théorème 5.14.2, les polynômes minimaux $m^*_{\underline{a}}$ et $m^*_{\underline{b}}$ de ces deux séquences sont primitifs. Ils sont aussi les polynômes minimaux de $\alpha$ et $\alpha^s$, donc irréductibles. Comme $s$ est premier avec $N$ l'ordre de $\alpha$, alors $\alpha$ et $\alpha^s$ ne sont pas conjugués et leur polynômes minimaux sont distincts. Posons $h(X) = m^*_{\underline{a}}(X) m^*_{\underline{b}}(X)$. D'après le théorème 5.14.3,

$$G^*(h) = G^*(m^*_{\underline{a}}) \oplus G^*(m^*_{\underline{b}}).$$

**Définition 5.22.3** (Gold-pair séquences)**.** *Si $r$ est impair et si $s$ est de la forme $2^k + 1$ avec $k$ et $r$ premiers entre eux, alors les séquences de $G^*(h)$ sont appelées les Gold-pair séquences.*

### 5.22.3 Méthode quadratique de Welch

Nous calculons l'inter-corrélation des Gold-pair séquences par la méthode de Welch. D'après le théorème 5.16.1, on peut décrire les ensembles $G^*(m^*_{\underline{a}})$ et $G^*(m^*_{\underline{b}})$ de la manière suivante

$$G^*(m^*_{\underline{a}}) = \left\{(\mathtt{Tr}(\beta\alpha^i))_i \text{ telle que } \beta \in \mathbb{F}_{2^r}\right\} \text{ et}$$
$$G^*(m^*_{\underline{b}}) = \left\{(\mathtt{Tr}(\beta\alpha^{s\tau}\alpha^{si}))_i \text{ telle que } \beta \in \mathbb{F}_{2^r}\right\}.$$

Ces deux ensembles peuvent aussi se décrire par les décalages de tout $\underline{a}$ et de tout $\underline{b}$ par le corollaire 5.14.1. On choisit $\beta = 1$ et on a $\underline{a} = (\mathtt{Tr}(\alpha^i))_{i\in\mathbb{N}}$ et on choisit le décalage $N - \tau$ de $\underline{b}$, on a alors $\underline{b} = (\mathtt{Tr}(\alpha^{si}))_{i\in\mathbb{N}}$. On en déduit que pour toute paire $(\underline{c}, \underline{d})$ de séquence de $G^*(h)$, il existe $k$ et $j$, tels que :

$$\underline{c} = L^k(\underline{a}) \text{ et } \underline{d} = L^j(\underline{b}).$$

Le calcul de l'inter-corrélation de toute paire de séquences de Gold dans $G^*(h)$ se déduit donc du calcul de l'inter-corrélation entre $\underline{a}$ et $\underline{b}$. En effet, d'après le lemme 5.22.1 :

$$\mathcal{C}_{\underline{c},\underline{d}}(\tau) = \mathcal{C}_{L^k(\underline{a}),L^j(\underline{b})}(\tau) = \mathcal{C}_{\underline{a},\underline{b}}(\tau + j - k).$$

Pour ce choix de $\underline{a}$ et $\underline{b}$, les fonctions $f$ et $g$ sont définies par $f(x) = \mathtt{Tr}(x)$ et $g(x) = \mathtt{Tr}(x^s)$.

**Lemme 5.22.3.** *Dans ces hypothèses, on a :*

$$\forall\, y \in \mathbb{F}_{2^r},\ \Delta_{g,f}(y) = \begin{cases} 0 & \Leftrightarrow \quad \mathtt{Tr}(y) = 0 \\ \pm 2^{\frac{r+1}{2}} & \Leftrightarrow \quad \mathtt{Tr}(y) = 1 \end{cases}$$

*Démonstration.*

$$\begin{aligned}
\Delta_{g,f}(y) &= \sum_{x\in\mathbb{F}_{2^r}} (-1)^{g(x)+f(xy)} \\
&= \sum_{x\in\mathbb{F}_{2^r}} (-1)^{\mathtt{Tr}(x^s)+\mathtt{Tr}(xy)} \\
(\Delta_{g,f}(y))^2 &= \sum_{x\in\mathbb{F}_{2^r}} (-1)^{\mathtt{Tr}(x^s)+\mathtt{Tr}(xy)} \sum_{z\in\mathbb{F}_{2^r}} (-1)^{\mathtt{Tr}(z^s)+\mathtt{Tr}(zy)} \\
&= \sum_{x,z\in\mathbb{F}_{2^r}} (-1)^{\mathtt{Tr}(x^s)+\mathtt{Tr}(z^s)+\mathtt{Tr}((x+z)y)} \\
&= \sum_{x,z\in\mathbb{F}_{2^r}} (-1)^{\mathtt{Tr}(x^s)+\mathtt{Tr}((w+x)^s)+\mathtt{Tr}(wy)} \text{ avec } w = x + z
\end{aligned}$$

$$\begin{aligned}
(w+x)^s &= (w+x)^{2^k+1} = (w+x)^{2^k}(w+x) = (w^{2^k} + x^{2^k})(w+x) \\
&= w^{2^k+1} + w^{2^k}x + x^{2^k}w + x^{2^k+1} = w^s + x^s + w^{2^k}x + x^{2^k}w.
\end{aligned}$$

$$\begin{aligned}
\mathtt{Tr}(x^s) + \mathtt{Tr}((w+x)^s) + \mathtt{Tr}(wy) &= \mathtt{Tr}(x^s) + \mathtt{Tr}(w^s) + \mathtt{Tr}(x^s) + \mathtt{Tr}(w^{2^k}x) + \mathtt{Tr}(x^{2^k}w) + \mathtt{Tr}(wy) \\
&= \mathtt{Tr}(w^s) + \mathtt{Tr}(w^{2^k}x) + \mathtt{Tr}(x^{2^k}w) + \mathtt{Tr}(wy).
\end{aligned}$$

$$(wx^{2^k})^{2^{-k}} = w^{2^{-k}}x^{2^k 2^{-k}} = w^{2^{-k}}x.$$

Donc ces deux éléments sont conjugués, leur trace est donc identique.

$$\mathtt{Tr}(wx^{2^k}) = \mathtt{Tr}(w^{2^{-k}}x).$$

$$\begin{aligned}(\Delta_{g,f}(y))^2 &= \sum_{x,w\in\mathbb{F}_{2^r}} (-1)^{\mathtt{Tr}(w^s)+\mathtt{Tr}(w^{2^k}x)+\mathtt{Tr}(w^{2^{-k}}x)+\mathtt{Tr}(wy)} \\ &= \sum_{x,w\in\mathbb{F}_{2^r}} (-1)^{\mathtt{Tr}(w^s)+\mathtt{Tr}((w^{2^k}+w^{2^{-k}})x)+\mathtt{Tr}(wy)} \\ &= \sum_{w\in\mathbb{F}_{2^r}} (-1)^{h(w)} \sum_{x\in\mathbb{F}_{2^r}} (-1)^{\mathtt{Tr}((w^{2^k}+w^{2^{-k}})x)},\end{aligned}$$

en posant $h(x) = \mathtt{Tr}(xy) + \mathtt{Tr}(x^s)$.
La trace de $w^{2^k} + w^{2^{-k}}$ prend deux valeurs possibles : 0 ou 1. On note l'ensemble

$$\Omega = \left\{ w \in \mathbb{F}_{2^r} \text{ tel que } w^{2^k} + w^{2^{-k}} = 0 \right\}.$$

$$\begin{aligned}(\Delta_{g,f}(y))^2 &= \sum_{w\in\Omega} (-1)^{h(w)} \sum_{x\in\mathbb{F}_{2^r}} (-1)^{\mathtt{Tr}(0.x)} + \sum_{w\in\Omega^c} (-1)^{h(w)} \sum_{x\in\mathbb{F}_{2^r}} (-1)^{\mathtt{Tr}(x)} \\ &= \sum_{w\in\Omega} (-1)^{h(w)} \sum_{x\in\mathbb{F}_{2^r}} 1 + \sum_{w\in\Omega^c} (-1)^{h(w)} (2^{n-1} - 2^{n-1}) \\ &= 2^r \sum_{w\in\Omega} (-1)^{h(w)}.\end{aligned}$$

$$\begin{aligned}w \in \Omega &\Leftrightarrow w^{2^{-k}} + w^{2^k} = 0 \Leftrightarrow w^{2^{-k}} = w^{2^k} \Rightarrow (w^{2^{-k}})^{2^k} = (w^{2^k})^{2^k} \\ &\Rightarrow w^{2^{2k}} = w \Rightarrow \mathtt{ord}(w) / 2^{2k} - 1 \\ w \in \mathbb{F}_{2^r} &\Rightarrow w^{2^r-1} = 1 \Rightarrow \mathtt{ord}(w) / 2^r - 1.\end{aligned}$$

On en conclut que $\mathtt{ord}(w)$ divise $\mathtt{PGCD}(2^{2k} - 1, 2^r - 1)$. Calculons ce PGCD. Les entiers $k$ et $r$ sont premiers entre eux et $r$ est impaire, donc $2k$ et $r$ sont premiers entre eux. Le PGCD de $2^{2k} - 1$ et de $2^r - 1$ est $2^{\mathtt{PGCD}(2k,r)} - 1$. En effet, la division euclidienne de $2k$ par $r$ donne après un certain nombre d'itération le $\mathtt{PGCD}(2k, r)$. Or

$$2k = ur + v \text{ avec } 0 \leq v < r.$$

$$2^{2k} - 1 = 2^v(2^r - 1)(2^{r(u-1)} + \ldots + 1) + 2^v - 1.$$

On trouve que $0 \leq 2^v - 1 < 2^r - 1$ donc c'est le reste de la division euclidienne de $2^{2k} - 1$ par $2^r - 1$. Par le même nombre d'itération, on trouve

$$2^{\mathtt{PGCD}(2k,r)} - 1 = \mathtt{PGCD}(2^{2k} - 1, 2^r - 1).$$

Donc $\mathtt{ord}(w)$ divise 1 et $w = 1$. Autrement dit, il existe deux cas $w = 0, 1$.

$$\begin{aligned}(\Delta_{g,f}(y))^2 &= 2^r((-1)^{h(0)} + (-1)^{h(1)}) \\ &= 2^r(1 + (-1)^{\mathtt{Tr}(y)+1})\end{aligned}$$

Si $\mathtt{Tr}(y) = 0$, alors $(\Delta_{g,f}(y))^2 = 0$ et si $\mathtt{Tr}(y) = 1$, alors $(\Delta_{g,f}(y))^2 = 2^{r+1}$ ce qui achève la démonstration. □

**Théorème 5.22.1** (Théorème de Gold). *L'inter-corrélation entre une paire de séquences de Gold est de niveau 3. Elle prend les valeurs* $-1, -1 \pm 2^{\frac{r+1}{2}}$.

*Démonstration.* Soit $(\underline{c}, \underline{d})$ une paire de séquences de Gold quelconque

$$\mathcal{C}_{\underline{c},\underline{d}}(\tau) = \mathcal{C}_{\underline{a},\underline{b}}(\tau + j - k) = \mathcal{C}_{\underline{b},\underline{a}}(-(\tau + j - k)).$$

On vérifie que $f(0) = g(0) = \mathtt{Tr}(0) = 0$, et d'après le lemme 5.22.2,

$$\mathcal{C}_{\underline{c},\underline{d}}(\tau) = \Delta_{g,f}(\alpha^{-(\tau+j-k)}) - 1.$$

□

## 5.23 LFSR en mode Galois

Le mode Galois est une nouvelle représentation des Feedback Shift Registers développée par Goresky et Klapper [22]. Elle présente un avantage dans les applications hardware puisque toutes les cellules sont mises à jour simultanément. Dans cette section, nous présentons ce mode Galois ainsi que les propriétés basiques des LFSRs séquences en mode Galois.

### 5.23.1 Définitions et Conceptions

**Définition 5.23.1** (LFSR en mode Galois). *Un Linear Feedback Shift Register en mode Galois sur* $\mathbb{F}_{p^n}$ *de taille* $r$ *et de coefficients de connexion* $(q_1, \ldots, q_r) \in (\mathbb{F}_{p^n})^r$ *est un automate ou générateur de séquence dont les états sont de la forme suivante*

$$s(t) = (a_0(t), \ldots, a_{r-1}(t)) \in (\mathbb{F}_{p^n})^r.$$

*et dont l'opération de changement d'état est définie comme suit : Calculons*

$$a_i(t+1) = q_{i+1}a_0(t) + a_{i+1}(t) \text{ et } a_{r-1}(t+1) = q_r a_0(t).$$

*L'addition et la multiplication se font dans le corps fini* $\mathbb{F}_{p^n}$. *La fonction de retour est* $f(a_0(t), \ldots, a_{r-1}(t)) = (a_0(t+1), \ldots, a_{r-1}(t+1))$ *et la fonction de sorties est* $g(x_0, \ldots, x_{r-1}) = x_0$. *On répète ce procédé à l'infini. Le LFSR génère la séquence infinie*

$$(g(s(0)), g(f(s(0))), g(f^2(s(0))), \ldots) = (a_0(0), a_0(1), a_0(2), \ldots)$$

*appelée séquence de sorties. L'état* $s(0)$ *est appelé l'état initial de la séquence de sorties,* $r$ *la taille du LFSR,* $q_1, \ldots, q_r$ *les coefficients de connexion du LFSR.*

La figure 5.9 représente un LFSR en mode Galois. On peut aussi retenir en sortie toutes les cellules. À chaque cellule correspondra une séquence de sortie

$$\underline{a_i} = (a_i(0), a_i(1), \ldots, a_i(t), \ldots).$$

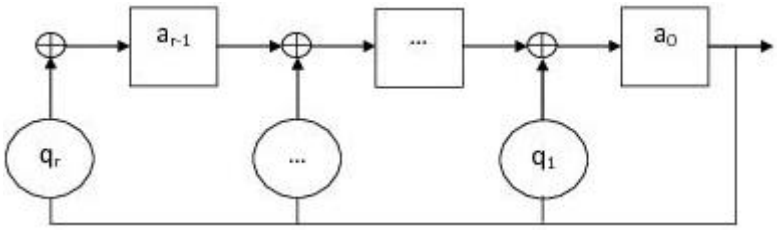



FIGURE 5.9 – Mode Galois des registres à décalage et à rétroaction linéaire.

Les sorties du LFSR peuvent être représentées par un seul élément : Considérons la séquence vectorielle de dimension $r$ sur $(\mathbb{F}_{p^n})^{\mathbb{N}}$ définie par

$$\underline{a} = (\underline{a}_0, \ldots, \underline{a}_{r-1}) \in ((\mathbb{F}_{p^n})^{\mathbb{N}})^r.$$

Nous utilisons pour l'analyse la représentation matricielle différente de la méthode de Goresky et Klapper.

### 5.23.2 Analyse et Représentation matricielle

À toute séquence de sorties $\underline{a}_i$, on associe sa fonction génératrice définie par la série formelle dans $\mathbb{F}_{p^n}[[X]]$ :

$$a_i(X) = \sum_{t=0}^{t=+\infty} a_i(t)X^t.$$

La séquence vectorielle $\underline{a}$ est donc associée au vecteur de dimension $r$ sur $\mathbb{F}_{p^n}[[X]]$ donné par

$$a(X) = (a_0(X), \ldots, a_{r-1}(X)) \in (\mathbb{F}_{p^n}[[X]])^r.$$

Le vecteur de série formelle de dimension $r$ sur $\mathbb{F}_{p^n}$ peut être vue comme une série formelle de vecteur de dimension $r$ sur $\mathbb{F}_{p^n}$. En effet :

$$\begin{aligned} a(X) &= \Big(\sum_{t=0}^{t=+\infty} a_0(t)X^t, \ldots, \sum_{t=0}^{t=+\infty} a_{r-1}(t)X^t\Big) \\ &= \sum_{t=0}^{t=+\infty} (a_0(t), \ldots, a_{r-1}(t))X^t \\ &= \sum_{t=0}^{t=+\infty} s(t)X^t \in (\mathbb{F}_{p^n})^r[[X]]. \end{aligned}$$

Nous définissons une matrice particulière. Le changement d'états peut se traduire par une multiplication matricielle suivante :

$$(a_0(t+1), a_1(t+1), \ldots, a_{r-1}(t+1)) = (a_0(t), a_1(t), \ldots, a_{r-1}(t)) \begin{pmatrix} q_1 & q_2 & \cdots & q_r \\ & & & 0 \\ & I_{r-1} & & \vdots \\ & & & 0 \end{pmatrix}$$

**Définition 5.23.2** (Matrice compagnon). *La matrice* $M = \begin{pmatrix} q_1 & q_2 & \dots & q_r \\ & & & 0 \\ & I_{r-1} & & \vdots \\ & & & 0 \end{pmatrix}$ *s'appelle la matrice compagnon du LFSR en mode Galois.*

$M$ est une matrice dans $\mathcal{M}_r(\mathbb{F}_{p^n})$. Elle caractérise non seulement le LFSR mais en plus elle détermine le mode. En effet, en mode Fibonacci la matrice est d'une autre forme. La taille de la matrice définie la taille du registre. Les coefficients de la matrice détermine les connexions du registre et la forme donne le mode. On verra par la suite que la représentation matricielle est la plus adéquate pour représenter un registre. Donc un LFSR en mode Galois peut être définie par le couple $(\mathbb{F}_{p^n}, M)$

**Théorème 5.23.1.** *Soit un LFSR* $\mathcal{L} = (\mathbb{F}_{p^n}, r, q(X))$ *en mode Galois. Soit un état initial* $(a_0(0), a_1(0), \dots, a_{r-1}(0))$ *et sa séquence de sorties* $\underline{a}_0$*. Alors la fonction génératrice de* $\underline{a}_0$ *est une fraction rationnelle de la forme suivante :*

$$a_0(X) = \frac{f(X)}{q(X)} \text{ où } -f(X) = a_0(0) + a_1(0)X + \ldots + a_{r-1}(0)X^{r-1}.$$

*Démonstration.* $a(X)$ vérifie le système linéaire à coefficient dans $\mathbb{F}_{p^n}[X]$.

$$\begin{aligned} a(X) &= s(0) + \sum_{t=1}^{t=+\infty} s(t)X^t \\ &= s(0) + \sum_{t=0}^{t=+\infty} s(t+1)X^tX \\ &= s(0) + \sum_{t=0}^{t=+\infty} (s(t).M)X^tX \\ &= s(0) + \sum_{t=0}^{t=+\infty} (s(t)X^t).XM \\ &= s(0) + a(X).XM \\ a(X).(I - XM) &= s(0) \end{aligned}$$

$I - XM$ est une matrice dans $\mathcal{M}_r(\mathbb{F}_{p^n}[X])$. L'anneau $\mathbb{F}_{p^n}[X]$ étant commutatif, il existe une comatrice de $I - XM$ notée $\texttt{Comat}(I - XM)$ telle que

$$(I - XM).\texttt{Comat}(I - XM) = \det(I - XM).I.$$

$\det(I - XM) \equiv 1 \mod X$ dans $\mathbb{F}_{p^n}[X]$. Il est donc non nul et inversible dans $\mathbb{F}_{p^n}(X)$. On a alors :

$$a(X) = \frac{1}{\det(I - XM)} s(0).\texttt{Comat}(I - XM).$$

$a(X)$ est donc un vecteur de fractions rationnelles dans $\mathbb{F}_{p^n}(X)$ ayant pour même dénominateur $\det(I - XM)$. On peut calculer les numérateurs, en particulier pour $a_0(X)$, c'est le produit scalaire entre la première colonne de la comatrice et le vecteur état initial.

On démontre par récurrence sur $r$ que $\det(I - XM) = -q(X) = 1 - q_1X - \ldots - q_rX^r$. La comatrice est de la forme

$$\texttt{Comat}(I - XM) = \begin{pmatrix} 1 & * & \ldots & * \\ X & * & \ldots & * \\ \vdots & \vdots & \vdots & \\ X^{r-1} & * & \ldots & * \end{pmatrix}.$$

Donc

$$a_0(X) = -\frac{1}{q(X)}(a_0(0), a_1(0), \ldots, a_{r-1}(0)). \begin{pmatrix} 1 \\ X \\ \vdots \\ X^{r-1} \end{pmatrix}.$$

□

Avec cette méthode matricielle, on a démontré que $a(X) \in (\mathbb{F}_{p^n}(X))^r$. La forme du numérateur de $a_i(X)$ se détermine en multipliant la $i^{\text{ième}}$ colonne de la comatrice de $M$ par l'état initial. Le dénominateur est toujours $-q(X) = \det(I - XM)$.

**Corollaire 5.23.1.** *Soit un LFSR $(\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$. Les séquences de sorties de chaque cellule sont périodiques. La période divise l'ordre de $q$. Si $q_r \neq 0$, alors toutes les séquences de sorties $\underline{a}_i$ sont strictement périodiques.*

*Démonstration.* Ce corollaire est une conséquence du corollaire 5.4.2. □

La proposition 5.17.1 donne la représentation exponentielle des LFSR séquences en mode Galois :

$$a_i = (-f(X)X^{-i}) \pmod{q(X)} \pmod{X}.$$

Une séquence générée par un LFSR en mode Galois peut être générée par un LFSR en mode Fibonacci.

**Théorème 5.23.2.** *Soit un LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$ en mode Galois. Soit un état initial $s(0) = (a_0(0), \ldots, a_{r-1}(0))$. La séquence de sorties $\underline{a}_0$ peut être générée par le LFSR $\mathcal{L} = (\mathbb{F}_{p^n}, r, q)$ en mode Fibonacci à partir de l'état initial $(a_0(0), \ldots, a_0(r-1))$.*

*Démonstration.* D'après le théorème 5.23.1, la fonction génératrice de $\underline{a}_0$ est

$$a_0(X) = \frac{-1}{q(X)}\Big(a_0(0) + a_1(0)X + \ldots + a_{r-1}(0)X^{r-1}\Big).$$

On a donc la relation $-q(X)a_0(X) = a_0(0)+a_1(0)X+\ldots+a_{r-1}(0)X^{r-1}$. En développant et par identification sur les degrés, on trouve pour tout $k \geq r$

$$a_0(k) - q_1a_0(k-1) - \ldots - q_ra_{k-r} = 0.$$

Cette relation de récurrence définie le LFSR en mode Fibonacci et l'état initial. □

Les LFSR séquences en mode Galois sont donc des LFSR séquences en mode Fibonacci. Nous n'iront pas plus loin dans l'étude des LFSRs en mode Galois qui reste semblable à celle des LFSRs en mode Fibonacci. Dans la suite, nous présentons un mode plus général appelé le mode Ring.

## 5.24 Généralisation et Mode Ring

Il existe une généralisation des LFSRs appelés Registre à décalage et à rétroaction ou Linear Feedback Registers. On les appelle ainsi car il n'y a pas forcément de décalage dans le registre. En effet, un décalage peut se traduire comme une connexion entre une cellule vers la cellule plus à droite. Les connexions d'un LFR sont choisies arbitrairement, les décalages peuvent donc être effacés. Cependant le décalage joue un rôle essentiel dans le registre car il permet de relier toutes les cellules du registre principal, sinon des cellules peuvent devenir inutiles. Les Linear Feedback Registers se définissent à partir d'une matrice choisie arbitrairement.

### 5.24.1 Définitions et Conceptions

**Définition 5.24.1** (LFR). *Un Linear Feedback Registers (LFR) construit sur $\mathbb{F}_{p^n}$ de longueur $r$ et de matrice de transition $T = (t_{i,j})_{i,j} \in \mathcal{M}_{r\times r}(\mathbb{F}_{p^n})$ est un automate ou générateur de séquences dont les états sont des éléments de la forme*

$$s(t) = (a_0(t), \ldots, a_{r-1}(t)) \in (\mathbb{F}_{2^n})^r$$

*et dont l'opération de changement d'état est donnée par*

$$s(t+1) = s(t)T.$$

**Définition 5.24.2** (le mode Ring). *On dit qu'un LFR est en mode Ring si sa matrice de transition vérifie $t_{1,r} \neq 0$ et $t_{i+1,i} = 1$ pour tout $1 \leq i \leq r-1$.*

La matrice de transition du mode Ring est de la forme suivante :

$$T = \begin{pmatrix} t_{1,1} & \ldots & t_{1,r-1} & t_{1,r} \\ 1 & \ldots & t_{2,r-1} & t_{2,r} \\ \vdots & \ddots & \vdots & \vdots \\ t_{r,1} & \ldots & 1 & t_{r,r} \end{pmatrix}.$$

On l'appelle Ring puisqu'en anglais Ring signifie Anneau, or on peut représenter graphiquement le registre par un anneau formé par les cellules du registre. Il a été introduit par Mrugaski, Rajski, and Tyszer [23]Ce mode généralise les modes de Fibonacci et de Galois. Ces deux derniers modes sont représentés respectivement par les matrice de la forme $F$ et de la forme $G$.

$$F = \begin{pmatrix} 0 & \ldots & 0 & q_r \\ 1 & \ldots & 0 & q_{r-1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & q_1 \end{pmatrix} \quad G = \begin{pmatrix} q_1 & \ldots & q_{r-1} & q_r \\ 1 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 \end{pmatrix}.$$

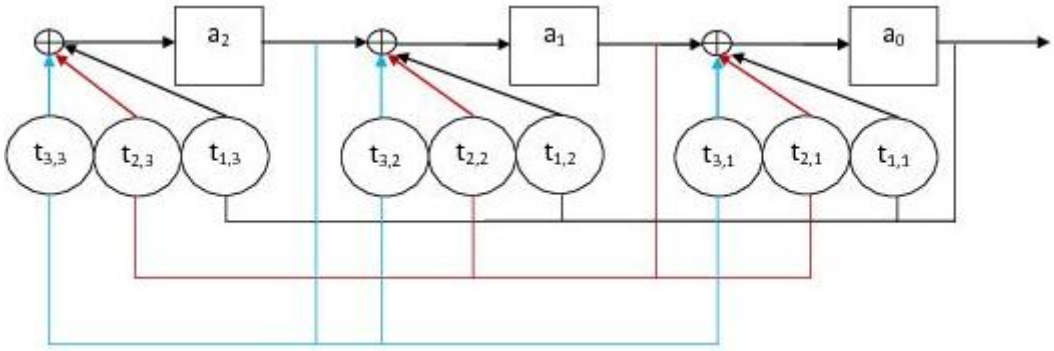



FIGURE 5.10 – Registre à rétroaction linéaire ou LFR de taille 3.

La figure 5.10 illustre un Linear Feedback Register de taille 3.

### 5.24.2 Analyse

L'analyse des LFRs démontrent que les sorties des LFRs sont les sorties des LFSRs. Autrement dit, nous obtenons les mêmes séquences et les mêmes propriétés développées dans les sections précédentes.

**Théorème 5.24.1.** *Une séquence de sorties d'un LFR de matrice de transition $T$ est aussi générée par un LFSR de polynôme de connexion* $\det(I - XT)$.

*Démonstration.* La preuve est identique à celle du théorème 5.23.1. □

En somme, les LFRs ne sont pas plus puissants que les LFSRs en terme de propriétés basiques. Cependant le mode généralisé des LFRs permet de varier les connexions afin d'obtenir des registres plus rapides en calcul en réduisant le nombre de connexions et plus simples à construire en hardware.

# Chapitre 6

# Registre à décalage et à rétroaction linéaire avec retenue ou FCSR

## 6.1 Introduction

En 1993, Goresky et Klapper introduisent un nouveau type de registre à décalage et à rétroaction (Feedback Shift Register) appelés les registres à décalage et à rétraocation linéaire avec retenue ou FCSRs (Feedback with Carry Shift Register). Ce sont des générateurs de séquences pseudo-aléatoires binaires, dites $p$-aires, c'est-à-dire construites sur le corps premier $\mathbb{F}_p$ où $p$ est premier impair. Les FCSRs se différencient des LFSRs essentiellement par l'ajout d'une cellule mémoire qui leur confère une structure $p$-adique élégante et par le fait que les opérations du registre ne se font pas dans le corps $\mathbb{F}_p$ mais dans l'anneau $\mathbb{Z}$ suite à un relèvement (de préférence dans l'ensemble $\{0, 1, \ldots, p-1\}$). Cette structure $p$-adique joue le même rôle que la structure algébrique de l'anneau des séries formelles $\mathbb{F}_p[[X]]$ pour les LFSRs. Elle permet de démontrer les propriétés des FCSRs séquences étonnamment similaires aux propriétés des séquences récurrentes linéaires (ou LFSRs séquences).

Dans cette partie, on présente les FCSRs sur $\mathbb{F}_p$ ainsi que les résultats développés par Goresky et Klapper (en particulier sur $\mathbb{F}_2$ car tous les résultats se généralisent à $\mathbb{F}_p$ pour tout $p$ premier) dans [7], [8], [9], [11], [22] et [42]. On organise cette partie dans un style particulier qui mettra en évidence le parallèle avec les résultats sur les LFSRs.

## 6.2 Pourquoi les FCSRs ?

Depuis 1955, les scientifiques cherchent d'autres méthodes pour générer des séquences avec de bonnes qualités pseudo-aléatoires autre que les LFSRs, puisque la plupart des PSGs (Pseudo-randomn Sequence Generator) sont basés sur les LFSRs donc dépendent en définitive de la structure linéaire de ces derniers.

Cependant les PSGs basés sur les FSRs non-linéaires (Non Linear Feedback Shift Register) s'avèrent être très difficiles pour l'analyse. Jusqu'à aujourd'hui, même la plus

basique des propriétés, c'est-à-dire la périodicité, est difficile à étudier voir inconnue pour un NLFSR quelconque. En pratique, on doit choisir une fonction de retour (feedback) simple et spéciale afin de rendre l'analyse du NLFSR possible. Après quarante années de recherche, seul le cas linéaire a été maitrisé en ce qui concerne l'analyse des propriétés.

En 1993, avec l'introduction des registre à rétroaction linéaire avec retenue, on dispose enfin d'un modèle alternatif au modèle linéaire parce qu'il jouit d'une structure $p$-adique élégante qui le rend analysable via la théorie $p$-adique, contrairement aux autres NLFSRs qui restent difficiles à étudier.

## 6.3 Définitions et Conception

Dans cette section, nous allons définir un Feedback with carry shift register sur un corps premier $\mathbb{F}_p$ ainsi que les séquences récurrentes linéaires avec retenue modulo $p$. Soit un nombre premier $p$. Nous nous placons dans le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Nous définissons les FCSRs en tant qu'automate. On notera la partie entière d'un réel par [.].

**Définition 6.3.1** (FCSR en mode Fibonacci)**.** *Un Feedback with carry shift register en mode Fibonacci sur $\mathbb{F}_p$ de taille $r$ et de coefficients de connexion $(q_1, \ldots, q_r) \in {\mathbb{F}_p}^r$ est un automate ou générateur de séquences dont les états sont définis de la manière suivante :*

$$s = (a_0, \ldots, a_{r-1}, m_{r-1}) \in {\mathbb{F}_p}^r \times \mathbb{Z},$$

*et dont l'opération de changement d'état est la suivante : Calculons dans $\mathbb{Z}$ l'entier*

$$\sigma_r = \sum_{i=1}^{i=r} a_{r-i} q_i + m_{r-1},$$

*puis calculons*

$$a_r = \sigma_r(\mathtt{mod}p) \text{ et } m_r = \sigma_r(\mathtt{div}p)$$

*où $(\mathtt{mod}p)$ est la fonction reste modulo $p$ et $(\mathtt{div}p)$ la fonction quotient modulo $p$ définie aussi par*

$$x(\mathtt{div}p) = [\frac{x}{p}] = \frac{x - x(\mathtt{mod}p)}{p}.$$

*La fonction de retour est $f(a_0, \ldots, a_{r-1}, m_{r-1}) = (a_1, \ldots, a_r, m_r)$ et la fonction de sorties est $g(x_0, \ldots, x_{r-1}, y) = x_0$. On répète ce procédé à l'infini. Le FCSR génère la séquence infinie*

$$(g(s), g(f(s)), g(f^2(s)), \ldots) = (a_0, a_1, a_2, \ldots)$$

*appelée séquence de sorties. L'état $s$ est appelé l'état initial de la séquence de sorties, $m_{r-1}$ la mémoire initiale, $r$ la taille du FCSR, $q_1, \ldots, q_r$ les coefficients de connexion du FCSR.*

La figure 6.1 représente un FCSR en mode Fibonacci. Avec cette définition, un FCSR est un triplet $\mathcal{F} = (\mathbb{F}_p, r, (q_1, \ldots, q_r))$. On retient à la sortie la séquence $\underline{a} = (a_0, a_1, \ldots)$ dans $\mathbb{F}_p$ et la séquence "mémoire" $\underline{m} = (m_r, m_{r-1}, \ldots)$ dans $\mathbb{Z}$. Dans la suite, on identifiera toujours les éléments dans $\mathbb{F}_p$ avec leur relèvement dans $\{0, 1, \ldots, p-1\}$.

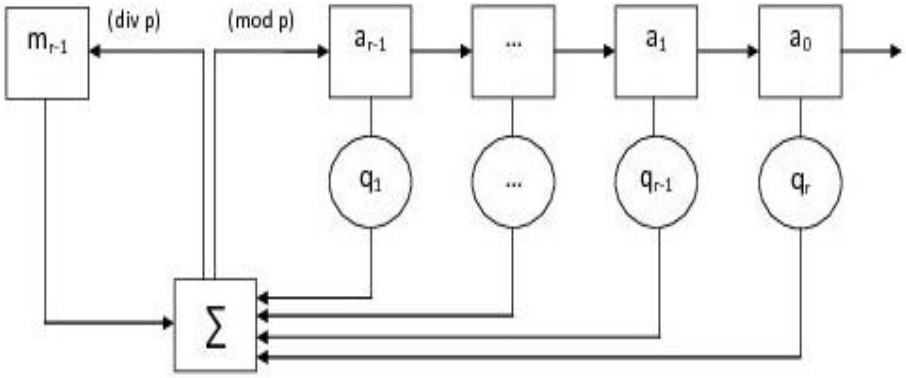



FIGURE 6.1 – Registre à décalage et à rétroaction linéaire avec retenue ou FCSR.

**Définition 6.3.2** (séquence récurrente linéaire avec retenue modulo $p$ ). *Une séquence $\underline{a} = (a_0, a_1, \ldots)$ dans $\mathbb{F}_p$ est dite séquence récurrente linéaire avec retenue modulo $p$ s'il existe un vecteur $(q_1, \ldots, q_r)$ dans $\mathbb{F}_p$ et une séquence infinie $\underline{m} = (m_{r-1}, m_r, \ldots)$ dans $\mathbb{Z}$ tels que : pour tout $i \geq r$, on a :*

$$a_i + pm_i = q_1 a_{i-1} + \ldots + q_r a_{i-r} + m_{i-1}$$

*Cette équation est appelée relation de récurrence linéaire avec mémoire modulo $p$.*

Aurement dit, cette définition est équivalente à dire que la séquence $\underline{a}$ est générée par un FCSR avec pour séquence mémoire $\underline{m}$. On les appelle aussi les FCSR séquences.

## 6.4 Analyse des FCSRs

Dans cette section, nous construisons la relation fondamentale entre les entiers $p$-adiques et les séquences récurrentes linéaires avec retenue modulo $p$ pour analyser la séquence de sorties d'un FCSR. Cette relation découle de la correspondance entre les entiers $p$-adiques et les séquences dans $\mathbb{F}_p$ extraite de leur développement de Hensel. Soit l'application suivante :

$$\begin{array}{rcl} (\mathbb{F}_p)^{\mathbb{N}} & \to & \mathbb{Z}_p \\ \underline{a} = (a_0, a_1, \ldots) & \mapsto & \alpha = \sum_{i=0}^{i=+\infty} a_i p^i. \end{array}$$

C'est une correspondance (ou bijection) entre $\mathbb{Z}_p$ l'anneau des entiers $p$-adiques et l'anneau produit infini $(\mathbb{F}_p)^{\mathbb{N}}$ mais ce n'est pas un isomorphisme car $(\mathbb{F}_p)^{\mathbb{N}}$ est de caractéristique $p$ alors que $\mathbb{Z}_p$ est de caractéristique 0. C'est une des raisons pour lesquelles l'analyse des FCSRs est un peu difficile et nous verrons par la suite que beaucoup de notions changent par rapport aux LFSR séquences comme la plus petite taille du registre qui génère la séquence ou l'expression de l'inter-corrélation.

**Définition 6.4.1.** *On appelle $\alpha$ l'entier p-adique associé à $\underline{a}$ et inversement $\underline{a}$ la séquence dans $\mathbb{F}_p$ associée à $\alpha$ que l'on note $\underline{a} = \mathtt{seq}_p(\alpha)$.*

**Définition 6.4.2** (entier de connexion)**.** *Soit un FCSR $\mathcal{F} = (\mathbb{F}_p, r, (q_1, \ldots, q_r))$. On appelle entier de connexion de $\mathcal{F}$ l'entier défini par :*

$$q = \sum_{i=1}^{i=r} q_i p^i - 1.$$

On peut donc définir un FCSR par le triplet $\mathcal{F} = (\mathbb{F}_p, r, q)$. Remarquons que l'entier de connexion à lui seul ne définit pas un FCSR. En effet, pour un même entier de connexion, on peut avoir des tailles de registre différentes. La seule condition nécessaire pour que ce triplet ait un sens est que la taille $r$ du registre soit supérieure ou égale $\log_p(q+1)$.

**Théorème 6.4.1.** *Soit un FCSR sur $\mathbb{F}_p$ de taille $r$ et d'entier de connexion $q$. Soit une séquence de sorties $\underline{a}$ avec pour état initial $(a_0, \ldots, a_{r-1}, m_{r-1})$. Soit $\alpha$ son entier p-adique associé. Alors :*

$$\alpha = \frac{s}{q} \text{ avec } s = \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - m_{r-1} p^r - \sum_{i=0}^{i=r-1} a_i p^i.$$

*De manière équivalente $\underline{a} = \mathtt{seq}_p\left(\frac{s}{q}\right)$.*

*Démonstration.* $\underline{a}$ étant une FCSR séquence, elle vérifie la relation de récurrence linéaire avec mémoire modulo $p$, pour tout $j \geq r$ : $a_j = \sum_{i=1}^{i=r} q_i a_{j-i} + m_{j-1} - p m_j$. Cette relation de récurrence et l'arithmétique dans $\mathbb{Z}_p$ donnent :

$$\begin{aligned}
\alpha &= \sum_{j=0}^{j=+\infty} a_j p^j \\
&= \sum_{j=0}^{j=r-1} a_j p^j + \sum_{j=r}^{j=+\infty} a_j p^j \\
&= \sum_{j=0}^{j=r-1} a_j p^j + \sum_{j=r}^{j=+\infty} (\sum_{i=1}^{i=r} q_i a_{j-i} + m_{j-1} - p m_j) p^j \\
&= \sum_{i=0}^{i=r-1} a_i p^i + \sum_{j=r}^{j=+\infty} (m_{j-1} - p m_j) p^j + \sum_{i=1}^{i=r} q_i p^i (\sum_{j=r}^{j=+\infty} a_{j-i} p^{j-i}) \\
&= \sum_{i=0}^{i=r-1} a_i p^i + m_{r-1} p^r + \sum_{i=1}^{i=r-1} q_i p^i (\alpha - \sum_{j=0}^{j=r-i-1} a_j p^j) + q_r p^r \alpha \\
&= \sum_{i=0}^{i=r-1} a_i p^i + m_{r-1} p^r + \sum_{i=1}^{i=r} q_i p^i \alpha - \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i p^i a_j p^j) \\
-q\alpha &= \sum_{i=0}^{i=r-1} a_i p^i + m_{r-1} p^r - \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}).
\end{aligned}$$

On trouve alors que

$$\alpha = \frac{\sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - \sum_{i=0}^{i=r-1} a_i p^i - m_{r-1} p^r}{q}.$$

□

Les différences entre les FCSRs et les LFSRs sont l'ajout d'une mémoire en initialisation et la retenue d'une séquence mémoire en sortie. Si on fixe un LFSR $\mathcal{F} = (\mathbb{F}_p, r, Q)$, pour chaque séquence de sorties $\underline{a}$, il existe un unique état initial $(a_0, \ldots, a_{r-1})$ qui génère cette séquence. De même si on fixe un FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$, il est évident que pour chaque couple $(\underline{a}, \underline{m})$ où $\underline{a}$ est la séquence de sorties et $\underline{m}$ la séquence mémoire, il existe un unique état initial $(a_0, \ldots, a_{r-1}, m_{r-1})$ qui génère ce couple. Par contre, il n'est pas évident que pour chaque séquence de sorties $\underline{a}$, il existe un unique état initial $(a_0, \ldots, a_{r-1}, m_{r-1})$ qui la génère. C'est une évidence pour les LFSR séquences mais ici la mémoire initiale joue un rôle, il pourrait donc exister deux mémoires initiales différentes avec lesquelles on génère une même séquence. Or on démontre que c'est impossible.

**Proposition 6.4.1.** *Soit un FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$. Deux états initiaux différents génèrent deux séquences différentes.*

*Démonstration.* Soient deux états initiaux quelconques,

$$(a_0, \ldots, a_{r-1}, m_{r-1}) \text{ et } (a_0^{'}, \ldots, a_{r-1}^{'}, m_{r-1}^{'}).$$

Supposons qu'ils génèrent la même séquence en sortie. Alors

$$(a_0, \ldots, a_{r-1}) = (a_0^{'}, \ldots, a_{r-1}^{'}).$$

Donc dans ce cas, seules les mémoires initiales peuvent différer. C'est la principale différence avec les LFSR séquences parce que l'état initial est composé seulement du début de la séquence, alors qu'ici il y a l'ajout d'une mémoire initiale indépendante de la séquence de sorties. Il reste donc à démontrer que la mémoire initiale est unique.

$$a_r = a_r^{'} \Rightarrow m_{r-1} - p m_r = m_{r-1}^{'} - p m_r^{'} \Rightarrow m_{r-1} - m_{r-1}^{'} = p(m_r - m_r^{'})$$

Par récurrence, on montre que $p^n$ divise $m_{r-1} - m_{r-1}^{'}$ pour tout $n$.
Donc $m_{r-1} - m_{r-1}^{'} = 0$. □

On se fixe un FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$. D'après le théorème 6.4.1, pour tout état initial $(a_0, \ldots, a_{r-1}, m_{r-1})$, le numérateur $s$ de l'entier $p$-adique associé à la séquence de sorties est entiérement déterminé par cet état initial. De même on se pose la question suivante pour un rationnel $\frac{s}{q}$, existe-t-il un unique état initial qui génère la séquence $\mathtt{seq}_p(\frac{s}{q})$ ? D'après la proposition 6.4.1, deux états initiaux différents génèrent deux séquences différentes donc leurs entiers $p$-adiques associés sont différents. De plus, il y a bijection

entre les entiers $p$-adiques et les séquences $p$-aires ; et il y a bijection entre les rationnels dont le dénominateur est premier avec $p$ et les séquences périodiques. On en déduit donc que leurs expressions sous forme rationnelle sont différentes. On démontre ce résultat de manière indépendante de la proposition précédente.

**Proposition 6.4.2.** *Soit un FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$. Soient deux états initiaux différents. Alors les nombres $p$-adiques associés aux séquences de sorties sont différents.*

*Démonstration.* Soint deux états initiaux quelconques,

$$(a_0, \ldots, a_{r-1}, m_{r-1}) \text{ et } (a_0^{'}, \ldots, a_{r-1}^{'}, m_{r-1}^{'}).$$

Supposons que $\frac{s}{q} = \frac{s^{'}}{q}$, alors $s = s^{'}$. On a donc :

$$\sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - \sum_{i=0}^{i=r-1} a_i p^i - m_{r-1} p^r = \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j^{'} p^{i+j}) - \sum_{i=0}^{i=r-1} a_i^{'} p^i - m_{r-1}^{'} p^r.$$

Il s'agit de montrer que l'écriture de $s$ est unique.

$$s = s^{'} \Rightarrow s = s^{'} \mod p.$$

On élimine les multiples de $p$ et il reste $-a_0 = -a_0^{'} \mod p$.

$$\left.\begin{array}{r} p \mid a_0 - a_0^{'} \\ -(p-1) \leq a_0 - a_0^{'} \leq p-1 \end{array}\right\} \Rightarrow a_0 = a_0^{'}$$

$$s = s^{'} \Rightarrow s = s^{'} \mod p^2.$$

On élimine les multiples de $p^2$ et il reste $q_1 a_0 - a_0 - a_1 p = q_1 a_0 - a_0 - a_1^{'} p \mod p^2$.

$$\left.\begin{array}{r} p \mid a_1 - a_1^{'} \\ -(p-1) \leq a_1 - a_1^{'} \leq p-1 \end{array}\right\} \Rightarrow a_1 = a_1^{'}$$

Par récurrence on démontre que $(a_0, \ldots, a_{r-1}) = (a_0^{'}, \ldots, a_{r-1}^{'})$. On en déduit que $-m_{r-1} p^r = -m_{r-1}^{'} p^r$. Donc les mémoires initiales sont égales. On en conclut que si on fixe un FCSR, pour chaque entier $s$, il existe un unique état initial tel que la séquence de sorties est $\mathtt{seq}_p(\frac{s}{q})$. □

## 6.5 Période et ordre de l'entier de connexion

**Définition 6.5.1** (Poids de Hamming)**.** *On pose $w = \sum_{i=1}^{i=r} q_i$. C'est le poids de Hamming de $q+1$.*

Si la fraction est irréductible alors la période est l'ordre de $p$ modulo le dénominateur. D'où le corollaire suivant :

**Corollaire 6.5.1.** *Soit un FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$. Soit une séquence de sorties et son entier p-adique associé $\frac{s}{q}$.*

1. *Les séquences de sorties sont périodiques.*
2. *Si $s$ et $q$ sont premiers entre eux, alors la période de la séquence de sorties est l'ordre de $p$ modulo $q$ noté $\mathtt{ord}_q(p)$.*
3. *Si $s$ et $q$ ne sont pas premiers entre eux, la période divise $\mathtt{ord}_q(p)$.*
4. *La séquence de sorties est strictement périodique si et seulement si $-q \leq s \leq 0$. Dans ce cas, la mémoire initiale prend sa valeur dans l'intervalle $[0, w[$.*

*Démonstration.* Tous ces points sauf le dernier ont été démontrés dans la démonstration du théorème 3.10.2. Il reste à prouver le dernier point. Soit $\underline{a} = (a_0, a_1, \ldots)$ une séquence de sorties du FCSR. Si elle est strictement périodique alors $-q \leq s \leq 0$.

$$
\begin{aligned}
-q \leq s \quad &\Rightarrow \quad -q \leq \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - m_{r-1}p^r - \sum_{i=0}^{i=r-1} a_i p^i \\
&\Rightarrow \quad m_{r-1} \leq \tfrac{q}{p^r} + \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j \frac{p^{i+j}}{p^r}) - \sum_{i=0}^{i=r-1} a_i \frac{p^i}{p^r} \\
&\Rightarrow \quad m_{r-1} \leq \tfrac{q}{p^r} + \sum_{k=1}^{k=r-1} \sum_{i=1}^{i=k} (q_i a_{k-i} \frac{p^k}{p^r}) - \sum_{k=0}^{k=r-1} a_k \frac{p^k}{p^r} \\
&\Rightarrow \quad m_{r-1} \leq \tfrac{q}{p^r} + \sum_{k=1}^{k=r-1} (\sum_{i=1}^{i=k} q_i) \frac{p^k}{p^r} \\
&\Rightarrow \quad m_{r-1} \leq \sum_{k=1}^{k=r} q_k \frac{p^k}{p^r} - \frac{1}{p^r} + \sum_{k=1}^{k=r-1} (\sum_{i=1}^{i=k} q_i) \frac{p^k}{p^r} \\
&\Rightarrow \quad m_{r-1} \leq q_r + \sum_{k=1}^{k=r-1} q_k \frac{p^k}{p^r} - \frac{1}{p^r} + \sum_{k=1}^{k=r-1} q_k \sum_{i=k}^{i=r-1} \frac{p^i}{p^r} \\
&\Rightarrow \quad m_{r-1} < q_r + \sum_{k=1}^{k=r-1} q_k \Big( \frac{p^k}{p^r} + \sum_{i=k}^{i=r-1} \frac{p^i}{p^r} \Big) \\
&\Rightarrow \quad m_{r-1} < q_r + \sum_{k=1}^{k=r-1} \frac{q_k}{p^r} \Big( 2p^k + \sum_{i=k+1}^{i=r-1} p^i \Big) \\
&\Rightarrow \quad m_{r-1} < q_r + \sum_{k=1}^{k=r-1} \frac{q_k}{p^r} \Big( 2p^k + \frac{p^r - p^{k+1}}{p-1} \Big) \\
&\Rightarrow \quad m_{r-1} < q_r + \sum_{k=1}^{k=r-1} \frac{q_k}{p^r} \Big( 2p^k + \frac{p^r - p^{k+1}}{p-1} \Big) \\
&\Rightarrow \quad m_{r-1} < q_r + \sum_{k=1}^{k=r-1} q_k \frac{2p^{k+1} - 2p^k + p^r - p^{k+1}}{p^{r+1} - p^r}
\end{aligned}
$$

$$\begin{aligned} 2p^{k+1} - 2p^k + p^r - p^{k+1} - (p^{r+1} - p^r) &= p^{k+1} - 2p^k + 2p^r - p^{r+1} \\ &= (p-2)(p^k - p^r) \\ &< 0 \end{aligned}$$

Donc $\dfrac{2p^{k+1} - 2p^k + p^r - p^{k+1}}{p^{r+1} - p^r} < 1$ pour $k < r$. On en déduit que

$$m_{r-1} < q_r + \sum_{k=1}^{k=r-1} q_k \Rightarrow m_{r-1} < w$$

$$\begin{aligned} s \leq 0 &\Rightarrow \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - m_{r-1}p^r - \sum_{i=0}^{i=r-1} a_i p^i \leq 0 \\ &\Rightarrow \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j \frac{p^{i+j}}{p^r}) - \sum_{i=0}^{i=r-1} a_i \frac{p^i}{p^r} \leq m_{r-1} \\ &\Rightarrow -\sum_{i=0}^{i=r-1} \frac{p^i}{p^r} \leq m_{r-1} \\ &\Rightarrow -\sum_{i=1}^{i=r} \frac{1}{p^i} \leq m_{r-1} \\ &\Rightarrow -\frac{1}{p-1}(1 - \frac{1}{p^r}) \leq m_{r-1} \\ &\Rightarrow -1 < m_{r-1} \\ &\Rightarrow 0 \leq m_{r-1} \end{aligned}$$

Si la fraction n'est pas irréductible, le dénominateur de la forme irréductible de $\alpha$ divise $q$. Or si un entier $q'$ divise un entier $q$, alors $\mathtt{ord}_{q'}(p)$ divise $\mathtt{ord}_q(p)$. Donc la période divise $\mathtt{ord}_q(p)$. □

Plus généralement, si $s \leq 0$ alors la mémoire initiale est positive et si $s \geq -q$ alors la mémoire initiale est strictement inférieure à $w$.

## 6.6 Comportement de la mémoire

Il est important de connaître l'évolution de la mémoire au fur et à mesure des étapes du registre. Dans cette section, on démontre qu'elle est soit bornée soit revient dans cet intervalle borné de manière monotone pour y rester par la suite.

**Proposition 6.6.1.**

- *Si $m_{r-1} \in [0, w[$, alors les valeurs de la mémoire suivantes restent dans l'intervalle $[0, w[$.*
- *Si $m_{r-1} \geq w$, alors les valeurs de la mémoire décroissent de manière monotone et reviennent dans l'intervalle $[0, w[$ après $[\log_p(m_{r-1} - w)] + r$ étapes.*

– *Si $m_{r-1} < 0$, alors les valeurs de la mémoire croissent de manière monotone et reviennent dans l'intervalle $[0, w[$ après $[\log_p(|m_{r-1}|) + r$ étapes.*

*Démonstration.* Par définition : $m_r = \frac{1}{p}(\sigma_r - a_r) = \frac{1}{p}(\sum_{i=1}^{i=r} q_i a_{r-i} + m_{r-1} - a_r)$. Si $0 \leq m_{r-1} < w$, alors $-1 < -\frac{p-1}{p} \leq m_r < \frac{1}{p}((p-1)w + w) = w$. La mémoire prend des valeurs entières, donc $0 \leq m_r < w$. Si $m_{r-1} \geq w$, alors

$$-1 < -\frac{p-1}{p} \leq \frac{w-(p-1)}{p} \leq m_r \leq \frac{1}{p}(w(p-1)+m_{r-1}) \leq \frac{1}{p}(m_{r-1}(p-1)+m_{r-1}) = m_{r-1}.$$

$m_r$ est un entier, donc $0 \leq m_r \leq m_{r-1}$. Si $0 \leq m_r < w$, c'est ce qu'il fallait démontrer. Sinon $m_r = w$, alors

$$\begin{aligned}
w &= \frac{1}{p}((\sum_{i=1}^{i=r} q_i a_{r-i} + m_{r-1} - a_r) \\
pw &= \sum_{i=1}^{i=r} q_i a_{r-i} + w - a_r \\
(p-1)w &= \sum_{i=1}^{i=r} q_i a_{r-i} - a_r \\
(p-1)w &\leq (p-1)w - a_r \\
a_r &\leq 0 \\
a_r &= 0
\end{aligned}$$

Ou bien $0 \leq m_{r+1} < w$ et c'est ce qu'il fallait démontrer, ou bien $m_{r+1} = w$ alors $a_{r+1} = 0$. Au bout de $r$ étapes, si $m_r = m_{r+1} = \ldots = m_{2r-1} = w$ alors $a_r = a_{r+1} = \ldots = a_{2r-1} = 0$.

$$\begin{aligned}
m_{2r} &= \frac{1}{p}(\sum_{i=1}^{i=r} q_i a_{2r-i} + m_{2r-1} - a_{2r}) \\
&= \frac{1}{p}(q_1 a_{2r-1} + \ldots + q_r a_r + w - a_{2r}) \\
&= \frac{1}{p}(w - a_{2r}) \\
&\leq \frac{w}{p} \\
m_{2r} &< w
\end{aligned}$$

Si $m_r > w$, on pose $e_r = m_r - w$.

$$\begin{aligned}
e_r &= m_r - w \\
&= \tfrac{1}{p}(\sum_{i=1}^{i=r} q_i a_{r-i} + m_{r-1} - a_r) - w \\
&= \tfrac{1}{p}(\sum_{i=1}^{i=r} q_i a_{r-i} + m_{r-1} - a_r - pw) \\
&= \tfrac{1}{p}(\sum_{i=1}^{i=r} q_i a_{r-i} + m_{r-1} - a_r - w - (p-1)w) \\
&= \tfrac{1}{p}(m_{r-1} - w) + \tfrac{1}{p}(\sum_{i=1}^{i=r} q_i a_{r-i} - a_r - (p-1)w) \\
&\leq \tfrac{1}{p}e_{r-1} + \tfrac{1}{p}((p-1)w - (p-1)w) \\
e_r &\leq \tfrac{1}{p}e_{r-1} \\
e_{r-1+k} &\leq \tfrac{1}{p^k}e_{r-1}
\end{aligned}$$

La mémoire décroit de manière monotone. Après $\log_p(m_r - w) + 1$ étapes, $e_{r-1+k} \leq 0$. Donc $m_r \leq w$, on revient au cas précédent.

Si $m_{r-1} < 0$, alors

$$\frac{1}{p}(m_{r-1} - 1) \leq m_r < \frac{1}{p}(p-1)w < w.$$

Si $\sigma_r \geq 0$, alors $m_r \geq 0$, c'est ce qu'il fallait démontrer. Sinon $m_r < 0$. Supposons que $m_{r-1+k} < 0$ jusqu'à $k = [\log_p |m_{r-1}|] + 1$, alors

$$\frac{m_{r-1}}{p^k} - \left(\frac{1}{p} + \ldots + \frac{1}{p^k}\right) \leq m_{r-1+k}$$

$$\frac{1}{p} + \ldots + \frac{1}{p^k} = \frac{p^k - 1}{p^k}\frac{1}{p-1} < 1 \Rightarrow \frac{1}{p^k}m_{r-1} - 1 < m_{r-1+k}$$

$$k = [\log_p |m_{r-1}|] + 1 > \log_p |m_{r-1}| \Rightarrow p^k > |m_{r-1}| \Rightarrow \frac{m_{r-1}}{p^k} > \frac{m_{r-1}}{|m_{r-1}|} = -1$$

Donc après $k = [\log_p |m_{r-1}|] + 1$ étapes, la mémoire prend une valeur $m_{r-1+k} > -2$, comme elle est entière $m_{r-1+k} \geq -1$.

$$\begin{aligned}
m_{r+k} &= \tfrac{1}{p}(\sum_{i=1}^{i=r} q_i a_{r+k-i} - 1 - a_{r+k}) \\
&\geq \tfrac{1}{p}(-1 - (p-1)) \\
m_{r+k} &\geq -1
\end{aligned}$$

Si $m_{r+k} \geq 0$, donc après $[\log_p |m_{r-1}|] + 2$ étapes, la mémoire prend des valeurs dans l'intervalle $[0, w[$. Sinon si $m_{r+k} = -1$, on distingue deux cas. Tout d'abord

$$\begin{aligned} m_{r+k} = -1 &\Rightarrow \sum_{i=1}^{i=r} q_i a_{r+k-i} - 1 - a_{r+k} = -p \\ &\Rightarrow \sum_{i=1}^{i=r} q_i a_{r+k-i} + p - 1 = a_{r+k} \\ &\Rightarrow 0 \leq \sum_{i=1}^{i=r} q_i a_{r+k-i} + p - 1 = a_{r+k} \leq p - 1 \\ m_{r+k} = -1 &\Rightarrow \sum_{i=1}^{i=r} q_i a_{r+k-i} = 0 \text{ et } a_{r+k} = p - 1. \end{aligned}$$

Si $q = -1$, alors tous les coefficients de connexion sont nuls et le calcul des mémoires suivantes donnent $-1$ à l'infini. Si $q > -1$, alors il existe un coefficient de connexion non nul. Après au plus $r - 1$ étapes, $a_{r+k}$ est décalé vers un coefficient de connexion non nul et la mémoire devient positive. □

**Proposition 6.6.2.** *Si l'état initial $(a_0, \ldots, a_{r-1}, m_{r-1})$ du FCSR est strictement périodique alors la mémoire initiale $m_{r-1}$ prend une valeur dans l'intervalle $[0, w[$.*

*Démonstration.* Supposons l'inverse, c'est-à-dire que la mémoire initiale prenne sa valeur à l'extérieur de cet intervalle, alors les mémoires suivantes ne reviendront jamais vers cette valeur, mais plutôt vont croître ou décroître suivant le cas pour arriver et rester indéfiniment dans cet intervalle. Donc l'état initial ne peut pas être strictement périodique puisque la mémoire ne peut pas revenir à sa valeur initiale. □

## 6.7 Initialisation et Algorithme

Dans cette section, on se pose la question inverse. Donnons nous un rationnel $\frac{s}{q}$ où $q$ est un entier positif premier avec $p$. Comment déterminer un FCSR et un état initial qui génère la séquence $\mathtt{seq}_p(\frac{s}{q})$ ? On développe un algorithme qui donne les paramètres d'un FCSR et l'initialisation qui génère cette séquence.

**Algorithme 6.7.1.**

1. *On doit écrire $\frac{s}{q}$ avec un dénominateur ayant $p-1$ pour reste modulo $p$. Si $q = p-1 \pmod p$, c'est bon. Sinon on multiplie $s$ et $q$ par l'inverse de $q \pmod p$ modulo $p$ et par $p - 1$. Le dénominateur est alors congru à -1 modulo p. Supposons que $q$ vérifie cela.*
2. *On calcule $r = [\log_p(q + 1)]$ et on écrit $q$ sous la forme $q = q_r p^r + \ldots + q_1 p - 1$.*

3. *On calcule les $r$ premiers coefficients du développement $p$-adique de $\frac{s}{q}$ :*

$$a_0 + a_1 2 + \ldots + a_{r-1}2^{r-1} = \frac{s}{q} \pmod{2^r}$$

.

4. *On calcule* $z = \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - \sum_{i=0}^{i=r-1} a_i p^i$.

5. *On calcule* $m_{r-1} = \frac{1}{p^r}(z - s)$.

**Proposition 6.7.1.** *Soit un rationnel $\frac{s}{q}$. Supposons que l'algorithme 6.7.1 ait été appliqué. Alors le FCSR $(\mathbb{F}_p, r, q)$ et l'état initial $(a_0, a_1, \ldots, a_{r-1}, m_{r-1})$ en sorties de cet algorithme génèrent la séquence $\mathtt{seq}_p(\frac{s}{q})$.*

Cet algorithme donne le FCSR et l'état initial les plus naturels qui génèrent $\mathtt{seq}_p(\frac{s}{q})$. La difficulté de cet algorithme réside principalement dans le fait de calculer les premiers coefficients du développement $p$-adique d'un rationnel quelconque. On possède un autre algorithme sensiblement identique qui donne plus facilement le FCSR et l'initialisation qui génère $\mathtt{seq}_p(\frac{s}{q})$.

**Algorithme 6.7.2.**

1. *On calcule* $r = [\log_p(q+1)]$ *et on écrit $q$ sous la forme* $q = q_r p^r + \ldots + q_1 p - 1$.
2. *On pose* $m_{-1} = -s$.
3. *Pour tout* $i = 0, 1, \ldots, r-1$, *on calcule les entiers suivants :*
   (a) $\sigma_i = \sum_{k=0}^{k=i-1} q_{i-k} a_k + m_{i-1}$.
   (b) $a_i = \sigma_i \pmod{p}$.
   (c) $m_i = \frac{1}{p}(\sigma_i - a_i)$.
4. *On retient en sortie* $\mathcal{F} = (\mathbb{F}_p, r, q)$ *et* $(a_0, \ldots, a_{r-1}, m_{r-1})$.

**Proposition 6.7.2.** *Soit un rationnel $\frac{s}{q}$. Supposons que l'algorithme 6.7.2 ait été appliqué. Alors le FCSR $(\mathbb{F}_p, r, q)$ et l'état initial $(a_0, a_1, \ldots, a_{r-1}, m_{r-1})$ en sortie de cet algorithme génèrent la séquence $\mathtt{seq}_p(\frac{s}{q})$.*

*Démonstration.* Supposons que l'algorithme 6.7.2 ait été appliqué au rationnel $\frac{s}{p}$ et retenons à la sortie un FCSR $(\mathbb{F}_p, r, q)$ et une initialisation $(a_0, \ldots, a_{r-1}, m_{r-1})$. Il reste à vérifier que le FCSR et l'initialisation génèrent bien la séquence $\mathtt{seq}_p(\frac{s}{q})$. D'après le théorème 6.4.1, ils génèrent en sortie la séquence associée à $\mathtt{seq}_p(\frac{s'}{q})$ avec

$$s' = \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - \sum_{i=0}^{i=r-1} a_i p^i - m_{r-1} p^r.$$

Montrons que $s = s^{'}$.

$$\begin{aligned}
s^{'} &= \sum_{k=1}^{k=r-1}\sum_{i=1}^{i=k}(q_k a_{k-i})p^k - \sum_{k=0}^{k=r-1} a_k p^k - m_{r-1}p^r \\
&= \sum_{k=1}^{k=r-1}(\sigma_k - m_{k-1})p^k - \sum_{k=0}^{k=r-1}(\sigma_k - pm_k)p^k - m_{r-1}p^r \\
&= \sum_{k=1}^{k=r-1}(\sigma_k - m_{k-1} - \sigma_k + pm_k)p^k - m_{r-1}p^r - \sigma_0 + pm_0 \\
&= m_{r-1}p^r - pm_0 - m_{r-1}p^r - \sigma_0 + pm_0 \\
s^{'} &= s
\end{aligned}$$

□

Soit un FCSR $(\mathbb{F}_p, r^{'}, q^{'})$ qui génère la séquence $\mathtt{seq}_p(\frac{s}{q})$. D'après le théorème 6.4.1, il existe alors un entier $s^{'}$ tel que $\mathtt{seq}_p(\frac{s}{q}) = \mathtt{seq}_p(\frac{s^{'}}{q^{'}})$. Par correspondance entre les rationnels et les séquences périodiques, on trouve que $\frac{s}{q} = \frac{s^{'}}{q^{'}}$. Inversement, soit un rationnel $\alpha = \frac{s}{q} = \frac{s^{'}}{q^{'}}$. Si on applique l'algorithme 6.7.2 à $\frac{s}{q}$ et à $\frac{s^{'}}{q^{'}}$, on trouve deux FCSRs qui génèrent la séquence $\mathtt{seq}_p(\alpha)$. Autrement dit, une infinité de FCSR et d'état initiaux peuvent générer une séquence $\mathtt{seq}_p(\alpha)$.

**Proposition 6.7.3.** *Soit un rationnel $\alpha = \dfrac{s}{q}$. Soit le FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$ en sortie de l'algorithme 6.7.2. Si $s$ et $q$ sont premiers entre eux, $\mathcal{F}$ est le FCSR de plus petite taille $r$ qui génère $\mathtt{seq}_p(\alpha)$.*

*Démonstration.* Soit un autre FCSR $(\mathbb{F}_p, r^{'}, q^{'})$ qui génère la séquence $\mathtt{seq}_p(\alpha)$, alors $pq^{'} = p^{'}q$. Or $p$ et $q$ sont premiers entre eux, donc $q \mid q^{'}$.

$$r = \log_p(q+1) \leq \log_p(q^{'}+1) = r^{'}.$$

□

**Théorème 6.7.1.** *Les séquences périodiques sur $\mathbb{F}_p$ sont les FCSR séquences sur $\mathbb{F}_p$.*

*Démonstration.* Une FCSR séquence est périodique d'après le corollaire 6.5.1. Inversement une séquence périodique a pour développement $p$-adique un rationnel. D'après l'algorithme 6.7.1, c'est une FCSR séquence. □

## 6.8 Représentation exponentielle des FCSRs séquences

Les FCSRs séquences possèdent une représentation exponentielle qui est un outil puissant pour l'analyse de ces séquences notamment pour le calcul de l'inter-corrélation. Cette représentation est similaire à la représentation par la trace des LFSRs. Rappelons

la représentation par la trace d'une LFSR séquence. Soit une séquence périodique $\underline{a} = (a_0, a_1, \ldots)$ dans $\mathbb{F}_p$ générée par un LFSR de taille $r$ et de polynôme de connexion $Q$ irréductible. Soit $\gamma$ une racine de $Q$ dans $\mathbb{F}_{p^r}$, alors il existe un élément $A \in \mathbb{F}_{p^r}$ tel que pour tout $i \in \mathbb{N}$

$$a_i = \mathtt{Tr}(A\gamma^i).$$

**Proposition 6.8.1.** *Soit un entier $q = q_r p^r + \ldots + q_1 p - 1$ tel que $0 \leq q_i < p$. Alors $q$ est inversible dans l'anneau des entiers $p$-adiques $\mathbb{Z}_p$.*
*Soit $s$ un entier avec $-q < s \leq 0$. Soit le développement $p$-adique de $\frac{s}{q}$ :*

$$\frac{s}{q} = a_0 + a_1 p + a_2 p^2 + \ldots$$

*Alors pour tout $i \geq 0$, $a_i = (-sp^{-i}) \pmod q \pmod p$.*

*Démonstration.* Voir le chapitre 7 à la page 229. □

**Remarque 6.8.1.** *Remarquons que $\frac{s}{q} = -1$ si et seulement si $\mathtt{seq}_p(\frac{s}{q}) = (p-1, p-1, \ldots)$. En effet*

$$(1-p)((p-1) + (p-1)p + (p-1)p^2 + \ldots) = p - 1$$
$$\Rightarrow (p-1) + (p-1)p + (p-1)p^2 + \ldots = -1$$

**Théorème 6.8.1** (Représentation exponentielle)**.** *Soit un FCSR $(\mathbb{F}_p, r, q)$ et soit une séquence de sorties $\underline{a} = (a_0, a_1, \ldots)$ strictement périodique différente de la séquence $(p-1, p-1, \ldots)$, alors il existe un entier $-q < s \leq 0$ tel que pour tout $i \geq 0$*

$$a_i = (-sp^{-i}) \pmod q \pmod p.$$

*Démonstration.* Une FCSR séquence strictement périodique différente de la séquence $(p-1, p-1, \ldots)$ a pour développement $p$-adique un rationnel $\frac{s}{q}$ tel que $-q < s \leq 0$. Elle vérifie donc les conditions de la propositions 6.8.1 et donc admet une écriture exponentielle. □

## 6.9 État initial dégénéré

Dans cette section, nous étudions les cas particuliers où la séquence de sorties est de période 1 avec pour sortie 0 ou $p-1$. À partir d'une certaine étape, le registre sort toujours le même coefficient à l'infini.

**Définition 6.9.1** (état initial dégénéré)**.** *On dit qu'un état est dégénéré si le nombre $p$-adique $\alpha$ associé à la séquence de sorties est un entier.*

**Proposition 6.9.1.** *Si l'état initial est dégénéré, alors il existe deux cas possibles :*

1. *après la pré-période, le FCSR ne sort en coefficient que des 0,*
2. *ou après la prépériode, le FCSR ne sort en coefficient que des $p-1$.*

*Démonstration.* Soit un état initial dégénéré et soit $\underline{a}$ la séquence de sorties de période $T$ et de prépériode de longueur $N$

$$(a_0, \ldots, a_{N-1}, \underbrace{a_N, \ldots, a_{N+T-1}}_{T}, \ldots).$$

Soit $\alpha$ son entier 2-adique associé

$$\alpha = \sum_{i=0}^{i=N-1} a_i p^i + p^N \frac{\sum_{i=0}^{i=T-1} a_{i+N} p^i}{1-p^T}.$$

$$\alpha \in \mathbb{Z} \Leftrightarrow \frac{\sum_{i=0}^{i=T-1} a_{i+N} p^i}{1-p^T} \in \mathbb{Z}.$$

Or $-1 \leq \frac{\sum_{i=0}^{i=T-1} a_{i+N} p^i}{1-p^T} \leq 0$, donc $\alpha \in \mathbb{Z} \Leftrightarrow \frac{\sum_{i=0}^{i=T-1} a_{i+N} p^i}{1-p^T} = 0$ ou $-1$.
Si $\sum_{i=0}^{i=T-1} a_{i+N} p^i = 0$, alors après la pré-période, tous les coefficients de sorties sont nuls.
Si $\sum_{i=0}^{i=T-1} a_{i+N} p^i = p^T - 1$, alors après la pré-période, tous les coefficients de sorties sont $p-1$. En effet, si l'un des coefficients est strictement inférieur à $p-1$, alors

$$\sum_{i=0}^{i=T-1} a_{i+N} p^i < \sum_{i=0}^{i=T-1} (p-1) p^i = (p-1) \frac{p^T - 1}{p-1} = p^T - 1.$$

□

**Remarque 6.9.1.** *Soit un état initial dégénéré et sa séquence de sorties $\underline{a}$. Soit $\alpha$ l'entier 2-adique associé à $\underline{a}$. On a donc deux cas, les coefficients de sorties sont tous nuls ou sont tous égaux à $p-1$ après la pré-période. Si les coefficients sont tous nuls après la pré-période, alors $\alpha \geq 0$ et si les coefficients sont tous égaux à $p-1$, alors $\alpha < 0$. En effet, dans le premier cas, on a*

$$\alpha = \sum_{i=0}^{N-1} a_i p^i + p^N \frac{\sum_{i=0}^{i=T-1} a_i p^i}{1-p^T} = \sum_{i=0}^{N-1} a_i p^i \geq 0$$

*et dans le second cas, on a*

$$\alpha = \sum_{i=0}^{N-1} a_i p^i - p^N \frac{\sum_{i=0}^{i=T-1} a_i p^i}{1-p^T} = \sum_{i=0}^{N-1} a_i p^i - p^N < 0.$$

**Définition 6.9.2** (état final). *Si l'état d'un FCSR est périodique de période* 1*, alors on appellera l'état redondant à l'infini l'état final.*

**Proposition 6.9.2.** *Soit un FCSR* $(\mathbb{F}_p, r, q)$*. Soit un état initial* $(a_0, \ldots, a_{r-1}, m_{r-1})$*. Si cet état initial est dégénéré alors les états du FCSR sont périodiques de période 1 et l'état final est* $(0, \ldots, 0, 0)$ *ou* $(p-1, \ldots, p-1, w-1)$*.*

*Démonstration.* Si les coefficients de la séquence de sorties sont tous nuls après la pré-période $(a_0, \ldots, a_{N-1}, 0, 0\ldots)$, alors à partir de l'étape $N+r$, tous les coefficients de la séquence en entrée et le coefficient de sorties sont nuls. Ainsi $\sigma_{N+r} = m_{N+r-1}$ et $m_{N+r} = \dfrac{m_{N+r-1}}{p}$. Les mémoires suivantes sont :

$$\begin{aligned} m_{N+r+1} &= \frac{m_{N+r}}{p} = \frac{m_{N+r-1}}{p^2} \\ m_{N+r+2} &= \frac{m_{N+r+1}}{p} = \frac{m_{N+r-1}}{p^3} \\ &\vdots \end{aligned}$$

La valeur de la mémoire converge vers 0, étant entière, elle devient stationnaire en 0.
Si les coefficients de la séquence de sorties sont tous égaux à $p-1$ après la pré-période $(a_0, \ldots, a_{N-1}, p-1, p-1\ldots)$, alors à partir de l'étape $N+r$, tous les coefficients de la séquence en entrée et le coefficient de sorties sont $p-1$. D'après la proposition 6.6.1, la valeur de la mémoire reste dans l'intervalle $[0, w-1]$ après une certaine étape $t$ du registre. Ainsi pour un $t$ grand,

$$\begin{aligned} m_{t+1} &= \frac{(p-1)w + m_t - (p-1)}{p} \\ \frac{(p-1)w - (p-1)}{p} m_{t+1} &\leq \frac{(p-1)w + w - 1 - (p-1)}{p} \\ \frac{(p-1)(w-1)}{p} &\leq m_{t+1} \leq w-1 \end{aligned}$$

Par récurrence, on trouve pour tout $n$ que

$$\frac{(w-1)(p-1)}{p}\Big(1 + \frac{1}{p} + \ldots + \frac{1}{p^n} + \frac{p-1}{p^{n+1}}\Big) \leq m_{t+n+1} \leq w-1$$

Quand $n$ tend vers l'infini, le membre de gauche tend vers $w-1$. En effet :

$$\begin{aligned} \tfrac{(w-1)(p-1)}{p}\Big(1 + \tfrac{1}{p} + \ldots + \tfrac{1}{p^n} + \tfrac{p-1}{p^{n+1}}\Big) &= \tfrac{(w-1)(p-1)}{p}\Big(\tfrac{1-\frac{1}{p^{n+1}}}{1-\frac{1}{p}} + \tfrac{p-1}{p^{n+1}}\Big) \\ &= \tfrac{(w-1)(p-1)}{p}\Big(\tfrac{p}{p-1}(1 - \tfrac{1}{p^{n+1}}) + \tfrac{p-1}{p^{n+1}}\Big) \\ &= (w-1)(1 - \tfrac{1}{p^{n+1}}) + \tfrac{(w-1)(p-1)^2}{p^n p^2} \end{aligned}$$

Comme la mémoire prend des valeurs entières, elle est stationnaire et prend la valeur $w-1$ indéfiniment. □

**Proposition 6.9.3.** *Soit un FCSR $(\mathbb{F}_p, r, q)$. Soit un état initial $(a_0, \ldots, a_{r-1}, m_{r-1})$. Supposons cet état initial dégénéré.*

1. *Si $m_{r-1} > 0$, alors à partir de l'étape $[\log_p(m_{r-1}+1)]+1$, les coefficients de sorties ne prennent que la valeur $p-1$.*
2. *Si $m_{r-1} = 0$, il existe deux cas. Si pour tout $j \neq r$, $q_j = 0$, alors la séquence de sorties est $(p-1, p-1, \ldots)$. S'il existe $j \neq r$ tel que $q_j \neq 0$, alors la séquence de sorties est nulle.*
3. *Si $m_{r-1} < 0$, il existe deux cas. Si pour tout $j \neq r$, $q_j = 0$, alors après $[\log_p(\frac{-m_{r-1}p^r}{p^r-1})]+1$, les coefficients de sorties ne prennent que la valeur 0. S'il existe $j \neq r$ tel que $q_j \neq 0$, alors après $[\log_p(m_{r-1}+1)]+1$ étapes, les coefficients de sorties prennent tous la valeur 0.*

*Démonstration.* Soit un état initial dégénéré qui génère la séquence $\mathtt{seq}_p(\alpha)$ avec $\alpha \in \mathbb{Z}$. Nous allons examiner tous les cas possibles. Si $\alpha = 0$, alors $a_i = 0$ pour tout $i$ et $s = 0$. D'après le théorème 6.4.1,

$$s = \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - m_{r-1}p^r - \sum_{i=0}^{i=r-1} a_i p^i,$$

donc $m_{r-1} = 0$.
Si $\alpha \neq 0$, on considère trois cas, $m_{r-1} > 0$, $m_{r-1} = 0$ et $m_{r-1} < 0$.
Si $m_{r-1} > 0$ et si $\alpha > 0$, d'après la remarque 6.9.1, tous les coefficients de sorties après la pré-période sont tous nuls. D'après la proposition 6.9.2, l'état final est $(0, \ldots, 0, 0)$. À partir d'un certain rang, la mémoire prend une valeur nulle à l'infini. Soit $s_1$ le dernier état du registre tel que la mémoire soit non-nulle. Soit $s_2$ le dernier état tel qu'il existe un $a_i$ soit non-nul. L'état $s_2$ est de la forme

$$s_2 = (\underbrace{c, 0, \ldots, 0}_{r}, m)$$

avec $c \neq 0$, puisque $c$ étant le dernier coefficient non nul en sortie, le reste des coefficients sont nuls et $c$ est en première position dans l'état.
Si $s_1 = s_2$ ou si $s_1$ est avant $s_2$, alors $s_2 = (c, 0 \ldots, 0, 0)$. l'état suivant est $s' = (0, 0, \ldots, 0, 0)$ puisque la mémoire devient nulle ainsi que tous les coefficients de sorties. Or la mémoire de $s'$ est égale à $\frac{q_r c}{p} = 0$. Or $q_r \neq 0$ et $c \neq 0$, donc c'est absurde.
Si $s_2$ précède $s_1$, alors $s_1 = (0, \ldots, 0, m)$. Les états suivants sont tous nuls. Or la mémoire suivante prend la valeur $\frac{m}{p}$ et donc $m = 0$. C'est absurde. On en déduit que le cas $m_{r-1} > 0$ et $\alpha > 0$ est impossible. Si $m_{r-1} > 0$ et $\alpha < 0$, d'après la remarque 6.9.1, tous les coefficients de sorties après la pré-période sont tous égaux à $p-1$. D'après la proposition 6.9.2, l'état final est $(p-1, \ldots, p-1, w-1)$. À partir d'un certain rang, la

mémoire prend pour valeur $w-1$ à l'infini. De plus,

$$\begin{aligned}
\alpha<0 \Rightarrow\ & s<0 \\
\Rightarrow\ & -m_{r-1}p^r-\sum_{i=0}^{i=r-1}a_ip^i \leq \sum_{i=1}^{i=r-1}\sum_{j=0}^{j=r-i-1}(q_ia_jp^{i+j})-m_{r-1}p^r-\sum_{i=0}^{i=r-1}a_ip^i<0 \\
\Rightarrow\ & |s| \leq \Big|-m_{r-1}p^r-\sum_{i=0}^{i=r-1}a_ip^i\Big| \\
\Rightarrow\ & |s| \leq m_{r-1}p^r+p^r-1 \\
\Rightarrow\ & |s|<(m_{r-1}+1)p^r.
\end{aligned}$$

Comme $q_r \neq 0$, alors $q \geq p^r-1$.
Supposons $q>p^r-1$, or $q$ et $p$ sont premiers entre eux, donc $q>p^r$. On déduit que $\frac{|s|}{q}<m_{r-1}+1$ et donc $-(m_{r-1}+1)<\frac{s}{q}$. Soit $b_dp^d+\ldots+b_kp^k$ le développement $p$-adique de $m_{r-1}+1$ avec $k=[\log_p(m_{r-1}+1)]$. D'après l'arithmétique dans $\mathbb{Z}_p$, $-(m_{r-1}+1)$ a pour développement $p$-adique

$$(p-b_d)p^d+(p-1-b_{d+1})p^{d+1}+\ldots+(p-1-b_k)p^k+(p-1)p^{k+1}+(p-1)p^{k+2}+\ldots$$

Comme $\frac{|s|}{q}<m_{r-1}+1$, le développement $p$-adique de $\frac{|s|}{q}$ est de la forme $b_{d'}p^{d'}+\ldots+b_{k'}p^{k'}$ avec $k' \leq k$. De même le développement $p$-adique $\frac{s}{q}$ est de la forme

$$(p-b_{d'})p^{d'}+(p-1-b_{d'+1})p^{d'+1}+\ldots+(p-1-b_{k'})p^{k'}+(p-1)p^{k'+1}+(p-1)p^{k'+2}+\ldots$$

Autrement dit, après $k'$ étapes, le FCSR a pour coefficients de sorties à l'infini $p-1$. Comme $k' \leq k$, alors après $k=[\log_p(m_{r-1}+1)]$ étapes le FCSR a pour coefficient de sorties à l'infini $p-1$.
Si $q=p^r-1$ alors $\frac{|s|}{q}<(m_{r-1}+1)\frac{p^r}{p^r-1}$. Le FCSR a pour coefficient de sorties à l'infini $p-1$.
Supposons $q=p^r-1$, alors $\frac{|s|}{q}<(m_{r-1}+1)\frac{p^r}{p^r-1}$. Le dernier coefficient non nul dans le développement $p$-adique de $\frac{|s|}{q}$ est d'indice $[\log_p(\frac{|s|}{q})]$. On a donc

$$[\log_p\Big(\frac{|s|}{q}\Big)]<[\log_p(m_{r-1}+1)+\log_p\Big(\frac{p^r}{p^r-1}\Big)].$$

On démontre que pour tout $a$ et $b$, $[a+b] \leq [a]+[b]+1$ et que pour tout $r \geq 1$, $\dfrac{p^r}{p^r-1} \leq \dfrac{p}{p-1}$. On en déduit que

$$\begin{aligned}
[\log_p\Big(\tfrac{|s|}{q}\Big)] &< [\log_p(m_{r-1}+1)]+[\log_p\Big(\tfrac{p}{p-1}\Big)]+1 \\
&< [\log_p(m_{r-1}+1)]+[1-\log_p(p-1)]+1 \\
&< [\log_p(m_{r-1}+1)]+1 \\
&\leq [\log_p(m_{r-1}+1)].
\end{aligned}$$

Par les mêmes arguments que précédemment, en posant $k = [\log_p(m_{r-1}+1)]$, l'écriture $p$-adique de $\frac{s}{q}$ est de la forme

$$a_0 + a_1 p + \ldots + (p-1)p^{k+1} + (p-1)p^{k+2} + \ldots$$

Autrement dit, après au plus $[\log_p(m_{r-1}+1)]$ étapes, le FCSR a pour coefficient de sorties $p-1$ à l'infini.
Si $m_{r-1} < 0$ et si $\alpha < 0$, alors $m_{r-1} \leq -1$ et $s < 0$. On en déduit que

$$\begin{aligned} \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) &< m_{r-1}p^r + \sum_{i=0}^{i=r-1} a_i p^i \\ &\leq -p^r + p^r - 1 \\ &< 0. \end{aligned}$$

C'est absurde car le membre de gauche est positif ou nul.
Si $m_{r-1} < 0$ et si $\alpha > 0$, alors l'état final est $(0, \ldots, 0, 0)$. On en déduit que

$$s = |s| \leq |m_{r-1}|p^r + \Big| \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} q_i a_j p^{i+j} - \sum_{i=0}^{i=r-1} a_i p^i \Big|.$$

$$\begin{aligned} -\sum_{i=0}^{i=r-1} p^i \leq \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} q_i a_j p^{i+j} - \sum_{i=0}^{i=r-1} a_i p^i &\leq \sum_{i=1}^{i=r-1} q_i p^i \sum_{j=0}^{j=r-i-1} p^j \\ -\frac{p^r-1}{p-1} \leq &\leq \sum_{i=1}^{i=r-1} q_i p^i - \frac{p^{r-i}-1}{p-1} \\ -p^r < &\leq \sum_{i=1}^{i=r-1} q_i p^i p^{r-i} \\ -p^r < &\leq \sum_{i=1}^{i=r-1} q_i p^r \\ -p^r < \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} q_i a_j p^{i+j} - \sum_{i=0}^{i=r-1} a_i p^i &\leq (w-q_r)p^r. \end{aligned}$$

Cet encadrement permet de dire que $-(1+m_{r-1})p^r < s \leq (w-q_r-m_{r-1})p^r$ et donc que $|s| \leq \max\{(1-m_{r-1}), w-q_r-m_{r-1}\}\, p^r$.

Supposons que pour tout $1 \leq i \leq r-1$, $q_i = 0$, alors $s = -m_{r-1}p^r - \sum_{i=1}^{i=r-1} a_i p^i$ et $q = q_r p^r - 1$. Comme $m_{r-1} < 0$, alors $-m_{r-1} \geq 1$. Supposons que $s < 0$, alors :

$$\begin{aligned} s < 0 &\Rightarrow -m_{r-1}p^r - \textstyle\sum_{i=0}^{i=r-1} a_i p^i < 0 \\ &\Rightarrow p^r \leq -m_{r-1}p^r < \textstyle\sum_{i=0}^{i=r-1} a_i p^i \leq p^r - 1 \\ &\Rightarrow p^r < p^r - 1. \end{aligned}$$

C'est donc absurde. Ainsi $s > 0$, donc

$$0 < s \leq -m_{r-1}p^r \Rightarrow 0 < \alpha \leq \frac{-m_{r-1}p^r}{q_r p^r - 1} \leq -m_{r-1}\frac{p^r}{p^r - 1}.$$

D'après le développement de Hensel de $-m_{r-1}\frac{p^r}{p^r-1}$, après $\log_p(-m_{r-1}\frac{p^r}{p^r-1})$ étapes, les coefficients de sorties sont tous nuls.
Supposons qu'il existe $i \neq r$ tel que $q_i \neq 0$, alors

$$w \geq q_r + 1 \Rightarrow (w - q_r)p^r \geq p^r \Rightarrow (-m_{r-1} + w - q_r) \geq 1 - m_{r-1}.$$

Ainsi $0 \leq s \leq (-m_{r-1} + w - q_r)p^r$ et $q > q_r p^r - 1 \geq p^r - 1$. Donc $q \geq p^r$ et $0 \leq \alpha(-m_{r-1} + w - q_r)$. On en déduit qu'après $[\log_p(-m_{r-1} + w - q_r)] + 1$ étapes, tous les coefficients de sorties sont nuls.
Si $m_{r-1} = 0$, alors

$$s = \sum_{i=1}^{i=r} \sum_{j=0}^{j=r-i-1} q_i a_j p^{i+j} - \sum_{i=0}^{i=r-1} a_i 2^i \quad .$$
$$-(p^r - 1) \leq s \leq q(p^r - 1).$$

Comme $q_r \neq 0$, alors $q \geq q_r p^r - 1 \geq p^r - 1$.

$$-1 \leq -\frac{p^r - 1}{q} \leq \alpha \leq p^r - 1.$$

Si $\alpha = -1$, alors la séquence de sorties est $(p-1, p-1, \ldots)$. On peut calculer les mémoires du registre.

$$\begin{array}{rcrcl} \sigma_r = w(p-1) & \Rightarrow & m_r = (p-1)\frac{(w-1)}{p} & \Rightarrow & p/w - 1 \\ \sigma_{r+1} = w(p-1) + \frac{(w-1)(p-1)}{p} & \Rightarrow & m_{r+1} = (p-1)(p+1)\frac{(w-1)}{p^2} & \Rightarrow & p^2/w - 1 \\ \vdots & & \vdots & & \end{array}$$

Par récurrence, on trouve que pour tout $n$, $p^n$ divise $w - 1$, donc $w = 1$. Toutes les mémoires sont nulles, tous les coefficients de connexion sont nuls sauf $q_r$ et tous les coefficients de la séquence de sorties sont égaux à $p - 1$.
Si $\alpha = 0$, alors la séquence de sorties est nulle, les mémoires sont nulles.
Sinon $1 \leq \alpha \leq p^r - 1$, alors la séquence de sorties n'est pas nulle. On en déduit que l'état initial n'est pas nul non plus, puisque s'il était nul, la mémoire initiale étant nulle, on aurait une séquence de sorties nulle. Soit $e$ le dernier état tel qu'il existe un coefficient $a_i$ du registre principal non nul. Alors $e$ s'écrit

$$e = (c, 0 \ldots, 0, m)$$

avec $c \neq 0$. Supposons toutes les mémoires nulles, donc l'état suivant est nul. Or l'état suivant est

$$(0, \ldots, 0, \frac{cq_r}{p}).$$

On en déduit que $cq_r = 0$. On a supposé $q_r$ et $c$ non nuls, c'est donc absurde. Supposons alors qu'il existe une mémoire non-nulle. Soit $e^{'}$ le dernier état tel que la mémoire soit non-nulle. On l'écrit

$$e^{'} = (*, \ldots, *, m^{'})$$

avec $m^{'} \neq 0$. Si $e = e^{'}$, alors l'état suivant est nul et est égal à

$$(0, \ldots, (cq_r + m) \pmod p, \frac{cq_r + m}{p}).$$

Donc $m = -cq_r < 0$, ce qui est absurde. Si $e$ précède $e^{'}$, alors

$$e^{'} = (0, \ldots, 0, m^{'}).$$

L'état suivant est nul et est de la forme $(0, \ldots 0, \frac{m^{'}}{p})$. Donc $m^{'} = 0$, ce qui est absurde. Si $e^{'}$ précède $e$, alors

$$e = (c, 0, \ldots, 0, 0).$$

L'état suivant est nul et est de la forme $(0, \ldots, 0, \frac{q_r c}{p})$. Donc $q_r c = 0$, ce qui est absurde. □

## 6.10 Un exemple

Considérons le FCSR $\mathcal{F} = (\mathbb{F}_2, 5, 53)$ avec $53 = 2^5+2^4+2^2+2-1$. La figure 6.2 illustre ce FCSR. En chargeant l'état initial $(a_0, a_1, a_2, a_3, a_4, m_1) = (1, 0, 1, 1, 0, 6)$, on obtient en sortie une $l$-séquence de période 52 illustrée dans le tableau 6.1. C'est une séquence ultimement périodique de pré-période 2. On observe bien que la mémoire décroit puis reste dans l'intervalle $[0, w-1]$ avec $w = 4$.

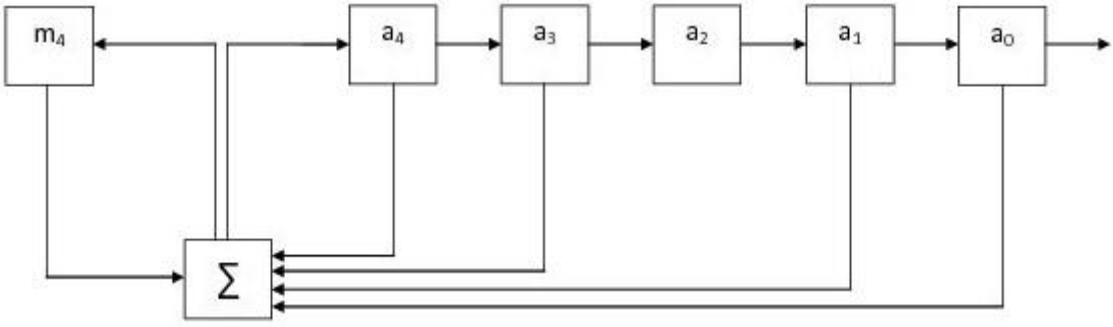



FIGURE 6.2 – FCSR de taille 5 et d'entier de connexion $q = 53$.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_i$ | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| $m_{i+1}$ | 6 | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 2 | 2 |
| $i$ | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| $a_i$ | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| $m_{i+1}$ | 1 | 2 | 2 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 3 | 2 |
| $i$ | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 |
| $a_i$ | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| $m_{i+1}$ | 2 | 2 | 2 | 2 | 1 | 1 | 2 | 1 | 1 | 2 | 2 | 2 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 |
| $i$ | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 |
| $a_i$ | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| $m_{i+1}$ | 2 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 2 | 2 | 1 | 1 | 1 | 0 | 0 |

TABLE 6.1 – séquence de sorties pour l'état initial $(1, 0, 1, 1, 0, 6)$.

## 6.11 $l$-séquences

### 6.11.1 Définitions et Existence

Dans la génération de séquences pseudo-aléatoires, on cherche à obtenir en sortie des séquences avec une période maximale. Pour un LFSR de taille $r$ sur le corps premier $\mathbb{F}_p$, la période ne peut dépasser $p^r - 1$. Les séquences dont la période atteint cette limite sont appelées $m$-séquences (maximal sequences). Elles sont obtenues en utilisant un polynôme primitif sur $\mathbb{F}_p$ comme polynôme de connexion pour le LFSR.

Dans le cas d'un FCSR $(\mathbb{F}_p, r, q)$, d'après le corollaire 6.5.1, la période divise l'ordre de $p$ modulo $q$. Le groupe multiplicatif des éléments inversibles de l'anneau quotient $\mathbb{Z}/q\mathbb{Z}$ est de cardinal $\phi(q)$ où $\phi$ est la fonction indicatrice d'Euler. L'ordre d'un élément divise l'ordre du groupe, donc l'ordre de $p$ modulo $q$ divise $\phi(q)$. Soit $\underline{a}$ une séquence engendrée par le FCSR $(\mathbb{F}_p, r, q)$, alors

$$\mathtt{per}(\underline{a}) \mid \mathtt{ord}_q(p) \mid \phi(q) \leq q - 1.$$

**Proposition 6.11.1.** *Soit un FCSR $(\mathbb{F}_p, r, q)$. Soit $\underline{a}$ une séquence de sorties strictement périodique. La période de $\underline{a}$ est maximale ($\mathtt{per}(\underline{a}) = q-1$) si et seulement si $q$ est premier, $p$ est une racine primitive modulo $q$ et $\underline{a}$ est différente de $(0, 0, \ldots)$ et de $(p-1, p-1, \ldots)$.*

*Démonstration.* Si $\mathtt{per}(\underline{a})$ est maximale, alors $\mathtt{per}(\underline{a}) = q - 1$. Donc $\underline{a} \neq (0, 0, \ldots)$ et $\underline{a} \neq (p - 1, p - 1, \ldots)$. On en déduit aussi que

$$\mathtt{per}(\underline{a}) = \mathtt{ord}_q(p) = \phi(q) = q - 1.$$

si $\phi(q) = q - 1$, alors $|(\mathbb{Z}/q\mathbb{Z})^*| = q - 1$. Donc tout entier non nul strictement inférieur à $q$ est premier avec $q$, ce qui signifie que $q$ est premier. Si $\mathtt{ord}_q(p) = \phi(q)$, alors la classe de $p$ génère le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^*$. On dit que $p$ est une racine primitive modulo $q$. La séquence $\underline{a}$ étant strictement périodique, son entier 2-adique associé vérifie $-1 \leq \frac{s}{q} \leq 0$. Si $s = -q$, alors la séquence de sorties est $(p - 1, p - 1, \ldots)$. Si $s = 0$, alors la séquence de sorties est $(0, 0, \ldots)$. Si $-q < s < 0$, alors $s$ et $q$ sont premiers entre eux. D'après le corollaire 6.5.1, la période de la séquence de sorties est $\mathtt{ord}_q(p)$. Comme la séquence est de période maximale, on est dans ce dernier cas.

Supposons l'inverse. Si $q$ est premier et $p$ est racine primitive modulo $q$, alors $\mathtt{ord}_q(p) = \phi(q) = q-1$. La séquence de sorties est strictement croissante alors $-q \leq s \leq 0$.

$$\begin{aligned} s = 0 &\Leftrightarrow \underline{a} = (0,0,\ldots) \\ s = -q &\Leftrightarrow \underline{a} = (p-1, p-1, \ldots). \end{aligned}$$

La séquence est supposée différente de ces deux séquences qui correspondent aux deux états initiaux dégénérés. Donc $-q < s < 0$. Ainsi $s$ est premier à $q$, donc la période est $\mathtt{ord}_q(p)$. La période est maximale □

Si on se donne un FCSR $(\mathbb{F}_p, r, q)$, pour que la période de la séquence de sorties atteigne le maximum $q-1$, $q$ doit être un nombre premier avec $p$ comme racine primitive modulo $q$. L'existence de tels nombres est un problème ouvert.

D'un point de vue théorique, si on fixe un nombre premier $p$, l'existence de nombre premier $q$ dont $p$ est une racine primitive est l'objet de conjecture. La conjecture d'Artin affirme que le nombre de $q$ premiers inférieur ou égal à un $n$ fixé avec 2 pour racine primitive modulo $q$ est à peu prés $0.374\frac{n}{\log(n)}$. Autrement dit 37.4 pour cent des nombres premiers admettent 2 pour racine primitive. Hooley démontre que si l'hypothèse de Riemann étendue à la fonction zêta de Dedekind est vraie alors la conjecture d'Artin est vraie.

Si on fixe un nombre premier $q$, il y a $\phi(q-1)$ racines primitives modulo $q$. Ils peuvent être générés par des programmes informatiques simples. On dispose de liste déjà faite de nombres premiers $q$ admettant comme racine primitive un nombre premier $p$ (Hua Loo Keng, Introduction to Number Theory, page 52-56). Goresky et Klapper fournissent une liste de nombre premier $q$ dont $p$ est racine primitive pour $p = 2, 3, 5$ et 7.

$q-1$ est la période maximale, cependant d'autres cas engendrent des séquences avec de très grande période. La période divise $\mathtt{ord}_q(p)$ qui divise $\phi(q)$, on cherche alors les nombres $q$ tels que $\mathtt{ord}_q(p) = \phi(q)$. Autrement dit, la classe de $p$ est un générateur du groupe cyclique $(\mathbb{Z}/q\mathbb{Z})^*$. Or $(\mathbb{Z}/q\mathbb{Z})^*$ est cyclique si et seulement si $q = 1, 2, 4, n^k$ ou $2n^k$ où $n$ est premier impair et $k$ est un entier. Pour tout $q$ de cette forme, il existe $\phi(\phi(q))$ racines primitives modulo $q$. Avec des programmes informatiques simples, on peut générer les racines primitives modulo un entier fixé. Pour les cas $q = 1, 2, 4$, on connait les racines primitives. Pour le cas $q = 2n^k$, le groupe multiplicatif $(\mathbb{Z}/2n^k\mathbb{Z})^*$ est isomorphe à $(\mathbb{Z}/n^k\mathbb{Z})^*$. En effet :

**Proposition 6.11.2.** *Soit $n$ et $m$ deux entiers naturels premiers entre eux. Alors*

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

*et*

$$(\mathbb{Z}/nm\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*.$$

*Démonstration.* L'application

$$\begin{aligned} \rho : \mathbb{Z}/nm\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ x \mod nm &\mapsto (x \mod n, x \mod m) \end{aligned}$$

est bien définie et est un homomorphisme d'anneaux. L'application $\rho$ est injective car

$$\begin{array}{rcl} \rho(x) = 0 & \Leftrightarrow & x \mod n = 0 \text{ et } x \mod m = 0 \\ & \Leftrightarrow & n \mid x \text{ et } m \mid x \\ n \text{ et } m \text{ premiers entre eux} & \Rightarrow & nm \mid x \\ & \Rightarrow & x \mod nm = 0. \end{array}$$

Par cardinalité, elle est aussi surjective. C'est donc un isomorphisme d'anneaux. Si la classe de $x$ modulo $nm$ est inversible alors la classe de $x$ modulo $n$ et la classe de $x$ modulo $m$ sont aussi inversibles. Inversement, soit un couple $(y \mod n, z \mod m)$ inversible dans le produit direct $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Il possède un inverse noté $(y^{-1} \mod n, z^{-1} \mod m)$ et un antécédent $x \mod nm$ tels que $\rho(x \mod nm) = (y \mod n, z \mod m)$. De même pour l'inverse, il existe un antécédent $t \mod nm$ tel que $\rho(t \mod nm) = (y^{-1} \mod n, z^{-1} \mod m)$.

$$\begin{array}{rcl} \rho(xt \mod nm) & = & \rho(x \mod nm \times t \mod nm) \\ & = & \rho(x \mod nm) \times \rho(t \mod nm) \\ & = & (y \mod n, z \mod m) \times (y^{-1} \mod n, z^{-1} \mod m) \\ & = & (1,1) \\ & = & \rho(1). \end{array}$$

Par bijectivité, $xt \mod nm = 1$. Donc les sous-groupes multiplicatifs $(\mathbb{Z}/nm\mathbb{Z})^*$ et $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ sont isomorphes. □

Ainsi, comme $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$, alors $(\mathbb{Z}/2n^k\mathbb{Z})^* \cong (\mathbb{Z}/n^k\mathbb{Z})^*$. On peut donc se restreindre au cas $q = n^k$ avec $n$ un nombre premier impair. Pour ce cas là, il existe un moyen simple pour vérifier si $p$ est une racine primitive modulo.

**Lemme 6.11.1.** *Soient $n$ un nombre premier, $p$ un entier, $j$ et $k$ deux entiers naturels. Alors*

$$p \in (\mathbb{Z}/n^k\mathbb{Z})^* \Leftrightarrow p \in (\mathbb{Z}/n^j\mathbb{Z})^*.$$

*Démonstration.* Nous allons montrer que $p$ est inversible dans $\mathbb{Z}/n^k\mathbb{Z}$ si et seulement si $p$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

$$p \in (\mathbb{Z}/n^k\mathbb{Z})^* \Leftrightarrow \exists u \in \mathbb{Z}/n^k\mathbb{Z}; n^k \mid pu - 1 \Rightarrow n \mid pu - 1 \Rightarrow p \in (\mathbb{Z}/n\mathbb{Z})^*.$$

Supposons que $p \in (\mathbb{Z}/n^k\mathbb{Z})^*$. il existe donc $u$ et $v$ tels que $n^k v = pu - 1$.

$$(pu)^n = (1 + n^k v)^n = 1 + \sum_{i=1}^{i=n-1} \mathcal{C}_n^i (n^k v)^i + n^{kn} v^n.$$

Comme $n$ est premier, $n$ divise $\mathcal{C}_n^i$ pour $1 \leq i \leq n-1$.
Donc $n^{k+1}$ divise $\sum_{i=1}^{i=n-1} \mathcal{C}_n^i (n^k v)^i + n^{kn} v^n$. Il existe alors un inverse de $p$ modulo $n^{k+1}$. En effet, on a

$$n^{k+1} \mid p.p^{n-1} u^n - 1.$$

Par récurrence, on vient de montrer que

$$p \in (\mathbb{Z}/n\mathbb{Z})^* \Rightarrow p \in (\mathbb{Z}/n^2\mathbb{Z})^* \Rightarrow \dots p \in (\mathbb{Z}/n^k\mathbb{Z})^* \dots$$

□

**Proposition 6.11.3.** *Soient $p$ un entier, $n$ un nombre premier impair et $q = n^e$ avec $e \geq 3$. alors $p$ est une racine primitive modulo $q$ si et seulement si $p$ est une racine primitive modulo $n^2$. L'entier $p$ est une racine primitive modulo $n^2$ si et seulement si $p$ est une racine primitive modulo $n$ et $n^2$ ne divise pas $p^{n-1} - 1$.*

*Démonstration.* Si $p$ est une racine primitive modulo $q$, alors c'est un inversible modulo $q$ et d'après le lemme précédent, $p$ est aussi un inversible modulo $n^2$. Il reste à montrer que c'est bien une racine primitive modulo $n^2$. Comme $p$ est une racine primitive modulo $q$, cela signifie que pour tout entier $b \in (\mathbb{Z}/q\mathbb{Z})^*$, il existe un entier $t$ tel que $b \equiv p^t \mod q$. On a alors

$$\begin{array}{rcl} b \equiv p^t \mod q & \Rightarrow & q \mid (b - p^t) \\ & \Rightarrow & n^2 \mid (b - p^t) \\ & \Rightarrow & b \equiv p^t \mod n^2 \end{array}$$

Donc pour tout entier $b \in (\mathbb{Z}/n^2\mathbb{Z})^*$, il existe un $t$ tel que $b = p^t$ modulo $n^2$ ce qui signifie que $p$ génère $(\mathbb{Z}/n^2\mathbb{Z})^*$, c'est donc une racine primitive modulo $n^2$.

De même, si $p$ est une racine primitive modulo $n^2$, $p$ est aussi racine primitive modulo $n$, par le même argument.

Inversement supposons que $p$ soit une racine primitive modulo $n^2$, donc $p$ génère $(\mathbb{Z}/n^2\mathbb{Z})^*$ et son ordre est $\mathtt{ord}_{n^2}(p) = n(n-1)$. L'entier $p$ est un inversible modulo $n^3$. Donc son ordre $\mathtt{ord}_{n^3}(p)$ divise l'ordre du groupe $(\mathbb{Z}/n^3\mathbb{Z})^*$ qui est $n^2(n-1)$. Il existe $m$ tel que $\mathtt{ord}_{n^3}(p)m = n^2(n-1)$. Le groupe $(\mathbb{Z}/n^3\mathbb{Z})^*$ est cyclique, il admet donc un générateur qu'on notera encore $b$. Il existe un entier $t$ tel que $p \equiv b^t \mod n^3$. On a alors

$$\begin{array}{rcl} p^{\frac{n^2(n-1)}{m}} \equiv 1 \mod n^3 & \Rightarrow & b^{t\frac{n^2(n-1)}{m}} \equiv 1 \mod n^3 \\ & \Rightarrow & n^2(n-1) \mid \frac{t}{m} n^2(n-1) \\ & \Rightarrow & m \mid t \end{array}$$

Comme $b$ est primitif modulo $n^3$, il l'est aussi modulo $n^2$. Donc

$$\begin{array}{rcl} b^{n(n-1)} \equiv 1 \mod n^2 & \Rightarrow & b^{\frac{t}{m}n(n-1)} \equiv 1 \mod n^2 \\ & \Rightarrow & p^{\frac{n(n-1)}{m}} \equiv 1 \mod n^2 \\ & \Rightarrow & n(n-1) \mid \frac{n(n-1)}{m} \\ & \Rightarrow & m = 1 \\ & \Rightarrow & \mathtt{ord}_{n^3}(p) = n^2(n-1). \end{array}$$

Par récurrence et en utilisant le même argument, on prouve que $p$ est aussi racine primitive modulo $q$. C'est ce qu'il fallait démontrer.

D'autre part, il reste à démontrer une partie de la dernière assertion. Si $p$ est racine primitive modulo $n^2$, alors $\mathtt{ord}_{n^2}(p) = n(n-1)$, donc $p^{n-1} \not\equiv 1 \mod n^2$ sinon $n(n-1)$ diviserait $n-1$. On en déduit que $n^2$ ne divise pas $p^{n-1} - 1$.

Inversement supposons que $p$ soit racine primitive modulo $n$ et $n^2$ ne divise pas $p^{n-1}-1$. Alors $p$ est inversible modulo $n$, il est donc inversible modulo $n^2$, ce qui implique que $p^{n(n-1)} \equiv 1 \mod n^2$. On en déduit que $\mathtt{ord}_{n^2}(p) \mid n(n-1)$. Donc il existe $k$ tel que $\mathtt{ord}_{n^2}(p)k = n(n-1)$. Si $n \nmid \mathtt{ord}_{n^2}(p)$, alors $n \mid k$ et $\mathtt{ord}_{n^2}(p) \mid n-1$ et $n^2$ divise $p^{n-1}-1$, ce qui contredit les hypothèses de départ. Si $n \mid \mathtt{ord}_{n^2}(p)$, alors $k$ et $n$ sont premiers entre eux. dans ce cas, $k \mid n-1$. Donc $\mathtt{ord}_{n^2}(p) = n\frac{n-1}{k}$. Le groupe $(\mathbb{Z}/n^2\mathbb{Z})^*$ est cyclique, donc il admet un générateur $b$. Il existe $t$, tel que $p = b^t \mod n^2$. On a alors :

$$\begin{array}{lll} p^{n\frac{n-1}{k}} \equiv 1 \mod n^2 & \Rightarrow & b^{tn\frac{n-1}{k}} \equiv 1 \mod n^2 \\ & \Rightarrow & tn\frac{n-1}{k} \mid \mathtt{ord}_{n^2}(b) = n(n-1) \\ & \Rightarrow & k \mid t. \end{array}$$

$b$ est aussi une racine primitive modulo $n$. Donc

$$b^{n-1} \equiv 1 \mod n \Rightarrow b^{t\frac{n-1}{k}} \equiv 1 \mod n \Rightarrow p^{\frac{n-1}{k}} \equiv 1 \mod n$$

Rappelons que par hypothèse $p$ est une racine primitive modulo $n$, donc $\mathtt{ord}_n(p) = n-1$ $\frac{n-1}{k}$. Donc $k = 1$ et $\mathtt{ord}_{n^2}(p) = n(n-1)$. On en conclut que $p$ est une racine primitive modulo $n^2$. □

Il est donc simple de vérifier si $p$ est une racine primitive modulo $q$ quand $q$ est puissance d'un nombre premier impaire.

**Définition 6.11.1** ($l$-séquence)**.** *Une $l$-séquence est une séquence strictement périodique $\underline{a}$, non-triviale, générée par un FCSR d'entier de connexion $q$ puissance d'un nombre premier dont $p$ est racine primitive modulo $q$ telle que $\underline{a}$ soit de période $\phi(q)$.*

En règle générale, on s'intéressera surtout aux $l$-séquences de période $q-1$, c'est à dire au cas où $q$ est premier. Un exemple puissant est l'entier de connexion

$$q = 2^{128} + 2^5 + 2^4 + 2^2 - 1.$$

Cet entier est premier et 2 est une racine primitive modulo $q$. Donc les séquences de sorties d'un FCSR de cet entier de connexion seront de période $2^{128} + 2^5 + 2^4 + 2$ !

### 6.11.2 Tableaux de valeurs d'entiers de connexion de $l$-séquences

Goresky et Klapper fournissent une liste de nombres premiers avec la plus petite racine primitive et classés suivant leur longueur $p$-adique. Les trois premiers tableaux concernent les nombres premiers $q$ dont 2 est racine primitive modulo $q$ de longueur 2-adique inférieure ou égale à 13. Ces nombres définissent des FCSRs de taille inférieure ou égale à 13 qui génèrent des $l$-séquences binaires. Le dernier tableau donnent les nombres premiers $q$ inférieurs à 10000 dont 3 est racine primitive modulo $q$. Ces nombres définissent des FCSRs d'entier de connexion inférieur à 10000 qui génèrent des $l$-séquences 3-aires.

| $[\log_2(q)]$ | $q$ |
|---|---|
| 1 | 3 |
| 2 | 5 |
| 3 | 11, 13 |
| 4 | 19, 29 |
| 5 | 37, 53, 59, 61 |
| 6 | 67, 83, 101, 107 |
| 7 | 131, 139, 149, 163, 173, 179, 181, 197, 211, 227 |
| 8 | 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461, 467, 491, 509 |
| 9 | 523, 541, 547, 557, 563, 587, 613, 619, 653, 659, 661,<br>677, 701, 709, 757, 773, 787,<br>797, 821, 827, 829, 853, 859 , 877, 883 , 907, 941, 947, 1019 |
| 10 | 1061, 1091, 1109, 1117, 1123, 1171, 1187, 1213, 1229,<br>1237, 1259, 1277, 1283, 1291,<br>1301, 1307, 1373, 1381, 1427, 1451, 1453, 1483, 1493, 1499,<br>1523, 1531, 1549, 1571,<br>1619, 1621, 1637, 1667, 1669, 1693, 1733, 1741, 1747, 1787,<br>1861, 1867, 1877, 1901,<br>1907, 1931, 1949, 1973, 1979, 1987, 1997, 2027, 2029 |
| 11 | 2053, 2069, 2083, 2099, 2131, 2141, 2213, 2221, 2237, 2243, 2267, 2269,<br>2293, 2309,2333, 2339, 2357, 2371, 2389, 2437, 2459, 2467, 2477, 2531,<br>2539, 2549, 2557, 2579,2621, 2659, 2677, 2683, 2693, 2699, 2707, 2741,<br>2789, 2797, 2803, 2819, 2837, 2843,2851, 2861, 2909, 2939, 2957, 2963,<br>3011, 3019, 3037, 3067, 3083, 3187, 3203, 3253,3299, 3307, 3323, 3347,<br>3371, 3413, 3461, 3467, 3469, 3491, 3499, 3517, 3533, 3539,3547, 3557,<br>3571, 3581, 3613, 3637, 3643, 3659, 3677, 3691, 3701, 3709, 3733, 3779,<br>3797, 3803, 3851, 3853, 3877, 3907, 3917, 3923, 3931, 3947,<br>3989, 4003, 4013, 4019,4021, 4091, 4093 |

TABLE 6.2 – Valeurs de $q$ premier avec 2 racines primitives et de longueur $\leq 11$

| $[\log_2(q)]$ | $q$ |
|---|---|
| 12 | 4099, 4133, 4139, 4157, 4219, 4229, 4243, 4253, 4259,<br>4261, 4283, 4349, 4357, 4363,<br>4373, 4397, 4451, 4483, 4493, 4507, 4517, 4547, 4603, 4621,<br>4637, 4691, 4723, 4787,<br>4789, 4813, 4877, 4933, 4957, 4973, 4987, 5003, 5011, 5051,<br>5059, 5077, 5099, 5107,<br>5147, 5171, 5179, 5189, 5227, 5261, 5309, 5333, 5387, 5443,<br>5477, 5483, 5501, 5507,<br>5557, 5563, 5573, 5651, 5659, 5683, 5693, 5701, 5717, 5741,<br>5749, 5779, 5813, 5827,<br>5843, 5851, 5869, 5923, 5939, 5987, 6011, 6029, 6053, 6067,<br>6101, 6131, 6173, 6197,<br>6203, 6211, 6229, 6269, 6277, 6299, 6317, 6323, 6373, 6379,<br>6389, 6397, 6469, 6491,<br>6547, 6619, 6637, 6653, 6659, 6691, 6701, 6709, 6733, 6763,<br>6779, 6781, 6803, 6827,<br>6829, 6869, 6883, 6899, 6907, 6917, 6947, 6949, 6971, 7013,<br>7019, 7027, 7043, 7069,<br>7109, 7187, 7211, 7219, 7229, 7237, 7243, 7253, 7283, 7307,<br>7331, 7349, 7411, 7451,<br>7459, 7477, 7499, 7507, 7517, 7523, 7541, 7547, 7549, 7573,<br>7589, 7603, 7621, 7643,<br>7669, 7691, 7717, 7757, 7789, 7829, 7853, 7877, 7883, 7901,<br>7907, 7933, 7949, 8053,<br>8069, 8093, 8117, 8123, 8147, 8171, 8179 |

TABLE 6.3 – Valeurs de $q$ premier avec 2 racines primitives et de longueur 12

| $[\log_2(q)]$ | $q$ |
|---|---|
| 13 | 8219, 8221, 8237, 8243, 8269, 8291, 8293, 8363, 8387,<br>8429, 8443, 8467, 8539, 8563,8573, 8597, 8627, 8669, 8677,<br>8693, 8699, 8731, 8741, 8747,8803, 8819, 8821, 8837,<br>8861, 8867, 8923, 8933, 8963, 8971, 9011, 9029, 9059, 9173,<br>9181, 9203, 9221, 9227,9283, 9293, 9323, 9341, 9349,<br>9371, 9397, 9419, 9421, 9437,<br>9467, 9491, 9533, 9539, 9547, 9587, 9613, 9619, 9629,<br>9643, 9661, 9677, 9733, 9749,9803, 9851, 9859, 9883,<br>9901, 9907, 9923, 9941, 9949, 10037, 10067, 10069, 10091,<br>10093, 10099, 10133, 10139,10141, 10163, 10181, 10253, 10259,<br>10267, 10301, 10331,10357, 10427, 10459, 10477,<br>10499, 10501, 10589, 10613, 10667, 10691, 10709, 10723,<br>10733, 10789, 10837, 10853,10859, 10861, 10867, 10883, 10891,<br>10909, 10949, 10973,10979, 10987, 11003, 11027,<br>11069, 11083, 11093, 11131, 11171, 11197, 11213, 11261,<br>11317, 11437, 11443, 11483,11549, 11579, 11587, 11621,<br>11677, 11699, 11717, 11779,11789, 11813, 11821, 11827,<br>11867, 11909, 11933, 11939, 11981, 11987, 12011, 12043,<br>12107, 12149, 12157, 12197,12203, 12211, 12227, 12251,<br>12253, 12269, 12277, 12301,12323, 12347, 12373, 12379,<br>12413, 12437, 12491, 12539, 12547, 12589, 12611, 12613,<br>12619, 12637, 12653, 12659,12739, 12757, 12763, 12781,<br>12821, 12829, 12899, 12907,12917, 12923, 12941, 12979,<br>13037, 13043, 13109, 13147, 13163, 13187, 13229, 13291,<br>13331, 13339, 13397, 13411,13451, 13469, 13477, 13523,<br>13613, 13619, 13627, 13691,13709, 13723, 13757, 13763,<br>13829, 13859, 13877, 13883, 13901, 13907, 13931, 13933,<br>13997, 14011, 14051, 14107,14173, 14221, 14243, 14341,<br>14387, 14389, 14411, 14419,14461, 14533, 14549, 14557,<br>14621, 14627, 14629, 14653, 14669, 14699, 14717, 14723,<br>14741, 14747, 14771, 14797,14813, 14821, 14827, 14843,<br>14851, 14867, 14869, 14891,14923, 14939, 14947, 14957,<br>15013, 15053, 15061, 15077, 15083, 15091, 15101, 15107,<br>15131, 15139, 15149, 15173,15187, 15227, 15259, 15269,<br>15299, 15331, 15349, 15373,15413, 15427, 15443, 15461,<br>15581, 15629, 15661, 15667, 15683, 15731, 15739, 15749,<br>15773, 15787, 15797, 15803,15859, 15907, 15923, 15971,<br>16067, 16069, 16139, 16187,16189, 16229, 16253, 16301,<br>16333, 16339, 16349, 16363, 16381 |

TABLE 6.4 – Valeurs de $q$ premier avec 2 racines primitives et de longueur 13

| $[\log_3(q)]$ | $q$ |
|---|---|
| 1 | 5, 7 |
| 2 | 17, 19 |
| 3 | 29, 31, 43, 53, 79 |
| 4 | 89, 101, 113, 127, 137, 139, 149, 163, 173, 197, 199, 211, 223, 233 |
| 5 | 257, 269, 281, 283, 293, 317, 331, 353, 379, 389, 401, 449, 461, 463, 487, 509, 521, 557,569, 571, 593, 607, 617, 631, 641, 653, 677, 691, 701 |
| 6 | 739, 751, 773, 797, 809, 811, 821, 823, 857, 859, 881, 907, 929, 941, 953, 977, 1013,1039,1049, 1061, 1063, 1087, 1097, 1109, 1123, 1193, 1217, 1229, 1231, 1277, 1279,1291, 1301, 1327, 1361, 1373, 1409, 1423, 1433, 1447, 1459, 1481, 1483, 1493, 1553,1567, 1579, 1601, 1613, 1627, 1637, 1663, 1697, 1699, 1709, 1721, 1723, 1733, 1747,1831, 1889, 1901, 1913, 1949, 1951, 1973, 1987, 1997, 1999, 2011, 2069, 2081, 2083,2129, 2141, 2143, 2153 |
| 7 | 2213, 2237, 2239, 2273, 2309, 2311, 2333, 2347, 2357, 2371, 2381, 2393, 2417, 2467, 2477, 2503, 2539, 2549, 2609, 2633, 2647, 2657, 2659, 2683, 2693, 2707, 2719, 2729,2731, 2741, 2753, 2767, 2777, 2789, 2801, 2837, 2861, 2897, 2909, 2957, 2969, 3041, 3089, 3137, 3163, 3209, 3257, 3259, 3271, 3307, 3329, 3331, 3389, 3391, 3413, 3449,3461, 3463, 3533, 3547, 3557, 3559, 3571, 3581, 3583, 3593, 3617, 3643, 3677, 3701,3727, 3761, 3797, 3821, 3823, 3833, 3917, 3919, 3929, 3931, 3943, 3989, 4001, 4003,4013, 4027, 4049, 4073, 4133, 4157, 4159, 4217, 4219, 4229, 4231, 4241, 4243, 4253,4289, 4327, 4337, 4349, 4363, 4373, 4397, 4409, 4421, 4423, 4447, 4457, 4481, 4493,4507, 4517, 4519, 4567, 4603, 4637, 4639, 4649, 4651, 4663, 4673, 4723, 4759, 4793,4817, 4831, 4877, 4889, 4903, 4937, 4973, 4987, 4999, 5009, 5021, 5023, 5081, 5119,5189, 5237, 5261, 5273, 5297, 5309, 5333, 5347, 5381, 5393, 5407, 5417, 5419, 5431,5441, 5443, 5477, 5479, 5503, 5563, 5573, 5647, 5657, 5669, 5683, 5693, 5717, 5741,5779, 5801, 5813, 5827, 5849, 5861, 5897, 5923, 5981, 6007, 6029, 6053, 6089, 6113,6151, 6163, 6173, 6197, 6199, 6221, 6257, 6269, 6317, 6329, 6343, 6353, 6367, 6379, 6389, 6427, 6449, 6451, 6473, 6547 |
| 8 | 6569, 6571, 6607, 6619, 6653, 6689, 6691, 6737, 6761, 6763, 6823, 6833, 6857, 6869, 6871, 6907, 6917, 6977, 7001, 7013, 7039, 7109, 7121, 7159, 7193, 7207, 7229, 7243, 7253, 7349, 7411, 7433, 7457, 7459, 7517, 7529, 7541, 7577, 7603, 7649, 7673, 7699, 7723, 7759, 7793, 7817, 7829, 7867, 7877, 7879, 7901, 7927, 7937, 7949, 8009, 8059, 8069, 8081, 8093, 8117, 8167, 8179, 8237, 8263, 8273, 8287, 8297, 8311, 8369, 8419, 8429, 8431, 8443, 8467, 8537, 8539, 8563, 8573, 8597, 8599, 8609, 8623, 8647, 8669, 8693, 8719, 8731, 8741, 8753, 8837, 8839, 8849, 8861, 8863, 8887, 8923, 8969, 8971, 9007, 9029, 9041, 9043, 9067, 9091, 9127, 9137, 9151, 9161, 9173, 9187, 9199, 9209, 9257, 9281, 9283, 9293, 9319, 9377, 9391, 9403, 9413, 9461, 9463, 9473, 9497, 9511, 9521, 9533, 9547, 9629, 9631, 9643, 9677, 9679, 9689, 9739, 9749, 9787, 9811, 9833,9871, 9883, 9907, 9929, 9967 |

TABLE 6.5 – Valeurs de $q$ premier avec 3 racines primitives et $q \leq 10000$

## 6.12 Propriétés de distribution et Décimations des $l$-séquences

Dans cette section, nous montrons quelques propriétés de distribution des $l$-séquences.

**Proposition 6.12.1.** *Soit $q$ un entier puissance d'un nombre premier impair $n$ dont $p$ est racine primitive modulo $q$. Soit $\underline{a}$ une $l$-séquence générée par le FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$. Alors pour toute période,*

$$a_{i+\frac{\pi(q)}{2}} = p - 1 - a_i.$$

*Démonstration.* Il existe un nombre premier $n$ impair et un entier $t$ tel que $q = n^t$. L'entier $p$ est racine primitive modulo $q$, donc $p^{\phi(q)} \equiv 1 \mod q$. L'entier $\pi(q) = n^{t-1}(n-1)$ est pair.

$$\begin{aligned} q \mid p^{\phi(q)} - 1 &\Rightarrow n^t \mid p^{\frac{\phi(q)}{2}} - 1 \\ &\Rightarrow n^t \mid (p^{\frac{\phi(q)}{2}} - 1)(p^{\frac{\phi(q)}{2}} + 1) \\ &\Rightarrow n \mid (p^{\frac{\phi(q)}{2}} - 1)(p^{\frac{\phi(q)}{2}} + 1). \end{aligned}$$

Le PGCD de $p^{\frac{\phi(q)}{2}} - 1$ et $p^{\frac{\phi(q)}{2}} + 1$ divise 2. En effet $(p^{\frac{\phi(q)}{2}} + 1 - (p^{\frac{\phi(q)}{2}} - 1) = 2$, tout diviseur commun divise 2. Si $n$ divise les deux alors $n$ divise 2, ce qui est absurde étant donné que $n$ est impair. Donc $n$ divise un seul parmi les deux facteurs. Il ne peut pas diviser $p^{\frac{\phi(q)}{2}} - 1$, car dans ce cas $n^t$ le divise aussi et donc $p$ est d'ordre divisant $\frac{\phi(q)}{2}$ modulo $q$, ce qui est absurde. Donc $n^t$ divise $p^{\frac{\phi(q)}{2}} + 1$. On a alors

$$p^{\frac{\phi(q)}{2}} \equiv -1 \mod q \Rightarrow p^{-\frac{\phi(q)}{2}} \equiv -1 \mod q.$$

D'après le théorème 6.8.1, il existe $s$ tel que pour tout $i$ :

$$a_i = (-sp^{-i}) \pmod q \pmod p.$$

Donc $a_{i+\frac{\phi(q)}{2}} = (-sp^{-i-\frac{\phi(q)}{2}}) \pmod q \pmod p = (sp^{-i}) \pmod q \pmod p$. Soit $q$ un entier. Comparons le reste de $a$ modulo $q$ puis modulo $p$ au reste de $-a$ modulo $q$ puis modulo $p$. On fait deux divisions euclidiennes :

$$\begin{aligned} a &= qk + r \text{ avec } 0 \leq r < q \\ r &= pl + s \text{ avec } 0 \leq s < p. \end{aligned}$$

Si $r = 0$, alors $q \mid a$ et donc $q \mid -a$. Donc $(-a) \pmod q = a \pmod q = 0$ et $(-a) \pmod q \pmod p = a \pmod q \pmod p = 0$. Ce cas là est exclu car il a lieu quand $\underline{a} = \underline{0}$ et $\underline{a}$ est supposée être une $l$-séquence.
Sinon $0 < r < q$ et donc $0 < q - r < q$. Or $-a = -qk - r = -q(k+1) + q - r$. Donc $(-a) \pmod q = q - r$. En outre, on a :

$$q - r = q - (pl + s) = q - pl - s = q - pl - p + 1 + p - 1 - s = q + 1 - p(l+1) + (p - 1 - s).$$

Or $0 \leq s \leq p - 1 \Rightarrow 0 \leq p - 1 - s \leq p - 1$. D'autre part, $q \mid p^{\mathtt{ord}(q)} - 1 \Rightarrow p \mid q + 1$. Donc $(q - r) \pmod p = p - 1 - s$. On en conclut que :

$$(-a) \pmod q \pmod p = (p-1) - a \pmod q \pmod p.$$

On applique le résultat $a = -sp^{-i}$ et on trouve que $a_{i+\frac{\phi(q)}{2}} = p - 1 - a_i$. □

**Corollaire 6.12.1.** *Soit $q$ un entier puissance d'un nombre premier impair $n$ et dont $p$ est racine primitive modulo $q$. Soient $\underline{a}$ une $l$-séquence générée par le FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$ et $\underline{b}$ une $d$-décimation première de $\underline{a}$. Alors pour tout $i$,*

$$b_{i+\frac{\phi(q)}{2}} = p - 1 - b_i.$$

*Démonstration.* $d$ est premier avec $\phi(q)$ qui est pair, donc $q$ est impair, $d = 2k + 1$.

$$b_{i+\frac{\phi(q)}{2}} = a_{di+d\frac{\phi(q)}{2}} = a_{di+d\frac{\phi(q)}{2}} = a_{di+k\phi(q)+\frac{\phi(q)}{2}} = a_{di+\frac{\phi(q)}{2}} = p - 1 - a_{di} = p - 1 - b_i.$$

□

**Corollaire 6.12.2.** *Soit $q$ un entier puissance d'un nombre premier impair $n$ et dont 2 est racine primitive modulo $q$. Considérons $\underline{a}$ une $l$-séquence binaire ou $\underline{b}$ une décimation première d'une $l$-séquence binaire générée par le FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$. Alors la première moitié d'une période est le complémentaire en bit de la seconde moitié. Le nombre de uns et le nombre de zéros sont égaux dans une période.*

*Démonstration.* Avec $p = 2$, on a $a_{i+\frac{\phi(q)}{2}} = 1 - a_i$. La preuve est évidente. □

Une $l$-séquence et ses décimations premières sont équilibrées.

## 6.13 Inter-corrélation arithmétique

Les $m$-séquences ont une inter-corrélation idéale. Nous avons donné l'exemple des paires de séquences de Gold ou Gold-pair séquences. Pour les FCSRs séquences, l'inter-corrélation se définie différemment de l'inter-corrélation des LFSRs séquences. Dans cette section, nous définissons l'inter-corrélation arithmétique des FCSRs séquences puis nous calculons l'inter-corrélation arithmétique entre deux décimations premières d'une $l$-séquence.

Reprenons le caractére additif introduit dans la définition 5.20.4. Le caractére $\chi$ est définie comme suit :

$$\begin{array}{rcl} \chi : \mathbb{F}_p & \to & \mathcal{C}^* \\ x & \mapsto & e^{\frac{2i\pi}{p}x}. \end{array}$$

L'inter-corrélation des FCSRs séquences est définie de la manière suivante :

**Définition 6.13.1** (Inter-corrélation arithmétique)**.** *Soient $\underline{a}$ et $\underline{b}$ deux séquences $p$-aires strictement périodiques de même période $T$. Soit $\underline{b}_\tau$ un $\tau$ décalage de $\underline{b}$. Soient $a$ et $b_\tau$ les développements $p$-adiques respectifs de $\underline{a}$ et de $\underline{b}_\tau$. Posons $\underline{c} = \mathtt{seq}_p(a - b_\tau)$. L'inter-corrélation relative à $\chi$ entre $\underline{a}$ et $\underline{b}$ pour un décalage $\tau$ est*

$$\mathcal{C}^A_{\underline{a},\underline{b}}(\tau) = \sum_{i=0}^{i=T-1} \chi(c_i).$$

L'inter-corrélation arithmétique diffère de l'inter-corrélation classique du fait que $\underline{c}$ n'est pas la séquence $\underline{a} - \underline{b}_\tau$ coefficient à coefficient, mais c'est la séquence extraite du développement $p$-adique de $a - b_\tau$. Dans la soustraction des développements $p$-adiques, il y a une retenue. Avant de calculer l'inter-corrélation arithmétique entre deux décimations premières d'une $l$-séquence, on doit d'abord introduire un petit résultat intermédiaire.

**Lemme 6.13.1.** *Soit $q$ un entier puissance d'un nombre premier impair $n$ et dont 2 est racine primitive modulo $q$. Considérons $\underline{a}$ une $l$-séquence binaire générée par le FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$ et $\underline{b}$ une décimation première de $\underline{a}$. Posons $b = \frac{s'}{q'}$ l'entier $p$-adique associé à $\underline{b}$ tel que $s'$ et $q'$ soient premiers entre eux. Alors $q'$ divise $p^{\frac{\phi(q)}{2}} + 1$.*

*Démonstration.*

$$\begin{aligned}
\tfrac{s'}{q'} &= \sum_{i=0}^{i=+\infty} b_i p^i \\
&= \sum_{i=0}^{i=\frac{\phi(q)}{2}-1} b_i p^i + \sum_{i=\frac{\phi(q)}{2}}^{i=\phi(q)-1} b_i p^i + \sum_{i=\phi(q)}^{i=\frac{3\phi(q)}{2}-1} b_i p^i + \sum_{i=\frac{3\phi(q)}{2}}^{i=2\phi(q)-1} b_i p^i + \ldots \\
&= \sum_{i=0}^{i=\frac{\phi(q)}{2}-1} b_i p^i (1 + p^{\phi(q)} + \ldots) + \sum_{i=\frac{\phi(q)}{2}}^{i=\phi(q)-1} b_i p^i (1 + p^{\phi(q)} + \ldots) \\
&= (\sum_{i=0}^{i=\frac{\phi(q)}{2}-1} b_i p^i + \sum_{i=0}^{i=\frac{\phi(q)}{2}-1} b_{i+\frac{\phi(q)}{2}} p^i p^{\frac{\phi(q)}{2}})(1 + p^{\phi(q)} + \ldots) \\
&= (\sum_{i=0}^{i=\frac{\phi(q)}{2}-1} b_i p^i + \sum_{i=0}^{i=\frac{\phi(q)}{2}-1} (p - 1 - b_i) p^i p^{\frac{\phi(q)}{2}}) \tfrac{1}{1-p^{\phi(q)}} \\
&= \tfrac{1-p^{\frac{\phi(q)}{2}}}{1-p^{\phi(q)}} \sum_{i=0}^{i=\frac{\phi(q)}{2}-1} b_i p^i + \tfrac{(p-1)p^{\frac{\phi(q)}{2}}}{1-p^{\phi(q)}} \sum_{i=0}^{i=\frac{\phi(q)}{2}-1} p^i \\
&= \tfrac{1}{1+p^{\frac{\phi(q)}{2}}} \sum_{i=0}^{i=\frac{\phi(q)}{2}-1} b_i p^i + \tfrac{(p-1)p^{\frac{\phi(q)}{2}}}{1-p^{\phi(q)}} \tfrac{1-p^{\frac{\phi(q)}{2}}}{1-p} \\
&= \tfrac{1}{1+p^{\frac{\phi(q)}{2}}} \sum_{i=0}^{i=\frac{\phi(q)}{2}-1} b_i p^i - \tfrac{p^{\frac{\phi(q)}{2}}}{1+p^{\frac{\phi(q)}{2}}} \\
(1 + p^{\frac{\phi(q))}{2}}) s' &= (\sum_{i=0}^{i=\frac{\phi(q)}{2}-1} b_i p^i - p^{\frac{\phi(q)}{2}}) q'.
\end{aligned}$$

$q'$ est premier avec $s'$ donc divise $(1 + p^{\frac{\phi(q))}{2}})$. □

### 6.13.1 Compilation de l'inter-corrélation arithmétique

L'inter-corrélation classique entre deux séquences binaires $\underline{a}$ et $\underline{b}$ est définie comme le nombre de zéros moins le nombre de uns de la séquence obtenue par $\underline{a} - \underline{b}$. La séquence $\underline{a} - \underline{b}$ est strictement périodique si $\underline{a}$ et $\underline{b}$ sont strictement périodiques. Donc l'inter-corrélation se calcule à partir des premiers coefficients des séquences en question. Dans le

cas de l'inter-corrélation arithmétique, on calcule la différence entre le nombre de zéros et le nombre de uns de la séquence $\mathtt{seq}_2(a-b)$ où $a$ et $b$ sont les développements 2-adiques respectifs des séquences $\underline{a}$ et $\underline{b}$. Cette séquence n'est pas forcément strictement périodique. Le calcul de l'inter-corrélation arithmétique est donc problématique.

**Proposition 6.13.1.** *Considérons $\underline{a}$ et $\underline{b}$ deux séquences strictement périodiques de même période $N$ et de développement 2-adique respectifs $a$ et $b$. La séquence $\mathtt{seq}_2(a-b)$ est ultimement périodique de pré-période au plus $N$ et de période divisant $N$.*

*Démonstration.* Comme $\underline{a}$ et $\underline{b}$ sont strictement périodiques de période $N$, alors il existe deux entiers $-(2^N-1) \leq s \leq 0$ et $-(2^N-1) \leq r \leq 0$ tels que $a = \frac{s}{2^N-1}$ et $b = \frac{r}{2^N-1}$.

$$-1 \leq a - b = \frac{s-r}{2^N-1} \leq 1.$$

Si $-1 \leq a-b \leq 0$, alors $\mathtt{seq}_2(a-b)$ est strictement périodique de période divisant $N$. Si $0 \leq a-b \leq 1$, alors $-1 \leq a-b-1 \leq 0$. Notons $c = a-b-1$, la séquence $\mathtt{seq}_2(c)$ est strictement périodique de période divisant $N$. Notons cette séquence $\underline{c} = (c_0, c_1, \ldots, c_{N-1}, \ldots)$.

$$a - b = 1 + c = 1 + c_0 + c_1 2 + \ldots.$$

Si $c_0 = 0$, alors $\mathtt{seq}_2(1+c) = (1, c_1, \ldots, c_{N-1}, \ldots)$. Donc $\mathtt{seq}_2(a-b)$ a une pré-période au plus 1 et une période divisant $N$. Si $c_0 = 1$, alors $1 + c = (c_1+1)2 + c_2 2^2 + \ldots$. Si $c_1 = 0$, alors $seq_2(1+c) = (0, 1, c_2, \ldots)$. Donc $\mathtt{seq}_2(a-b)$ est de pré-période au plus 2 et de période divisant $N$. Si $c_1 = 1 \ldots$, on réitère le même raisonnement, jusqu'à $c_{N-1}$. Si $c_{N-1} = 0$, alors $\mathtt{seq}_2(1+c) = (0, \ldots, 0, 1, c_N)$. Donc $\mathtt{seq}_2(a-b)$ est de pré-période au plus $N$ et de période divisant $N$. Si $c_{N-1} = 1$, alors $\underline{c} = (1, 1, \ldots)$ et $1 + c = 0$. Donc $\mathtt{seq}_2(a-b)$ est la séquence nulle. □

On calcule l'inter-corrélation arithmétique à partir de $2N$ bits de la séquence $\mathtt{seq}_2(a-b)$ et on regarde la différence du nombre de zéros et de uns sur les $N$ derniers bits de ces $2N$ bits.

### 6.13.2 Inter-corrélation entre décimations premières

L'inter-corrélation arithmétique entre deux décimations premières d'une $l$-séquence est à deux niveaux.

**Théorème 6.13.1.** *Soit $q$ un entier puissance d'un nombre premier impair $n$ et dont 2 est racine primitive modulo $q$. Considérons $\underline{a}$ une $l$-séquence binaire générée par le FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$. Soient $\underline{b}$ et $\underline{c}$ deux décimations premières de $\underline{a}$, alors :*

$$\mathcal{C}^A_{\underline{b},\underline{c}}(\tau) = \begin{cases} \phi(q) & si\ \underline{b} = \underline{c}_\tau \\ 0 & sinon. \end{cases}$$

*Démonstration.* Posons $b$, $c$ et $c_\tau$ les développements $p$-adiques respectifs de $\underline{b}$, $\underline{c}$, $\underline{c}_\tau$.

$$\begin{aligned} c_\tau &= \sum_{i=0}^{i=+\infty} c_{i+\tau}p^i = \sum_{i=\tau}^{i=+\infty} c_i p^{i-\tau} \\ &= \sum_{i=\tau}^{i=\phi(q)-1} c_i p^{i-\tau} + \sum_{i=0}^{i=+\infty} c_{i+\phi(q)} p^{i+\phi(q)-\tau} \\ &= \sum_{i=\tau}^{i=\phi(q)-1} c_i p^{i-\tau} + p^{\phi(q)-\tau} \sum_{i=0}^{i=+\infty} cp^i \\ &= \sum_{i=\tau}^{i=\phi(q)-1} c_i p^{i-\tau} + p^{\phi(q)-\tau} c \end{aligned}$$

Posons $x = \sum_{i=\tau}^{i=\phi(q)-1} c_i p^{i-\tau}$. L'inter-corrélation arithmétique entre $\underline{b}$ et $\underline{c}$ pour un décalage $\tau$ dans le cas binaire est la différence entre le nombre de zéros et le nombre de uns dans une période de la séquence extraite du développement 2-adique de $b - c_\tau$. Si $\underline{b}$ est un $\tau$-décalage de $\underline{c}$, alors $b = c_\tau$ et donc la séquence extraite est nulle et dans une période de longueur $\phi(q)$, il y a $\phi(q)$ zéros et 0 uns, donc l'inter-corrélation est $\phi(q)$. Sinon définissons les fractions rationnelles irréductibles $b = \frac{s'}{q'}$ et $c = \frac{s''}{q''}$.

$$b - c_\tau = b - x - 2^{\phi(q)-\tau}c = \frac{s'}{q'} - x - 2^{\phi(q)-\tau}\frac{s''}{q''} = \frac{q''s' - q'q''x - 2^{\phi(q)-\tau}s''q'}{q'q''}.$$

Soit $d = \mathtt{PGCD}(q', q'')$ et $r = \mathtt{PPCM}(q', q'')$. Alors $q'q'' = dr$ et on a :

$$b - c_\tau = \frac{s'\frac{q''}{d} - rx - 2^{\phi(q)-\tau}s''\frac{q'}{d}}{r}.$$

D'après le lemme 6.13.1, $q'$ et $q''$ divisent $2^{\frac{\phi(q)}{2}} + 1$, donc par définition $r$ divise $2^{\frac{\phi(q)}{2}} + 1$.

Les séquences $\underline{b}$ et $\underline{c}_\tau$ sont strictement périodiques de période $\phi(q)$. D'après la proposition 6.13.1, $\mathtt{seq}_2(b - c_\tau)$ est ultimement périodique de pré-période au plus $\phi(q)$ et de période divisant $\phi(q)$. Posons $\underline{u} = \mathtt{seq}_2(b - c_\tau)$, la séquence décalée $\underline{u}_{\phi(q)}$ est strictement périodique de période $T$ diviseur de $\phi(q)$. Son développement 2-adique est de la forme $\frac{y}{r}$ avec $-r \leq y \leq 0$. L'inter-corrélation entre $\underline{b}$ et $\underline{c}$ en $\tau$ est égale au nombre de zéros moins le nombre de uns dans une période de $\underline{u}_{\phi(q)}$ :

$$\sum_{i=\phi(q)}^{i=2\phi(q)-1} (-1)^{u_i}.$$

D'après le théorème 6.8.1, $\underline{u}_{\phi(q)}$ admet une représentation exponentielle :

$$u_i = (-y2^{-i})(\mathtt{mod}r)(\mathtt{mod}2).$$

$\underline{u}$ est une séquence balancée, en effet $r$ divise $2^{\frac{\phi(q)}{2}}+1$ et d'après la démonstration de la proposition 6.12.1, $u_{i+\frac{\phi(q)}{2}} - 1 - u_i$. On a alors

$$\sum_{i=\phi(q)}^{i=2\phi(q)-1} (-1)^{u_i} = \frac{\phi(q)}{2} - \frac{\phi(q)}{2} = 0.$$

□

## 6.14 Décimations premières cycliquement distinctes

Nous avons démontré l'existence d'une nouvelle famille de séquences autres que les $m$-séquences ayant une inter-corrélation idéale c'est-à-dire de second niveau. Ce sont les décimations premières d'une $l$-séquence donnée. L'inter-corrélation est nulle si les deux décimations sont cycliquement distinctes. Il faut donc prouver l'existence de tels couples de décimations d'une $l$-séquence. Goresky et Klapper fournissent une conjecture à ce sujet :

**Conjecture 6.14.1.** *Si $q$ est un nombre premier et $q > 13$, et si 2 est une racine primitive modulo $q$ et si $\underline{a}$ est une $l$-séquence d'entier de connexion $q$, alors deux décimations premières de $\underline{a}$ sont cycliquement distinctes.*

Cette conjecture a été vérifiée pour $q < 2000000$. Il est beaucoup plus simple d'étudier un couple $(\underline{a}, \underline{a}^d)$ formé d'une $l$-séquence $\underline{a}$ et d'une décimation première que d'étudier un couple $(\underline{a}^c, \underline{a}^d)$ de décimations premières de $\underline{a}$. En effet, il existe une équivalence.

**Proposition 6.14.1.** *Considérons $q$ un nombre premier ayant 2 pour racine primitive modulo $q$ et $\underline{a}$ une $l$-séquence d'entier de connexion $q$. Soient $d$ et $e$ deux entiers naturels. Notons $e^{-1}$ l'inverse de $e$ dans $\mathbb{F}_{q-1}$. Les décimations $\underline{a}^d$ et $\underline{a}^e$ sont cycliquement distinctes si et seulement si $\underline{a}$ et $\underline{a}^{de^{-1}}$ sont cycliquement distinctes.*

*Démonstration.* Si $\underline{a}$ et $\underline{a}^{de^{-1}}$ sont cycliquement identiques alors il existe un décalage $0 \leq \tau < q-1$ tel que pour tout $i \in \mathbb{N}$, $a_i = a_{de^{-1}i+\tau}$. Donc pour tout $i \in \mathbb{N}$, $a_{ei} = a_{dee^{-1}i+e\tau}$. Or $e^{-1}$ étant un inverse de $e$ dans $\mathbb{F}_{q-1}$, alors il existe $k \in \mathbb{N}$ tel que $ee^{-1} = 1 + (q-1)k$. Ainsi $a_{ei} = a_{d(1+(q-1)k)i+\tau} = a_{di+d(q-1)ki+\tau} = a_{di+\tau}$ puisque $\underline{a}$ est de période $q-1$. On en conclut que $\underline{a}^d$ et $\underline{a}^e$ sont cycliquement identiques. Inversement, si $\underline{a}^d$ et $\underline{a}^e$ sont cycliquement identiques alors il existe $0 \leq \tau < q-1$ tel que $\forall i \in \mathbb{N}$, $a_{di} = a_{ei+\tau}$. L'élément $e^{-1}$ étant l'inverse il existe $k \in \mathbb{N}$ tel que $ee^{-1} = 1 + (q-1)k$. Ainsi $\forall i \in \mathbb{N}$, $a_{de^{-1}i} = a_{ee^{-1}i+\tau} = a_{(1+(q-1)k)i+\tau} = a_{i+(q-1)ki+\tau} = a_{i+\tau}$ puisque $\underline{a}$ est de période $q-1$. Donc $\underline{a}$ et $\underline{a}^{de^{-1}}$ sont cycliquement identiques. □

Le fait qu'une $l$-séquence et une décimation première soient cycliquement distinctes peut être reformulé plus simplement.

**Proposition 6.14.2.** *Soit $q$ un nombre premier avec 2 pour racine primitive modulo $q$ et soit $d$ premier avec $q-1$. Considérons $E$ l'ensemble des paires de $\mathbb{F}_q$. Soit $\underline{a}$ une l-séquence d'entier de connexion $q$. Les séquences $\underline{a}$ et $\underline{a}^d$ sont cycliquement identiques si et seulement si la fonction $g : \begin{cases} \mathbb{Z} & \to & \mathbb{Z} \\ x & \mapsto & 2^{-\tau}x^d \mod q \end{cases}$ conserve $E$.*

*Démonstration.* Les séquences $\underline{a}$ et $\underline{a}^d$ sont cycliquement identiques si et seulement si il existe $\tau$ tel que pour tout $i$, $a_{di+\tau} = a_i$. Or nous avons :

$$\begin{array}{rcl} \forall i,\, a_{di+\tau} = a_i & \Leftrightarrow & \forall\, i,\, A2^{-(di+\tau)} \pmod q \pmod 2 = A2^{-i} \pmod q \pmod 2 \\ & \Leftrightarrow & \forall i,\, A(2^{-i})^d 2^{-\tau} \pmod q \pmod 2 = A2^{-i} \pmod q \pmod 2 \end{array}$$

En d'autres termes, les séquences $\underline{a}$ et $\underline{a}^d$ sont cycliquement identiques si et seulement si pour tout $i$, $A(2^{-i})^d 2^{-\tau} \pmod q$ et $A2^{-i} \pmod q$ sont de même reste modulo 2 donc de même parité. Si on les multiplie par un même élément de $\mathbb{F}_q$, ils gardent encore la même parité. Multiplions par l'inverse de $A$ dans $\mathbb{F}_q$, $A^{-1} \bmod q$, on obtient que pour tout $i$, $2^{-\tau}(2^{-i})^d \bmod q$ et $2^{-i} \bmod q$ sont de même parité. Or 2 est primitif dans $\mathbb{F}_q$, donc tous les éléments de $\mathbb{F}_q$ s'écrivent sous la forme d'une puissance de 2. Ainsi pour tout $x \in \mathbb{F}_q$, $2^{-\tau}x^d \bmod q$ et $x \bmod q$ sont de même parité. En d'autres termes, les séquences $\underline{a}$ et $\underline{a}^d$ sont cycliquement identiques si et seulement si la fonction $g : \begin{cases} \mathbb{F}_q & \to & \mathbb{F}_q \\ x & \mapsto & 2^{-\tau}x^d \bmod q \end{cases}$ conserve $E$ l'ensemble des paires de $\mathbb{F}_q$. □

Grâce à cette proposition, on exprime la conjecture d'une autre manière. Cette conjecture résiste aux techniques de calculs habituels. Cependant on arrive à démontrer dans certaines conditions sur $d$, que les séquences $\underline{a}$ et $\underline{a}^d$ sont cycliquement distinctes. Nous allons donner des exemples de ces décimations premières cycliquement distinctes à leur séquence d'origine.

**Théorème 6.14.1.** *Soit $q$ un entier premier strictement supérieur à 13 admettant 2 pour racine primitive modulo $q$. Soit $d$ un entier premier avec $q-1$. Considérons $\underline{a}$ une l-séquence d'entier de connexion $q$ et sa décimation $\underline{a}^d$. Si une des conditions suivantes est vérifiée, alors $\underline{a}$ et $\underline{a}^d$ sont cycliquement distinctes :*

1. $d = -1$,
2. $d \equiv 1 \bmod 4$ *et* $d = \dfrac{q+1}{2}$,
3. $1 < d \leq \dfrac{(q^2-1)^4}{2^{16}q^7(\log q + 2)^4} \approx \dfrac{q}{(16 \log q)^4}$,
4. $1 \leq d \leq \dfrac{(q^2-1)^4}{2^{24}q^7}$,
5. *ou* $-\dfrac{(q^2-1)^4}{2^{25}q^7} \leq d < 0$.

La démonstration de ces exemples nécessite des résultats intermédiaires.

### 6.14.1 Résultats intermédiaires.

Soit $\zeta = e^{\frac{2i\pi}{q}}$ une racine $q$-ième primitive de l'unité. Soit la somme exponentielle :

$$S_d(a,b) = \sum_{x=0}^{q-1} \zeta^{ax^d+bx}$$

Calculons les premières valeurs pour $a$ et $b$ triviaux.

$$S_d(0,0) = \sum_{x=0}^{q-1} 1 = q$$

$$\forall b \neq 0,\ S_d(0,b) = \sum_{x=0}^{q-1} \zeta^{bx} = \sum_{x=0}^{q-1} (\zeta^b)^x = \frac{(\zeta^b)^q - 1}{\zeta^b - 1} = \frac{(\zeta^q)^b - 1}{\zeta^b - 1} = 0$$

car $\zeta^q = 1$. Si $a \neq 0$, alors $S_d(a,0) = \sum_{x=0}^{q-1} \zeta^{ax^d}$. Soit $f : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^d$ avec $d$ premier à $q-1$.

**Lemme 6.14.1.** *Soit $d$ premier avec $q-1$, alors* $f : \left\{ \begin{array}{ccc} \mathbb{F}_q & \to & \mathbb{F}_q \\ x & \mapsto & x^d \end{array} \right.$ *est bijective.*

*Démonstration.* Soit $g$ primitif dans $\mathbb{F}_q$. Supposons $f(x) = f(x')$, on distingue plusieurs cas :

1. Si $x^d = (x')^d = 0$ alors par intégrité $x = x' = 0$.
2. Si $x^d \neq 0$ et $(x')^d \neq 0$ alors par intégrité $x \neq 0$ et $x' \neq 0$. Donc il existe des entiers $i$ et $i'$ tels que $x = g^i$ et $x' = g^{i'}$. Ainsi $g^{di} = g^{di'} \Rightarrow g^{d(i-i')} = 1$. Donc l'ordre de $g$ divise $d(i-i')$ ou $d(i-i') = 0$. Donc ou bien $q-1$ divise $d(i-i')$ ou bien $i = i'$. Or $d$ et $q-1$ sont premiers entre eux. Donc $q-1$ divise $i-i'$ ce qui implique que $i' = i + (q-1)l$ avec $l$ un entier. On en conclut que ou bien $i' = i + (q-1)l$ ou bien $i' = i$. Donc $x = x'$. On a démontré que $f$ est injective et comme c'est une fonction qui va de $\mathbb{F}_q$ dans $\mathbb{F}_q$, $f$ est bijective.

□

On revient au calcul de la somme exponentielle et on trouve :

$$S_d(a,0) = \sum_{x=0}^{q-1} \zeta^{ax^d} = \sum_{x'=0}^{q-1} \zeta^{ax'} = \sum_{x'=0}^{q-1} (\zeta^a)^{x'} = \frac{(\zeta^a)^q - 1}{\zeta^a - 1} = 0.$$

Soit $\lambda \neq 0$, alors :

$$S_d(\lambda^d, \lambda b) = \sum_{x=0}^{q-1} \zeta^{\lambda^d x^d + \lambda bx} = \sum_{x=0}^{q-1} \zeta^{(\lambda x)^d + b(\lambda x)}$$

La multiplication par $\lambda$ est une bijection de $\mathbb{F}_q$, donc pour tout $x^{'} \in \mathbb{F}_q$, il existe $x$ tel que $x^{'} = \lambda x$. On a alors $S_d(\lambda^d, \lambda b) = \sum_{x^{'}=0}^{q-1} \zeta^{(x^{'})^d + bx^{'}} = S_d(1, b)$. Donc :

$$\forall \lambda \neq 0,\ S_d(\lambda^d, \lambda b) = S_d(1, b).$$

**Lemme 6.14.2.** *Si $a \neq 0$, $d > 1$, alors :* $\sum_{b=0}^{q-1} |S_d(a, b)|^4 \leq (d-1)q^3$.

**Remarque 6.14.1.**

1. *Si $a = 0$,* $S_d(a, b) = 0 \Rightarrow \sum_{b=0}^{q-1} |S_d(0, b)|^4 = 0 \leq (d-1)q^3$.
2. *Si $d = 1$,* $S_d(a, b) = \sum_{x=0}^{q-1} \zeta^{ax+bx} = \sum_{x=0}^{q-1} \zeta^{(a+b)x}$.
3. *Si $a + b = 0$,* $S_d(a, b) = \sum_{x=0}^{q-1} 1 = q > (d-1)q^3$. *Si $a + b \neq 0$,* $S_d(a, b) = 0$ *et* $(d-1)q^3 = 0$.

*Démonstration.* □

Étudions la somme $T = \sum_{a=0}^{q-1} \sum_{b=0}^{q-1} |S_d(a, b)|^4$.

$$\begin{aligned}
T &= \sum_{a=0}^{q-1} \sum_{b=0}^{q-1} (|S_d(a, b)|^2)^2 \\
&= \sum_{a,b=0}^{q-1} (S_d(a, b) S_d(\bar{a}, b))^2 \\
&= \sum_{a,b=0}^{q-1} \sum_{x_1=0}^{q-1} \zeta^{ax_1^d + bx_1} \sum_{x_2=0}^{q-1} \zeta^{ax_2^d + bx_2} \sum_{x_3=0}^{q-1} \zeta^{-ax_3^d - bx_3} \sum_{x_4=0}^{q-1} \zeta^{-ax_4^d - bx_4} \\
T &= \sum_{a,b=0}^{q-1} \sum_{x_1,x_2,x_3,x_4=0}^{q-1} \zeta^{a(x_1+x_2-x_3-x_4)^d - b(x_1+x_2-x_3-x_4)}.
\end{aligned}$$

Soient $w$ et $t \in \mathbb{F}_q$. On pose $S(w, t) = \left\{x_1, x_2 \in \mathbb{F}_q; x_1^d + x_2^d = t,\ x_1 + x_2 = w\right\}$ et $R(w, t)$

le cardinal de $S(w,t)$. On a alors :

$$\begin{aligned}
T &= \sum_{a,b=0}^{q-1}\sum_{t,w=0}^{q-1}\sum_{x_1,x_2\in S(w,t)} \zeta^{at+bw}\sum_{t',w'=0}^{q-1}\sum_{x_3,x_4\in S(w',t')} \zeta^{at'+bw'}\\
&= \sum_{a,b=0}^{q-1}\sum_{t,w=0}^{q-1} R(w,t)\zeta^{at+bw}\sum_{t',w'=0}^{q-1} R(w',t')\zeta^{-at'-bw'}\\
&= \sum_{a,b=0}^{q-1}\sum_{t,t',w,w'=0}^{q-1} R(w,t)R(w',t')\zeta^{a(t-t')+b(w-w')}\\
&= \sum_{a,b=0}^{q-1}\left[\sum_{t\neq t' \ ou\ w\neq w'} R(w,t)R(w',t')\zeta^{a(t-t')+b(w-w')} + \sum_{t,w=0}^{q-1} R(w,t)^2\right]\\
&= \sum_{t\neq t' \ ou\ w\neq w'} R(w,t)R(w',t')\sum_{a,b=0}^{q-1}\zeta^{a(t-t')+b(w-w')} + \sum_{t,w=0}^{q-1} R(w,t)^2\sum_{a,b=0}^{q-1} 1\\
T &= \sum_{t\neq t' \ ou\ w\neq w'} R(w,t)R(w',t')\sum_{a=0}^{q-1}\zeta^{a(t-t')}\sum_{b=0}^{q-1}\zeta^{b(w-w')} + \sum_{t,w=0}^{q-1} R(w,t)^2q^2.
\end{aligned}$$

On a vu précédemment que : $\sum_{a=0}^{q-1}\zeta^{a(t-t')} = \sum_{b=0}^{q-1}\zeta^{b(w-w')} = 0$, donc on a :

$$T = q^2\sum_{t,w=0}^{q-1} R(w,t)^2.$$

Maintenant étudions $R(w,t)$ le nombre de solution du système d'équation

$$\begin{cases} x^d + y^d &\equiv t \bmod q\\ x+y &\equiv w \bmod q. \end{cases}$$

**Lemme 6.14.3.**

$$R(w,t) = \begin{cases} q & si \quad t=w=0\\ 0 & si \quad t=0, w\neq 0 \ ou\ t\neq 0, w=0 \end{cases}$$

$$R(w,t) \leq d-1 \ si \ w\neq 0, t\neq 0$$

*Démonstration.* On distingue 4 cas différents :

1. Si $w=t=0$, alors :

$$\begin{cases} x^d+y^d &\equiv 0 \bmod q\\ x+y &\equiv 0 \bmod q \end{cases} \Leftrightarrow \begin{cases} x^d+y^d &\equiv 0 \mod q\\ y &\equiv -x \mod q \end{cases}$$
$$\Leftrightarrow \begin{cases} x^d+(-x)^d &\equiv 0 \mod q\\ y &\equiv -x \mod q \end{cases}$$
$$\Leftrightarrow \begin{cases} 0 &\equiv 0 \mod q\\ y &\equiv -x \mod q \end{cases}$$
$$\Leftrightarrow \begin{cases} (x,y) = (x,-x)\\ x\in\mathbb{F}_q \end{cases}$$

   Il y a $q$ solutions au système.

2. Si $w = 0$ et $t \neq 0$, alors :

$$\left\{ \begin{array}{rcl} x^d + y^d & \equiv & t \bmod q \\ x + y & \equiv & 0 \bmod q \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} y & \equiv & -x \bmod q \\ x^d - x^d & \equiv & t \bmod q \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} y & \equiv & -x \bmod q \\ 0 & \equiv & t \bmod q \end{array} \right.$$

C'est absurde car $t \neq 0$, donc il y a 0 zéros solutions.

3. Supposons $w \neq 0$ et $t = 0$ : Soit $d^{-1}$ l'inverse de $d$ dans $\mathbb{Z}/q\mathbb{Z}$, donc il existe $k \in \mathbb{Z}$ tel que $dd^{-1} = 1+(q-1)k$. Si $x = 0$, alors $\left\{ \begin{array}{rcl} y & \equiv & w \bmod q \\ y^d & \equiv & 0 \bmod q \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} y & \equiv & w \bmod q \\ y & \equiv & 0 \bmod q \end{array} \right.$
C'est absurde. Ainsi $x$ est forcément non nul dans ce système. De même $y$ est aussi non nul par le même raisonnement. On a alors $x^{dd^{-1}} = xx^{(q-1)k} = x(x^{q-1})^k = x$ car $x^{q-1} = 1$. Le système devient :

$$\left\{ \begin{array}{rcl} x^{dd^{-1}} + y^{dd^{-1}} & \equiv & w \bmod q \\ x^d + y^d & \equiv & 0 \bmod q \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} (x^d)^{d^{-1}} + (y^d)^(d^{-1} & \equiv & w \bmod q \\ x^d + y^d & \equiv & 0 \bmod q \end{array} \right.$$

$$\Leftrightarrow \left\{ \begin{array}{rcl} (x^{'})^{d^{-1}} + (y^{'})^{d^{-1}} & \equiv & w \bmod q \\ x^{'} + y^{'} & \equiv & 0 \bmod q \\ x^{'} & = & x^d. \end{array} \right.$$

Ainsi on revient au cas précédent, puisque $d$ est premier avec $q-1$, donc $d^{-1}$ aussi par le théorème de Bézout et la relation $dd^{-1} = 1 + (q-1)k$. On en conclut que il y a 0 solutions dans ce cas.

4. Supposons $w \neq 0$ et $t \neq 0$ :

$$\left\{ \begin{array}{rcl} x + y & \equiv & w \bmod q \\ x^d + y^d & \equiv & t \bmod q \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} y & \equiv & w - x \bmod q \\ x^d + (w-x)^d & \equiv & t \bmod q \end{array} \right.$$
$$\Leftrightarrow \left\{ \begin{array}{rcl} y & \equiv & w - x \bmod q \\ x^d + w^d - dw^{d-1}x + \ldots + dwx^{d-1} - x^d & \equiv & t \bmod q \end{array} \right.$$
$$\Leftrightarrow \left\{ \begin{array}{rcl} y & \equiv & w - x \bmod q \\ w^d - dw^{d-1}x + \ldots + dwx^{d-1} & \equiv & t \bmod q \end{array} \right.$$
$$\Leftrightarrow \left\{ \begin{array}{rcl} y & \equiv & w - x \bmod q \\ -dw^{d-1}x + \ldots + dwx^{d-1} & \equiv & t - w^d \bmod q. \end{array} \right.$$

Cela revient à résoudre un polynôme de degré $d-1$, on en déduit qu'il y a au plus $d-1$ solutions pour ce cas. D'autre part :

$$\sum_{w=0}^{q-1} \sum_{t=0}^{q-1} R(w,t) = q^2$$

En effet

$$(\mathbb{F}_q)^2 = \bigcup_{t,w=0}^{q-1} S(w,t)$$

En comparant leur cardinal respectif, on obtient l'égalité ci-dessus. Revenons au calcul de $T$.

$$\begin{aligned} T &= q^2 \sum_{w,t=0}^{q-1} R(w,t)^2 \\ &= q^2 \sum_{w,t=1}^{q-1} R(w,t)^2 + q^2 R(0,0)^2 \\ &\leq q^2(d-1)(\sum_{w,t=0}^{q-1} R(w,t) - q) + q^4 \\ &\leq q^2(d-1)(q^2-q) + q^4 \\ T &\leq dq^4 - (d-1)q^3. \end{aligned}$$

$$\begin{aligned} \sum_{a=0}^{q-1}\sum_{b=0}^{q-1} |S_d(a,b)|^4 &\leq dq^4 - (d-1)q^3 \\ \sum_{a=1}^{q-1}\sum_{b=0}^{q-1} |S_d(a,b)|^4 + \sum_{b=0}^{q-1} |S_d(0,b)|^4 &\leq dq^4 - (d-1)q^3 \\ \sum_{a=1}^{q-1}\sum_{b=0}^{q-1} |S_d(a,b)|^4 + q^4 &\leq dq^4 - (d-1)q^3 \\ \sum_{a=1}^{q-1}\sum_{b=0}^{q-1} |S_d(a,b)|^4 &\leq (d-1)q^4 - (d-1)q^3 \\ \sum_{a=1}^{q-1}\sum_{b=0}^{q-1} |S_d(a,b)|^4 &\leq (d-1)(q^4-q^3). \end{aligned}$$

Précédemment on a démontré que la fonction $f : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^d$ est une permutation, donc $\forall a \in \mathbb{F}_q$, il existe un unique $\lambda \in \mathbb{F}_q$ tel que $a = \lambda^d$.

$$\begin{aligned} \sum_{b=0}^{q-1} |S_d(a,b)|^4 &= \sum_{b=0}^{q-1} \left|S_d(\lambda^d, \lambda\lambda^{-1}b)\right|^4 \\ \sum_{b=0}^{q-1} |S_d(a,b)|^4 &= \sum_{b=0}^{q-1} \left|S_d(1, \lambda^{-1}b)\right|^4. \end{aligned}$$

La multiplication étant une permutation, on a alors :

$$\begin{aligned} \sum_{b=0}^{q-1} |S_d(1,b)|^4 &= \tfrac{1}{q-1}((q-1)\sum_{b=0}^{q-1} |S_d(1,b)|^4) \\ &= \tfrac{1}{q-1}(\sum_{\lambda=1}^{q-1}\sum_{b=0}^{q-1} \left|S_d(\lambda^d, \lambda b)\right|^4) \\ &\leq \tfrac{1}{q-1}(\sum_{\lambda=1}^{q-1}\sum_{b=0}^{q-1} \left|S_d(\lambda^d, \lambda b)\right|^4) + q^4 \\ &\leq \tfrac{1}{q-1}(\sum_{u=1}^{q-1}\sum_{v=0}^{q-1} |S_d(u,v)|^4) + q^4 \\ &\leq \tfrac{1}{q-1}(\sum_{u=0}^{q-1}\sum_{v=0}^{q-1} |S_d(u,v)|^4) \\ &\leq (d-1)\tfrac{q^4-q^3}{q-1} \\ \sum_{b=0}^{q-1} |S_d(1,b)|^4 &\leq (d-1)q^3. \end{aligned}$$

Maintenant que nous avons démontrés le résultat recherché, nous allons énoncer un autre résultat qui nous sera utile dans la démonstration du théorème 6.14.1. Soit $E = \{0, 2, 4, \ldots, q-1\}$ l'ensemble des éléments pairs de $\mathbb{F}_q$. On définit :

$$\sigma_d(b) = \sum_{x \in E} \zeta^{blx^d} = \sum_{x=0}^{\frac{q-1}{2}} \zeta^{bl2^d x^d}.$$

On a : $\sigma_d(0) = \sum_{x \in E} 1 = |E| = \frac{q+1}{2}$.

□

**Lemme 6.14.4.** *$\forall b \neq 0$, on a :*

$$|\sigma_d(b)| \leq \frac{2^{\frac{14}{4}}}{\pi}(d-1)^{\frac{1}{4}} q^{\frac{3}{4}} + 4\log q + 4 < 2^3 (d-1)^{\frac{1}{4}} q^{\frac{3}{4}}$$

### 6.14.2 Démonstration du troisième exemple

Supposons le contraire à savoir que les séquences $\underline{a}$ et $\underline{a}^d$ sont cycliquement identiques. En d'autres termes, la fonction $g : \left\{ \begin{array}{ccc} \mathbb{F}_q & \rightarrow & \mathbb{F}_q \\ x & \mapsto & 2^{-\tau} x^d \bmod q \end{array} \right.$ conserve $E$ l'ensemble des éléments pairs de $\mathbb{F}_q$.
Maintenant définissons la fonction suivante :

$$f_e(x) = \left\{ \begin{array}{ll} 1 & \text{si } x \in E \\ 0 & \text{sinon} \end{array} \right.$$

Sa transformée de Fourier est : $\hat{f}_e(b) = \frac{1}{q} \sum_{c=0}^{q-1} f_e(c) \zeta^{-bc}$.

La formule d'inversion de Fourier donne : $f_e(a) = \sum_{b=0}^{q-1} \hat{f}_e(b) \zeta^{ba}$.

Posons $l = 2^{-\tau}$.

$$\begin{aligned} \sum_{x \in E} f_e(lx^d) &= \sum_{x \in E} \sum_{b=0}^{q-1} \hat{f}_e(b) \zeta^{blx^d} \\ &= \sum_{b=0}^{q-1} \hat{f}_e(b) \sum_{x \in E} \zeta^{blx^d} \\ &= \sum_{b=0}^{q-1} \hat{f}_e(b) \sigma_d(b) \\ \sum_{x \in E} f_e(lx^d) &= \hat{f}_e(0)\sigma_d(0) + \sum_{b=1}^{q-1} \hat{f}_e(b)\sigma_d(b) \end{aligned}$$

$$\hat{f}_e(0) = \frac{1}{q} \sum_{c=0}^{q-1} f_e(c) \zeta^0 = \frac{1}{q} \sum_{c=0}^{q-1} f_e(c) = \frac{1}{q} \sum_{c=0}^{q-1} 1 = \frac{1}{q} \frac{q+1}{2} = \frac{q+1}{2q}$$

$$\sigma_d(0) = \frac{q+1}{2}$$

$$\sum_{b=1}^{q-1} \hat{f}_e(b)\sigma_d(b) = \sum_{b=1}^{q-1} \hat{f}_e(b) \sum_{x\in E} \zeta^{blx^d}$$

Or $g$ préserve $E$, donc $\forall x \in E\, f_e(lx^d) = 1$.

$$\begin{array}{rcl} |E| & = & \frac{q+1}{2q} + \sum_{b=1}^{q-1} \hat{f}_e(b)\sigma_d(b) \\ \sum_{b=1}^{q-1} \hat{f}_e(b)\sigma_d(b) & = & \frac{q+1}{2} - \frac{q+1}{2q}\frac{q+1}{2} \\ \sum_{b=1}^{q-1} \hat{f}_e(b)\sigma_d(b) & = & \frac{q^2-1}{4q} \end{array}$$

On obtient alors la majoration suivante :

$$\frac{q^2-1}{4q} = \sum_{b=1}^{q-1} \hat{f}_e(b)\sigma_d(b) \leq \left( \sum_{b=1}^{q-1} \left|\hat{f}_e(b)\right| \right) \max_{b\neq 0} |\sigma_d(b)|$$

Maintenant il faut majorer $\sum_{b=1}^{q-1} \left|\hat{f}_e(b)\right|$.

**Lemme 6.14.5.** $\sum_{b=1}^{q-1} \left|\hat{f}_e(b)\right| \leq 1 + \frac{1}{2}\log(\frac{q-3}{2}) < \frac{\log q+2}{2}$.

Ainsi on a :

$$\frac{q^2-1}{4q} \leq \left(1 + \frac{1}{2}\log(\frac{q-3}{2})\right) \max_{b\neq 0} |\sigma_d(b)| < \frac{\log q+2}{2} \max_{b\neq 0} |\sigma_d(b)|\,.$$

D'après le lemme de la partie précédente :

$$\frac{q^2-1}{4q} \leq \left(1 + \frac{1}{2}\log(\frac{q-3}{2})\right)\frac{2^{\frac{14}{4}}}{\pi}(d-1)^{\frac{1}{4}}q^{\frac{3}{4}} + 4\log q + 4 < \frac{\log q+2}{2} 2^3 (d-1)^{\frac{1}{4}} q^{\frac{3}{4}}$$

$$\begin{array}{rcl} \frac{q^2-1}{4q} & < & \frac{\log q+2}{2} 2^3 d^{\frac{1}{4}} q^{\frac{3}{4}} \\ \frac{(q^2-1)^4}{4^4 q^4} & < & \frac{(\log q+2)^4}{2^4} 2^{12} d q^3 \\ \frac{(q^2-1)^4}{2^{12}2^8 2^{-4}(\log q+2)^4 q^3 q^4} & < & d \\ d & > & \frac{(q^2-1)^4}{2^{16} q^7 (\log q+2)^4}. \end{array}$$

La démonstration du point 3 du théorème est achevée.

### 6.14.3 Démonstration du quatrième exemple

Supposons que les séquences $\underline{a}$ et $\underline{a}^d$ soient cycliquement identiques, alors comme dans la démonstration précédente, cela implique que la fonction $g : \begin{cases} \mathbb{F}_q & \to & \mathbb{F}_q \\ x & \mapsto & 2^{-\tau} x^d \bmod q \end{cases}$ conserve $E$ l'ensemble des éléments pairs de $\mathbb{F}_q$. La méthode que nous allons utiliser

consiste à calculer de 2 manières différentes une somme exponentielle et comparer les 2 résultats obtenus. Soit

$$W = \left\{ z \in \mathbb{Z} \text{ tel que } 0 \leq z \leq \left[ \frac{q-1}{4} \right] \right\}$$

et soit

$$s = 2 \left[ \frac{q-1}{4} \right] + 1.$$

**Lemme 6.14.6.** *La congruence $lx^d \equiv 2(u-v) + s \bmod q$ telle que $x \in E$, $u$ et $v \in W$ n'a pas de solution.*

Considérons la somme exponentielle suivante : $\frac{1}{q} \sum_{u,v \in W} \sum_{x \in E} \sum_{b=0}^{q-1} \zeta^{b(lx^d - 2(u-v) - s)}$.
D'après le lemme précédent, $lx^d - 2(u-v) - s$ n'est pas congrue à 0 modulo $q$. Donc $\forall u, v \in W, x \in E \ \zeta^{lx^d - 2(u-v) - s} \neq 1$, ainsi $\sum_{b=0}^{q-1} (\zeta^{lx^d - 2(u-v) - s} \neq 1)^b = 0$. Alors :

$$\frac{1}{q} \sum_{u,v \in W} \sum_{x \in E} \sum_{b=0}^{q-1} \zeta^{b(lx^d - 2(u-v) - s)} = 0.$$

Calculons cette somme d'une autre manière :

$$\begin{aligned}
\tfrac{1}{q} \sum_{u,v \in W} \sum_{x \in E} \sum_{b=0}^{q-1} \zeta^{b(lx^d - 2(u-v) - s)} &= \tfrac{1}{q} \sum_{b=0}^{q-1} \sum_{u \in W} \zeta^{-2bu} \sum_{v \in W} \zeta^{2bv} \sum_{x \in E} \zeta^{blx^d} \zeta^{-bs} \\
&= \tfrac{1}{q} \sum_{b=0}^{q-1} \sigma_b(d) \zeta^{-bs} \sum_{u \in W} \zeta^{-2bu} \sum_{v \in W} \zeta^{\overline{-2}bv} \\
&= \tfrac{1}{q} \sum_{b=0}^{q-1} \sigma_b(d) \zeta^{-bs} \left| \sum_{u \in W} \zeta^{-2bu} \right|^2 \\
0 &= \tfrac{1}{q} \sigma_0(d) \left| \sum_{u \in W} 1 \right|^2 + \tfrac{1}{q} \sum_{b=1}^{q-1} \sigma_b(d) \zeta^{-bs} \left| \sum_{u \in W} \zeta^{-2bu} \right|^2 \\
0 &= \tfrac{1}{q} \tfrac{q+1}{2} |W|^2 + \tfrac{1}{q} \sum_{b=1}^{q-1} \sigma_b(d) \zeta^{-bs} \left| \sum_{u \in W} \zeta^{-2bu} \right|^2 \\
\tfrac{q+1|W|^2}{2q} &= -\tfrac{1}{q} \sum_{b=1}^{q-1} \sigma_b(d) \zeta^{-bs} \left| \sum_{u \in W} \zeta^{-2bu} \right|^2 \\
\tfrac{q+1|W|^2}{2q} &\leq \tfrac{1}{q} \sum_{b=1}^{q-1} |\sigma_b(d)| \left| \zeta^{-bs} \right| \left| \sum_{u \in W} \zeta^{-2bu} \right|^2 \\
\tfrac{q+1|W|^2}{2q} &\leq \tfrac{1}{q} \sum_{b=1}^{q-1} |\sigma_b(d)| \left| \sum_{u \in W} \zeta^{-2bu} \right|^2 .
\end{aligned}$$

D'après le lemme page 134 [42], on a : $|\sigma_d(b)| < 2^3 (d-1)^{\frac{1}{4}} q^{\frac{3}{4}}$.

$$\begin{aligned}
\tfrac{q+1|W|^2}{2q} &< \tfrac{1}{q}2^3(d-1)^{\frac{1}{4}}q^{\frac{3}{4}}\sum_{b=1}^{q-1}\left|\sum_{u\in W}\zeta^{-2bu}\right|^2\\
&< \tfrac{1}{q^{\frac{1}{4}}}2^3(d-1)^{\frac{1}{4}}\sum_{b=1}^{q-1}\sum_{u\in W}\left|\zeta^{-2bu}\right|^2\\
&< \tfrac{1}{q^{\frac{1}{4}}}2^3(d-1)^{\frac{1}{4}}\sum_{b=1}^{q-1}\sum_{u\in W}\left|\zeta^{-2bu}\right|^2\\
&< \tfrac{1}{q^{\frac{1}{4}}}2^3(d-1)^{\frac{1}{4}}\sum_{b=1}^{q-1}\sum_{u\in W}1\\
&< \tfrac{1}{q^{\frac{1}{4}}}2^3(d-1)^{\frac{1}{4}}\sum_{b=1}^{q-1}|W|\\
&< \tfrac{1}{q^{\frac{1}{4}}}2^3(d-1)^{\frac{1}{4}}(q-1)\,|W|\\
&< \tfrac{1}{q^{\frac{1}{4}}}2^3(d-1)^{\frac{1}{4}}q\,|W|\\
&< q^{\frac{3}{4}}2^3(d-1)^{\frac{1}{4}}\,|W|\\
\tfrac{q+1|W|}{2q} &< q^{\frac{3}{4}}2^3(d-1)^{\frac{1}{4}}\\
q+1\,|W| &< q^{\frac{7}{4}}2^4(d-1)^{\frac{1}{4}}\\
(d-1)^{\frac{1}{4}} &> \tfrac{q+1|W|}{q^{\frac{7}{4}}2^4}\\
d-1 &> \tfrac{(q+1)^4|W|^4}{q^7 2^{16}}.
\end{aligned}$$

Or $|W| \geq \frac{q-1}{4}$.

$$\begin{aligned}
d-1 &> \tfrac{(q+1)^4(q-1)^4}{q^7 2^{16}2^8}\\
d &> \tfrac{(q^2-1)^4}{2^{24}q^7}.
\end{aligned}$$

La démonstration du point 4 du thèorème 6.14.1 est achevée.

## 6.15 Durée et Complexité $p$-adique

Dans le cas linéaire (LFSR), la complexité linéaire est la taille du plus petit registre générant une séquence donnée. Cette taille est définie par le nombre de connexions nécessaires. Elle correspond au degré du polynôme minimal de la séquence. Dans le cas d'un registre à retenue (FCSR), en plus de la taille du registre principal, il faut tenir compte de la taille de la mémoire. La mémoire étant un entier, elle prend un certain nombre de bits non négligeable. Il faut donc redéfinir la complexité du registre dans le cas 2-adique.

Pour une séquence strictement périodique, la mémoire reste dans l'intervalle $[0, \sum_{i=1}^{i=r} q_i[$ où les $q_i$ sont les coefficients de connexion (proposition 6.6.1). La taille de la mémoire est ainsi limitée et dépend de la taille du registre principal. Par contre, dans le cas d'une séquence ultimement périodique, la mémoire initiale peut prendre une très grande valeur. Nous définissons deux notions : la complexité $p$-adique et la durée $p$-adique et nous montrons qu'elle diffère au plus de "$\log_p(\texttt{complexité})$".

Soit $\underline{a}$ une séquence strictement ou ultimement périodique. Considérons un FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$ générant cette séquence. On sait que $r \geq [\log_p(q+1)]$. Comme on cherche à mesurer la taille du plus petit FCSR générant une séquence donnée, alors ici on prendra les plus petits FCSRs, c'est-à-dire qu'on impose $r = [\log_p(q+1)]$. C'est équivalent à supposer que $q_r \neq 0$. Notons aussi $m$ la mémoire initiale du registre. On définit alors l'entier suivant :

$$\lambda = \begin{cases} r + \max\left([\log_p(\sum_{i=1}^{i=r} q_i)], [\log_p(|m|)] + 1\right) & \text{si } m \neq 0 \\ r + [\log_p(\sum_{i=1}^{i=r} q_i)] & \text{si } m = 0 \end{cases}$$

$r$ est la taille du plus registre d'entier de connexion $q$ qui génère $\underline{a}$. D'après la proposition 6.6.1, la valeur de la mémoire retourne vers l'intervalle $[0, \sum_{i=1}^{i=r} q_i[$. Donc la mémoire après un certain temps a une taille en bits inférieure ou égale à $[\log_p(\sum_{i=1}^{i=r} q_i)]$. Il existe donc deux cas : Dans le premier, la mémoire initiale est dans cet intervalle et alors la taille du registre est définie comme étant la taille du registre principal plus la taille en bits de la case mémoire

$$[\log_p(q+1)] + [\log_p(\sum_{i=1}^{i=r} q_i)],$$

dans le deuxième, la mémoire initiale ne se situe pas dans cet intervalle et dans ce cas, la taille du registre est définie par la taille du registre principal plus la taille en bits de la case mémoire. Cependant, malgré que la mémoire ne se situe pas dans l'intervalle $[0, \sum_{I=1}^{i=r} q_i[$, elle peut être négative et avoir sa valeur absolue dans cet intervalle, alors la taille de la mémoire reste inférieure à $[\log_p(\sum_{i=1}^{i=r} q_i)]$. Pour tenir compte de ce cas, on ajoute un "+1" :

$$[\log_p(q+1)] + [\log_p(|m|)] + 1.$$

**Définition 6.15.1** (Durée $p$-adique). *La durée $p$-adique d'une séquence périodique $\underline{a}$ est le plus petit entier $\lambda$ défini par les FCSRs et les mémoires initiales générant $\underline{a}$. On le note $\lambda_p(\underline{a})$.*

**Définition 6.15.2** (complexité $p$-adique). *Considérons une séquence périodique $\underline{a}$ et son entier $p$-adique associé $\alpha$ sous sa forme irréductible $\frac{s}{q}$. La complexité $p$-adique de $\underline{a}$ est* $\log_p(\max(|s|, |q|)$. *On la note $\phi_p(\underline{a})$.*

**Remarque 6.15.1.** *Si $\underline{a}$ est strictement périodique, alors sa complexité $p$-adique est la taille du registre principal.*

**Proposition 6.15.1.** *Soient $\underline{a}$ une séquence périodique et $\frac{s}{q}$ son entier $p$-adique associé sous sa forme irréductible. Alors*

$$|\lambda_p(\underline{a}) - \phi_p(\underline{a})| \leq \log_p(\phi_p(\underline{a})) + 2.$$

Avant d'entamer la démonstration de cette proposition, nous avons besoin du lemme suivant :

**Lemme 6.15.1.** *Considérons un entier $q = q_r p^r + \ldots + q_1 p - 1$ avec $q_r \neq 0$ et un entier $m$. Considérons $a_0, \ldots, a_{r-1} \in \mathbb{F}_p$ et*

$$s = \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - m_{r-1} p^r - \sum_{i=0}^{i=r-1} a_i p^i,$$

*alors*

1. $\sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) \leq (w-1)p^r$.
2. *Si $s > 0$, alors $m \leq w - q_r - 1$ et*
$$-(m+1)p^r < s \leq (w - q_r - m)p^r.$$
3. *Si $s < 0$, alors $m \geq 0$ et*
$$\max(0, (m - w + q_r)p^r) \leq |s| < |m+1|p^r.$$

*Démonstration.* La première assertion se démontre ainsi :

$$\begin{aligned}
\sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) &\leq \sum_{i=1}^{i=r-1} q_i p^i \sum_{j=0}^{j=r-i-1} a_j p^j \\
&\leq \sum_{i=1}^{i=r-1} q_i p^i (p-1)(1 + p + \ldots + p^{r-i-1}) \\
&\leq \sum_{i=1}^{i=r-1} q_i p^i (p-1)\tfrac{p^{r-i}-1}{p-1} \\
&\leq \sum_{i=1}^{i=r-1} q_i (p^r - p^i) \\
&\leq \sum_{i=1}^{i=r-1} q_i p^r \\
&\leq (w - q_r)p^r \\
&\leq (w-1)p^r.
\end{aligned}$$

La deuxième assertion se démontre à partir de la première :

$$\begin{aligned}
s > 0 &\Rightarrow \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) > m_{r-1} p^r + \sum_{i=0}^{i=r-1} a_i p^i \\
&\Rightarrow (w - q_r)p^r > m p^r \\
&\Rightarrow w - q_r > m \\
&\Rightarrow w - q_r - 1 \geq m.
\end{aligned}$$

$$\begin{aligned}
s &= \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - m_{r-1} p^r - \sum_{i=0}^{i=r-1} a_i p^i \\
&\leq (w - q_r)p^r - m p^r \\
s &\leq (w - q_r - m)p^r.
\end{aligned}$$

$$\begin{aligned} s &\geq -\sum_{i=0}^{i=r-1} a_i p^i - mp^r \\ &\geq -(p-1)\tfrac{p^r-1}{p-1} - mp^r \\ &\geq -p^r + 1 - mp^r \\ s &> -(m+1)p^r. \end{aligned}$$

La troisième assertion se démontre ainsi :

$$\begin{aligned} s > 0 \quad &\Rightarrow \quad mp^r > \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - \sum_{i=0}^{i=r-1} a_i p^i \\ &\Rightarrow \quad mp^r > -\sum_{i=0}^{i=r-1} a_i p^i \\ &\Rightarrow \quad mp^r > -(p^r - 1) \\ &\Rightarrow \quad mp^r > -p^r \\ &\Rightarrow \quad m > -1 \\ &\Rightarrow \quad m \geq 0. \end{aligned}$$

$$\begin{aligned} 0 &> s > -m_{r-1}p^r - \sum_{i=0}^{i=r-1} a_i p^i \\ 0 &> s > -mp^r - p^r + 1 \\ 0 &\quad s > -(m+1)p^r \\ &\quad |s| < |m+1|p^r. \end{aligned}$$

Or $m \geq 0$, donc $|s| < (m+1)p^r$.

$$\begin{aligned} s &\leq (w - q_r)p^r - mp^r \\ s &\leq -(m - w + q_r)p^r. \end{aligned}$$

Si $m - w + q_r > 0$ alors $|s| \geq (m - w + q_r)p^r$. Sinon $|s| \geq 0$. On alors

$$|s| \geq \max(0, (m - w + q_r)p^r).$$

□

*proposition 6.15.1.* En élevant exponentiellement cette inégalité, on obtient :

$$\begin{aligned} -\log_p(\phi_p(\underline{a})) - 2 \leq \quad & \lambda_p(\underline{a}) - \phi_p(\underline{a}) \quad && \leq \log_p(\phi_p(\underline{a})) + 2 \\ p^{-\log_p(\phi_p(\underline{a}))}p^{-2} \leq \quad & p^{\lambda_p(\underline{a})}p^{-\phi_p(\underline{a})} && \leq p^{\log_p(\phi_p(\underline{a}))}p^2 \\ \frac{p^{\phi_p(\underline{a})}}{\phi_p(\underline{a})p^2} \leq \quad & p^{\lambda_p(\underline{a})} && \leq p^{\phi_p(\underline{a})}\phi_p(\underline{a})p^2. \end{aligned}$$

Or $p^{\phi_p(\underline{a})} = p^{\log_p(\max(|s|,|q|)} = \max(|s|, |q|)$ et

$p^{\lambda_p(\underline{a})} = p^{[\log_p(q+1)]} \max\left(p^{[\log_p(\sum_{i=1}^{i=r} q_i)]}, p^{[\log_p(|m|)]}p\right)$. L'inégalité se traduit alors par

$$\begin{aligned} \tfrac{\max(|s|,|q|)}{\log_p(\max(|s|,|q|))} &\leq p^2 p^{[\log_p(q+1)]} \max\left(p^{[\log_p(\sum_{i=1}^{i=r} q_i)]}, p^{[\log_p(|m|)]}p\right) \\ p^{[\log_p(q+1)]} \max\left(p^{[\log_p(\sum_{i=1}^{i=r} q_i)]}, p^{[\log_p(|m|)]}p\right) &\leq p^2 \max(|s|, |q|) \log_p(\max(|s|, |q|)). \end{aligned}$$

Posons, $r = [\log_p(q+1)]$, $w = \sum_{i=1}^{i=r}$ et $\Phi = \max(|s|,|q|)$. Il faut donc démontrer les inégalités suivantes :

$$\begin{aligned} \frac{\Phi}{\log_p(\Phi)} &\leq p^{r+2} \max\left(p^{[\log_p(w)]}, p^{[\log_p(|m|)]}p\right) \\ p^r \max\left(p^{[\log_p(w)]}, p^{[\log_p(|m|)]}p\right) &\leq p^2 \Phi \log_p(\Phi). \end{aligned}$$

Rappelons qu'ici $\lambda$ est le plus petit des lambda en fonction de $r$, $q$ et $m$. Nous étudions 4 cas possibles.

1. Si $s < -q$, alors

$$|s| > |q| \Rightarrow \Phi = \max\Big(|s|,|q|\Big) = |s| \Rightarrow \phi_p(\underline{a}) = \log_p |s|.$$

Si $r \geq 2$, alors :

$$q \geq q_r p^r - 1 \geq p^r - 1 \geq p^2 - 1 \geq 2^2 - 1 = 3.$$

$$q \geq 3 \Rightarrow s < -3 \Rightarrow |s| > 3.$$

Notons $g(x) = \frac{x}{\log_p(x)}$. Sa dérivée $g'(x) = \frac{\log_p(x) - \log_p(e)}{\log_p(x)^2} \geq 0$ si et seulement si $x \geq e$. Donc $g$ est croissante sur $[e, +\infty[$. Le lemme 6.15.1 implique que $m \geq 0$ et $|s| \leq (m+1)p^r$.

$$\begin{aligned} 3 < |s| \geq (m+1)p^r &\Rightarrow \frac{|s|}{\log_p(|s|)} \leq \frac{(m+1)p^r}{\log_p((m+1)p^r)} \\ &\Rightarrow \frac{\Phi}{\log_p(\Phi)} \leq \frac{(m+1)p^r}{\log_p(m+1)+r}. \end{aligned}$$

$$\begin{aligned} m \geq 0 &\Rightarrow m+1 \geq 1 \Rightarrow \log_p(m+1) \geq 0 \\ &\Rightarrow \log_p(m+1) + r \geq r \Rightarrow \frac{1}{\log_p(m+1)+r} \geq \frac{1}{r}. \end{aligned}$$

$$\frac{\Phi}{\log_p(\Phi)} \leq \frac{(m+1)p^r}{\log_p(m+1)+r} \leq \frac{(m+1)p^r}{r} \leq \frac{m+1}{2} p^r.$$

Si $m = 0$, alors

$$\begin{aligned} s < -q &\Rightarrow \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - \sum_{i=0}^{i=r-1} a_i p^i < -q \\ &\Rightarrow \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) < \sum_{i=0}^{i=r-1} a_i p^i - q \\ &\Rightarrow 0 < 1 + p + \ldots + p^{r-1} - q_r p^r + 1 \\ &\Rightarrow 0 < p + (p-1)p + \ldots + (p-1)p^{r-1} - q_r p^r \\ &\Rightarrow 0 < (1 - q_r)p^r \leq 0. \end{aligned}$$

C'est absurde, donc $m \geq 1$.

$$\begin{array}{rcl} m \geq 1 & \Rightarrow & m \geq \frac{m+1}{2} \Rightarrow [\log_p(m)] + 1 \geq [\log_p(m+1)] + 1 \\ & \Rightarrow & [\log_p(m)] + 1 \geq \log_p(\frac{m+1}{2}) \Rightarrow p^{[\log_p(m)]+1} \geq \frac{m+1}{2} \\ & \Rightarrow & \dfrac{\Phi}{\log_p(\Phi)} \leq p^r p^{[\log_p(m)]+1} \\ & \Rightarrow & \dfrac{\Phi}{\log_p(\Phi)} \leq p^r p^2 \max\left(p^{[\log_p(w)]}, p^{[\log_p(m)]+1}\right). \end{array}$$

On a démontré la première inégalité, il reste à montrer la deuxième inégalité.

$$q_r \neq 0 \Rightarrow q \geq p^r - 1 \Rightarrow |s| > q \geq p^r - 1 \Rightarrow |s| \geq p^r.$$

Supposons que $|m| \geq r$ et rappelons que $w \leq r$.

$$\begin{array}{rcl} p^r \max\left(p^{[\log_p(w)]}, p^{[\log_p(|m|)]}p\right) & \leq & p^r \max\left(p^{[\log_p(w)]}p, p^{[\log_p(|m|)]}p\right) \\ & \leq & p^{r+1} \max\left(w, |m|\right) \\ & \leq & p^{r+1} r \\ & \leq & p r p^r \\ & \leq & p \log_p(|s|)|s| \\ p^r \max\left(p^{[\log_p(w)]}, p^{[\log_p(|m|)]}p\right) & \leq & p^2 \Phi \log_p(\Phi). \end{array}$$

Supposons que $|m| \geq r+1$. Comme $s < 0$ alors d'après le lemme 6.15.1, $|s| \geq (m - w + 1)p^r$.

$$(m - r + 1)r - m = (m - r)(r - 1) \geq 0 \Rightarrow (m - r + 1)m \geq m.$$

$$\begin{array}{rcl} p^2 \Phi \log_p(\Phi) & \geq & p^2 (m - w + 1) p^r \log_p\left((m - w + 1)p^r\right) \\ & \geq & p^{r+2}(m - w + 1)\Big(\log_p(m - w + 1) + r\Big) \\ & \geq & p^{r+2}(m - r + 1)\Big(\log_p(m - r + 1) + r\Big) \end{array}$$

$$m - r + 1 = (m - r - 1) + 2 \geq 2 \Rightarrow \log_p(m - r + 1) \geq 0.$$

$$\begin{array}{rcl} p^2 \Phi \log_p(\Phi) & \geq & p^{r+2}(m - r + 1)r \\ & \geq & p^{r+2} m \\ & \geq & p^{r+2} p^{\log_p(m)} \\ & \geq & p^{r+2} p^{[\log_p(m)]} \\ & \geq & p^r p^{[\log_p(m)]+1} \\ & \geq & p^r \max\left(p^{[\log_p(w)]+1}, p^{[\log_p(m)]+1}\right) \\ p^2 \Phi \log_p(\Phi) & \geq & p^r \max\left(p^{[\log_p(w)]}, p^{[\log_p(m)]+1}\right). \end{array}$$

2. Si $s > q$, alors :

$$\Phi = \max(|s|, |q|) = s \Rightarrow \phi_p(\underline{a}) = \log_p(s).$$

D'après le lemme 6.15.1, on trouve que

$$s > q \geq p - 1 \Rightarrow s > 0 \Rightarrow s \leq (w - q_r - m)p^r.$$

$$\frac{\Phi}{\log_p(\Phi)} = \frac{s}{\log_p(s)} \leq \frac{(w - q_r - m)p^r)}{r + \log_p(w - q_r - m)}.$$

$$w - q_r - m \geq s > 0 \Rightarrow w - q_r - m \geq 1 \Rightarrow \log_p(w - q_r - m) \geq 0.$$

$$\frac{\Phi}{\log_p(\Phi)} \leq \frac{(w - q_r - m)p^r)}{r} \leq \frac{wp^r)}{r}.$$

$$w \leq r \Rightarrow \frac{w}{r} \leq 1 < p.$$

$$\frac{\Phi}{\log_p(\Phi)} \leq p^{r+1}.$$

$$w \geq 1 \Rightarrow \log_p(w) \geq 0 \Rightarrow p^{[\log_p(w)]} \geq 1.$$

$$|m| \neq 0 \Rightarrow |m| \geq 1 \Rightarrow p^{[\log_p(|m|)]+1} \geq p.$$

$$p^{r+2} \max\left(p^{[\log_p(w)]}, p^{[\log_p(|m|)]+1}\right) \geq p^{r+2}p = p^{r+3} > p^{r+1} > \frac{\Phi}{\log_p(\Phi)}.$$

Pour la deuxième inégalité, on trouve que

$$\begin{aligned} p^r \max\left(p^{[\log_p(w)]}, p^{[\log_p(|m|)]}p\right) &\leq p^r \max\left(p^{\log_p(w)}, p^{\log_p(|m|)}p\right) \\ &\leq p^r \max\left(w, p|m|\right). \end{aligned}$$

D'après lemme 6.15.1, $m \geq w - q_r - 1$. Si $m > 0$, alors :

$$m \leq w - q_r - 1 < w \leq r < pr.$$

$$\begin{aligned} p^r \max\left(p^{[\log_p(w)]}, p^{[\log_p(|m|)]}p\right) &\leq p^r \max\left(pr, pm\right) \\ &\leq p^r pr \leq p^{r+2}r \leq p^2 r p^r. \end{aligned}$$

$$s > q \geq q_r p^r - 1 \geq p^r - 1 \Rightarrow s \geq p^r.$$

$$p^r \max\left(p^{[\log_p(w)]}, p^{[\log_p(|m|)]}p\right) \leq p^2 \log_p(s)s = p^2 \Phi \log_p(\Phi).$$

Si $m < 0$, alors

$$\begin{aligned} s &= \sum_{i=1}^{i=r-1} \sum_{j=0}^{j=r-i-1} (q_i a_j p^{i+j}) - m_{r-1}p^r - \sum_{i=0}^{i=r-1} a_i p^i \\ &\geq -(p-1)\tfrac{p^r-1}{p-1} + |m|p^r = p^r|m| - p^r + 1 > p^r(|m| - 1). \end{aligned}$$

$$p^r \max\left(w, p|m|\right) = p^2 p^r(|m|-1) \max\left(\frac{w}{p^2(|m|-1)}, \frac{|m|}{p(|m|-1)}\right) \leq p^2 sr \leq p^2 \Phi \log_p(\Phi).$$

3. Si $-q < s < 0$, alors :

$$\Phi = \max(|s|, |q|) = q \Rightarrow \phi_p(\underline{a}) = \log_p(q).$$

$$q = q_r p^r + \ldots + q_1 p - 1 \leq (p-1)(1 + p + \ldots + p^r) - 1 = p^{r+2} - 2 < p^{r+2}.$$

$$[\log_p(w)] \geq [\log_p(1)] = 0 \Rightarrow p^{[\log_p(w)]} \geq 1.$$

$$[\log_p |m|] \geq [\log_p(1)] = 0 \Rightarrow p^{[\log_p |m|]+1} \geq p > 1.$$

$$\frac{\Phi}{\log_p(\Phi)} = \frac{q}{\log_p(q)} < \frac{p^{r+1}}{r} \leq p^{r+1} < p^{r+2} < p^{r+2} \max\left(p^{[\log_p(w)]}, p^{[\log_p |m|]+1}\right).$$

Pour la deuxième inégalité, d'après le corollaire 6.5.1, la séquence $\underline{a} = \mathtt{seq}_p(\frac{s}{q})$ est strictement périodique et la mémoire initiale prend sa valeur dans $[0, w[$.

$$\begin{aligned} p^r \max\left(p^{[\log_p(w)]}, p^{[\log_p(m)]+1}\right) &\leq p^r \max(w, pm) \\ &\leq p^r \max(r, pr) \\ &\leq p^r p^2 r \leq p^2 q \log_p(q) \leq p^2 \Phi \log_p(\Phi). \end{aligned}$$

C'est vrai si et seulement si $q > p^r$. Or $q \geq q_r p^r - 1$ et

$$q > p^r \Leftrightarrow q \neq q_r p^r - 1 \Leftrightarrow w \neq 1.$$

Dans le cas contraire, $m = 0$ et c'est exclu. C'est ce qu'il fallait démontrer pour ce troisième cas.

4. Si $0 < s < q$, alors

$$\Phi = \max(|s|, q) = q.$$

On revient à la démonstration de la première inégalité dans le cas précédent. Pour la seconde inégalité, d'après le lemme 6.15.1, $m \leq w - q_r - 1$. Si $m \geq 0$, alors

$$\begin{aligned} p^r \max\left(p^{[\log_p(w)]}, p^{[\log_p(m)]+1}\right) &\leq p^r \max(w, pm) \\ &\leq p^r \max(w, p(w - q_r - 1)) \\ &\leq p^r pw \leq p^2 p^r r. \end{aligned}$$

Si $q = p^r - 1$, alors $w = 1$ et

$$p^{r+1} w = p^{r+1} \leq p^{r+1} r \leq\leq ppq \log_p(q) = p^2 \Phi \log_p(\Phi).$$

En effet $pq = q_r p^{r+1} - 1 > p^r$. Si $q > p^r - 1$, alors

$$q \geq p^r \Rightarrow p^2 p^r r \leq p^2 q \log_p(q) = p^2 \Phi \log_p(\Phi).$$

Si $m < 0$, alors d'après le lemme 6.15.1,

$$p^{r+1} > q > s > -(1 - |m|)p^r = (|m| - 1)p^r \Rightarrow |m| - 1 < p \Rightarrow |m| < p.$$

$$|m| < p \Rightarrow \log_p |m| < 1 \Rightarrow [\log_p |m|] \leq 0 \Rightarrow p^{[\log_p |m|]+1} \leq p.$$

$$p^r \max\left(p^{[\log_p(w)]}, p^{[\log_p |m[]+1}\right) \leq p^r \max(w, p) \leq p^r rp \leq pq \log_p(q) p = p^2 \Phi \log_p(\Phi).$$

□

**Proposition 6.15.2.** *Soient $\underline{a}$ et $\underline{b}$ deux séquences strictement périodiques. Soient $a$ et $b$ leur entier $p$-adique associé. Considérons la séquence $\underline{c} = \mathtt{seq}_p(a+b)$. Alors la complexité $p$-adique et la durée $p$-adique de $\underline{c}$ sont bornées :*

$$\phi_p(\underline{c}) \leq \phi_p(\underline{a}) + \phi_p(\underline{b}) + \log_p(2)$$
$$\lambda_p(\underline{c}) \leq \lambda_p(\underline{a}) + \lambda_p(\underline{b}) + 2\log_p(\lambda_p(\underline{a})) + 2\log_p(\lambda_p(\underline{b})) + 3\log_p(2) + \log_p(3) + 2$$

*Démonstration.* La séquence $\underline{c}$ est extraite du développement $p$-adique de $a+b$.

$$a + b = \frac{s_1}{q_1} + \frac{s_2}{q_2} = \frac{s_1 q_2 + s_2 q_1}{q_1 q_2}.$$

$$\Phi = \max(s_1 q_2 + s_2 q_1, q_1 q_2, q_1 q_2) \leq 2\max(q_1, s_1)\max(q_2, s_2).$$

$$\phi_p(\underline{c}) = \log_p(\max(q_1, s_1)) + \log_p(\max(q_2, s_2)) + \log_p(2) = \phi_p(\underline{a}) + \phi_p(\underline{b}) + \log_p(2).$$

Pour la suite de la preuve, on renvoit aux pages 127-132 de [8]. □

Il existe des $m$-séquences de durée 2-adique très grande.

**Théorème 6.15.1.** *Soit $\underline{a}$ une séquence strictement périodique de période $T$. Considérons $q$ le plus petit diviseur premier de $2^T - 1$. Alors $\lambda_2(\underline{a})$ la durée 2-adique de $\underline{a}$ est au moins égale à $\log_2(q+1) + 1$. Si $2^T - 1$ est premier, alors $\lambda_2(\underline{a}) = T + 1$.*

*Démonstration.* La durée 2-adique dépend de l'entier de connexion et de la mémoire initiale.

$$\lambda_2(\underline{a}) = \inf_{q,m} \left\{ [\log_2(q+1)] + \max\left( [\log_2(\sum_{i=1}^{i=r} q_i)], ([\log_2(|m|)] + 1)\mathbf{1}_{m \neq 0} \right) \right\}.$$

Comme $\underline{a}$ est de période $T$, alors son entier 2-adique associée est $\frac{\sum_{i=0}^{i=T-1} a_i 2^i}{2^T - 1}$. Le FCSR de plus petit entier de connexion $q'$ qui génère $\underline{a}$ divise $2^T - 1$. L'entier $q'$ est supérieur ou égal au plus petit diviseur premier de $2^T - 1$. Donc $[\log_2(q'+1)] \geq [\log_2(q+1)]$. On a $\max\left( [\log_p(\sum_{i=1}^{i=r} q_i')], [\log_p(|m|)] + 1 \right) \geq 1$ et $[\log_p(\sum_{i=1}^{i=r} q_i')] \geq 1$. D'autre part, si $2^T - 1$ est premier, il est son plus petit diviseur. Donc $\lambda_2(\underline{a}) \geq \log_2(2^T) + 1 = T + 1$. En même temps, le FCSR $(\mathbb{F}_2, T, 2^T - 1)$ et la mémoire initiale $m = 0$ génèrent $\underline{a}$. La durée 2-adique de ce FCSR est

$$r + [\log_p(\sum_{i=1}^{i=r} q_i)] = T + 1.$$

□

Pour construire le plus petit FCSR générant une séquence donnée, on dispose de l'algorithme d'approximation rationnel. Pour une séquence périodique de durée 2-adique égale à $M$, il permet de construire le plus petit FCSR à partir de seulement $2M + 2\log_p(M)$ bits. On renvoit aux pages 132-137 de [8] et à l'article [44] pour plus de détails.

## 6.16 FCSRs en mode Galois

Les FCSRs en mode Galois sont développés par Goresky et Klapper dans [22].

### 6.16.1 Définitions et Conceptions

**Définition 6.16.1** (FCSR en mode Galois). *Un Feedback with Carry Shift Register en mode Galois sur $\mathbb{F}_p$ de taille $r$ et de coefficients de connexion $(q_1, \ldots, q_r) \in (\mathbb{F}_p)^r$ est un automate ou générateur de séquence dont les états sont des couples de la forme suivante $s(t) = (a(t), m(t))$ avec*

$$a(t) = (a_0(t), \ldots, a_{r-1}(t)) \in (\mathbb{F}_p)^r \text{ et } m(t) = (m_1(t), \ldots, m_r(t)) \in (\mathbb{Z})^r;$$

*et dont l'opération de changement d'état est définie comme suit : Calculons*

$$\sigma_i(t+1) = q_{i+1}a_0(t) + a_{i+1}(t) + m_{i+1}(t) \text{ et } \sigma_{r-1}(t+1) = q_r a_0(t) + m_r(t).$$

*L'addition et la multiplication se font dans $\mathbb{Z}$. Puis on calcule*

$$a_i(t+1) = \sigma_i(t+1)(\mathtt{mod} p) \text{ et } m_{i+1}(t+1) = \sigma_i(t+1)(\mathtt{div} p).$$

*La fonction de retour est $f(s(t)) = s(t+1)$ et la fonction de sorties est $g(s(t)) = a_0(t)$. On répète ce procédé à l'infini. Le FCSR génère la séquence infinie*

$$(g(s(0)), g(f(s(0))), g(f^2(s(0))), \ldots) = (a_0(0), a_0(1), a_0(2), \ldots)$$

*appelée séquence de sorties. L'état $s(0)$ est appelé l'état initial de la séquence de sorties, $r$ la taille du FCSR, $q_1, \ldots, q_r$ les coefficients de connexion du FCSR.*

La figure 6.3 représente un FCSR en mode Galois. On peut aussi retenir en sortie

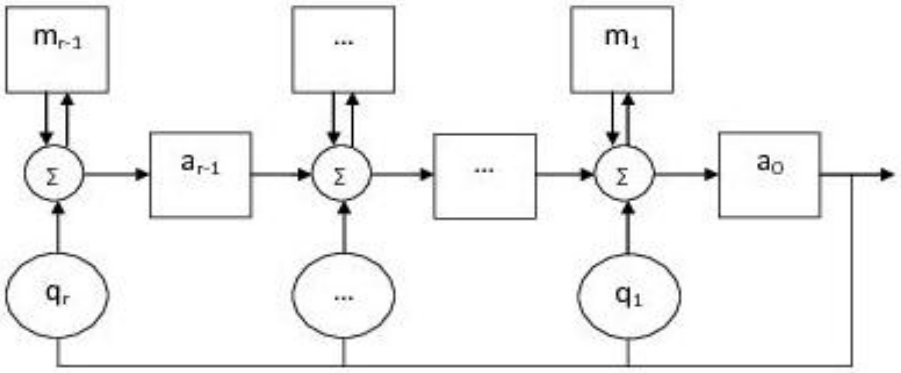



FIGURE 6.3 – Mode Galois des registres à décalage et à rétroaction linéaire avec retenue.

toutes les cellules. À chaque cellule correspondra une séquence de sortie

$$\underline{a_i} = (a_i(0), a_i(1), \ldots, a_i(t), \ldots).$$

Les sorties du FCSR peuvent être représentées par un seul élément : Considérons la séquence vectorielle de dimension $r$ sur $(\mathbb{F}_p)^{\mathbb{N}}$ définie par

$$\underline{a} = (\underline{a}_0, \ldots, \underline{a}_{r-1}) \in ((\mathbb{F}_{p^n})^{\mathbb{N}})^r.$$

Nous utilisons pour l'analyse la représentation matricielle.

### 6.16.2 Analyse et Représentation Matricielle

À toute séquence de sorties $\underline{a}_i$, on associe son développement $p$-adique défini par la série formelle dans $\mathbb{Z}_p$ :

$$\alpha_i = \sum_{t=0}^{t=+\infty} a_i(t)p^t.$$

La séquence vectorielle $\underline{a}$ est donc associée au vecteur de dimension $r$ sur $\mathbb{Z}_p$ donné par

$$\alpha = (\alpha_0, \ldots, \alpha_{r-1}) \in (\mathbb{Z}_p)^r.$$

Le changement d'états peut se traduire par la multiplication matricielle suivante :

$$(\sigma_0(t+1), \sigma_1(t+1), \ldots, \sigma_{r-1}(t+1)) = a(t).\begin{pmatrix} q_1 & q_2 & \cdots & q_r \\ & & & 0 \\ & I_{r-1} & & \vdots \\ & & & 0 \end{pmatrix} + m(t)$$

**Définition 6.16.2** (Matrice compagnon)**.** *Cette matrice notée $M$ s'appelle la matrice compagnon du FCSR en mode Galois.*

$M$ est une matrice dans $\mathbb{Z}$. Elle caractérise le FCSR en mode Galois. Donc un FCSR en mode Galois peut être défini par le couple $(\mathbb{F}_p, M)$ ou par le triplet $(\mathbb{F}_p, r, q)$ avec $q$ étant toujours l'entier de connexion.

**Théorème 6.16.1.** *Soit un FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$ en mode Galois. Soit un état initial $(a_0(0), \ldots, a_{r-1}(0), m_1(0), \ldots, m_r(0))$ et sa séquence de sorties $\underline{a}_0$. Alors $\alpha_0$ est un nombre rationnel de la forme suivante :*

$$\alpha_0 = \frac{s}{q} \text{ où } -s = a_0(0) + a_1(0)p + \ldots + a_{r-1}(0)p^{r-1} + m_1(0)p + \ldots + m_r(0)p^r.$$

*Démonstration.* $\alpha$ vérifie le système linéaire à coefficients dans $\mathbb{Z}$ suivant :

$$\alpha(I_r - pM) = a(0) + pm(0).$$

$I - pM$ est une matrice dans $\mathcal{M}_r(\mathbb{Z})$. L'anneau $\mathbb{Z}$ étant commutatif, il existe une comatrice de $I - pM$ notée $\texttt{Comat}(I - pM)$ telle que

$$(I - pM).\texttt{Comat}(I - pM) = \det(I - pM).I.$$

$\det(I - pM) \equiv 1 \mod p$ dans $\mathbb{Z}$. Il est donc non nul et inversible dans $\mathbb{Q}$. On a alors :

$$\alpha = \frac{1}{\det(I - pM)}\Big(a(0) + pm(0)\Big).\texttt{Comat}(I - pM).$$

$\alpha$ est donc un vecteur de nombre rationnel dans $\mathbb{Q}$ ayant pour même dénominateur $\det(I - pM)$. On peut calculer les numérateurs, en particulier pour $\alpha_0$, c'est le produit scalaire entre la première colonne de la comatrice et $a(0) + pm(0)$. On démontre par récurrence sur $r$ que $\det(I - pM) = -q = 1 - q_1 p - \ldots - q_r p^r$. La comatrice est de la forme

$$\texttt{Comat}(I - pM) = \begin{pmatrix} 1 & * & \ldots & * \\ p & * & \ldots & * \\ \vdots & \vdots & \vdots & \\ p^{r-1} & * & \ldots & * \end{pmatrix}.$$

Donc

$$\alpha_0 = -\frac{1}{q}(a(0) + pm(0)).\begin{pmatrix} 1 \\ p \\ \vdots \\ p^{r-1} \end{pmatrix}.$$

□

Avec cette méthode matricielle, on a démontré que $\alpha \in \mathbb{Q}^r$. La forme du numérateur de $\alpha_i$ se détermine en multipliant le vecteur $a(0) + pm(0))$ par la $i^{\text{ième}}$ colonne de la comatrice de $M$. Le dénominateur est toujours $-q = \det(I - pM)$.

**Corollaire 6.16.1.** *Soit un FCSR $(\mathcal{F} = (\mathbb{F}_p, r, q)$. Les séquences de sorties de chaque cellule sont périodiques. La période divise l'ordre de $p$ modulo $q$. Si $-1 \leq \alpha_i \leq 0$, alors la séquence de sorties $\underline{a}_i$ est strictement périodique.*

*Démonstration.* Ce corollaire est une conséquence du corollaire 6.5.1. □

La proposition 6.8.1 donne la représentation exponentielle des FCSR séquences en mode Galois :

$$a_i = (-sp^{-i}) \pmod q \pmod p.$$

Une séquence générée par un FCSR en mode Galois peut être générée par un FCSR en mode Fibonacci.

**Théorème 6.16.2.** *Soit un FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$ en mode Galois. Soit un état initial $s(0) = (a(0), m(0))$. La séquence de sorties $\underline{a}_0$ peut être générée par le FCSR $\mathcal{F} = (\mathbb{F}_{p^n}, r, q)$ en mode Fibonacci à partir de l'état initial*

$$a(0) = (a_0(0), \ldots, a_0(r-1)).$$

*Démonstration.* D'après l'algorithme 6.7.1, on peut déterminer une mémoire initiale $m$ tel que l'état initial $(a_0(0), \ldots, a_0(r-1), m)$ génère la séquence $\underline{a}_0$ à partir du FCSR $\mathcal{F} = (\mathbb{F}_p, r, q)$ en mode Fibonacci. □

Les FCSR séquences en mode Galois sont donc des FCSR séquences en mode Fibonacci.

## 6.17 Généralisation et mode Ring

Les FCSRs en mode Ring ont été introduits et étudiés par Arnault, Berger, Lauradoux, Minier, et Pousse [24].

### 6.17.1 Définitions et Conceptions

**Définition 6.17.1** (FCR). *Un Feedback with Carry Registers (FCR) construit sur $\mathbb{F}_p$ de longueur $r$ et de matrice de transition $T = (t_{i,j})_{i,j} \in \mathcal{M}_{r\times r}(\mathbb{F}_p)$ est un automate ou générateur de séquence dont les états sont des couples de la forme $s(t) = (a(t), m(t))$ où $a(t) = (a_0(t), \ldots, a_{r-1}(t)) \in (\mathbb{F}_p)^r$ et $m(t) = (m_1(t), \ldots, m_r(t)) \in \mathbb{Z}^r$ ; et dont l'opération de changement d'état est donnée par*

$$\begin{aligned} a(t+1) &= \Big(a(t)T + m(t)\Big)(\mathtt{mod}p) \\ m(t+1) &= \Big(a(t)T + m(t)\Big)(\mathtt{div}p). \end{aligned}$$

**Définition 6.17.2** (le mode Ring). *On dit qu'un FCR est en mode Ring si sa matrice de transition vérifie $t_{1,r} \neq 0$ et $t_{i+1,i} = 1$ pour tout $1 \leq i \leq r-1$.*

La matrice de transition du mode Ring est de la forme suivante

$$T = \begin{pmatrix} t_{1,1} & \ldots & t_{1,r-1} & t_{1,r} \\ 1 & \ldots & t_{2,r-1} & t_{2,r} \\ \vdots & \ddots & \vdots & \vdots \\ t_{r,1} & \ldots & 1 & t_{r,r} \end{pmatrix}.$$

On rappelle que les modes Fibonacci et les modes Galois sont représentés respectivement par ces deux matrices.

$$F = \begin{pmatrix} 0 & \ldots & 0 & q_r \\ 1 & \ldots & 0 & q_{r-1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & q_1 \end{pmatrix} \quad G = \begin{pmatrix} q_1 & \ldots & q_{r-1} & q_r \\ 1 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 \end{pmatrix}.$$

La figure 6.4 représente un FCR de taille 3.

### 6.17.2 Analyse

L'analyse des FCRs montrent que les sorties sont identiques à celles des FCSRS. Les FCRs permettent toutefois de construire des registres à retenue avec une implantation plus efficace.

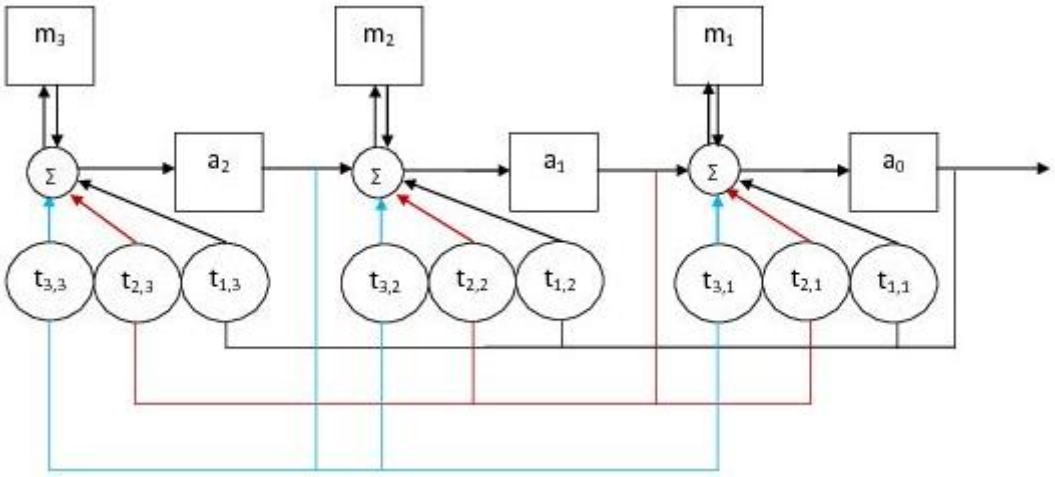



FIGURE 6.4 – Registre à rétroaction linéaire avec retenue de taille 3

**Théorème 6.17.1.** *Une séquence de sorties d'un FCR de matrice de transition $T$ est aussi générée par un FCSR d'entier de connexion* $-\det(I - XT)$.

*Démonstration.* La preuve est identique à celle du théorème 6.16.1. □

# Chapitre 7

# Registre vectoriel à rétroaction linéaire avec retenue

## 7.1 Introduction

Les LFSRs se construisent sur $\mathbb{F}_p$ comme sur $\mathbb{F}_{p^n}$. En effet, dans la théorie des valuations, dans le cas d'égale caractéristique, il existe un unique anneau de valuation discrète complet de corps résiduel $\mathbb{F}_{p^n}$ à isomorphisme près. Il s'agit des séries formelles sur le corps $\mathbb{F}_{p^n}$. Dans le cas des FCSRs, un problème se pose. Les FCSRs se construisent facilement sur $\mathbb{F}_p$, puisque l'anneau des entiers $p$-adiques est un outil facile et puissant pour l'analyse des FCSRs. Par contre, quand on cherche à construire les FCSRs sur $\mathbb{F}_{p^n}$, on bute sur les vecteurs de Witt. En effet, les FCSRs correspondent au cas d'inégale caractéristique des anneaux de valuation discrète complets de corps résiduel $\mathbb{F}_{p^n}$. Pour $n = 1$, il s'agit de $W(\mathbb{F}_p) \cong \mathbb{Z}_p$ l'anneau des entiers $p$-adiques. Mais pour $n \geq 2$, il s'agit de $W(\mathbb{F}_{p^n})$. Or l'anneau des vecteurs de Witt est difficilement utilisable de par sa structure algébrique compliquée. Il faut donc trouver un autre moyen pour étudier les FCSRs construits sur $\mathbb{F}_{p^n}$.

En 1994, Andrew Klapper introduit brièvement une conception vectorielle des FCSRs [26] mais se cantonne à une analyse formelle. Nous avons développé une analyse vectorielle des FCSRs qui donne des résultats similaires à ceux que l'on obtient pour les FCSRs. La méthode d'analyse repose sur l'anneau de valuation discrète complet $\mathbb{Z}_p[X]/(P)$ (voir corollaire 4.8.2) où $P$ est un polynôme irréductible et unitaire sur $\mathbb{F}_P$ relevé canoniquement sur $\mathbb{Z}_p$. Nous avons présenté ces résultats pour la première fois devant l'équipe Maathicah de l'Université Paris 8 puis nous avons publié une communication à la revue SETA 2010 aux éditions Springer [27], communication exposée lors des conférences SETA 2010 à Paris Telecom. Dans ce chapitre, nous présentons ces résultats sur les FCSRs Vectoriels en mode Fibonacci.

## 7.2 Le mode Fibonacci

### 7.2.1 Formalisme

L'entier $p$ reste un nombre premier et $n$ un entier quelconque. Nous conservons le même schéma que les FCRS sur $\mathbb{F}_p$. Cependant, nous devons redéfinir les espaces sur lesquels nous opérons. Le corps $\mathbb{F}_{p^n}$ est un $\mathbb{F}_p$-espace vectoriel de dimension $n$. Il est unique à isomorphisme près et se construit à l'aide d'un polynôme $P$ de degré $n$ irréductible sur $\mathbb{F}_p$. Pour tout $p$ premier et pour tout $n$, il existe au moins un tel polynôme. On le choisit unitaire. Le corps $\mathbb{F}_{p^n}$ est isomorphe à $\mathbb{F}_p[X]/(P)$. Le choix du polynôme est important. En effet, sa forme influe sur la difficulté des calculs du registre puisque le polynôme définit les lois d'addition et de multiplication. En règle générale, on choisira un trinôme. L'existence de telle forme trinomiale sera étudiée par la suite.

Pour les FCSRs, l'état initial est relevé dans $\mathbb{Z}$. Ici, nous choisissons le relèvement canonique de $P$ dans $\mathbb{Z}[X]$ identifiée à lui même. Le polynôme $P$ reste irréductible dans $\mathbb{Z}$ puisqu'il l'est sur $\mathbb{F}_p$ et qu'il est unitaire donc de contenu primitif. On construit $\mathbb{Z}[X]/(P)$ qui est un $\mathbb{Z}$-module libre de rang $n$.

Enfin, pour décrire les calculs vectoriels, nous devons fixer une base. On choisit la base canonique $\left\{1, \bar{X}, \ldots, \bar{X}^{n-1}\right\}$ où $\bar{X}$ est la classe de $X$ modulo $P$. On la notera $\mathcal{B}$ pour $\mathbb{Z}[X]/(P)$. Cette méthode vectorielle permet d'obtenir des résultats facilement implémentables en hardware comme en software.

**Définition 7.2.1** (automate VFCSR)**.** *Un Feedback with Carry Shift Register Vectoriel ou VFCSR en mode Fibonacci sur le triplet $(\mathbb{F}_p, P, \mathcal{B})$ de taille $r$ et de coefficients de connexion $q_1, \ldots, q_r \in \mathbb{F}_p[X]/(P)$ est un automate ou un générateur de séquences dont les états sont des éléments*

$$s = (a_0, a_1, \ldots, a_{r-1}, m_{r-1})$$

*où les $a_i$ sont dans $\mathbb{F}_p[X]/(P)$ et $m_{r-1}$ est dans $\mathbb{Z}[X]/(P)$ ; et dont le changement d'état s'opère de la manière suivante :*
*On écrit tous les éléments sous forme de vecteur.*

$$\begin{aligned}
\forall\, i \in \mathbb{N}, \quad a_i &= \sum_{j=0}^{j=n-1} a_j^i \bar{X}^j \ \text{ où } a_j^i \in \{0, 1, \ldots, p-1\}, \\
\forall\, 1 \leq i \leq r, \quad q_i &= \sum_{j=0}^{j=n-1} q_j^i \bar{X}^j \ \text{ où } q_j^i \in \{0, 1, \ldots, p-1\}, \\
\forall\, i \geq r-1, \quad m_i &= \sum_{j=0}^{j=n-1} m_j^i \bar{X}^j \ \text{ où } m_j^i \in \mathbb{Z}.
\end{aligned}$$

*On prend le relèvement canonique des $a_i$ et des $q_i$ dans la base $\mathcal{B}$ puis on calcule*

$$\sigma_r = \sum_{i=1}^{i=r} q_i a_{r-i} + m_{r-1}$$

*comme un vecteur sur $\mathcal{B}$. Pour tout $i \geq r$, $\sigma_i = \sum_{j=0}^{j=n-1} \sigma_j^i \bar{X}^j$ où $\sigma_j^i \in \mathbb{Z}$. L'élément $\sigma$ est une expression polynomiale en $\bar{X}$ de degré $2n-2$ et on élimine les degrés strictement supérieurs à $n-1$ en utilisant l'expression vectorielle des puissances $\bar{X}^i$ dans la base $\mathcal{B}$ déterminée par $P$. Supposons que pour tout $j \geq n$,*

$$X^j = \sum_{t=0}^{t=n-1} b_t^j \bar{X}^t \text{ où } b_t^j \in \mathbb{Z}.$$

*On obtient les coordonnées de $\sigma$ par des calculs directs,*

$$\sigma_t^r = \sum_{k=0}^{k=t} \sum_{i=1}^{i=r} (q_k^i a_{t-k}^{r-i}) + \sum_{j=n}^{j=2n-2} (b_t^j \sum_{k=j-n+1}^{k=n-1} \sum_{i=1}^{i=r} (q_k^i a_{j-k}^{r-i})) + m_t^{r-1}.$$

*Puis on calcule les coordonnés de $a_r$ et celle de $m_r$ dans la base $\mathcal{B}$,*

$$a_t^r = \sigma_t^r \pmod p \text{ et } m_t^r = \frac{1}{p}(\sigma_t^r - a_t^r).$$

*La fonction de retour (feedback function) est $f(s) = (a_1, \ldots, a_r, m_{r-1})$ et la fonction de sorties (output function) est $g(x_0, \ldots, x_{r-1}, y) = x_0$. Le FCSR vectoriel génère une séquence vectorielle infinie*

$$\underline{a} = (g(s), g(f(s)), g(f^2(s)), \ldots) = (a_0, a_1, a_2, \ldots).$$

*$s$ est appelé l'état initial, $q_1, \ldots, q_r$ les coefficients de connexion de la récurrence et la séquence entière $\underline{m} = (m_{r-1}, m_r, \ldots)$ est appelée séquence mémoire.*

**Définition 7.2.2.** *Les séquences de sorties des VFCSR sont appelées VFCSR-séquences.*

### 7.2.2 Calcul vectoriel

Dans cette section, on détaille les techniques de calcul vectoriel qu'on utilise pour les VFCSRs. Le calcul $\sigma_z$, pour tout $z \geq r$, se fait de la manière suivante

$$\begin{aligned}
\sigma_z &= \sum_{i=1}^{i=r} \underbrace{q_i} \quad \underbrace{a_{z-i}} \quad + \underbrace{m_{z-1}} \\
&= \sum_{i=1}^{i=r} \sum_{k=0}^{k=n-1} q_k^i \bar{X}^k \sum_{j=0}^{j=n-1} a_j^{z-i} \bar{X}^j + \sum_{j=0}^{j=n-1} m_j^{z-1} \bar{X}^j \\
&= \sum_{i=1}^{i=r} \sum_{j,k=0}^{n-1} (q_k^i a_j^{z-i}) \bar{X}^{k+j} + \sum_{j=0}^{j=n-1} m_j^{z-1} \bar{X}^j \\
&= \sum_{j,k=0}^{n-1} \sum_{i=1}^{i=r} (q_k^i a_j^{z-i}) \bar{X}^{k+j} + \sum_{j=0}^{j=n-1} m_j^{z-1} \bar{X}^j \\
\sigma_z &= \sum_{j=0}^{2n-2} \Big( \sum_{k+l=j}^{0 \leq l,k \leq n-1} \sum_{i=1}^{i=r} q_k^i a_l^{z-i} \Big) \bar{X}^j + \sum_{j=0}^{j=n-1} m_j^{z-1} \bar{X}^j
\end{aligned}$$

On exprime les $\bar{X}^j$ dans la base $\mathcal{B}$. Pour cela, on utilise les lois de multiplication et d'addition définies le polynôme $P$. On suppose que $X^j = \sum_{t=0}^{t=n-1} b_t^j \bar{X}^t$ où $b_t^j \in \mathbb{F}_p$.

$$\begin{aligned}
\sigma_z &= \sum_{j=n}^{j=2n-2} \sum_{k+l=j}^{0\leq l,k\leq n-1} \sum_{i=1}^{i=r} (q_k^i a_l^{z-i}) \sum_{t=0}^{t=n-1} (b_t^j \bar{X}^t) + \sum_{j=0}^{n-1} \sum_{k+l=j}^{0\leq l,k\leq n-1} \sum_{i=1}^{i=r} (q_k^i a_l^{z-i}) \bar{X}^j + \sum_{t=0}^{t=n-1} m_t^{z-1} \bar{X}^t \\
&= \sum_{t=0}^{t=n-1} \sum_{j=n}^{j=2n-2} b_t^j \sum_{k=j-n+1}^{k=n-1} \sum_{i=1}^{i=r} (q_k^i a_{j-k}^{z-i}) \bar{X}^t + \sum_{t=0}^{t=n-1} \sum_{k=0}^{k=t} \sum_{i=1}^{i=r} (q_k^i a_{t-k}^{z-i}) \bar{X}^t + \sum_{t=0}^{t=n-1} m_t^{z-1} \bar{X}^t \\
\sigma_z &= \sum_{t=0}^{t=n-1} \Big[ \sum_{j=n}^{j=2n-2} (b_t^j \sum_{k=j-n+1}^{k=n-1} \sum_{i=1}^{i=r} (q_k^i a_{j-k}^{z-i})) + \sum_{k=0}^{k=t} \sum_{i=1}^{i=r} (q_k^i a_{t-k}^{z-i}) + m_t^{z-1} \Big] \bar{X}^t.
\end{aligned}$$

On en déduit donc les coordonnées dans la base $\mathcal{B}$ de $\sigma_r$ données dans la définition des VFCSRs. De la relation $\sigma_z = pm_z + a_z$, on obtient la relation de récurrence vectorielle suivante

$$a_t^z = \sum_{k=0}^{k=t} \sum_{i=1}^{i=r} (q_k^i a_{t-k}^{z-i}) + \sum_{j=n}^{j=2n-2} (b_t^j \sum_{k=j-n+1}^{k=n-1} \sum_{i=1}^{i=r} (q_k^i a_{j-k}^{z-i})) + m_t^{z-1} - pm_t^z.$$

## 7.3 Analyse des VFCSRs

Dans cette section, nous présentons les bénéfices de cette construction vectorielle dans l'analyse des FCSRs construits sur $\mathbb{F}_{p^n}$. En effet, on construit une correspondance entre $\mathbb{F}_{p^n}^{\mathbb{N}}$ l'ensemble des séquences et ${\mathbb{Z}_p}^n$ le produit direct de l'anneau des entiers $p$-adiques. ainsi, on évite les vecteurs de Witt et leur structure algébrique complexe. Les séquences de sorties du VFCSR correspondent à $n$ séquences $p$-aires.

$$\underline{a} = (a_i)_{i\in\mathbb{N}} = \sum_{j=0}^{j=n-1} (a_j^i)_{i\in\mathbb{N}} \bar{X}^j = \sum_{j=0}^{j=n-1} \underline{a}_j \bar{X}^j$$

$$\underline{a} = \begin{pmatrix} \underline{a}_0 \\ \underline{a}_1 \\ \vdots \\ \underline{a}_{n-1} \end{pmatrix} = \begin{pmatrix} a_0^0 & a_0^1 & a_0^2 \cdots \\ \vdots & \vdots & \vdots \\ a_{n-1}^0 & a_{2n-1}^1 & a_{n-1}^2 \cdots \end{pmatrix}$$

À chaque séquence $p$-aire, on associe son développement $p$-adique noté $\beta_t$ et on obtient un vecteur $p$-adique.

$$\beta = \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_{n-1} \end{pmatrix} = \begin{pmatrix} a_0^0 & +a_0^1 p & +a_0^2 p^2 & +\cdots \\ \vdots & \vdots & \vdots & \\ a_{n-1}^0 & +a_{n-1}^1 p & +a_{n-1}^2 p^2 & +\cdots \end{pmatrix}.$$

On a donc construit une correspondance entre ${\mathbb{F}_{p^n}}^{\mathbb{N}}$ et ${\mathbb{Z}_p}^n$.

$$\begin{aligned}
{\mathbb{F}_p}^{\mathbb{N}} &\to {\mathbb{Z}_p}^n \\
\underline{a} &\mapsto \Big( \sum_{z\in\mathbb{N}} a_t^z p^z \Big)_{t=0}^{t=n-1}.
\end{aligned}$$

L'entier de connexion joue un rôle central dans l'analyse des FCSRs. Ici, la construction vectorielle nécessite d'exprimer l'entier de connexion sous forme vectorielle. En effet, $q$ est un élément du $\mathbb{Z}$-module libre $\mathbb{Z}[X]/(P)$.

$$q = \sum_{i=1}^{i=r} q_i p^i - 1 = \sum_{i=1}^{i=r} \sum_{j=0}^{j=n-1} q_j^i \bar{X}^j p^i - 1 = \sum_{j=0}^{j=n-1} (\sum_{i=1}^{i=r} q_j^i p^i) \bar{X}^j - 1.$$

$$\begin{array}{c} \\ 1 \\ \bar{X} \\ \vdots \\ \bar{X}^{n-1} \end{array} \begin{array}{c} p^r \\ \left( \begin{array}{c} q_0^r \\ q_1^r \\ \vdots \\ q_{n-1}^r \end{array} \right) \\ \downarrow \\ q_r \end{array} \cdots \begin{array}{c} p \\ \left( \begin{array}{c} q_0^1 \\ q_1^1 \\ \vdots \\ q_{n-1}^1 \end{array} \right) \\ \downarrow \\ q_1 \end{array} \begin{array}{c} \\ \left( \begin{array}{c} \rightarrow \tilde{q}_0 \\ \rightarrow \tilde{q}_1 \\ \vdots \\ \rightarrow \tilde{q}_{n-1} \end{array} \right) \\ \\ \\ \end{array}$$

On pose $\tilde{q}_0 = \sum_{i=1}^{i=r} q_0^i p^i - 1$ et $\tilde{q}_j = \sum_{i=1}^{i=r} q_j^i p^i$ pour tout $1 \leq j \leq n-1$. Ce sont les coordonnées vectorielles de $q$ dans la base $\mathcal{B}$.

$$q = \begin{pmatrix} \tilde{q}_0 \\ \tilde{q}_1 \\ \vdots \\ \tilde{q}_{n-1} \end{pmatrix}_{\mathcal{B}} - \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{\mathcal{B}}.$$

**Définition 7.3.1** (vecteur de connexion)**.** *On appelle $(\tilde{q}_0, \tilde{q}_1, \ldots, \tilde{q}_{n-1})$ le vecteur de connexion du VFCSR sur le triplet $(\mathbb{F}_{p^n}, P, \mathcal{B})$.*

**Proposition 7.3.1.** *Soit un VFCSR sur le triplet $(\mathbb{F}_{p^n}, P, \mathcal{B})$ de vecteur de connexion $(\tilde{q}_0, \tilde{q}_1, \ldots, \tilde{q}_{n-1})$. Soit $\underline{a}$ une séquence de sorties et $\beta$ son vecteur p-adique associé. Alors $\beta$ vérifie un système linéaire à coefficients entiers de la forme suivante*

$$\left\{ \beta_t - \sum_{j=n}^{j=2n-2} \sum_{k=j-n+1}^{k=n-1} (b_t^j \tilde{q}_k \beta_{j-k}) - \sum_{k=0}^{k=t} \tilde{q}_k \beta_{t-k} = \tilde{p}_t \right\}_{t=0}^{t=n-1},$$

*où les $\tilde{p}_t$ sont des entiers déterminés par l'état initial.*

*Démonstration.* On fait un calcul direct :

$$\begin{aligned}
\beta_t &= \sum_{z=0}^{z=+\infty} a_t^z p^z \\
&= \sum_{z=0}^{z=r-1} a_t^z p^z + \sum_{z=r}^{z=+\infty} a_t^z p^z \\
&= \sum_{z=0}^{z=r-1} a_t^z p^z + \sum_{z=r}^{z=+\infty} \Big[ \sum_{j=n}^{2n-2} \sum_{k=j-n+1}^{k=n-1} \sum_{i=1}^{i=r} (b_t^j q_k^i a_{j-k}^{z-i}) + \sum_{k=0}^{k=t} \sum_{i=1}^{i=r} (q_k^i a_{t-k}^{z-i}) \Big] p^z \\
&\quad + \sum_{z=r}^{z=+\infty} \Big[ m_t^{z-1} - p m_t^z \Big] p^z \\
&= \sum_{z=0}^{z=r-1} a_t^z p^z + \sum_{j=n}^{2n-2} \sum_{k=j-n+1}^{k=n-1} \Big[ b_t^j \sum_{i=1}^{i=r} \Big( q_k^i p^i \sum_{z=r}^{z=+\infty} (a_{j-k}^{z-i} p^{z-i}) \Big) \Big] \\
&\quad + \sum_{k=0}^{k=t} \sum_{i=1}^{i=r} \Big[ q_k^i p^i \sum_{z=r}^{z=+\infty} (a_{t-k}^{z-i} p^{z-i}) \Big] + m_t^{r-1} p^r \\
&= \sum_{z=0}^{z=r-1} a_t^z p^z + \sum_{j=n}^{2n-2} \sum_{k=j-n+1}^{k=n-1} \Big[ b_t^j \sum_{i=1}^{i=r} \Big( q_k^i p^i (\beta_{j-k} - \sum_{z=0}^{z=r-i-1} (a_{j-k}^z p^z) \Big) \Big] \\
&\quad + \sum_{k=0}^{k=t} \sum_{i=1}^{i=r} \Big[ q_k^i p^i \Big( \beta_{t-k} - \sum_{z=0}^{z=r-i-1} (a_{t-k}^z p^z) \Big) \Big] + m_t^{r-1} p^r \\
&= \sum_{z=0}^{z=r-1} a_t^z p^z + \sum_{j=n}^{2n-2} \sum_{k=j-n+1}^{k=n-1} (b_t^j \tilde{q}_k \beta_{j-k}) - \sum_{j=n}^{2n-2} \sum_{k=j-n+1}^{k=n-1} \sum_{i=1}^{i=r} \sum_{z=0}^{z=r-i-1} (b_t^j q_k^i a_{j-k}^z p^{z+i}) \\
&\quad + \sum_{k=0}^{k=t} (\tilde{q}_k \beta_{t-k}) - \sum_{k=0}^{k=t} \sum_{i=1}^{i=r} \sum_{z=0}^{z=r-i-1} (q_k^i a_{t-k}^z p^{i+z}) + m_t^{r-1} p^r \\
\beta_t &= \sum_{z=0}^{z=r-1} a_t^z p^z + m_t^{r-1} p^r - \sum_{j=n}^{2n-2} \sum_{k=j-n+1}^{k=n-1} \sum_{i=1}^{i=r} \sum_{z=0}^{z=r-i-1} (b_t^j q_k^i a_{j-k}^z p^{z+i}) - \sum_{k=0}^{k=t} \sum_{i=1}^{i=r} \sum_{z=0}^{z=r-i-1} (q_k^i a_{t-k}^z p^{z+i}) \\
&\quad + \sum_{j=n}^{2n-2} \sum_{k=j-n+1}^{k=n-1} (b_t^j \tilde{q}_k \beta_{j-k}) + \sum_{k=0}^{k=t} (\tilde{q}_k \beta_{t-k}).
\end{aligned}$$

On pose

$$\tilde{p}_t = \sum_{z=0}^{z=r-1} a_t^z p^z + m_t^{r-1} p^r - \sum_{j=n}^{2n-2} \sum_{k=j-n+1}^{k=n-1} \sum_{i=1}^{i=r} \sum_{z=0}^{z=r-i-1} (b_t^j q_k^i a_{j-k}^z p^{z+i}) - \sum_{k=0}^{k=t} \sum_{i=1}^{i=r} \sum_{z=0}^{z=r-i-1} (q_k^i a_{t-k}^z p^{z+i}).$$

□

La matrice représentant ce système a des coefficients diagonaux congrus à 1 modulo $p$ et tous ses autres coefficients multiples de $p$. Donc le déterminant de cette matrice est congru à 1 modulo $p$. Elle est donc inversible. Ses coefficients sont des combinaisons linéaires des coordonnés vectorielles de l'entier de connexion $q$ dans la base $\mathcal{B}$. Le résolution du système donne comme solution

$$\beta = \frac{1}{|\det(M)|} \mathtt{sgn}(\det M) \mathtt{Comat}(M) (\tilde{p}_t)_{0 \leq t \leq n-1},$$

où $\mathtt{sgn}(x)$ représente le signe de $x$ et $\mathtt{Comat}(M)$ représente la comatrice de $M$.

**Définition 7.3.2** (Matrice de connexion)**.** *On appelle cette matrice la matrice de connexion du VFCSR sur le triplet* $(\mathbb{F}_p, P, \mathcal{B})$.

**Théorème 7.3.1.** *Soit un VFCSR sur le triplet* $(\mathbb{F}_p, P, \mathcal{B})$ *de vecteur de connexion* $(\tilde{q}_0, \tilde{q}_1, \ldots, \tilde{q}_{n-1})$ *et de matrice de connexion* $M$*. Pour toute séquence de sorties* $\underline{a}$*, son vecteur p-adique associé est un vecteur de rationnels dans* $\frac{1}{|\det M|}\mathbb{Z}^n$ *et* $\det M$ *est un entier impair.*

*Démonstration.* C'est une conséquence directe de la résolution du système obtenu précédemment. □

## 7.4 Norme de connexion et Changement de base

Dans cette section, nous présentons l'analyse du VFCSR sous une forme intrinsèque, c'est-à-dire ne dépendant pas de la base choisie. Rappelons que $\mathbb{Q}[X]/(P)$ est une extension du corps $\mathbb{Q}$ de degré $n$. En effet, $P$ est irréductible sur $\mathbb{Z}$ et de contenu 1, donc il est irréductible sur $\mathbb{Q}$. Comme $\mathbb{Q}$ est un corps, $\mathbb{Q}[X]$ est euclidien. L'idéal principal engendré par $P$ est maximal. Le quotient $\mathbb{Q}[X]/(P)$ est donc un corps. C'est un $\mathbb{Q}$-espace vectoriel de dimension $n$.

**Définition 7.4.1** (Norme)**.** *Soit* $x$ *un élément de* $\mathbb{Q}[X]/(P)$*. La norme de* $x$ *est le déterminant de la transformation linéaire définie par la multiplication par l'élément* $x$ *dans* $\mathbb{Q}[X]/(P)$*. Cette norme sera notée dans la suite* $\mathbb{N}_{\mathbb{Q}}^{\mathbb{Q}[X]/(P)}(x)$ *ou* $\mathbb{N}(x)$*. [45]*

**Lemme 7.4.1.** *La norme de* $q$ *est entière.*

*Démonstration.* Dans la base $\mathcal{B}$, $q$ a des coordonnées entières. Sa matrice de multiplication est donc à de coefficients entiers et donc son déterminant est aussi entier. □

**Proposition 7.4.1.** *La matrice de connexion* $M$ *est la matrice de multiplication dans la base canonique* $\mathcal{B}$ *de la transformation linéaire définie par la multiplication par* $-q$*. Le déterminant de* $M$ *est la norme de* $-q$*.*

$$\det M = \mathtt{N}(-q) = (-1)^n \mathtt{N}(q).$$

*Démonstration.* Nous devons faire le calcul direct. soit $\beta$ un élément de $\mathbb{Q}[X]/(P)$.

$$\begin{aligned}
-q\beta &= (1 - \sum_{k=0}^{k=n-1} \tilde{q}_k \bar{X}^k)(\sum_{j=0}^{j=n-1} \beta_j \bar{X}^j) \\
&= \sum_{j=0}^{j=n-1} \beta_j \bar{X}^j - \sum_{j=0}^{j=n-1} \sum_{k=0}^{k=n-1} \beta_j \tilde{q}_k \bar{X}^{j+k} \\
&= \sum_{j=0}^{j=n-1} \beta_j \bar{X}^j - \sum_{t=0}^{t=2n-2} \sum_{k+j=t} \beta_j \tilde{q}_k \bar{X}^t \\
&= \sum_{j=0}^{j=n-1} \beta_j \bar{X}^j - \sum_{t=0}^{t=n-1} \sum_{k=0}^{k=t} \tilde{q}_k \beta_{t-k} \bar{X}^t - \sum_{t=0}^{t=n-1} \sum_{j=n}^{j=2n-2} b_t^j \sum_{k=j-n+1}^{j=n-1} \tilde{q}_k \beta_{j-k} \bar{X}^t
\end{aligned}$$

La $t^{\text{ième}}$ coordonnée de $-q\beta$ dans la base $\mathcal{B}$ est

$$\beta_t - \sum_{k=0}^{k=t} \tilde{q}_k \beta_{t-k} - \sum_{j=n}^{j=2n-2} \sum_{k=j-n+1}^{j=n-1} b_t^j \tilde{q}_k \beta_{j-k}.$$

Elle coincide avec la $^{\text{ième}}$ ligne du système linéaire définie par $M$. Donc la matrice de multiplication par $-q$ est $M$. Le déterminant de $M$ est donc $\mathtt{N}(-q)$ □

Le vecteur $p$-adique associé à la séquence de sorties du VFCSR est donc un vecteur de rationnels ayant le même dénominateur $\mathtt{N}(-q)$ où $q$ est l'entier de connexion. La norme de $-q$ ne dépend pas de la base choisie. En effet, le changement de base revient à remplacer $M$ par une matrice équivalente, c'est-à-dire de la forme $PMP^{-1}$ où $P$ est inversible et de déterminant $\det P = 1$. Choisissons donc une autre base.
Posons la base

$$\mathbb{F}_{p^n} \cong \mathbb{F}_p \bar{\mu}_1 + \ldots + \mathbb{F}_p \bar{\mu}_{n-1}$$

et son relèvement dans $\mathbb{Z}[X]/(P)$

$$\mathbb{Z}\mu_1 + \ldots + \mathbb{Z}\mu_{n-1}.$$

Définissons la loi de multiplication de la manière suivante

$$\mu_j \mu_k = \sum_{t=0}^{t=n-1} b_t^{j,k} \mu_t.$$

En redéfinissant l'écriture vectorielle de tous les paramètres et données du registre dans cette nouvelle base, on obtient la relation de récurrence vectorielle suivante :

$$a_r^t = \sum_{j,k=0}^{n-1} b_t^{j,k} \sum_{i=1}^{i=r} q_j^i a_k^{r-i} + m_t^{r-1} - p m_t^r.$$

Les séquences de sorties s'écrivent aussi comme vecteurs de séquences $p$-aires dans cette nouvelle base. Nous avons la correspondance entre $(\mathbb{F}_{p^n})^{\mathbb{N}}$ et $(\mathbb{Z}_p)^n$ définie par

$$\begin{array}{rcl} (\mathbb{F}_{p^n})^{\mathbb{N}} & \to & (\mathbb{Z}_p)^n \\ \underline{a} = \sum_{t=0}^{t=n-1} \underline{a}_t \mu_t & \mapsto & \beta = \left( \sum_{z=0}^{z=+\infty} a_t^z p^z \right)_{t=0}^{t=n-1} \end{array}.$$

$\beta$ vérifie un système linéaire à coefficients entiers de la forme suivante

$$\left\{ \beta_t - \sum_{j,k=0}^{n-1} b_t^{j,k} \tilde{q}_j \beta_k = \tilde{p}_t \right\}_{0 \le t \le n-1}$$

où les $\tilde{p}_t$ sont des entiers à déterminer. On vérifie de même que la matrice qui définit ce système linéaire est la matrice de la transformation linéaire définie par la multiplication

par $-q$ dans la base $\{\mu_1, \ldots, \mu_{n-1}\}$. Les coefficients diagonaux sont congrus à 1 modulo $p$ tandis que les autres coefficients sont congrus à 0 modulo $p$. Donc son déterminant qui est la norme de $-q$ est inversible. On vient de vérifier par des calculs explicites que le quelque soit la base sur laquelle nous construisons les VFCSRs, les vecteurs $p$-adiques associés aux séquences de sorties sont des vecteurs dans $\frac{1}{|N(q)|}\mathbb{Z}^n$.

**Définition 7.4.2** (Norme de connexion)**.** *La valeur absolue de la norme de l'entier de connexion est appelée la norme de connexion du FCSR construit sur le couple* $(\mathbb{F}_p, P)$ *et on la notera* $\tilde{q}$*.*

## 7.5 Périodicité

Dans cette section, nous discutons de la périodicité des séquences de sorties d'un VFCSR. Toute séquence de sorties peut être décomposée en vecteur de séquences dites $p$-aires. Nous étudions la périodicité de la séquences de sorties à travers la périodicité de ces séquences $p$-aires qui forment ses composantes vectorielles.

**Proposition 7.5.1.** *Soit* $\underline{a} = (\underline{a}_t)_{0 \le t \le n-1}$ *une séquence vectorielle dans une base* $\mathbb{B}$*. La séquence* $\underline{a}$ *est périodique si et seulement si* $\underline{a}_t$ *est périodique. La période de* $\underline{a}$ *est le plus petit commun multiple des périodes de* $\underline{a}_t$*. La séquence* $\underline{a}$ *est strictement périodique si et seulement si pour tout* $t$*,* $\underline{a}_t$ *est strictement périodique.*

*Démonstration.* La preuve est évidente. □

**Théorème 7.5.1.** *Toute séquence générée par un VFCSR construit sur le triplet* $(\mathbb{F}_p, P, \mathcal{B})$ *est périodique. Elle est strictement périodique si et seulement si* $-1 \le \beta_t \le 0$ *pour tout* $0 \le t \le n-1$*.*

*Démonstration.* D'après le théorème 7.3.1, $\beta_t$ l'entier $p$-adique associé à $\underline{a}_t$ est rationnel, donc d'après le théorème 3.10.2, $\underline{a}$ est périodique. Elle est strictement périodique si et seulement si pour tout $0 \le t \le n-1$, $\underline{a}_t$ est strictement périodique. La séquence $\underline{a}_t$ est strictement périodique si $-1 \le \beta_t \le 0$. Le reste suit. □

**Corollaire 7.5.1.** *Soit* $\beta = \left(\frac{\tilde{r}_t}{\tilde{q}}\right)_{t=0}^{t=n-1}$ *le vecteur p-adique associé à la séquence de sorties* $\underline{a}$ *d'un* ***VFCSR****. S'il existe* $t$ *tel que* $\tilde{r}_t \notin \tilde{q}\mathbb{Z}$*, alors :*

$$\mathtt{per}(\underline{a}) = \mathtt{PPCM}_{0 \le t \le n-1} \left\{ \mathtt{ord}_{q_t}(p); \quad q_t = \frac{\tilde{q}}{\mathtt{PGCD}(\tilde{q}, \tilde{p}_t)} \text{ et } p_t \notin \tilde{q}\mathbb{Z} \right\}.$$

*Sinon* $\mathtt{per}(\underline{a}) = 1$*.*

*Démonstration.* Si $\beta_t = \frac{\tilde{r}_t}{\tilde{q}}$, on distingue deux cas : si $\tilde{q}$ divise $\tilde{r}_t$, alors $\mathtt{per}(\underline{a}_t) = 1$, sinon on réduit $\beta_t$ sous forme irréductible $\frac{\tilde{r}'_t}{\tilde{q}'}$ et $\mathtt{per}(\underline{a}_t) = \mathtt{ord}_{\tilde{q}'}(p)$ et $\tilde{q}' = \frac{\tilde{q}}{\mathtt{PGCD}(\tilde{q}, \tilde{r}_t)}$.
La période de $\underline{a}$ est le PPCM des périodes des $\underline{a}_t$. Si pour tout $0 \le t \le n-1$, $\tilde{q}$ divise $\tilde{r}_t$, alors $\mathtt{per}(\underline{a}_t) = 1$ pour tout $0 \le t \le n-1$ et donc $\mathtt{per}(\underline{a}) = 1$. Sinon, $\mathtt{per}(\underline{a})$ est le PPCM des périodes de $\underline{a}_t$ tel que $\tilde{q}$ ne divise pas $\tilde{r}_t$. □

L'entier $\tilde{q}$ est représenté par une $n$-forme dont les arguments sont $\tilde{q}_0 - 1, \tilde{q}_1, \ldots, \tilde{q}_{n-1}$. De plus, la période divise toujours $\mathtt{ord}_{\tilde{q}}(p)$ et $\mathtt{ord}_{\tilde{q}} = (p) \leq \tilde{q} - 1$. Donc la période maximale est $\tilde{q} - 1$.

## 7.6 Comportement de la mémoire

Dans le cas des FCSRs $p$-aires, nous avons vu que la mémoire croit ou décroit vers l'intervalle $[0, \sum_{i=1}^{i=r} q_i[$ puis y reste indéfiniment. Dans cette section, nous étudions le comportement de la mémoire des VFCSRs.

Pour tout $0 \leq k \leq n-1$, définissons le poids de Hamming des entiers $\tilde{q}_k$

$$w_k = \sum_{i=1}^{i=r} q_k^i.$$

et définissons les constantes suivantes

$$K_t = \sum_{k=0}^{k=t} w_k + \sum_{j=n}^{j=2n-2} b_t^j \sum_{k=j-n+1}^{k=n-1} w_k.$$

**Proposition 7.6.1.** *Pour tout $0 \leq t \leq n-1$ :*

1. *Si $m_t^{r-1} \in [0, K_t[$, alors la mémoire suivante $m_t^r$ reste dans $[0, K_t[$.*
2. *Si $m_t^{r-1} = K_i$, alors la mémoire suivante $m_t^r$ décroit de manière monotone et après au plus $r$ étapes, elle est dans $[0, K_t[$.*
3. *Si $m_t^{r-1} > K_i$, alors la mémoire suivante $m_t^r$ décroit de manière monotone et après au plus $[\log_p(m_t^{r-1} - K_t)] + r$ étapes, elle est dans $[0, K_t[$.*
4. *Si $m_t^{r-1} < 0$, alors la mémoire suivante $m_t^r$ décroit de manière monotone et après au plus $[\log_p |m_t^{r-1}|] + r + 1$ étapes, elle est dans $[0, K_t[$.*

*Démonstration.* Nous démontrons la proposition pour $n = 2$. On cherche deux constantes minimales $K_0$ et $K_1$ telles qu'on ait des résultats similaires.

$$\left.\begin{array}{rcccl} 0 & \leq & m_1^{r-1} & \leq & K_1 \\ 0 & \leq & \sigma_1^r & \leq & 2w_1 + w_0 + m_1^{r-1} \end{array}\right\} \Rightarrow 0 \leq m_1^r \leq w_1 + \tfrac{w_0}{2} + \tfrac{K_1}{2}$$

$$\left.\begin{array}{rcccl} 0 & \leq & m_0^{r-1} & \leq & K_0 \\ 0 & \leq & \sigma_0^r & \leq & w_1 + w_0 + K_0 \end{array}\right\} \Rightarrow 0 \leq m_0^r \leq \tfrac{w_1}{2} + \tfrac{w_0}{2} + \tfrac{K_0}{2}$$

On cherche $K_1$ et $K_0$ tels que $w_1 + \frac{w_0}{2} + \frac{K_1}{2} \leq K_1$ et $\frac{w_1}{2} + \frac{w_0}{2} + \frac{K_0}{2} \leq K_0$. On obtient alors les constantes minimales $K_1 = 2w_1 + w_0$ et $K_0 = w_1 + w_0$. Pour le point 2), on a :

$$m_1^{r-1} = K_1 \Rightarrow K_1 \leq \sigma_1^r \leq 2K_1$$

1. Si $K_1 = 0$, alors $m_1^{r-1} = w_0 = w_1 = 0$ et donc pour tout $i$, $q_1^i = q_0^i = 0$. Du coup, $\sigma_1^r = 0 \Rightarrow a_1^r = 0 \Rightarrow m_1^r = 0$ et par récurrence $(m_1^i)_{i \geq r} = 0$. CQFD

2. Si $K_1 \geq 1$, alors :

$$\begin{array}{rcccl} K_1 & \leq & \sigma_1^r & \leq & 2K_1 \\ 1 & \leq & \sigma_1^r & \leq & 2K_1 \\ 0 & \leq & \sigma_1^r - a_1^r & \leq & 2K_1 \\ 0 & \leq & m_1^r & \leq & K_1 \end{array}$$

– Si $0 \leq m_1^r < K_1$, alors CQFD.

–

$$\begin{array}{rcl} m_1^r = K_1 & \Rightarrow & \sigma_1^r = 2K_1 + a_1^r \\ & \Rightarrow & \sum_{i=1}^{i=r} \left( q_1^i a_1^{z-i} + q_1^i a_0^{z-i} + q_0^i a_1^{z-i} \right) + K_1 = 2K_1 + a_1^r \\ & \Rightarrow & \sum_{i=1}^{i=r} \left( q_1^i a_1^{z-i} + q_1^i a_0^{z-i} + q_0^i a_1^{z-i} \right) = K_1 + a_1^r \\ & \Rightarrow & 0 \leq K_1 + a_1^r \leq K_1 \Rightarrow a_1^r = 0 \\ & \Rightarrow & \sigma_1^r = 2K_1 \end{array}$$

Cela implique que si $q_1^i = 1 \Rightarrow \left\{ \begin{array}{rcl} a_1^{r-i} & = & 1 \\ a_0^{r-i} & = & 1 \end{array} \right.$ et que si $q_0^i = 1 \Rightarrow a_1^{r-i} = 1$. Pour l'état suivant, avec l'incrémentation de $a_1^r$ et la sortie de $a_0$, on a un 0 en plus. après au plus $r-1$ états, $a_1^r$ coincide alors avec un $q_1^i$ ou un $q_0^i$ non-nul. Donc il existe $1 \leq j \leq r$ tel que :

$$\sum_{i=1}^{i=r} \left( q_1^i a_1^{z+j-i} + q_1^i a_0^{z+j-i} + q_0^i a_1^{z+j-i} \right) < 2w_1 + w_0 \Rightarrow 0 \leq m_1^{r+j} < K_1$$

Pour le point 3), on a : Posons $e_1^{r-1} = m_1^{r-1} - K_1 > 0$.

$$\begin{array}{rcl} e_1^{r-1} & = & m_1^r - K_1 = \frac{1}{2}(\sigma_1^r - a_1^r) - K_1 \\ & = & \frac{1}{2}\Big[ \sum_{i=1}^{i=r} \left( q_1^i a_1^{z+j-i} + q_1^i a_0^{z+j-i} + q_0^i a_1^{z+j-i} \right) + m_1^{r-1} - a_1^r - 2K_1 \Big] \\ & = & \frac{e_1^{r-1}}{2} + \frac{1}{2}\Big[ \sum_{i=1}^{i=r} \left( q_1^i a_1^{z+j-i} + q_1^i a_0^{z+j-i} + q_0^i a_1^{z+j-i} \right) - a_1^r - 2K_1 \Big] \\ e_1^r & \leq & \frac{e_1^{r-1}}{2} \\ e_1^r & \leq & [\frac{e_1^{r-1}}{2}] \end{array}$$

Par récurrence, on trouve $e_1^{r-1+k} \leq \frac{e_1^{r-1}}{2^k}$ et $e_1^{r-1+k} \leq \left[ \frac{e_1^{r-2+k}}{2} \right]$.

$\frac{e_1^{r-1}}{2^k} < 2 \Leftrightarrow e_1^{r-1} < 2^{k+1} \Leftrightarrow \log_2(e_1^{r-1}) < k+1 \Leftrightarrow k+1 = [\log_2(e_1^{r-1})] + 1 \Leftrightarrow k = [\log_2(e_1^{r-1})]$
$\frac{e_1^{r-1}}{2^k} < 2 \Rightarrow e_1^{r-1+k} \leq 1 \Rightarrow e_1^{r+k} \leq [\frac{1}{2}] = 0 \Rightarrow m_1^{r-k} \leq K_1$

Donc après $k = [\log_2(e_1^{r-1})]$ état, $m_1^{r-k} \leq K_1$, on revient au cas précédents et il faut au plus $r$ états pour que les mémoires $(m_1^i)_{i \geq k+r} \subseteq [0, K_1[$. Pour le point 4), on distingue deux cas :

1. Si $\sigma_1^r \geq 0$, alors $\sigma_1^r \geq a_1^r$ et donc $m_1^r \geq 0$ ce qui correspond aux propositions précédentes.
2. Si $\sigma_1^r < 0$, alors :

$$m_1^{r-1} \leq \sum_{i=1}^{i=r} \left( q_1^i a_1^{z-i} + q_1^i a_0^{z-i} + q_0^i a_1^{z-i} \right) + m_1^{r-1} < 0 \Rightarrow |\sigma_1^r| \leq |m_1^{r-1}|$$

$$\frac{\sigma_1^r - 1}{2} \leq m_1^r \leq \frac{\sigma_1^r}{2} < 0 \Rightarrow \frac{|\sigma_1^r|}{2} \leq |m_1^r| \leq \frac{|\sigma_1^r| + 1}{2}$$

Par récurrence $|m_1^{r-1+k}| \leq \frac{m_1^{r-1}}{2} + \frac{1}{2^k} + \ldots + \frac{1}{2}$.
On pose $L_1 = [\log_2(|m_1^{r-1}|)] + 1$.

$$\begin{array}{rcccl} L_1 - 1 & \leq & \log_2(|m_1^{r-1}|) & < & L_1 \\ 2^{L_1 - 1} & \leq & |m_1^{r-1}| & < & 2^{L_1} \\ \frac{1}{2} & \leq & \frac{|m_1^{r-1}|}{2^{L_1}} & < & 1 \end{array}$$

$$|m_1^{r-1+L_1}| \leq \frac{m_1^{r-1}}{2} + \frac{1}{2^{L^1}} + \ldots + \frac{1}{2} \leq 2 - \frac{1}{2^{L_1}} < 2$$

- Si $m_1^{r-1+L_1} \geq 0$, on utilise les propositions précédentes et il faut au plus $r-1$ états pour que la mémoire revienne dans l'intervalle en question.
- Si $m_1^{r-1+L_1} = -1$, alors :
  (a) Si $q_0 = q_1 = -1$ alors les mémoires $(m_1^{r-1+k})_{k \geq L_1}$ sont égales à $-1$.
  (b) Sinon il existe un $q_j^i = 1$, et ou bien $\sigma_1^{r+L_1+1} \geq 0$, ou bien $\sigma_1^{r+L_1+1} = -1$.
    i. Si $\sigma_1^{r+L_1+1} \geq 0$ alors $\sigma_1^{r+L_1+1} \geq a_1^{r+L_1+1} \Rightarrow m_1^{r+L_1+1} \geq 0$, c'est ce qu'il fallait démontrer.
    ii. Si $\sigma_1^{r+L_1+1} = -1$, alors $m_1^{r+L_1+1} = -1$ et $a_1^{r+L_1+1} = 1$. Donc les registres sont incrémentés de 1 dans les états suivants et au bout de $r-2$ états au plus, on revient au cas précédent.

□

On donnera pour exemple le cas quadratique et le cas cubique en caractéristique 2 explicités plus loin. Pour un VFCSR construit sur le triplet $(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$, nous trouvons $K_0 = w_0 + w_1$ et $K_1 = w_0 + 2w_1$. Pour le VFCSR construit sur le triplet $(\mathbb{F}_2, X^3 - X - 1, \mathcal{B})$, nous trouvons $K_0 = w_0 + w_1 + w_2$, $K_1 = w_0 + 2w_1 + 2w_2$ et $K_2 = w_0 + w_1 + 2w_2$.

Si l'on construit les VFCSRs sur une autre base $\mathcal{B}' = \{\mu_0, \ldots, \mu_{n-1}\}$ que la base canonique, il suffit de calculer les coordonnées vectorielles sur $\mathcal{B}'$ de l'élément

$$\sum_{i=1}^{i=r} q_i(\mu_0 + \ldots + \mu_{n-1})$$

et on a la relation

$$\sum_{i=1}^{i=r} q_i(\mu_0 + \ldots + \mu_{n-1}) = K_0^{'}\mu_0 + \ldots + K_{n-1}^{'}\mu_{n-1}.$$

## 7.7 Algorithme d'Initialisation

Dans cette section, nous répondons à la question inverse : considérons $\beta = (\frac{\tilde{r}_0}{\tilde{s}_0}, \ldots, \frac{\tilde{r}_{n-1}}{\tilde{s}_{n-1}})$ un vecteur de rationnel dont les dénominateurs sont tous impairs, comment déterminer un VFCSR construit sur un triplet $(\mathbb{F}_p, P, \mathcal{B})$ et un état initial qui donnent en sortie une séquence vectorielle dont le vecteur $p$-adique associé coincide avec $\beta$ ? Si un VFCSR génère la séquence extraite du développement $p$-adique de $\beta$, il doit être construit sur un triplet $(\mathbb{F}_p, P, \mathcal{B})$ avec $P$ un polynôme unitaire et irréductible de degré $n$. On choisira $\mathcal{B}$ comme base canonique de $\mathbb{Z}[X]/(P)$. En d'autres termes, nous cherchons un VFCSR construit sur le triplet $(\mathbb{F}_p, P, \mathcal{B})$ de taille $r$ avec le vecteur de connexion $(\tilde{q}_0, \ldots, \tilde{q}_{n-1})$ et un état initial $(a_0, \ldots, a_{r-1}, m_{r-1})$. Toutes ces inconnues satisfont à une équation de la forme

$$\beta = \frac{1}{|\det(M)|}\mathtt{sgn}(\det M)\mathtt{Comat}(M)(\tilde{p}_t)_{0\leq t\leq n-1}.$$

Pour résoudre cette équation, suivons la procédure suivante :

1. Calculons le PPCM des dénominateurs $\tilde{s}_t$.

   $$\tilde{q} = \mathtt{PPCM}\left\{\tilde{s}_0, \ldots, \tilde{s}_{n-1}\right\}.$$

   Le but étant de mettre $\beta$ sous une forme $\beta = (\frac{\tilde{r}_0}{\tilde{q}}, \ldots, \frac{\tilde{s}_{n-1}}{\tilde{q}})$.

2. Le triplet $(\mathbb{F}_p, P, \mathcal{B})$ détermine la forme de la matrice de connexion du VFCSR et ainsi nous avons une $n$-forme $\det(M) = f(\tilde{q}_0 - 1, \tilde{q}_1, \ldots, \tilde{q}_{n-1})$ ($f$ représente la $n$-forme). En effet, rechercher les coefficients de connexion revient à chercher l'entier de connexion ou autrement dit à chercher les coordonnées de $q$ dans la base $\mathcal{B}$. Ici, nous connaissons la norme de $q$.

   $$|\mathtt{N}(-q)| = \tilde{q}.$$

   On doit résoudre l'équation $|f(\tilde{q}_0 - 1, \tilde{q}_1, \ldots, \tilde{q}_{n-1})| = \tilde{q}$ avec les conditions suivantes : $\tilde{q}_0, \ldots, \tilde{q}_{n-1}$ sont des multiples de $p$ positifs. C'est un exercice algébrique difficile. Il peut être fait avec un outil informatique comme un simple programme sur Matlab qui consisterait à générer les entiers représentés par $f$ et chercher ceux qui coincident avec $\tilde{q}$. Supposons ce problème résolu.

3. Calculons $r = \max\left\{[\log_p(\tilde{q}_i)]; 0 \leq i \leq n-1\right\}$. C'est la taille du VFCSR.

4. Donnons le développement $p$-adique du vecteur de connexion obtenu. En déduire les coefficients de connexion $q_1, \ldots, q_r$.

5. Écrivons $a_i^0 + a_i^1 p + \ldots + q_i^{r-1}p^{r-1}$ les $r$ premiers coefficients du développement $p$-adique pour $\frac{\tilde{r}_i}{\tilde{q}}$ (pour tout $0 \leq i \leq n-1$).

6. Avec toutes ces données entrées dans l'équation de départ, il reste à déterminer la mémoire initiale. La mémoire $m_t^{r-1}$ apparait dans l'équation

$$\beta = \frac{1}{|\det(M)|}\mathtt{sgn}(\det M)\mathtt{Comat}(M)(\tilde{p}_t)_{0\leq t\leq n-1},$$

seulement dans l'expression de $\tilde{p}_t$ pour tout $0 \leq t \leq n-1$. C'est un système linéaire $n \times n$ à $n$ indéterminées.

Le VFCSR et l'état initial obtenus en sortie de cet algorithme génèrent la séquence vectorielle dont $\beta$ est le vecteur $p$-adique associé.

## 7.8 Représentation exponentielle vectorielle

Les FCSRs séquences possèdent une représentation dite représentation exponentielle. En effet, si $\underline{a}$ est une FCSR séquence strictement périodique différente de la séquence triviale $(p-1, p-1, \ldots)$ et si son développement $p$-adique coincide avec celui de $\frac{s}{q}$, alors pour tout $i \geq 0$,

$$a_i = (-sp^{-i}) \pmod q \pmod p.$$

Dans cette partie, nous énoncons un résultat semblable pour les VFCSR-séquences.

**Théorème 7.8.1.** *Considérons un VFCSR construit sur le triplet $(\mathbb{F}_p, P, \mathcal{B})$ de norme de connexion $\tilde{q}$. Soit $\underline{a}$ une séquence de sorties et $\beta = (\frac{\tilde{r}_0}{\tilde{q}}, \ldots, \frac{\tilde{r}_{n-1}}{\tilde{q}})$ son vecteur $p$-adique associé. Alors*

$$\forall i \in \mathbb{N}, \quad a_i = \Big( -p^{-i} \sum_{t=0}^{t=n-1} \tilde{r}_t \bar{X}^t \Big) \pmod{|\tilde{q}|} \pmod p.$$

Pour démontrer ce théorème, il faut d'abord le démontrer dans le cas $n = 1$, c'est-à-dire le cas binaire.

*Preuve de la proposition 6.8.1.* $\mathbb{Z}_p$ est un anneau de valuation discrète donc il possède un unique idéal premier qui est $p\mathbb{Z}_p$. L'ensemble des éléments inversibles de $\mathbb{Z}_p$ est $\mathbb{Z}_p - p\mathbb{Z}_p$. L'entier $q$ n'étant pas dans $p\mathbb{Z}_p$ est donc un entier $p$-adique inversible.

$$\begin{aligned}
\frac{s}{q} = a_0 + a_1 p + a_2 p^2 + \ldots \quad &\Rightarrow \quad s = q a_0 + q a_1 p + q a_2 p^2 + \ldots \\
&\Rightarrow \quad s \equiv q a_0 \mod p \\
&\Rightarrow \quad s \equiv (q_r p^r + \ldots + q_1 p - 1) a_0 \mod p \\
&\Rightarrow \quad s \equiv -a_0 \mod p \\
&\Rightarrow \quad a_0 \equiv -s \mod p \\
\\
0 \leq a_0 < p \quad &\Rightarrow \quad a_0 = (-s) \pmod p \\
\\
-q < s \leq 0 \quad &\Rightarrow \quad 0 \leq -s < q \\
&\Rightarrow \quad -s = (-s) \pmod q \\
&\Rightarrow \quad a_0 = (-s) \pmod q \pmod p
\end{aligned}$$

Comme $s \equiv qa_0 \pmod p$, alors $\dfrac{s-qa_0}{p} \in \mathbb{Z}$. On a de même

$$\frac{\frac{1}{p}(s-qa_0)}{q} = a_1 + a_2 p + a_3 p^2 + \ldots \quad \Rightarrow \quad a_1 = -\frac{1}{p}(s-qa_0) \pmod p$$

$$\begin{aligned} -q < s \leq 0 \quad &\Rightarrow \quad -2q < s - qa_0 \leq 0 \\ &\Rightarrow \quad -\frac{2}{p}q < \frac{s-qa_0}{p} \leq 0 \end{aligned}$$

$$\begin{aligned} p \geq 2 \quad &\Rightarrow \quad -q < \frac{s-qa_0}{p} \leq 0 \\ &\Rightarrow \quad 0 \leq -\frac{s-qa_0}{p} < q. \end{aligned}$$

$p$ et $q$ sont premiers entre eux, donc $p$ est inversible dans $\mathbb{Z}/q\mathbb{Z}$. Il existe alors un entier $0 \leq n < q$ et un entier $k$ tel que $np = qk + 1$.

$$-ns + \frac{s-qa_0}{p} = \frac{-nps + s - qa_0}{p} = \frac{-qks - s + s - qa_0}{p} = \frac{q(-ks-a_0)}{p}.$$

Donc $\dfrac{q(-ks-a_0)}{p} \in \mathbb{Z}$. Or $p$ et $q$ sont premiers entre eux, donc $p \mid -ks - a_0$. Ainsi $-ns + \dfrac{s-qa_0}{p} \in q\mathbb{Z}$.

$$-ns \equiv -\frac{s-qa_0}{p} \pmod q.$$

$$0 \leq -\frac{s-qa_0}{p} < q \Rightarrow -\frac{s-qa_0}{p} = -ns \pmod q.$$

On en conclut que $a_1 = -ns \pmod q \pmod p$. On notera $n$ par $p^{-1}$ l'inverse de $p$ modulo $q$ et on a par récurrence pour tout $i$ $a_i = (-p^i s) \pmod q \pmod p$. □

*Démonstration du théorème 7.8.1.* Nous avons $a_i = \sum_{t=0}^{t=n-1} a_t^i \bar{X}^t$. Or du développement $p$-adique

$$\frac{\tilde{r}_t}{\tilde{q}} = a_t^0 + a_t^1 p + a_t^2 p^2 + \ldots$$

, on déduit que $a_t^i = (-\tilde{r}_t p^{-i}) \pmod{\tilde{q}} \pmod p$. L'écriture vectorielle donne $a_i = \left(p^{-i} \sum_{t=0}^{t=n-1} (-\tilde{r}_t \bar{X}^t)\right) \pmod{|\tilde{q}|} \pmod 2$. □

## 7.9 $l$-séquences vectorielles

Nous avons vu que la période maximale d'une VFCSR-séquence est $\tilde{q} - 1$. Elle peut être atteinte si $\mathtt{ord}_{\tilde{q}}(p) = \tilde{q} - 1$ et si la séquence n'est pas triviale.

**Théorème 7.9.1.** *Considérons un VFCSR de norme de connexion $\tilde{q}$. Soit $\underline{a}$ une séquence de sorties et $\beta = (\frac{\tilde{r}_t}{\tilde{q}})_{t=0}^{t=n-1}$ son vecteur $p$-adique associé. La séquence $\underline{a}$ est de période maximale si et seulement si $\tilde{q}$ est premier, $p$ est racine primitive modulo $\tilde{q}$ et s'il existe $t$ tel que $\tilde{q}$ ne divise pas $\tilde{r}_t$.*

*Démonstration.* Si $\tilde{q}$ est premier et $p$ est racine primitive modulo $\tilde{q}$, alors $\mathtt{ord}_{\tilde{q}}(p) = \tilde{q}-1$. Comme il existe $t$ tel que $\tilde{r}_t$ n'est pas un multiple de $\tilde{q}$ premier, alors ils sont premiers entre eux et $\mathtt{PGCD}(\tilde{q}, \tilde{r}_t) = 1$. Donc la période de $\underline{a}_t$ est $\mathtt{ord}_{\tilde{q}}(p) = \tilde{q} - 1$. On a alors

$$\tilde{q} - 1 = \mathtt{per}(\underline{a}_t) \mid \mathtt{per}(\underline{a}) \mid \tilde{q} - 1.$$

On en déduit que la période de $\underline{a}$ est $\tilde{q} - 1$. Inversement, si $\mathtt{per}(\underline{a}) = \tilde{q} - 1$, alors

$$\tilde{q} - 1 = \mathtt{per}(\underline{a}) \mid \mathtt{ord}_{\tilde{q}}(p) \mid \tilde{q} - 1.$$

Donc $\mathtt{ord}_{\tilde{q}}(p) = \tilde{q} - 1$ ce qui implique que $\mathbb{Z}/\tilde{q}\mathbb{Z}$ a un sous-groupe multiplicatif cyclique d'ordre $\tilde{q} - 1$. Dit autrement, tout les éléments de $\mathbb{Z}/\tilde{q}\mathbb{Z}$ sont inversibles, c'est donc un corps. C'est vrai si et seulement si $\tilde{q}$ est premier. On a $\mathtt{ord}_{\tilde{q}}(p) = \tilde{q}-1$ si par définition $p$ est une racine primitive modulo $\tilde{q}$. Enfin, comme $\tilde{q}$ est premier, alors pour tout $0 \leq t \leq n-1$,

$$\mathtt{per}(\underline{a}) = \begin{cases} 1 & \text{si} \quad \tilde{q} \mid \tilde{r}_t \\ \tilde{q} - 1 & \text{s} \quad \tilde{q} \nmid \tilde{r}_t \end{cases}$$

Si pour tout $t$, $\mathtt{per}(\underline{a}_t) = 1$ alors $\mathtt{per}(\underline{a}) = 1$, ce qui est absurde, donc il existe un $t$ tel que $\tilde{q}$ ne divise pas $\tilde{r}_t$. □

**Remarque 7.9.1.** *Dans le cas où $\tilde{q}$ est premier de racine primitive $p$, alors les séquences $\underline{a}_t$ sont ou de période 1 ou de période $\tilde{q} - 1$. On distingue deux cas :*

1. *pour tout $t$, $\underline{a}_t$ est triviale, alors $\underline{a}$ l'est aussi.*
2. *sinon $\mathtt{per}(\underline{a}) = \tilde{q} - 1$.*

*On en déduit que dans ces conditions, une séquence de sorties est ou triviale ou de période maximale.*

**Définition 7.9.1** ($l$-séquences vectorielles)**.** *Soit un VFCSR de norme de connexion $\tilde{q}$. Supposons que $\tilde{q}$ est un nombre premier dont $p$ est racine primitive modulo $\tilde{q}$. Une séquence de sorties non-triviale est appelée $l$-séquence vectorielle et sa période est $\tilde{q} - 1$.*

L'existence d'une telle séquence est problématique. En effet, en plus des conditions standards de l'existence des $l$-séquences, c'est-à-dire $\tilde{q}$ premier et $p$ racine primitive modulo $\tilde{q}$, il y a une autre condition. L'entier $\tilde{q}$ est représenté par une $n$-forme particulière ayant une forme à déterminer et dépendante du choix du polynôme $P$ et de la base $\mathcal{B}$. Il faut donc pouvoir générer de tels nombres. On verra par la suite l'existence de tels nombres dans deux exemples, le cas quadratique et le cas cubique.

Notons que les séquences $p$-aires qui composent une $l$-séquence vectorielle sont soit triviales soit des $l$-séquences $p$-aires. Elles vérifient donc les propriétés de distribution des $l$-séquences comme la complémentarité des demi-périodes ou la propriété de l'équilibre etc. . .

## 7.10 Cas Quadratique et Cas Cubique en caractéristique 2

Dans cette partie, nous étudions deux cas particuliers : le cas quadratique et le cas cubique. Le cas quadratique désigne les VFCSRs construits sur $\mathbb{F}_{p^2}$ et le cas cubique désigne les VFCSRs construits sur $\mathbb{F}_{p^3}$. Ici, nous choisissons $p = 2$.

### 7.10.1 Cas Quadratique

Le cas quadratique en caractéristique 2 est très particulier, car il existe un unique polynôme de degré 2 irréductible modulo 2. Il s'agit du polynôme $X^2-X-1$. Le VFCSR construit sur le triplet $(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$ a pour matrice de connexion

$$M = \begin{pmatrix} 1-\tilde{q}_0 & -\tilde{q}_1 \\ -\tilde{q}_1 & 1-\tilde{q}_0-\tilde{q}_1 \end{pmatrix} \text{ et } \det M = (\tilde{q}_0-1)^2 + (\tilde{q}_0-1)\tilde{q}_1 - \tilde{q}_1^2$$

En posant $u = \tilde{q}_0 - 1$ et $v = \tilde{q}_1$, $\tilde{q}$ est de la forme $u^2 + uv - v^2$ avec $u$ impair et $v$ pair. Grâce à un programme sur Matlab, on peut générer des nombres premiers $\tilde{q}$ représentés par cette forme quadratique dont 2 est racine primitive modulo $\tilde{q}$. Voici un tableau de valeurs.

| $\tilde{q}$ | $u$ | $v$ |
|---|---|---|
| 11 | 3 | 2 |
| 59 | 7 | 2 |
| 61 | 7 | 4 |
| 101 | 9 | 4 |
| 131 | 11 | 10 |
| 211 | 13 | 6 |
| 269 | 15 | 4 |
| 701 | 27 | 28 |
| 1259 | 35 | 34 |

Tous ces nombres sont premiers, admettent 2 comme racine primitive et sont représentés par la forme quadratique $u^2 + uv - v^2$. En construisant notre VFCSR de vecteur de connexion $(u+1, v)$ et de taille $r = \max([\log_2(u+1)], [\log_2 v])$, on génère des $l$-séquences dite quadratiques.

### 7.10.2 Cas Cubique

Pour le cas cubique, on dispose d'un choix de polynôme irréductible modulo 2 de degré 3. Il s'agit de $X^3 - X - 1$ et $X^3 - X^2 - 1$. Prenons par exemple $X^3 - X - 1$. Le VFCSR construit sur le triplet $(\mathbb{F}_2, X^3 - X - 1, \mathcal{B})$ a pour matrice de connexion

$$M = \begin{pmatrix} 1-\tilde{q}_0 & -\tilde{q}_2 & -\tilde{q}_1 \\ -\tilde{q}_1 & 1-\tilde{q}_0-\tilde{q}_2 & -\tilde{q}_1-\tilde{q}_2 \\ -\tilde{q}_2 & -\tilde{q}_1 & 1-\tilde{q}_0-\tilde{q}_2 \end{pmatrix}$$

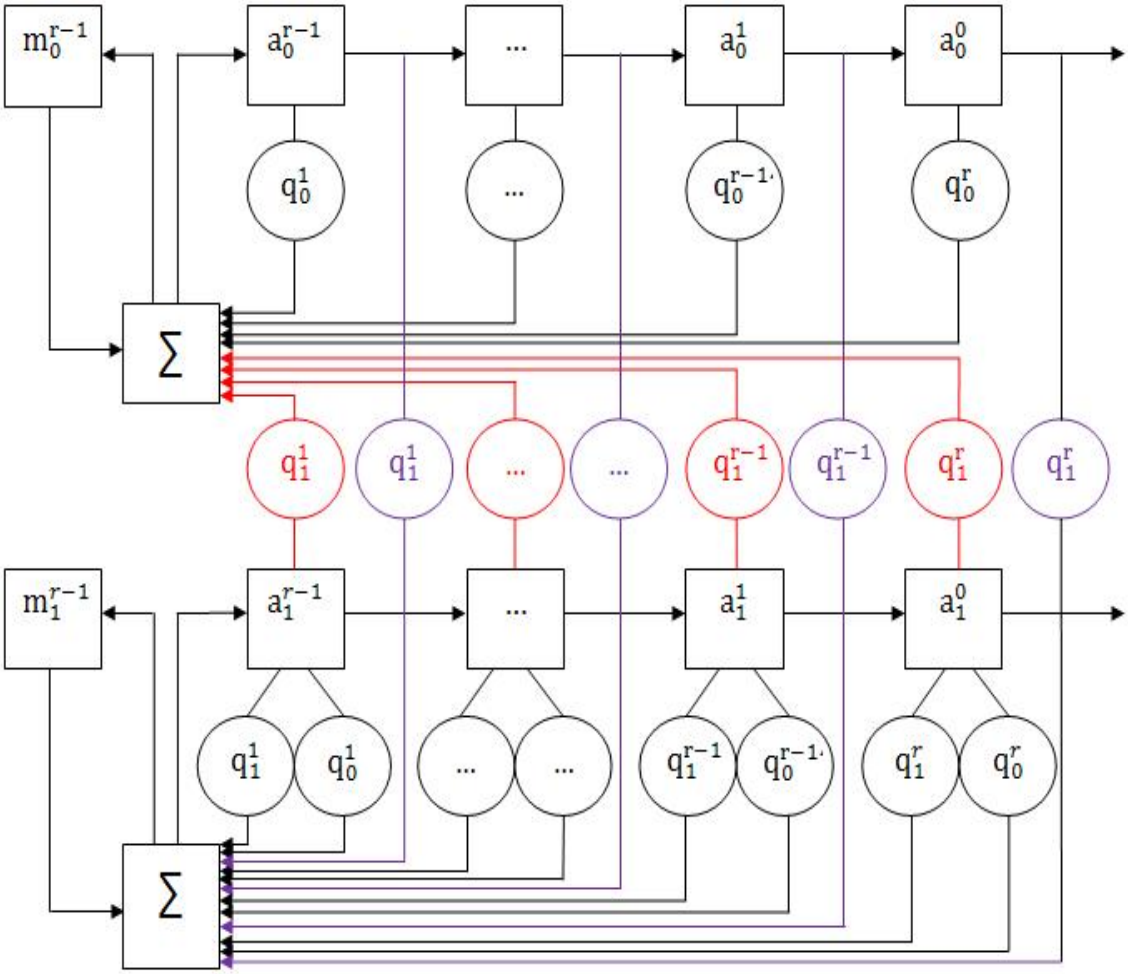



FIGURE 7.1 – Représentation des VFCSRs quadratiques en mode Fibonacci

$$\text{et } \det M = -u^3 - v^3 - w^3 + 3uvw + uv^2 - uw^2 - 2u^2w + vw^2.$$

avec $u = \tilde{q}_0 - 1$, $v = \tilde{q}_1$ et $w = \tilde{q}_2$. De même avec un simple programme informatique, on génère des nombres premiers représentés par cette forme cubique et admettant 2 comme racine primitive. Voici un tableau de telles valeurs.

| $\tilde{q}$ | $u$ | $v$ | $w$ |
|---|---|---|---|
| 11 | $-1$ | 2 | 0 |
| 37 | 1 | 2 | 4 |
| 59 | $-1$ | 2 | 4 |
| 83 | 3 | 0 | 2 |
| 101 | 5 | 4 | 2 |
| 149 | 5 | 4 | 4 |
| 173 | 5 | 2 | 2 |
| 4019 | 11 | 4 | 10 |
| 10133 | 17 | 2 | 8 |
| 15083 | 11 | 0 | 18 |

En construisant un VFCSR sur le triplet $(\mathbb{F}_2, X^3 - X - 1, \mathcal{B})$ de vecteur de connexion $(u+1, v, w)$ et de taille $\max([\log_2(u+1)], [\log_2 v], [\log_2 w])$, on génère des $l$-séquences dites cubiques.

## 7.11 Un Exemple

Dans cette partie, nous illustrons toute cette théorie sur les VFCSR à travers un exemple simple de $l$-séquence quadratique. Considérons le VFCSR construit sur le triplet $(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$ de taille $r = 2$ et de coefficients de connexion $q_1 = 1$ et $q_2 = \bar{X}$. Prenons pour état initial

$$(a_0, a_1, m_1) = (1, \bar{X} + 1, 3 - 4\bar{X}).$$

En sortie, nous avons la séquence vectorielle suivante :

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_0^i$ | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | $1\cdots$ |
| $a_1^i$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | $1\cdots$ |
| $m_0^{i+1}$ | 3 | 2 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | $1\cdots$ |
| $m_1^{i+1}$ | $-4$ | $-1$ | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | $2\cdots$ |

La pré-période est de longueur 6 et la période est 10. Le vecteur de connexion est $(\tilde{q}_0, \tilde{q}_1) = (4, 2)$ et la norme de connexion du VFCSR est $\tilde{q} = (4-1)^2 + (4-1).2 - 2^2 = 11$. C'est bien une $l$-séquence de période $11 - 1$ et 11 est un nombre premier représenté par la forme quadratique $u^2 + uv - v^2$ et 2 est racine primitive modulo 11.
Quand à l'évolution de la mémoire, on observe que $m_0^1 = 3$ et qu'au bout de 3 étapes, elle décroit vers l'intervalle $[0, 2[$ puis y reste indéfiniment après 2 étapes. On observe aussi que $m_1^1 = -4$ et qu'elle croit vers l'intervalle $[0, 3[$ puis y reste indéfiniment après 2 étapes. Rappelons que $w_0 = 1$, $w_1 = 1$ et donc $K_0 = 2$ et $K_1 = 3$. On vérifie bien les résultats théoriques qui imposent que $m_0^1$ doit retourner vers $[0, 2[$ après au plus 2 étapes et que $m_1^1$ doit retourner vers $[0, 3[$ après au plus $\log_2(4) + 2 + 1 = 5$ étapes.
Pour conclure sur les propriétés de distributions des bits, on remarque que dans une période, il y a 5 zéros et 5 uns et que la première moitié d'une période est le complémentaire en bits de la deuxième moitié de la période.

## 7.12 Tests Statistiques et Applications

Nous avons implémenté les VFCSRs dans le cas quadratique en caractésristique 2, c'est à dire tous les VFCSRs construits sur le triplet $(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$, pour vérifier s'ils sont conformes aux tests statistiques de référence. Dans cette partie, nous exposons très brièvement ces conclusions sur les VFCSRs et leur propriétés pseudo-aléatoires, ces conclusions ont été présentées dans [27].

### 7.12.1 Implantation des VFCSRs quadratiques en caractéristique 2

Comme vu précédemment le cas quadratique des VFCSRs est primordial pour plusieurs raisons, la première étant qu'il est le plus naturel à concevoir après le cas simple $n = 1$ qui correspond aux FCSRs classiques construits sur $\mathbb{F}_2$ et la deuxième étant qu'il y a un unique polynôme irréductible modulo 2. Nous explicitons le mode opératoire d'un VFCSR quadratique :

1. Calculons, pour tout $z \geq r$, les entiers $\sigma_1^z$ et $\sigma_0^z$, comme suit

$$\sigma_1^z = \sum_{i=1}^{i=r} \left(q_1^i a_1^{z-i} + q_1^i a_0^{z-i} + q_0^i a_1^{z-i}\right) + m_1^{z-1}$$

$$\sigma_0^z = \sum_{i=1}^{i=r} \left(q_1^i a_1^{z-i} + q_0^i a_0^{z-i}\right) + m_0^{z-1}$$

2. Décalons les éléments du premier registre et les éléments du deuxième registre vers la droite tout en mettant en sortie les bits les plus à droite $a_1^{z-i}$ et $a_1^{z-i}$ comme le montre la figure,
3. Entrons $a_1^{z-i} = \sigma_1^z \pmod 2$ et $a_0^{z-i} = \sigma_0^z \pmod 2$), $\forall z \geq r$
4. Remplaçons les mémoires précédentes par $m_1^z = \frac{\sigma_1^z - a_1^z}{2}$ et $m_0^z = \frac{\sigma_0^z - a_0^z}{2}$.

Un VFCSR construit sur le triplet $(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$ de norme de connexion $\tilde{q}$ génère des $l$-séquences vectorielles si et seulement si $\tilde{q}$ est premier et 2 est racine primitive modulo $\tilde{q}$. De plus par construction $\tilde{q}$ est représenté par la forme quadratique $u^2 + uv - v^2$. La recherche de tels nombres est fondamentale dans la mesure où pour un FCSR binaire cette dernière condition n'existe pas. La théorie des nombres fournit des conjectures classiques sur l'existence de tels nombres. Dans le cas d'un VFCSR quadratique, nous avons généré quelques valeurs qui serviront comme point de départ pour nos tests statistiques. Dans les tableaux 7.1, 7.2 et 7.3, pour chaque triplet $(\tilde{q}, u, v)$, on mentionne aussi la longueur 2-adique de $\tilde{q}$ et le maximum des longueurs 2-adique de $u$ et de $v$. On note

$$l_x = [\log_2(x)].$$

$$l_{(u,v)} = \max(l_u, l_v).$$

On remarque que certains triplets sont plus intéressants que d'autres dans la pratique. Par exemple, si on fixe $u$, alors on voit que la période $\tilde{q} - 1$ pour des valeurs $v > u$ est

| $l_{\widetilde{q}}$ | $\widetilde{q}$ | $l_{(u,v)}$ | $u$ | $v$ |
|---|---|---|---|---|
| 4 | 11 | 2 | 3 | 2 |
| 4 | 11 | 5 | 31 | 50 |
| 10 | 1259 | 5 | 35 | 34 |
| 9 | 829 | 5 | 35 | 44 |
| 13 | 8821 | 6 | 85 | 28 |
| 11 | 2389 | 6 | 85 | 124 |
| 12 | 8179 | 6 | 89 | 86 |
| 11 | 3581 | 6 | 89 | 124 |
| 13 | 9949 | 6 | 95 | 84 |
| 12 | 7621 | 6 | 95 | 108 |

TABLE 7.1 – Exemples de triplets de connexion pour $l_{(u,v)}$ égal à 5 et 6.

| $l_{\widetilde{q}}$ | $\widetilde{q}$ | $l_{(u,v)}$ | $u$ | $v$ |
|---|---|---|---|---|
| 16 | 101419 | 8 | 331 | 354 |
| 16 | 109891 | 8 | 331 | 330 |
| 16 | 115259 | 8 | 339 | 338 |
| 16 | 103451 | 8 | 339 | 370 |
| 16 | 112181 | 8 | 351 | 380 |
| 16 | 121421 | 8 | 351 | 332 |
| 17 | 132499 | 8 | 373 | 390 |
| 17 | 157141 | 8 | 373 | 316 |

TABLE 7.2 – Exemples de triplets de connexion pour $l_{(u,v)}$ égal à 8.

inférieur à la période pour des valeurs $v < u$. De plus pour un $\tilde{q}$ fixé, il existe plusieurs couple $(u, v)$ vérifiant la relation $u^2 + uv - v^2 = \tilde{q}$.

Comparer les FCSRs binaires et les VFCSRs quadratiques est important dans la mesure où il semble qu'un VFCSR quadratique correspond à deux FCSRs binaires superposés. Pourtant, ce n'est pas le cas, puisque le nombre de cellules d'un VFCSR quadratique est $2l_{(u,v)}$ qui est en général proche de $l_{\tilde{q}}$. Or chaque sortie du VFCSR nécessite un FCSR de taille $l_{\tilde{q}}$ et d'entier de connexion $\tilde{q}$. Autrement dit avec le même nombre de cellules, on gagne en sortie une séquence en plus dans le cas des VFCSRs quadratiques. Les figures 7.12.1 et 7.12.1 illustrent bien ce fait en prenant comme entier de connexion $q = 349$ pour le FCSR et comme norme de connexion $\tilde{q} = 349$ pour le VFCSR quadratique.

### 7.12.2 Propriétés aléatoires des VFCSRs

Afin de tester les propriétés statistiques pour conclure sur l'aléarité des séquences générées par les VFCSRs quadratiques, nous avons pris plusieurs triplets $(\tilde{q}, u, v)$ avec

| $l_{\widetilde{q}}$ | $\widetilde{q}$ | $l_{(u,v)}$ | $u$ | $v$ |
|---|---|---|---|---|
| 18 | 389219 | 9 | 637 | 662 |
| 18 | 395429 | 9 | 651 | 692 |
| 18 | 411491 | 9 | 639 | 634 |
| 18 | 424451 | 9 | 651 | 650 |
| 18 | 428339 | 9 | 657 | 662 |
| 18 | 443771 | 9 | 657 | 638 |
| 18 | 467171 | 9 | 683 | 682 |
| 18 | 481619 | 9 | 675 | 634 |
| 18 | 502499 | 9 | 689 | 646 |
| 20 | 1164589 | 9 | 1001 | 204 |
| 20 | 3932741 | 10 | 2001 | 2036 |

TABLE 7.3 – Exemples de triplets de connexion pour $l_{(u,v)}$ égal à 9 et 10.

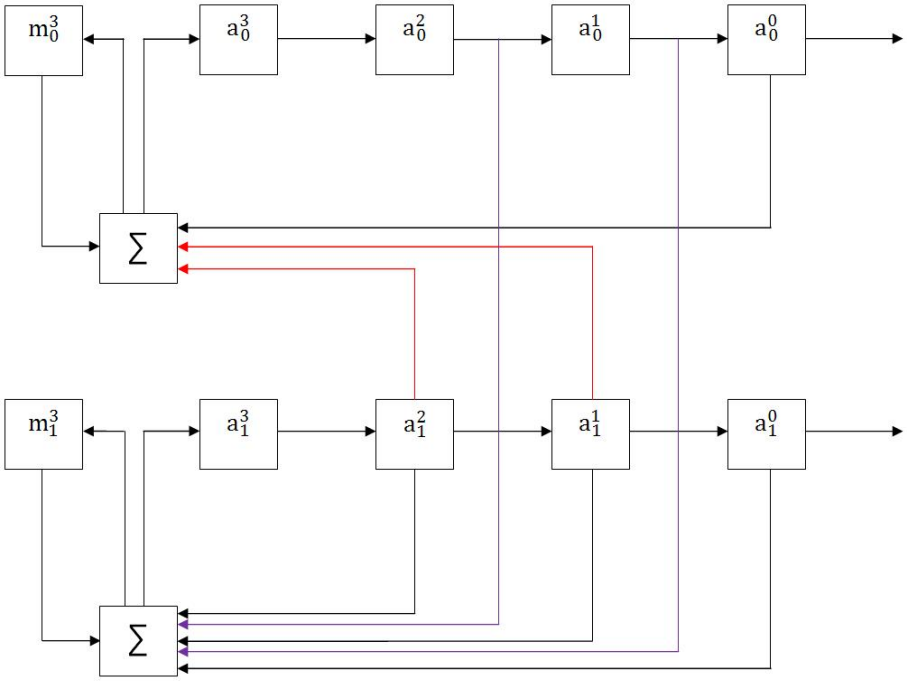



FIGURE 7.2 – VFCSR pour $\tilde{q} = 349$.

les cas où $u > v$ et $u < v$. Les tableaux 7.1, 7.2 et 7.3, montrent les paramètres choisis pour implanter le VFCSR quadratique. Ces valeurs ont été choisies en accord avec la quantité de données nécessaires pour effectuer ces tests.

Nous avons soumis les séquences de sorties du VFCSR aux tests statistiques. Dans

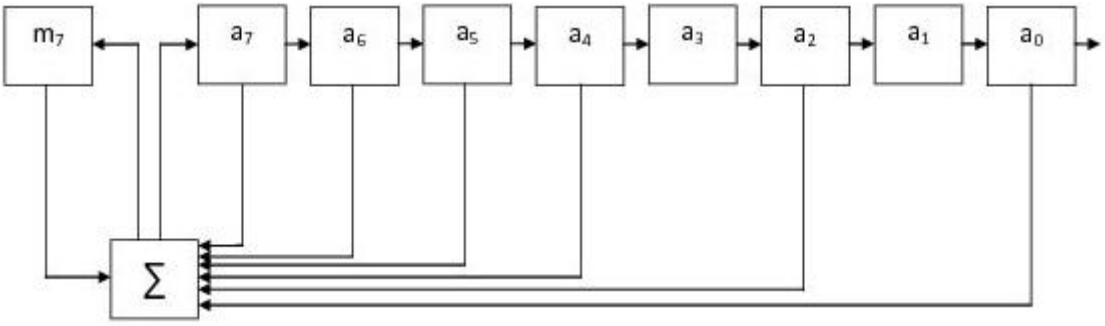



FIGURE 7.3 – FCSR pour $q = 349$.

notre étude, nous avons choisis comme outil d'analyse des propriétés statistiques des VFCSR-séquences, la batterie de test fournie par le NIST (National Institute of Standardization and Technology)[46].

Le STS de NIST est un outil de tests spécialement conçu pour tester les séquences produites par des générateurs aléatoires [47]. Les tests sont utiles dans la détection des écarts par rapport à une séquence véritablement aléatoire. Cette librairie fournit une implantation de 15 tests où chacun permet de tester une propriété particulière censée être vérifiée par nos séquences [46]-p.201. Les tests de NIST sont basés sur les tests d'hypothèses qui permettent d'accepter ou de rejeter l'hypothèse sur l'aléarité de la suite testée. Le résultat fourni par le test est la $P-value$ qui est une mesure de la force de la preuve fournie par les données contre l'hypothèse. Si $P-value \geq 0.01$, avec $P-value \in [0,1]$ et le niveau de confiance $\alpha = 0.01$, alors la séquence est considérée aléatoire.

Les tableaux 7.4 et 7.5 présentent les résultats de la première catégorie de tests statistiques. Ce sont des tests probabilistes dits de normalité dont :

- le test de fréquence,
- le test série,
- le test run,
- le test sur le rang de matrice binaire.

Les deux séquences $\underline{a}_0$ et $\underline{a}_1$ obtenues pour chaque triplet du tableau 7.1 ont passé les quatre tests. Ainsi, les suites suivent une distribution uniforme, équilibrées et ne présentent pas de tendances fluctuantes.

| $\widetilde{q}$ $(u,v)$ | Seq | Frequency Test | | Serial Test | |
|---|---|---|---|---|---|
| | | *P-value* | Task | *P-value* | Task |
| 829 | a0 | 0.972294 | Succ | 0.972260 | Succ |
| (35,34) | a1 | 0.972294 | Succ | 0.972260 | Succ |
| 1259 | a0 | 0.977516 | Succ | 0.932602 | Succ |
| (35,44) | a1 | 0.977516 | Succ | 0.932602 | Succ |
| 2389 | a0 | 0.983677 | Succ | 0.983670 | Succ |
| (85,28) | a1 | 0.983677 | Succ | 0.983670 | Succ |
| 3581 | a0 | 0.986667 | Succ | 0.986664 | Succ |
| (85,124) | a1 | 0.986667 | Succ | 0.986664 | Succ |
| 7621 | a0 | 0.990860 | Succ | 0.990859 | Succ |
| (89,86) | a1 | 0.990860 | Succ | 0.990859 | Succ |
| 8179 | a0 | 0.991178 | Succ | 0.973536 | Succ |
| (98,124) | a1 | 0.991178 | Succ | 0.973536 | Succ |
| 8821 | a0 | 0.991505 | Succ | 0.991504 | Succ |
| (95,84) | a1 | 0.991505 | Succ | 0.991504 | Succ |
| 9949 | a0 | 0.992001 | Succ | 0.992000 | Succ |
| (95,108) | a1 | 0.992001 | Succ | 0.992000 | Succ |

TABLE 7.4 – Resultats des tests statistiques de fréquences et de séries (fréquence de blocs) pour quelques triplets (q,u,v).

| $\widetilde{q}$ (u,v) | Seq | Test Cumulative Sums | | Test Run | |
|---|---|---|---|---|---|
| | | P-value | Task | P-value | Task |
| 829 | a0 | 0.498961 | Succ | 0.874766 | Succ |
| (35,34) | a1 | 0.498961 | Succ | 0.654567 | Succ |
| 1259 | a0 | 0.498961 | Succ | 0.317535 | Succ |
| (35,44) | a1 | 0.498961 | Succ | 0.472308 | Succ |
| 2389 | a0 | 0.498961 | Succ | 0.353726 | Succ |
| (85,28) | a1 | 0.498961 | Succ | 0.571931 | Succ |
| 3581 | a0 | 0.527464 | Succ | 0.856311 | Succ |
| (85,124) | a1 | 0.527464 | Succ | 0.949487 | Succ |
| 7621 | a0 | 0.498961 | Succ | 0.653463 | Succ |
| (89,86) | a1 | 0.512361 | Succ | 0.580758 | Succ |
| 8179 | a0 | 0.511447 | Succ | 0.891599 | Succ |
| (98,124) | a1 | 0.498961 | Succ | 0.865508 | Succ |
| 8821 | a0 | 0.498961 | Succ | 0.806508 | Succ |
| (95,84) | a1 | 0.498961 | Succ | 0.806508 | Succ |
| 9949 | a0 | 0.478444 | Succ | 0.521477 | Succ |
| (95,108) | a1 | 0.468205 | Succ | 0.917313 | Succ |

TABLE 7.5 – Résultats des tests statistiques de 3-4 sur quelques triplets $(\tilde{q}, u, v)$

La figure 7.4 illustre l'évolution de la $P - value$ obtenue par le test de rang de matrices binaires appliqué aux suites $\underline{a}_0$ et $\underline{a}_1$ produites par un VFCSR quadratique avec les triplets donnés dans le tableau 7.2. Toutes les $P - value$ obtenues sont supérieures au niveau de confiance. Ainsi le générateur passe ce test avec succès. Donc il n'y a pas de dépendance linéaire entre les chaînes de longueur fixe de la séquence originale.

Une deuxième catégorie de tests statistiques dite tests de compression dont les plus connus sont le test Universel de Maurer et le test de l'entropie, permet de déterminer si une suite peut être compressée. Si c'est le cas, une telle suite peut être distinguée d'une suite aléatoire. Sur la figure 7.5, toutes les suites engendrées par le VFCSR avec les triplets $\tilde{q} = 389219$ à $\tilde{q} = 502499$ du tableau 7.3 ont passé le test de Maurer. Il en résulte que les suites générées par un VFCSR quadratique sont non compressibles.

Alors que dans la figure 7.6, pour l'application du test DFT aux suites produites par un VFCSR quadratique avec le triplet $(\tilde{q}, u, v) = (1164589, 1001, 204)$, il est observé que au fur et à mesure que la taille des deux suites augmente, on tend vers la valeur de la période, avec un pas de 20000 *bits* le résultat du test tend vers zéro lorsque leurs longueurs dépassent le neuvième de la période. La raison de la diminution de la *P-value* est que les suites générées par le VFCSR quadratique commencent à montrer des répétitions dès qu'elles deviennent longues.

Enfin, nous avons pris le triplet $(3932741, 2001, 2036)$ et avons généré les suites $\underline{a}_0$ et $\underline{a}_1$. Avec chacune une taille de 3932740 bits nous avons appliqué tous les tests de la compilation STS. La figure 7.7 montre les résultats obtenus. Les deux suites ont passé tous les tests sauf un qui est le test DFT, ce qui est normal puisqu'on teste sur toute la période.

Pour valider le VFCSR quadratique comme générateur d'aléa, nous l'avons implanté. Nous avons généré plusieurs suites de bits avec différents triplets et leur avons fait passer les tests implantés dans la librairie STS de NIST. Tous les tests ont été passés avec succés. Les suites générées par la nouvelle conception des FCSRs présentent de bonnes propriétés d'aléarité. Elles sont équilibrées, d'une variation uniforme et non compressibles.

Le VFCSR quadratique est un bon candidat pour la génération de suites pseudo-aléatoires.

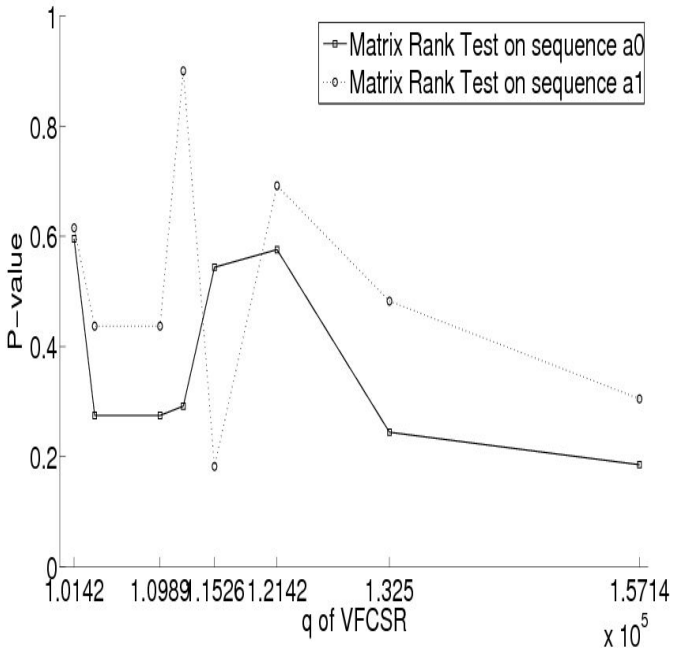



FIGURE 7.4 – Résultats du test Matrix Rank.

## 7.13 Le mode Galois

Dans cette section, nous présentons la version VFCSR en mode Galois. Le mode Galois est plus approprié pour les applications hardware que le mode Fibonacci. En effet le mode Galois met à jour de manière simultanée toutes les cellules du registre, alors que le mode Fibonacci met à jour une cellule dans le registre principal et la cellule "mémoire" et opère ensuite par décalage.

Le mode Galois a été introduit pour la première fois par Goresky et Klapper en 2002 [22]. Ils ont présentés ce nouveau mode de registre appliqué aux LFSRs, FCSRs et $d$-FCSRs. En 2008, Arnault, Berger et Lauradoux présentent une nouvelle famille de chiffrement par flot à base de FCSRs filtrés en mode Galois ([48] et [49]).

Dans cette partie, nous développons la conception des VFCSRs en mode Galois ainsi que leur analyse basique. Leur analyse est sensiblement identique à celle des VFCSRs en mode Fibonacci, donc leur étude ne tardera pas sur ces points. Cependant certains points semblent essentiels a développer. Les résultats suivant ont été publiés pour la revue WISA 2010 aux éditions Springer [30]. Une autre partie des résultats figure dans [50].

La partie concernant le mode Galois des VFCSRSs peut être lue en deux temps. La première partie concerne la théorie générale développée en insistant sur le parallèle avec le mode Fibonacci. La deuxième partie concerne les applications développées, notamment le VFCSR filtré en mode Galois (VFCSR-Q).

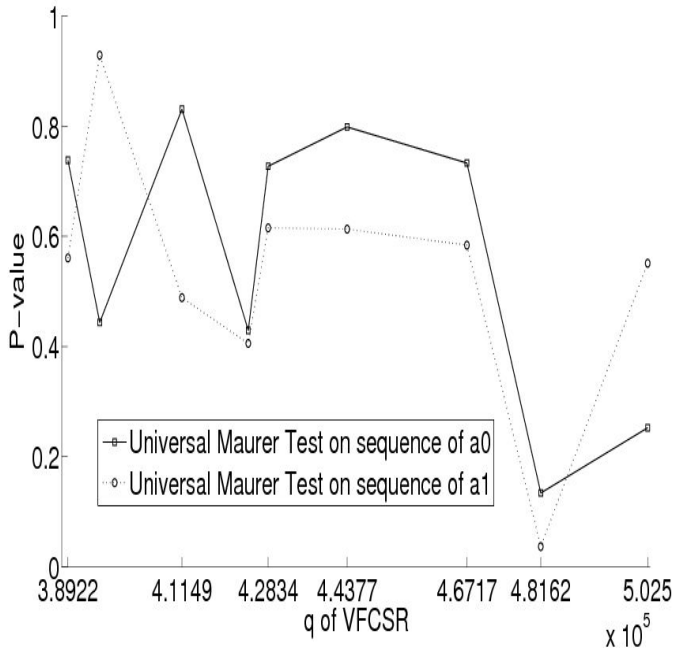



FIGURE 7.5 – Résultats du test Universal Maurer.

## 7.14 Conception des VFCSRs en mode Galois

Nous restons dans le même cadre algébrique que celui des VFCSRs en mode Fibonacci. On choisit donc un polynôme unitaire et irréductible de degré $n$ sur $\mathbb{F}_p$. On considère le corps fini $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(P)$. On identifie $P$ à son relèvement canonique dans $\mathbb{Z}[X]$ et on considère $\mathbb{Z}[X]/(P)$ le $\mathbb{Z}$-module libre de rang $n$ et on pose la base canonique $\mathcal{B} = \left\{1, \bar{X}, \ldots, \bar{X}^{n-1}\right\}$.

**Définition 7.14.1** (automate VFCSR en mode Galois)**.** *Un Vectorial Feedback with Carry Shift Register en mode Galois construit sur le triplet* $(\mathbb{F}_p, P, \mathcal{B})$ *de taille* $r$ *et d'entiers de connexion* $q_1, \ldots, q_r \in \mathbb{F}_p[X]/(P)$ *est un automate ou générateur de séquence dont les états sont des éléments*

$$s(t) = (\underbrace{a_0(t), \ldots, a_{r-1}(t)}_{\in \mathbb{F}_p[X]/(P)}, \underbrace{m_1(t), \ldots, m_r(t)}_{\in \mathbb{Z}[X]/(P)})$$

*où* $t$ *représente l'étape du registre et où les* $a_i(t)$ *sont dans* $\mathbb{F}_p[X]/(P)$ *et les* $m_i(t)$ *dans* $\mathbb{Z}[X]/(P)$ *; dont le changement d'état s'opère de la manière suivante :*

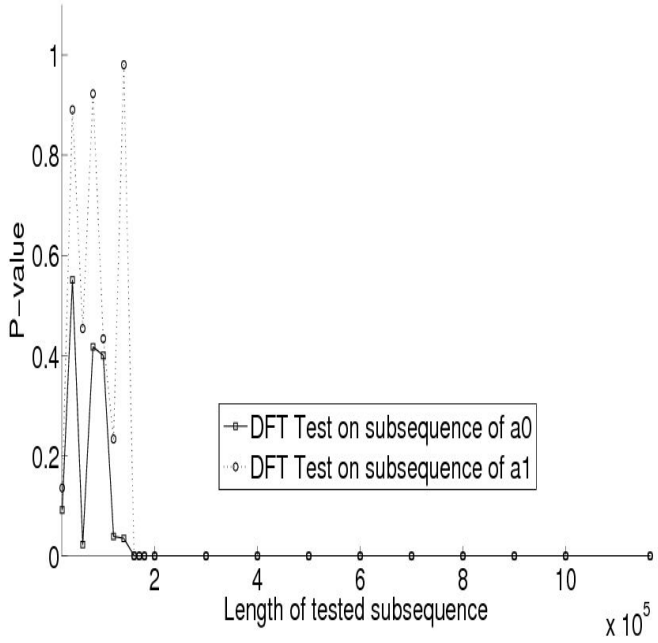



FIGURE 7.6 – Résultats du test DFT.

*On écrit tous les éléments sous forme de vecteurs sur la base* $\mathcal{B}$.

$$\forall 0 \leq i \leq r-1, \quad a_i(t) = \sum_{j=0}^{j=n-1} a_j^i(t)\bar{X}^j \text{ où } a_j^i(t) \in \{0,1\}$$
$$\forall 1 \leq i \leq r, \quad q_i = \sum_{j=0}^{j=n-1} q_j^i \bar{X}^j \text{ où } q_j^i \in \{0,1\}$$
$$\forall 1 \leq i \leq r, \quad m_i(t) = \sum_{j=0}^{j=n-1} m_j^i(t)\bar{X}^j \text{ où } m_j^i(t) \in \mathbb{Z}.$$

*On prend le relèvement canonique des* $a_i(t)$ *et des* $q_i$ *dans* $\mathbb{Z}[X]/(P)$, *puis on calcule pour tout* $0 \leq i \leq r-2$,

$$\sigma_i(t+1) = q_{i+1}a_0(t) + a_{i+1}(t) + m_{i+1}(t) \text{ et}$$
$$\sigma_{r-1}(t+1) = q_r a_0(t) + m_r(t).$$

*comme un vecteur sur* $\mathcal{B}$. *Pour tout* $1 \leq i \leq r$, $\sigma_i(t) = \sum_{l=0}^{l=n-1} \sigma_l^i(t)\bar{X}^j$ *où* $\sigma_l^i(t) \in \mathbb{Z}$. *L'élément* $\sigma_i$ *est une expression polynomiale en* $\bar{X}$ *de degré* $2n-2$ *et on élimine les degrés strictement supérieurs à* $n-1$ *en utilisant l'expression vectorielle des puissances*

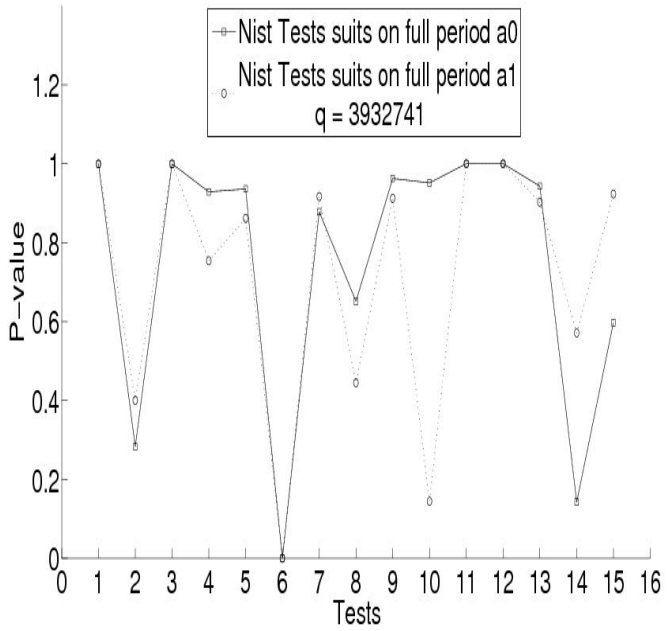



FIGURE 7.7 – Résultats des 15 tests de la batterie NIST.

*$\bar{X}^l$ dans la base $\mathcal{B}$ déterminées par $P$. Supposons que pour tout $j \geq n$,*

$$X^j = \sum_{t=0}^{t=n-1} b_t^j \bar{X}^t \text{ où } b_t^j \in \mathbb{Z}.$$

*On obtient les coordonnées de $\sigma_i$ par des calculs directs,*

$$\sigma_l^i(t+1) = \sum_{k=0}^{k=l} q_{l-k}^{i+1} a_k^0(t) + a_l^{i+1}(t) + m_l^{i+1}(t) + \sum_{j=n}^{j=2n-2} b_j^l \sum_{k=j-(n-1)}^{n-1} q_{k-l}^{i+1} a_k^0(t).$$

$$\sigma_l^{r-1}(t+1) = \sum_{k=0}^{k=l} q_{l-k}^{r} a_k^0(t) + m_l^{r}(t) + \sum_{j=n}^{j=2n-2} b_j^l \sum_{k=j-(n-1)}^{n-1} q_{k-l}^{r} a_k^0(t).$$

*Puis on calcule les coordonnées de $a_i(t+1)$ et celles de $m_{i+1}(t+1)$ suivant la base $\mathcal{B}$.*

$$a_l^i(t+1) = \sigma_l^i(t+1) \pmod p \text{ et}$$
$$m_l^{i+1}(t+1) = \tfrac{1}{p}(\sigma_l^i(t+1) - a_l^i(t+1)).$$

*Répétons cette procédure indéfiniment. L'état $s(0)$ est appelé l'état initial. La fonction de retour du VFCSR est définie par $f(s(t)) = s(t+1)$ et la fonction de sorties est définie par*

$$g(s) = g(x_0, \ldots, x_{r-1}, y_1, \ldots, y_r) = (g_0(s), \ldots, g_{r-1}(s)) = (x_0, \ldots, x_{r-1}).$$

*Le FCSR vectoriel en mode Galois génère $r$ séquences vectorielles infinies notées*

$$\begin{aligned}\forall 1 \leq i \leq r, \quad \underline{a}^i &= (g_i(s(0)), g_i \circ f(s(0)), g_i \circ f^2(s(0)), \ldots) \\ &= (a_i(0), a_i(1), a_i(2), \ldots).\end{aligned}$$

Les calculs vectoriels d'un VFCSR en mode Galois sont sensiblement identiques à ceux effectués pour un VFCSR en mode Fibonacci. On laisse donc ces calculs élémentaires comme exercice aux lecteurs.

## 7.15 Analyse des VFCSRs en mode Galois

Dans cette section, nous présentons l'analyse des VFCSRs en mode Galois qui diffère de l'analyse des VFCSRs en mode Fibonacci. On se base sur la même méthode, mais il y a quelques différences notables. Par exemple, nous devons analyser les $r$ cellules smultanément puisqu'elles sont mises à jour simultanément. De plus, on dispose de $r$ cellules mémoires qui ont un comportement différent de la mémoire d'un VFCSR en mode Fibonacci.

Les $r$ séquences de sorties d'un VFCSR en mode Galois peuvent être vues comme des vecteurs de $n$ séquences $p$-aires. On a en réalité une séquence vectorielle de dimension $nr$.

$$\underline{a} = \begin{pmatrix} \underline{a}^0 \\ \underline{a}^1 \\ \vdots \\ \underline{a}^{r-1} \end{pmatrix} = \begin{pmatrix} \underline{a}_0^0 \\ \vdots \\ \underline{a}_{n-1}^0 \\ \vdots \\ \underline{a}^{r-1_0} \\ \vdots \\ \underline{a}_{n-1}^{r-1} \end{pmatrix} = \begin{pmatrix} a_0^0(0) & a_0^0(1) & a_0^0(2) & \cdots \\ \vdots & \vdots & \vdots & \\ a_{n-1}^0(0) & a_{n-1}^0(1) & a_{n-1}^0(2) & \cdots \\ \vdots & \vdots & \vdots & \\ a_0^{r-1}(0) & a_0^{r-1}(1) & a_0^{r-1}(2) & \cdots \\ \vdots & \vdots & \vdots & \\ a_{n-1}^{r-1}(0) & a_{n-1}^{r-1}(1) & a_{n-1}^{r-1}(2) & \cdots \end{pmatrix}$$

Á chaque séquence $p$-aire, on associe son développement $p$-adique noté $\beta_j^i$ et on obtient un vecteur $p$-adique de dimension $nr$.

$$\beta = \begin{pmatrix} \beta_0^0 \\ \vdots \\ \beta_{n-1}^0 \\ \vdots \\ \beta_0^{r-1} \\ \vdots \\ \beta_{n-1}^{r-1} \end{pmatrix} = \begin{pmatrix} a_0^0(0) & +a_0^0(1)p & +a_0^0(2)p^2 & +\cdots \\ \vdots & \vdots & \vdots & \\ a_{n-1}^0(0) & +a_{n-1}^0(1)p & +a_{n-1}^0(2)p^2 & +\cdots \\ \vdots & \vdots & \vdots & \\ a_0^{r-1}(0) & +a_0^{r-1}(1)p & +a_0^{r-1}(2)p^2 & +\cdots \\ \vdots & \vdots & \vdots & \\ a_{n-1}^{r-1}(0) & +a_{n-1}^{r-1}(1)p & +a_{n-1}^{r-1}(2)p^2 & +\cdots \end{pmatrix}.$$

L'entier de connexion joue toujours un rôle central dans l'analyse des FCSRs. On garde toutes les notions développées dans le chapitre dédié aux VFCSR en mode Fibonacci, en

particulier la construction du vecteur de connexion $(\tilde{q}_0, \ldots, \tilde{q}_{n-1})$.

$$q = \begin{pmatrix} \tilde{q}_0 \\ \tilde{q}_1 \\ \vdots \\ \tilde{q}_{n-1} \end{pmatrix}_{\mathcal{B}} - \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{\mathcal{B}}.$$

**Proposition 7.15.1.** *Soit un VFCSR en mode Galois sur le triplet $(\mathbb{F}_{p^n}, P, \mathcal{B})$ de vecteur de connexion $(\tilde{q}_0, \tilde{q}_1, \ldots, \tilde{q}_{n-1})$. Soit $\underline{a}$ une séquence de sorties et $\beta$ son vecteur $p$-adique associé. Alors $\beta$ vérifie un système linéaire à coefficients entiers de la forme suivante*

$$\left\{ \begin{array}{c} (-pq_l^{i+1})\beta_0^0 + \sum_{k=1}^{k=l} \Big( -pq_{l-k}^{i+1} - \sum_{j=n}^{j=k+n-1} pb_l^j q_{j-k}^{i+1} \Big) \beta_k^0 \\ + \sum_{k=l+1}^{k=n-1} \Big( - \sum_{j=n}^{j=k+n-1} pb_l^j q_{j-k}^{i+1} \Big) \beta_k^0 + \beta_l^i - p\beta_l^{i+1} = a_l^i(0) + pm_l^{i+1}(0) \end{array} \right\}_{0 \le i \le r-1, 0 \le l \le n-1}.$$

*Démonstration.* C'est un calcul direct laissé en exercice. Il suffit d'utiliser la relation de récurrence suivante

$$a_l^i(t+1) = \sum_{k=0}^{k=l} q_{l-k}^{i+1} a_k^0(t) + a_l^{i+1}(t) + m_l^{i+1}(t) + \sum_{j=n}^{j=2n-2} b_j^l \sum_{k=j-(n-1)}^{n-1} q_{k-l}^{i+1} a_k^0(t) - pm_l^{i+1}(t+1),$$

puis de l'utiliser dans le développement $p$-adique de $\beta_l^i$ et on obtient alors

$$\beta_l^i = a_l^i(0) + pm_l^{i+1}(0) + \sum_{k=0}^{k=l} pq_{l-k}^{i+1} \beta_k^0 + \sum_{j=n}^{j=2n-2} b_l^j \sum_{k=j-n+1}^{n-1} pq_{j-k}^{i+1} \beta_k^0 + p\beta_l^{i+1}.$$

Le reste suit. □

La matrice représentant ce système est de dimension $nr \times nr$. On la note $M$. Elle est égale à la matrice identité $I_{nr}$ moins une matrice à coefficients entiers multiples de $p$. Sa $in + l^{ime}$ ligne est de la forme suivante

$$L_{i,l} = \Big( -pq_l^{i+1}, \underbrace{-pq_{l-k}^{i+1} - p \sum_{j=k+n-1}^{j=n} b_l^j q_{j-k}^{i+1}}_{1 \le k \le l}, \underbrace{-p \sum_{j=k+n-1}^{j=n} b_l^j q_{j-k}^{i+1}}_{l+1 \le k \le n-1}, \underbrace{0, \cdots, 0}_{n(i-1)+l}, 1, \underbrace{0, \cdots, 0}_{n-1}, -p, 0 \cdots, 0 \Big).$$

$M$ est donc de la forme

$$\mathcal{M} = \begin{pmatrix} 1-* & \cdots & * & -p & \cdots & \\ \vdots & \ddots & \vdots & & -p & \\ * & \cdots & 1-* & & & \ddots \\ * & \cdots & * & 1 & \cdots & \\ \vdots & & \vdots & & 1 & \\ * & \cdots & * & & \cdots & \ddots \end{pmatrix}.$$

C'est évidemment une matrice inversible à déterminant congru à 1 modulo $p$. Elle est composée de combinaisons linéaires des coordonnées vectorielles de l'entier de connexion $q$ dans la base $\mathcal{B}$.

**Définition 7.15.1.** *$M$ est appelée matrice de connexion du VFCSR en mode Galois.*

**Théorème 7.15.1.** *Soit un VFCSR en mode Galois construit sur le triplet $(\mathbb{F}_p, P, \mathcal{B})$ de taille $r$ et de matrice de connexion $M$. Pour toute séquence de sorties $\underline{a}$, son vecteur $p$-adique associé est un vecteur de rationnels dans $\frac{1}{|\det M|}\mathbb{Z}^{nr}$ et $\det M$ est un entier impair.*

*Démonstration.* Le système linéaire vérifié par $\beta$ admet une unique solution puisque $M$ est inversible. On a alors la solution suivante

$$\beta = \frac{1}{|\det(M)|}\mathtt{sgn}(\det M)\mathtt{Comat}(M)\Big(a_l^i(0) + pm_l^{i+1}(0)\Big)_{0\leq in+l\leq rn-1}.$$

C'est donc un vecteur de rationnels de dimension $nr$, rationnels dont les dénominateurs sont tous $\det M$. □

## 7.16 Norme de connexion

Nous avons vus que le résultat fondamental de l'analyse d'un VFCSR en mode Fibonacci pouvait s'exprimer intrinséquement. En effet, le vecteur $p$-adique associé à toute séquence de sorties appartient à $\frac{1}{|\mathtt{N}(q)|}\mathbb{Z}^n$. Dans cette partie, nous démontrons le même résultat. Toutefois, la démonstration nécessite un argument spécifique à ce cas, puisque qu'ici la matrice de connexion $M$ n'est pas la matrice de multiplication par $-q$.

**Théorème 7.16.1.** *Soit un VFCSR en mode Galois construit sur le triplet $(\mathbb{F}_p, P, \mathcal{B})$ de taille $r$ et d'entier de connexion $q$. Pour toute séquence de sorties $\underline{a}$, son vecteur $p$-adique associé est un vecteur de rationnels dans $\frac{1}{|\mathtt{N}(q)|}\mathbb{Z}^{nr}$.*

*Démonstration.* Posons $L'_{i,l} = \sum_{k=i}^{k=r-1} L_{k,l}p^{k-i}$ et $M' = (L'_{i,l})_{0\leq in+l\leq r(n-1)}$. La matrice $M'$ et la matrice $M$ ont même déterminant. La matrice $M'$ prend une forme particulière :

$$\begin{pmatrix} \mathcal{L} & 0 \\ \mathcal{N} & I_{n(r-1)} \end{pmatrix}.$$

La matrice $\mathcal{L}$ est une matrice $n \times n$ et $\mathcal{N}$ est une matrice $n(r-1) \times n$. Elle est formée des $n$ premiers coefficients extraits des $n$ premières lignes de $M'$.

$$\begin{pmatrix} L'_{0,0} \\ L'_{0,1} \\ \vdots \\ L'_{0,n-1} \end{pmatrix} \rightsquigarrow (\mathcal{L}).$$

Par un calcul direct, on trouve

$$L'_{0,l} = \Big( - \tilde{q}_l, \underbrace{-\tilde{q}_{l-k} - \sum_{j=k+n-1}^{j=n} b_l^j \tilde{q}_{j-k}}_{1 \leq k \leq l}, \underbrace{- \sum_{j=k+n-1}^{j=n} b_l^j \tilde{q}_{j-k}}_{l+1 \leq k \leq n-1}, 0 \ldots, 0 \Big).$$

Dans la démonstration de la proposition 7.4.1, en calculant la représentation matricielle de la multiplication par $-q$, on a donné l'expression de la $t^{\text{ième}}$ ligne. On trouve qu'elle coincide avec les $n$ premiers coefficients $L'_{0,t}$. autrement dit, $\mathcal{L}$ est la matrice de la transformation linéaire définie comme la multiplication par $-q$.

$$\det \mathcal{L} = \mathtt{N}(-q).$$

D'autre part, de la forme de $M'$, on déduit que

$$\det M' = \det \mathcal{L}.$$

On a donc démontré que le déterminant de $M$ est $N(-q)$. □

## 7.17 Propriétés basiques

Concernant les propriétés de périodicité, l'existence et la définition des $l$-séquences, les VFCSRs en mode Galois sont identiques aux VFCSRs en mode Fibonacci puisque toute cette théorie repose sur l'entier de connexion est exactement le même dans les deux modes et le fait que les séquences de sorties correspondent à des vecteurs de rationnels dont le dénominateur est $\tilde{q} = |\mathtt{N}(q)|$. Donc les séquences de sorties d'un VFCSR en mode Galois sont périodiques et la période divise toujours $\mathtt{ord}_{\tilde{q}}(p)$. La période maximale reste $\tilde{q}-1$ et elle est atteinte dans les mêmes conditions que celles des $l$-séquences vectorielles en mode Fibonacci. L'entier $\tilde{q}$ est représenté par une $n$-forme, la même que celle déterminée pour le mode Fibonacci, puisque cette $n$-forme n'est autre que le déterminant de $M$ (ici $\mathcal{L}$) dont les entrées sont les coordonnées vectorielles de l'entier de connexion $q$. Pour conclure sur les propriétés basiques des VFCSRs en mode Galois, les séquences de sorties en mode Galois vérifient toutes les propriétés des séquences de sorties du mode Fibonacci.

## 7.18 Cas quadratique et Applications

Dans cette section, nous détaillons le cas quadratique en caractéristique 2 des VFCSRs en mode Galois. Nous utilisons ce cas particulier dans les sections suivantes pour faire passer des tests statistiques et illustrer une application cryptographique.

### 7.18.1 Description du VFCSR-Q

Un VFCSR quadratique en mode Galois est un VFCSR construit sur le triplet $(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$. On se fixe une taille $r$ et un entier de connexion $q$. Les relations de

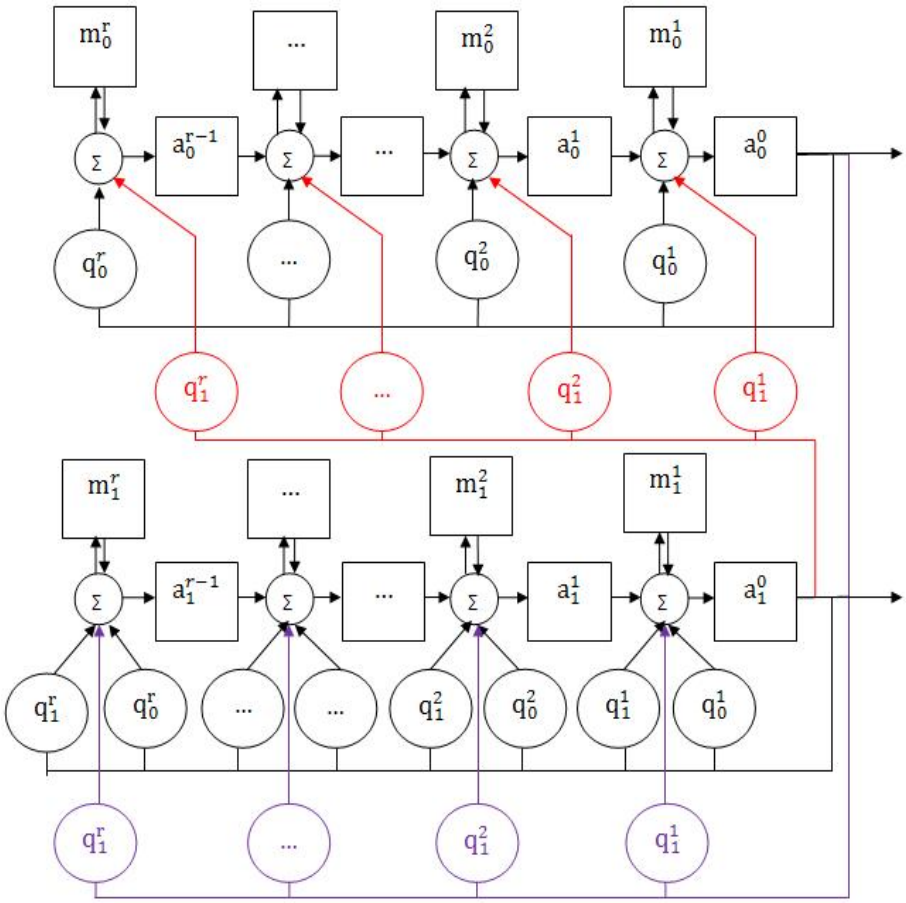



FIGURE 7.8 – Représentation des VFCSRs quadratiques en mode Galois

récurrences vectorielles qui définissent les changements d'états sont les suivantes : pour tout $0 \leq i \leq r-2$,

$$\begin{aligned} a_0^i(t+1) = &\quad q_1^{i+1}a_1^0(t) + q_0^{i+1}a_0^0(t) + a_0^{i+1}(t) + m_0^{i+1}(t) - 2m_0^{i+1}(t+1), \\ a_1^i(t+1) = &\quad q_1^{i+1}a_1^0(t) + q_1^{i+1}a_0^0(t) + q_0^{i+1}a_1^0(t) + a_1^{i+1}(t) + m_1^{i+1}(t) - 2m_1^{i+1}(t+1) \end{aligned}$$

et

$$\begin{aligned} a_0^{r-1}(t+1) = &\quad q_1^r a_1^0(t) + q_0^r a_0^0(t) + m_0^r(t) - 2m_0^r(t+1), \\ a_1^{r-1}(t+1) = &\quad q_1^r a_1^0(t) + q_1^r a_0^0(t) + q_0^r a_1^0(t) + m_1^r(t) - 2m_1^r(t+1). \end{aligned}$$

La matrice de connexion $M$ est de la forme suivante

$$M = \begin{pmatrix} 1-2q_0^1 & -2q_1^1 & -2 & 0 & \cdots & \cdots & \cdots & 0 & 0 \\ -2q_1^1 & 1-2q_0^1-2q_1^1 & 0 & -2 & \cdots & \cdots & \cdots & 0 & 0 \\ -2q_0^2 & -2q_1^2 & 1 & 0 & -2 & \ldots & \cdots & 0 & 0 \\ -2q_1^2 & -2q_0^2-2q_1^2 & 0 & 1 & 0 & -2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ -2q_0^r & -2q_1^r & 0 & 0 & 0 & 0 & \ldots & 1 & 0 \\ -2q_1^r & -2q_0^r-2q_1^r & 0 & 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}.$$

La transformation construite dans la démonstration du théorème 7.16.1, donne la matrice suivante

$$M' = \begin{pmatrix} 1-\tilde{q}_0 & -\tilde{q}_1 & 0 & 0 & \cdots & 0 \\ -\tilde{q}_1 & 1-\tilde{q}_0-\tilde{q}_1 & 0 & 0 & \cdots & 0 \\ * & * & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

On vérifie bien que son déterminant est de la forme $u^2 + uv - v^2$ avec $u = \tilde{q}_0 - 1$ et $v = \tilde{q}_1$.

### 7.18.2 Propriétés pseudo-aléatoires du VFCSR-Q

Réitérons l'analyse statistique du VFCSR quadratique, cette fois-ci en mode Galois, toujours par la batterie de tests du NIST. Pour l'implantation du VFCSR-Q, nous avons généré quelques triplets $(\tilde{q}, u, v)$ vérifiant les conditions des $l$-séquences pour un générateur de taille 160 bits. Voici deux exemples ayant servis de paramètres pour nos tests statistiques :

| | |
|---|---|
| $\tilde{q}$ | 39741402961906954206160047535539796042005214340820825272689327902761723128526374726419918065389 49 |
| $u$ | 19935245913182750153280416113442150364601400879 63 |
| $v$ | 19935245913182750153280416113442150364601400878 60 |

TABLE 7.6 – Exemple 1 de triplet

| | |
|---|---|
| $\tilde{q}$ | 42669948499185540522613538660909073394187803567919447365495441931015659537243024973441786752485 01 |
| $u$ | 19935245913182750153280416113442150364601400879 63 |
| $v$ | 18338289120761436060978627722716643152502713409 96 |

TABLE 7.7 – Exemple 2 de triplet

L'analyse de la qualité de l'aspect aléatoire du Galois VFCSR quadratique, est effectuée par la batterie de tests statistiques de NIST (National Institute of Standardization and Technology) STS. Le résultat d'un test est exprimé par la probabilité $P-value \in [0,1]$. Si $P-value \geq 0.01$, la séquence testée est considérée comme aléatoire.

Le tableau 7.8, présente les résultats obtenus de l'analyse des séquences des sorties $\underline{a}_0$ et $\underline{a}_1$ issues du générateur de la figure 7.8, sur des échantillons de 2200000 bits. Le paramètre utilisé est le premier exemple de triplet $(\tilde{q}, u, v)$ donné dans le tableau 7.6.

Tous les tests statistiques ont été passés avec succès. Pour ne pas encombrer le tableau des résultats, les tests contenant plusieurs $P$-valeurs n'en citera qu'un seul (cas où toutes les $P$-valeurs sont acceptées), comme pour les tests : Non-Overlapping Template, Random Excursions et Random Excursions Variant.

| **Statisticals Tests** | **Tests parameters** | **Sequence $\underline{a}_1$** | | **Sequence $\underline{a}_0$** | |
|---|---|---|---|---|---|
| | | **P-value** | **Task** | **P-value** | **Task** |
| Frequency | - | 0.774985 | Pass | 0.178398 | Pass |
| Block Frequency | m=128 | 0.805492 | Pass | 0.440320 | Pass |
| Runs | - | 0.264820 | Pass | 0.714705 | Pass |
| Longest Run | M=10000 | 0.063204 | Pass | 0.933766 | Pass |
| Rank | - | 0.833143 | Pass | 0.322493 | Pass |
| DFT | - | 0.980256 | Pass | 0.891733 | Pass |
| Non-Overlapping Template | m=9, B=110100010 | 0.465025 | Pass | 0.030875 | Pass |
| Overlapping Template | m=9 | 0.464561 | Pass | 0.351158 | Pass |
| Universal | L=8, Q=2456 | 0.099817 | Pass | 0.662900 | Pass |
| Linear Complexity | M=500 | 0.165002 | Pass | 0.734850 | Pass |
| Serial | m=16, $\nabla\psi_m^2$ | 0.977832 | Pass | 0.801563 | Pass |
| | m=16, $\nabla^2\psi_m^2$ | 0.981500 | Pass | 0.551655 | Pass |
| Approximate Entropy | m=10 | 0.828275 | Pass | 0.278716 | Pass |
| Cumulative Sums | Forward | 0.503953 | Pass | 0.221351 | Pass |
| | Reverse | 0.761476 | Pass | 0.137620 | Pass |
| Random Excursions | X=3 | 0.401433 | Pass | 0.794891 | Pass |
| Random Excursions Variant | X=1 | 0.074490 | Pass | 0.480395 | Pass |

TABLE 7.8 – Résultats des tests statistiques sur des séquences de sorties d'un VFCSR-Q en mode Galois.

L'application cryptographique consiste à construire un filtre pour le VFCSR-Q en mode Galois. Dans [30], nous explicitons cette construction (voir figure 7.9).

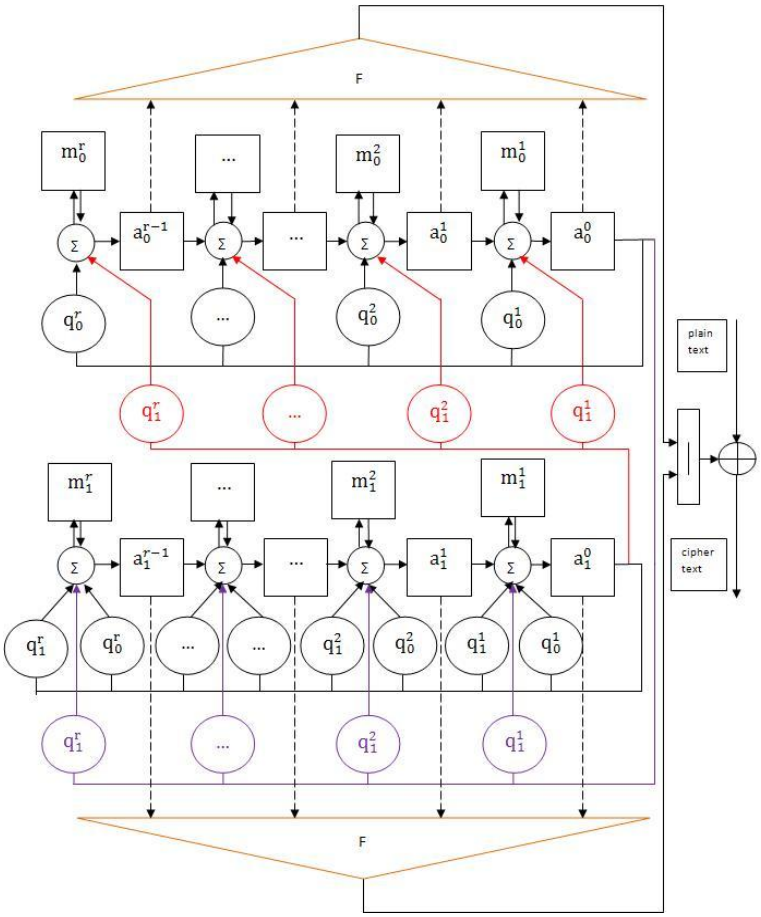



FIGURE 7.9 – Fonctionnement d'un VFCSR filtré.

## 7.19 Généralisation des registres vectoriels à rétroaction avec retenue.

Dans cette section, nous introduisons la généralisation des FCSRs vectoriels appelée Vectorial Feedback with Carry Registers ou VFCR. On rappelle que cette généralisation repose essentiellement sur le mode de connexion arbitrairement choisi, puisque le mode de Fibonacci et le mode de Galois sont des modes de connexion particuliers. Le mode Ring consiste à garder les décalages des registres sans imposer de connexion particulière. Les résultats qui suivent figurent dans [50].

On garde le contexte algébrique des FCSRs vectoriels, c'est-à-dire un corps premier $\mathbb{F}_p$, un polynôme $P$ irréductible et primitif de degré $n$ sur $\mathbb{F}_p$, le corps quotient $\mathbb{F}_p[X]/(P)$ et $\mathbb{Z}[X]/(P)$ le $\mathbb{Z}$-module libre de rang $n$.

**Définition 7.19.1** (VFCR). *Un FCR vectoriel construit sur le triplet $(\mathbb{F}_2, P, \mathcal{B})$ de taille $r$ et de matrice de transition $T = (t_{i,j}) \in \mathcal{M}_{r\times r}(\mathbb{F}_{p^n})$ est un automate dont les états sont*

*des couples* $(a(t), m(t))$ *où*

$$a(t) = (a_0(t), \ldots, a_{r-1}(t)) \in (\mathbb{F}_2[X]/(P))^r$$

*et*

$$m(t) = (m_1(t), \ldots, m_r(t)) \in (\mathbb{Z}[X]/(P))^r;$$

*et dont l'opération de changement d'état est donnée par la procédure suivante :*

- *Écrivons la collection des* $a_i(t)$, $m_i(t)$ *and* $t_{i,j}$ *dans la base* $\mathcal{B}$ *;*
- *Prenons le relèvement canonique des* $a_i(t)$ *et des* $t_{i,j}$ *dans* $\mathbb{Z}[X]/(P)$ *respectivement par rapport à* $\mathcal{B}$ *;*
- *Écrivons* $a(t)$ *et* $m(t)$ *comme des vecteurs de dimension* $nr$

$$\begin{aligned} a(t) = &\quad (a_0^0(t), \ldots, a_{n-1}^0(t), \ldots, a_0^{r-1}(t), \ldots, a_{n-1}^{r-1}(t)) \\ m(t) = &\quad (m_0^1(t), \ldots, m_{n-1}^1(t), \ldots, m_0^r(t), \ldots, m_{n-1}^r(t)); \end{aligned}$$

- *Traduisons la multiplication* $a_i(t)t_{i,j}$ *par la multiplication vectorielle* $\otimes$

$$a_i(t)t_{i,j} = (a_0^i(t), \ldots, a_{n-1}^i(t)) \otimes M_{t_{i,j}}$$

  *où* $M_{t_{i,j}}$ *est la matrice dans la base canonique* $\mathcal{B}$ *de la transformation linéaire définie comme la multiplication par* $t_{i,j}$*. ;*
- *Formons la matrice* $\mathcal{T} = (M_{t_{i,j}})_{i,j} \in \mathcal{M}_{rn \times rn}(\mathbb{Z})$ *avec les blocs* $M_{t_{i,j}}$ *;*
- *Écrivons l'addition avec* $m(t)$ *comme l'addition vectorielle* $\oplus$ *composante par composante et calculons* $a(t) \otimes \mathcal{T} \oplus m(t)$*.*
- *Appliquons la fonction* ( $\bmod p$) *et la fonction* (`divp`) *composante par composante.*

*Le mode Ring est représenté par la matrice de transition vérifiant* $t_{i+1,i} = 1$ *pour tout* $i$*.*

Un VFCR est entièrement déterminé par sa matrice de transition $\mathcal{T}$ de dimension $nr \times nr$. Elle se construit grâce à $r^2$ blocs matriciels $M_{t_{i,j}}$ ayant une forme particulière définis par la multiplication par $t_{i,j}$ dans $\mathbb{Z}[X]/(P)$. Le coefficient $t_{i,j}$ est considéré comme un vecteur de dimension $n$ sur $\mathbb{F}_p$. Le nombre de $t_{i,j}$ possibles est $p^n$, par correspondance il y a donc $p^n$ matrice bloc $M_{t_{i,j}}$. On peut donc construire $p^{nr^2}$ VFCRs possibles sur $(\mathbb{F}_p, X^n - \ldots - 1, \mathcal{B})$ de taille $r$.

## 7.20 Analyse des VFCRs

**Théorème 7.20.1.** *Considérons un VFCR construit sur le triplet* $(\mathbb{F}_p, P, \mathcal{B})$ *de matrice de transition* $T$*. Pour tout* $0 \leq i \leq r-1$ *et* $0 \leq j \leq n-1$*, la séquence de sorties* $(a_j^i(0), a_j^i(1), \ldots)$ *a pour développement* $p$*-adique le rationnel* $\frac{p_{i,j}}{\tilde{q}}$ *où* $\tilde{q} = \det(I_{rn} - p\mathcal{T})$*.*

*Démonstration.* Comme pour les modes classiques de Fibonacci et de Galois, on définit le vecteur $p$-adique

$$\beta = (\beta_0^0, \ldots, \beta_{n-1}^0, \ldots, \beta_0^i, \ldots, \beta_{n-1}^i, \ldots, \beta_0^{r-1}, \ldots, \beta_{n-1}^{r-1}),$$

avec $\beta_j^i$ le développement $p$-adique de la séquence $p$-aire $\underline{a}_j^i = (a_j^i(0), a_j^i(1), \ldots)$. On a donc :

$$\beta_j^i = a_j^i(0) + a_j^i(1)2 + a_j^i(2)2^2 + \ldots$$

$\beta$ vérifie le système matriciel suivant :

$$\beta = (a_j^i(0))_{i,j} \oplus \Big(\beta \otimes p\mathcal{T}\Big).$$

La matrice $I_{nr} - p\mathcal{T}$ admet une comatrice puisque $\mathbb{Z}$ est un anneau commutatif et son déterminant est congru à 1 modulo $p$, donc il est inversible. □

**Corollaire 7.20.1.** *Considérons un VFCR construit sur le triplet $(\mathbb{F}_p, P, \mathcal{B})$ de matrice de transition $T$. La séquence de sorties $\underline{a}_j^i$ est périodique et sa période divise $\mathtt{ord}_{\tilde{q}}(p)$ avec $\tilde{q} = |\det(I_{rn} - p\mathcal{T})|$.*

*Démonstration.* La preuve découle directement des résultats traités dans les chapitres précédents conséquences de résultats classiques de la théorie $p$-adique. □

Une VFCR-séquence est de période maximale si sa période est $\tilde{q} - 1$. On doit donc chercher des matrices $\mathcal{T}$ telles que $|\det(I_{nr} - p\mathcal{T})$ soit un nombre premier, $p$ est racine primitive modulo ce nombre. La recherche de $l$-séquences pour un VFCR revient donc à chercher des familles de matrice $\mathcal{T}$ vérifiant ces deux conditions.

## 7.21 Exemples

Dans cette section, nous illustrons les VFCR par des exemples simples.

### 7.21.1 VFCSR en mode Fibonacci

Les VFCSRs en mode Fibonacci peuvent être définis comme des VFCR avec la matrice de transition suivante

$$F = \begin{pmatrix} 0 & \ldots & 0 & q_r \\ 1 & \ldots & 0 & q_{r-1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & q_1 \end{pmatrix}.$$

Les calculs vectoriels du registre se traduisent par la matrice bloc suivante

$$\mathcal{F} = \begin{pmatrix} 0 & \ldots & 0 & M_{q_r} \\ I_n & \ldots & 0 & M_{q_{r-1}} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & I_n & M_{q_1} \end{pmatrix}.$$

En usant de combinaisons linéaires sur les lignes de $I_{nr} - p\mathcal{F}$, on la transforme en une matrice triangulaire inférieure de la forme suivante

$$\begin{pmatrix} M & 0 \\ * & I_{n(r-1)} \end{pmatrix}$$

où $M$ est la matrice de connexion d'un VFCSR en mode Fibonacci. On trouve que $\tilde{q} = \det(I_{nr} - p\mathcal{F}) = \det M$.

### 7.21.2 VFCSR en mode Galois

Les VFCSRs en mode Fibonacci peuvent être définis comme des VFCR avec la matrice de transition suivante

$$G = \begin{pmatrix} q_1 & \dots & q_{r-1} & q_r \\ 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix}.$$

Les calculs vectoriels du registre se traduisent par la matrice bloc suivante

$$\mathcal{G} = \begin{pmatrix} M_{q_1} & \dots & M_{q_{r-1}} & M_{q_r} \\ I_n & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & I_n & 0 \end{pmatrix}.$$

La matrice de connexion $M$ d'un VFCSR en mode Galois correspond ici à $(I_{nr} - p\mathcal{G})^t$.

### 7.21.3 FCRs binaires ou $p$-aires

Les FCRs $p$-aires correspondent tout simplement aux VFCRs en dimension $n = 1$. Les blocs $M_{q_i}$ coincident avec $q_i$.

### 7.21.4 VFCR-Q de taille 2

**Définition 7.21.1** (VFCR-Q). *On appelle par VFCR-Q ou VFCR quadratique, un VFCR construit sur le triplet* $(\mathbb{F}_p, X^2 - X - 1, \mathcal{B})$.

Pour $p = 2$, on peut décrire tous les VFCR-Q de taille 2. Il y en a $2^8$. Le registre peut être représenté de la manière suivante :

- Un registre principal composé de deux modules chacun ayant deux cellules.
- Un registre de retenues composé de deux modules chacun ayant deux cellules.

La Figure 7.10 représente un VFCR-Q pour $\tilde{q} = 61$. Les calculs du registre d'un VFCR-Q de taille 2 sont définis formellement par la matrice de transition $T = \begin{pmatrix} t_{1,1} & t_{1,2} \\ t_{2,1} & t_{2,2} \end{pmatrix}$ à qui on associe la matrice

$$\mathcal{T} = \begin{pmatrix} t_0^{1,1} & t_1^{1,1} & t_0^{1,2} & t_0^{1,2} \\ t_1^{1,1} & t_0^{1,1} + t_1^{1,1} & t_1^{1,2} & t_0^{1,2} + t_1^{1,2} \\ t_0^{2,1} & t_1^{2,1} & t_0^{2,2} & t_1^{2,2} \\ t_1^{2,1} & t_0^{2,1} + t_1^{2,1} & t_1^{2,2} & t_0^{2,2} + t_1^{2,2} \end{pmatrix}$$

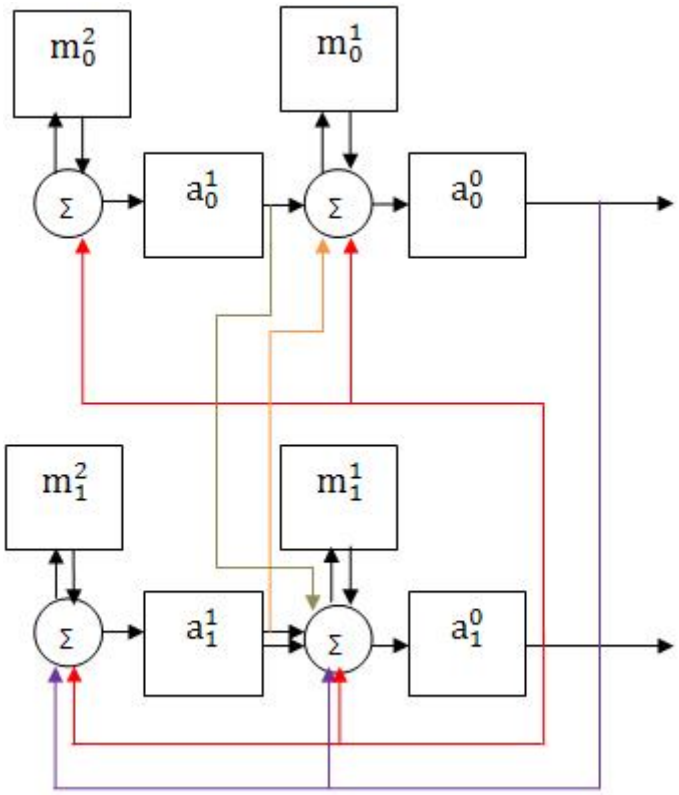



FIGURE 7.10 – VFCR pour $\tilde{q} = 61$.

pour effectuer les calculs vectoriels du registre donnés par la formule

$$(a_0^0(t), a_1^0(t), a_0^1(t), a_1^1(t)) \otimes \mathcal{T} \oplus (m_0^1(t), m_1^1(t), m_0^2(t), m_1^2(t)).$$

Il est intéressant de comparer les périodes des séquences générées par un VFCR-Q de taille 2 avec toutes les autres familles de registres étudiés dans les chapitres précédents, en particulier avec les FCRs binaires de taille 4. Le tableau 7.9 fournit les périodes des séquences en sortie de ces registres et on constate que les périodes maximales des VFCR-Q séquences sont les périodes maximales des FCR-séquences. Autrement dit, on ne perd pas sur la taille de la période tout en gagnant en structure algébrique. En effet, la matrice de transiiton $\mathcal{T}$ d'un VFCR-Q de taille 2 peut être vue comme un FCR binaire de taille 4 avec la même matrice de transition. Cependant dans le cas vectoriel, les formes matricielles obéissent à la structure sous-jacente des VFCRs. Par exemple, le maximum des périodes maximales est 60. Le VFCR-Q de matrice de transition $T = \begin{pmatrix} \overline{X} & \overline{X} \\ 1+\overline{X} & 0 \end{pmatrix}$

| Registers | differents models | values $\tilde{q} = \lvert\det(I - 2T)\rvert$ | maximal period $\mathtt{ord}_{\tilde{q}}(2) = \tilde{q} - 1$ |
|---|---|---|---|
| binary FCR of size 2 | $2^4$ | 1,3,5 | 2,4 |
| binary FCR of size 4 | $2^{16}$ | 1,3,5,7,9,$\cdots$,59,61,63, 69,75,77,81,87,91,99,135 | 2,4,10,12,18, 28,36,52,58,60 |
| VFCSR-Q in Fib. and Gal. of size 2 | $2^4$ | 1,5,9,11,19,25,29 ,31,41 | 4,10,18,28 |
| VFCR-Q of size 2 | $2^8$ | 1,5,9,11,19,25,29, 31,41,45,49,55,61,99 | 4,10,18,28,60 |

TABLE 7.9 – Comparaison des périodes maximales des FCRs de taille $2, 4$ et des VFCRs de taille 2.

et de matrice canoniquement associée $\mathcal{T} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \end{pmatrix}$ peut générer des séquences vectorielles de période 60. En effet $\det[I_4 - 2\mathcal{T}) = 61$, or 61 est premier et 2 est racine primitive modulo 61. En initialisant l'état $(a_0, a_1, m_1, m_2) = (1 + \bar{X}, 1, 0, \bar{X})$, on obtient en sortie la séquence du Tableau 7.10.

| i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_0^0$ | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| $a_0^1$ | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| $a_1^0$ | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| $a_1^1$ | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| i | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 |
| $a_0^0$ | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| $a_0^1$ | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| $a_1^0$ | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| $a_1^1$ | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| i | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | ... |
| $a_0^0$ | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | ... |
| $a_0^1$ | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | ... |
| $a_1^0$ | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | ... |
| $a_1^1$ | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | ... |

TABLE 7.10 – Exemple de VFCR-Q séquence de période 60.

# Chapitre 8

# Conclusion et Perspectives

Dans cette thèse, nous avons présenté une nouvelle conception des FCSRs en mode Fibonacci appelée VFCSR ou registre vectoriel à rétroaction linéaire avec retenue qui permet d'étendre les FCSRs à des corps finis $\mathbb{F}_{p^n}$ sans passer par des structures algébriques aussi complexes que les vecteurs de Witt. Cette méthode vectorielle permet d'obtenir des résultats similaires à ceux obtenus par Goresky et Klapper pour les FCSRs binaires ou dits $p$-aires (construit sur le corps premier $\mathbb{F}_p$). L'analyse utilise l'anneau de valuation discrète complet $\mathbb{Z}_p[X]/(P)$ de corps résiduel $\mathbb{F}[X]/(P)$. En plus de cela, ces résultats sont facilement implémentables. Cependant la conception vectorielle repose sur trois choix : le choix du nombre premier $p$, le choix d'un polynôme irréductible de degré $n$ sur $\mathbb{F}_p$ et le choix de la base. Les résultats fondamentaux obtenus dans cette étude ne dépendent pas de la base, mais choisir une base est nécessaire pour expliciter les calculs dans le registre et pouvoir représenter en pratique de tels registres et les séquences qu'ils génèrent. Le choix du polynôme influe sur la complexité des calculs du registre. En l'occurrence, il est préférable de choisir des formes trinomiales $X^n - X^k - 1$ irréductibles sur $\mathbb{F}_p$ si elles existent. Par exemple, pour tout $p$ premier, $X^p - X - 1$ est irréductible modulo $p$.

Ensuite, nous avons développés les autres représentations des VFCSRs notamment le mode de Galois et le mode Ring (VFCR). Les VFCRs de taille $r$ peuvent être vus comme des FCRs de taille $pr$ si l'on considère les registres comme des circuits. Cependant, les VFCRs jouissent d'une structure algébrique sous-jacente qui les rend analysables. En effet, ils sont représentables par une matrice carré de taille $pr$ constituée de blocs carrés de dimension $p$ ayant une forme déterminée, ainsi le choix des connexions se traduit comme un choix de blocs. Par contre, le FCR de taille $pr$ a une matrice carrée aléatoire de taille $pr$ où chaque coefficient représente une connexion choisie arbitrairement.

D'autres problèmes restent ouverts, comme l'existence d'une infinité de $l$-séquences pour un $p$ fixé et un $n$ fixé. Dans le cas simple de Goresky et Klapper, il existe des conjectures faisant état de l'existence d'une infinité de $q$ premier dont $p$ est racine primitive modulo $q$. Dans le cas des VFCSRs, il y a une condition supplémentaire : $\tilde{q}$ doit être représenté par une $n$-forme particulière. C'est d'ailleurs le premier point remarquable des VFCSRs : la construction de $l$-séquences revient à l'étude des nombres représentés par les $n$-formes. Par exemple, en dimension $n = 2$, on doit étudier la forme quadratique

$u^2 + uv - v^2$.

Enfin, il reste à étudier la complexité $p$-adique ou l'inter-corrélation pour les $l$-séquences vectorielles. Dans nos perspectives, nous développerons plusieurs points :

1. Étudier la complexité linéaire et la complexité $p$-adique des VFCSRs séquences.
2. Appliquer la conception et l'analyse vectorielle pour construire des $d$-FCSRs sur $\mathbb{F}_{p^n}$. On prendra un polynôme primitif et irréductible de degré $n$ sur $\mathbb{Q}[\pi]$ à coefficient entier où $\pi$ vérifie l'équation $\pi^d = p$.
3. Étendre la construction de registre à rétroaction sur la structure algébrique formée par les séries formelles doublement indexées.
4. Etudier la sécurité du F-VFCSR-Q.
5. Prévoir une implantation en hardware et en software du F-VFCSR-Q afin d'évaluer ses performances, notamment pour des applications dans des systèmes possédant des fortes contraintes en termes de capacité mémoire, de puissance de calcul (par exemple GSM, RFID, ...) ainsi que dans les systèmes à haut débit.
6. Construire une version de registre auto-rétrécissant à partir de VFCSRs.

# Bibliographie


[1] Guang Gong : Sequence Analysis, Lecture Notes for CO739x, Winter 1999

[2] S.W. Golomb, Shift register sequences, Aegean Park Press, Laguna Hills, California, 1982.

[3] J. L. MASSEY, Shift-register synthesis and BCH decoding, IEEE Transactions in Information Theory, Vol. IT-15, pp. 122-127, 1969.

[4] D. Coppersmith, H. Krawczyk, and Y. Mansour, The shrinking generator, in Advances in Cryptology-CRYPTO'93, ser. Lecture Notes in Computer Science, D. Stinson, Ed., vol. 773. Springer-Verlag, 1993, pp. 22–39.

[5] W. Meier and O. Staffelbach, The self-shrinking generator, in Advances in Cryptology-EUROCRYPT'94, ser. Lecture Notes in Computer Science, A. D. Santis, Ed., vol. 905. Springer-Verlag, 1994, pp. 205–214.

[6] Erik Zenner, Matthias Krause and Stefan Lucks, Improved Cryptanalysis, Proceedings of the 6th Australasian Conference on Information Security and Privacy (ACISP),LNCS Vol. 2119, pp. 21-35, 2001.

[7] A. Klapper and M. Goresky, 2-adic shift registers, fast software encryption, in Proc. Cambridge Security Workshop, LNCS, **vol. 809**, Cambridge, U.K, pp. 174–178, (1993).

[8] M. Goresky and A. Klapper : Feedback shift registers, 2-adic span, and combiners with memory, Journal of Cryptology, 10 (1997), 111-147.

[9] Andrew Klapper, Mark Goresky : Large Periods Nearly de Bruijn FCSR Sequences. EUROCRYPT 1995 : 263-273

[10] B.M.M. De Weger, Approximation lattices of p-adic numbers. Journal of Number Theory 24, 70–88 (1986).

[11] Andrew Klapper, Mark Goresky : Cryptoanalysis Based on 2-Adic Rational Approximation. CRYPTO 1995 : 262-273

[12] eSTREAM, the ECRYPT stream cipher project,
http ://www.ecrypt.eu.org/stream/.

[13] S. Babbage, C. De Cannière, A. Canteaut, C. Cid, H. Gilbert, T. Johansson, M. Parker, B. Preneel, V. Rijmen, and M.J.B. Robshaw, The eSTREAM Portfolio. April 15, 2008.
Disponible sur : http ://www.ecrypt.eu.org/stvl/.

[14] F. Arnault and T. P. Berger, Design and properties of a new pseudorandom generator based on a filtered FCSR automaton, IEEE Trans. Computers, 54(11) : pp. 1374–1383, (2005).

[15] F. Arnault and T. P. Berger, F-FCSR, Design of a new class of stream ciphers, In Henri Gilbert and Helena Handschuh, editors, Fast Software Encryption - FSE 2005, **vol. 3557** of LNCS, pp. 83–97, (2005).

[16] F. Arnault, T. P. Berger, and C. Lauradoux, F-FCSR stream ciphers, In Mathew Robshaw and Olivier Billet, editors, New Stream Cipher Designs, The eSTREAM Finalists, **vol. 4986** of LNCS, pp. 170–178, (2008).

[17] Mark Goresky, Andrew Klapper : Feedback Registers Based on Ramified Extensions of the 2-Adic Numbers (Extended Abstract). EUROCRYPT 1994 : 215-222

[18] Mark Goresky, Andrew Klapper : Periodicity and Correlation Properties of d-FCSR Sequences. Des. Codes Cryptography 33(2) : 123-148 (2004)

[19] Andrew Klapper : Distributional properties of d-FCSR sequences. J. Complexity 20(2-3) : 305-317 (2004)

[20] Andrew Klapper, Jinzhong Xu : Algebraic Feedback Shift Registers. Theor. Comput. Sci. 226(1-2) : 61-92 (1999)

[21] Andrew Klapper : Algebraic Feedback Shift Registers Based on Function Fields. SETA 2004 : 282-297

[22] M. Goresky and A. Klapper, Fibonacci and galois representations of feedback-with-carry shift registers, IEEE Transactions on Information Theory, 48(11), pp.2826-2836, (2002).

[23] G. Mrugalski, J. Rajski, and J. Tyszer, Ring generators - new devices for embedded test applications, IEEE Trans. on CAD of Integrated Circuits and Systems 23(9) (2004), 1306-1320. 267

[24] F. Arnault, T. P. Berger, Cédric Lauradoux, Marine Minier, and Benjamin Pousse : A new approach for FCSRs. In Selected Areas in Cryptography - SAC 2009, LNCS, **vol. 5867**, pp. 433-448, Calgary, Canada, (August 2009).

[25] T. P. Berger, M. Minier, and B. Pousse, Software oriented stream ciphers based upon fcsrs in diversified mode, In INDOCRYPT 2009, 10th International Conference on Cryptology in India, **vol. 5922** of LNCS, pp. 119–135, (2009).

[26] Andrew Klapper : Feedback with Carry Shift Registers over Finite Fields (extended abstract). FSE 1994 : 170-178.

[27] A. Marjane, B. Allailou, Vectorial Conception of FCSR, In C. Carlet and A. Pott (Eds.) : SETA 2010, LNCS 6338, pp. 240–252, (2010).

[28] S. Fischer, W. Meier, D. Stegemann, Equivalent representations of the F-FCSR Keystream Generator, In SASC 2008, pp.87 96, (2008) ;

[29] M.Hell, T Johansson, Breaking the F-FCSR-H stream cipher in real time, In Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, **vol. 5350**, pp. 557–569, (2008).

[30] B. Allailou, A. Marjane and A. Mokrane, Design of a Novel Pseudo-Random Generator Based on Vectorial FCSRs, In Y. Chung and M. Yung (Eds.) : WISA 2010, LNCS 6513, pp. 76-91, (2010).

[31] Serge Lang : Algèbre, éditions Dunod, 3ème édition révisée, p.476-498.

[32] Jean-Pierre Serre : Corps Locaux, Publications de l'Institut de Mathématique de l'Université de Nancago VIII, Actualités scientifiques et industrielles 1296, Hermann Paris, p.2-53.

[33] Helmut Hasse : Number Theory, Grundlehren der mathematischen Wissenschaften 229, A Series of Comprehensive Studies in Mathematics, Springer-Verlag Berlin Heidelberg New York, p.105-174.

[34] J.W.S. Cassels and A. Frohlich : Algebraic Number Theory, 1967 Academic Press, London and New York, p.1-52.

[35] Roger Descombes : Éléments de théorie des nombres, PUF, 1986, p.63-85

[36] Fernando Q.Gouvêa, $p$-adic Numbers, An introduction, Springer, Second Edition 1997, p.43-77.

[37] Yvette Amice. Les nombres p-adiques. Presses universitaires de France, 1975, p.15-71.

[38] Jurgen Neukirch. Algebraic Number Theory. Grundlehren der mathematischen Wissenschaften, Vol. 322, p.99-160. Springer, 1999.

[39] Eléments de mathématique. [Livre VII]. , Algèbre commutative. Chapitre 8. , Dimension. Chapitre 9. , Anneaux locaux noethériens complets Texte imprimé / N. Bourbaki

[40] Mark Goresky, Andrew Klapper : Algebraic Shift Register Sequences. http ://www.cs.uky.edu/ klapper/algebraic.html (2009)

[41] RudolfLidl, Harald Niederreiter : Finite Fields, Encyclopedia of Mathematics and its Applications, Volume 20, section Algebra, p.84 (1983).

[42] Mark Goresky, Andrew Klapper, Ram Murty, Igor Shparlinski : On Decimations of l-Sequences. SIAM J. Discrete Math. 18(1) : 130-140 (2004)

[43] Andrew Klapper : A Survey of Feedback with Carry Shift Registers. SETA 2004 : 56-71

[44] Andrew Klapper, Mark Goresky : Cryptoanalysis Based on 2-Adic Rational Approximation. CRYPTO 1995 : 262-273

[45] Théorie des Nombres, Borevitch et Safarevitch

[46] http ://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf

[47] http ://csrc.nist.gov/groups/ST/toolkit/rng/documents/sts-2.0.zip.

[48] F. Arnault and T. P. Berger : Design and properties of a new pseudo-random generator based on a filtered FCSR automaton. IEEE, Transactions on Computers, 54(11) :1374-1383, (November 2005).

[49] F. Arnault, T. P. Berger and M. Minier : On the security of FCSR-based pseudo-random generators. In SASC, the state of the Art of Stream Ciphers, pages 179-190, (January 2007).

[50] Marjane A., Mokrane A., Allailou B. : Vectorial Feedback with Carry Registers, arXiv :1103.1432v1 [cs.IT] 8 Mar 2011