Projet d'Initiation à la Recherche

M1 Mathématiques CRYPTIS

Décimations des *l*-séquences

Alexis Beaudin - Simon Gervais

Tuteur : M. Abdelkader Necer

12 mai 2017

Sommaire

Avant-Propos

La présence d'outils de plus en plus développés pour la cryptanalyse, a toujours poussé les cryptologues à chercher des méthodes d'encodage de signaux de plus en plus efficaces et difficiles à percer.

Le papier écrit par Hong *Xu et* Wen-Feng *Qi, "Further Results on the Distinctness of Decimations of l-sequences"[4], porte la trace de ses motivations. Basé sur les travaux des mathématiciens* Goresky *et* Klapper*[9]. Ce papier complète leurs conjectures afin d'offrir un outil efficace pour générer un grand nombre de suites aléatoires de manière efficace.*

Cette analyse à la fois historique et mathématique cherchera à comprendre les raisons exactes ayant poussé l'élaboration du papier, les concepts principaux nécessaires à sa compréhension, et les principaux théorèmes ainsi que ce que leurs résultats impliquent. Elle introduira et étudiera entre autres les concepts de suite, de nombres 2-adiques, de LFSR et FCSR, de décimation et d'autocorrélation.

En annexe se trouveront les diverses preuves développées, soit une preuve d'un théorème du papier, et différentes preuves sur l'un des pré-requis à avoir.

Les autres preuves pourront être trouvées dans différents documents de la bibliographie.

Chapitre 1

Introduction

1.1 Historique

En 1944 a lieu l'invention du premier registre à décalage. Son objectif était de servir d'outil de cryptanalyse lors de la Seconde Guerre Mondiale. Les registres à décalage deviennent ensuite l'objet d'études plus orientées sur les mathématiques.

Dans les années 1970, les LFSR commencent à être utilisés dans le but d'encrypter des signaux. C'est une application intuitive en vue de la rapidité et de la facilité d'utilisation des LFSR. Le système 'Summation Generator' (qui somme deux LFSR avec retenue pour tenter d'éliminer la linéarité) est alors une référence dans le milieu de la cryptographie.

Néanmoins, dans les années 1980, des failles sont mises en évidence sur cette utilisation des registres à décalage. Goresky et Klapper, mathématiciens, contestent cette utilisation considérée comme trop facilement prévisible – car linéaire – et introduisent leur propre modèle.[8]

1.2 Utilisation

Ce modèle de registre à décalage, le FCSR, est encore étudié et exploité de nos jours, en cryptographie où il joue un rôle similaire à celui du LFSR, ou encore en statistiques où il sert à élaborer des suites de quasi-Monte Carlo (suites pseudo-aléatoires de très grande longueur élaborées de manière déterministe).

Il est également utilisé pour le système CDMA, Code Division Multiple Access, un système de transmission de signaux. Le but de ce système est d'encoder plusieurs signaux numériques différents via le même canal. En se basant sur les propriétés obtenues dans le papier, il est possible à partir d'une seule et même suite de taille maximale générée par un FCSR d'obtenir plusieurs sous-suites indépendantes encodant chacun un signal.

Ces suites peuvent également être utilisées comme suites dites d'étalement de spectre. Elles confèrent à un signal une excellente immunité aux interférences et permettent à la transmission d'être cachée dans le bruit de fond.[1]

Chapitre 2

Pré-requis

2.1 Suites

Définition 1. *Une suite $(u_n)_{n\in\mathbb{N}}$ est une application de $\mathbb{N}$ dans $\mathbb{R}$. Elle associe à tout $n \in \mathbb{N}$ un nombre u_n.*
Une suite peut être définie de deux manières :

- *Par son terme général (ex : la suite définie par $u_n = 2^n$ est la suite (1,2,4,8,16...))*
- *Par récurrence (ex : la suite définie par $u_{n+1} = 2u_n+3$ et $u_1 = 1$ est la suite (1,5,13,29,...))*

Définition 2. *Une suite définie par récurrence est une suite définie par un certain nombre de termes initiaux et par une relation de récurrence permettant d'évaluer les suivants.*

Exemple : Un exemple bien connu est la suite de Fibonacci : $u_0 = 0$, $u_1 = 1$, et $\forall n \in \mathbb{N}$, $u_{n+2} = u_{n+1} + u_n$. On obtient bien la suite connue : (0,1,1,2,3,5,8,13,...)

Définition 3. *Une suite récurrente linéaire est une suite définie par récurrence dont la relation de récurrence est une relation linéaire.*
De manière plus générale, une suite récurrente linéaire d'ordre p est une suite dont les p premiers termes sont connus, et dont la relation de récurrence est de type :

$$\forall n \in \mathbb{N}, u_{n+p} = a_0u_n + a_1u_{n+1} + \ldots + a_{p-1}u_{n+p-1} \tag{2.1}$$

Exemple : La suite de Fibonacci est aussi un exemple de suite récurrente linéaire.

Proposition 1. *La relation de récurrence est associée à un polynôme dit polynôme caractéristique :*

$$P(X) = X^P - \sum_{i=0}^{p-1} a_iX^i \tag{2.2}$$

Les suites récurrentes linéaires ont de nombreuses applications, entre autres en analyse, pour l'étude des équations différentielles linéaires, mais aussi parce que ces suites peuvent être générées facilement à l'aide d'un LFSR.

2.2 Suites récurrentes linéaires (LFSR)

Un linear-feedback shift register (LFSR) est une machine à registre qui renvoie comme bit une fonction linéaire des bits précédents.

Un LFSR peut donc générer une suite récurrente linéaire d'ordre p.

Il suffit pour cela d'interpréter la fonction linéaire du LFSR comme le polynôme caractéristique d'une suite et de l'initialiser.

Proposition 2. *On peut interpréter un LFSR comme un développement en série formelle d'une fraction d'un quotient de polynome.*
Soit $(S_n)_{n\in\mathbb{N}}$ une suite engendrée par un LFSR. On lui associe la série génératrice :

$$S(X) = \sum_{n=0}^{\infty} S_n X^n \tag{2.3}$$

Définition 4. *Soit un LFSR dont la fonction de rétroaction est donnée par :*

$$s_n + L = c_1 s_{n+L-1} + c_2 s_{n+L-2} + \ldots + c_L s_n \tag{2.4}$$

On y associe le polynôme de rétroaction :

$$f(X) = 1 + c_1 X + c_2 X^2 + \ldots + c_L X^L \tag{2.5}$$

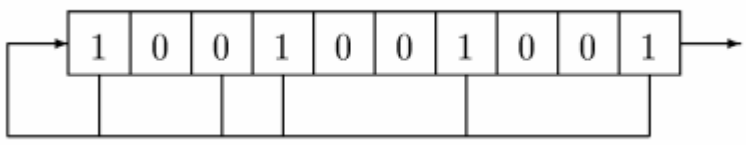
Proposition 3. *La suite $(S_n)_{n\in\mathbb{N}}$ est produite par un LFSR dont le polynôme de rétroaction est :*

$$f(X) = 1 + c_1 X + c_2 X^2 + \ldots + c_L X^L \tag{2.6}$$

si et seulement si son développement en série formelle $s(X) = n$ s'écrit :

$$s(X) = \frac{f(X)}{g(X)} \tag{2.7}$$

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



Exemple : [6]

Définition 5. *Les LFSR peuvent être utilisés comme des générateurs de suites pseudo-aléatoires. Une suite pseudo-aléatoire est une suite vérifiant certaines propriétés statistiques.*

Parmi ces propriétés, les plus classiques sont les trois critères de Golomb.
— Dans chaque période, le nombre de 0 est approximativement égal au nombre de 1 ;

— Une série (de 0 ou de 1) est une succession de bits identiques, maximale (i.e. encadrée par des bits opposés). Dans chaque période, soit S l'ensemble des séries ; on trouve $\frac{|S|}{2}$ séries de longueur 1, $\frac{|S|}{4}$ séries de longueur 2, . . . , $\frac{|S|}{2^k}$ séries de longueur k, et pour chaque longueur, autant de séries de 0 que de séries de 1 ;
— L'autocorrélation arithmétique de la suite est idéale. (Voir la partie corresponante)

Proposition 4. *Les m-sequences – suites de taille maximale générées par un LFSR – vérifient ces propriétés. Pour un polynôme caractéristique de degré maximal n, le nombre de bits généré est* 2^{n-1}.

Néanmoins, la linéarité du LFSR est aussi sa faille, car même si n est très élevé, il suffit d'avoir $2n$ bits de la suite engendrée pour déterminer quel est le LFSR qui l'a engendré. C'est une faille critique des LFSR.

2.3 Décimations

Définition 6. *Soit $(u_n)_{n\in\mathbb{N}}$ une suite. On appelle $D_{k,i}(u_n)$ (avec $i < k$) la fonction qui à associe à (u_n) la sous-suite extraite $(v_n) = (u_{dn+i})$, avec $d \in \mathbb{N}$ et $0 \leq i < d$.*
On dit que $(v_n)_{n\in\mathbb{N}}$ est une décimation de $(u_n)_{n\in\mathbb{N}}$.

Exemple : Soit la suite de terme général $u_n = n$. C'est une suite qui s'écrit explicitement $(0, 1, 2, 3, 4, 5, 6 \ldots)$
Elle se définie par récurrence par $u_0 = 0$ et $u_{n+1} = u_n + 1$.

On peut l'écrire autrement : $1 = u_{n+1} - u_n = u_{n+2} - u_{n+1}$
d'où $u_{n+2} - 2u_{n+1} + u_n = 0$.
On a donc un polynôme caractéristique $X^2 - 2X + 1$, de degré 2.

On prend la sous-suite $D_{2,1}(u_n) = u_{2n+1}$ qui est la suite $(1, 3, 5, 7, 9, \ldots)$.
Elle se définit par récurrence par $v_0 = 1$ et $v_{n+1} = v_{n+2}$.

On s'aperçoit rapidement qu'elle est de même polynôme caractéristique.
En effet, $v_{n+2} - 2v_{n+1} = v_n = 0$.

Remarque : Il semble que décimer une suite ne signifie pas abaisser le degré de son polynôme caractéristique.

Définition 7. *La fonction $D_{k,0}$ possède certaines propriétés : elle est commutative, et :*

$$D_{a,0}(D_{b,0}(u_n)) = D_{b,0}(D_{a,0}(un)) = D_{ab,0}(un) \tag{2.8}$$

$D_{k,i}$ n'est cependant plus commutative pour $i \neq 0$.

Définition 8. *Emboîter deux suites est l'opération "inverse" de décimer une suite.*
Soient les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$, l'emboîtement des deux est :

$$(w_n)_{n\in\mathbb{N}} = (u_0, v_0, u_1, v_1, u_2, v_2, \ldots) \tag{2.9}$$

Exemple : Faisons une combinaison de deux suites $(u_n)_{n\in\mathbb{N}}$ définies comme précédemment par $u_n = n$. On obtient
$(w_n)_{n\in\mathbb{N}} = (0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, \ldots)$
C'est une suite définie par récurrence par $u_0 = 0$, $u_1 = 0$, et $u_{n+2} = u_n + 1$.

On va procéder de même à une écriture alternative : $u_{n+4} - u_{n+2} = u_{n+2} - u_n$.
On a donc un polynôme caractéristique $X^4 - 2X^2 + 1$, de degré 2. On a multiplié par 2 les puissances de tous les X.
On peut vérifier rapidement que si on avait interpolé trois fois un, le polynôme caractéristique aurait été $X^6 - 2X^3 + 1$.

Remarque : Il semble donc que combiner des suites augmente parfois le degré du polynôme caractéristique, mais ce n'est pas une généralité (car combiner $(0, 2, 4, 6, 8, \ldots)$ et $(1, 3, 5, 7, 9 \ldots)$, deux suites de polynôme caractéristique de degré 2, donne une autre suite de polynôme caractéristique de degré 2).

Les décimations sont utilisées pour les signaux afin de garder uniquement l'information essentielle pour la compression de certains signaux. Elles peuvent aussi être utilisées, grâce à ce papier, pour générer à partir d'une unique suite pseudo aléatoire un grand nombre de suites pseudo aléatoires.

2.4 Nombres 2-adiques

2.4.1 Nombres et entiers p-adiques

Nous allons maintenant définir la notion de nombre p-adique[2, 11]. Elle peut être vue comme une extension de la notion de base p. Pour rappel :

Définition 9. $\forall x \in \mathbb{N}$, $\forall n \in \mathbb{N}^*$, *écrire x en base n revient à écrire x sous la forme :*

$$x = \sum_{i=0}^{\infty} a_i n^i \tag{2.10}$$

où, $\forall i \in \mathbb{N}$, $a_i \in \{0, 1, \ldots, n-1\}$

Exemple :

$$\begin{aligned} 353 &= 1 \cdot 1 + 0 \cdot 4 + 2 \cdot 16 + 1 \cdot 64 + 256 \\ &= 1 \cdot 4^0 + 0 \cdot 4^1 + 2 \cdot 4^2 + 1 \cdot 4^3 + 1 \cdot 4^4 \\ &= 10211_4 \end{aligned}$$

Un entier p-adique peut donc être vu comme une extension de cette définition dans $\mathbb{Z}$. Cependant ici, la "base" sera désormais un nombre premier p.

Définition 10. $\forall x \in \mathbb{Z}$, $\forall n \in \mathbb{N}^*$, *$x$ est un entier p-adique si et seulement si il peut s'écrire sous la forme :*

$$x = \sum_{i=0}^{\infty} a_i p^i \tag{2.11}$$

où, $\forall i \in \mathbb{N}$, $a_i \in \{0, 1, \ldots, p-1\}$

Remarque : La notation s'effectue en sens inverse de ce que l'on a l'habitude de rencontrer en écriture en base n, et peuvent éventuellement être infinis à gauche.

Exemple :

$$\begin{aligned} -1 &= \sum_{i=0}^{\infty} 2^i \\ &= \ldots 111111111111_2 \end{aligned}$$

Cela se vérifie facilement, car ajouter 1 à cette suite donnera 0 à droite puis ajoutera une retenue, qui donnera un 0, et ce infiniment, ce qui donnera au final 0. Notons que cette écriture a du sens car cette série converge selon une norme que nous détaillerons plus bas.

La suite logique est donc d'étendre cette écriture dans $\mathbb{Q}$. Nous allons donc introduire la notion de nombre p-adique :

Définition 11. *$\forall x \in \mathbb{Q}$, $\forall n \in \mathbb{N}^*$, x est un nombre p-adique si et seulement si il peut s'écrire sous la forme :*

$$x = \sum_{i=k}^{\infty} a_i p^i \tag{2.12}$$

où $k \in \mathbb{Z}$ et, $\forall i \in \mathbb{N}$, $a_i \in \{0, 1, \ldots, p-1\}$.

*On appelle cette forme la **Décomposition canonique de Hensel**.*

Remarque :

— Certains éléments de $\mathbb{Q}$ peuvent être des entiers p-adiques !

— Contrairement à ce que l'on a l'habitude de rencontrer en écriture en base n, il peut donc il y avoir une virgule dans la notation en décomposition canonique de Hensel, si x est un nombre p-adique mais pas un entier p-adique.

Exemples :

$$\begin{aligned} \frac{1}{5} &= \ldots 110011001101_2 \end{aligned}$$

Ce résultat peut se vérifier simplement en le multipliant par $= \ldots 0000101_2$. Ici, on voit bien que $\frac{1}{5}$ est un entier 2-adique ! !

$$\begin{aligned} \frac{21}{10} &= \ldots 222222222224,3_5 \end{aligned}$$

Ici, on voit que $\frac{21}{10}$ n'est pas un entier 5-adique mais est un nombre 5-adique ! !

2.4.2 Espace des nombres p-adiques

Nous allons maintenant voir dans quel ensemble se situent les nombres p-adiques.[3] Pour cela, nous allons avoir besoin de définir une fonction nommé valuation p-adique :

Définition 12. *$\forall x \in \mathbb{N}$, on appelle valuation p-adique, notée $v_p(x)$ de x l'exposant de p dans la décomposition de x en produits de facteurs premiers.*

Afin d'étendre ceci à $\mathbb{Q}$, $\forall x \in \mathbb{N}$, $\forall y \in \mathbb{N}$ on a :

$$v_p(\frac{x}{y}) = v_p(x) - v_p(y) \tag{2.13}$$

Remarque : Si $v_p(x) = 0$, alors x est un entier p-adique.

Cette valuation p-adique va nous permettre de définir une valeur absolue :

Définition 13. *$\forall x \in \mathbb{Q}^*$, on appelle valeur absolue p-adique, notée $|x|_p$:*

$$|x|_p = (\frac{1}{p})^{v_p(x)} = p^{-v_p(x)} \tag{2.14}$$

On admettra que $|0|_p = 0$, par prolongement.

Proposition 5. *La valeur absolue p-adique est une norme que $\mathbb{Q}$.*

Démonstration. En annexe □

Définition 14. *$\forall p$ premier, $\mathbb{Q}_p$ est l'ensemble des nombres p-adiques.*
Il s'agit en fait de l'espace normé $(\mathbb{Q}, |\cdot|_p)$.

Remarque : $\mathbb{Z}_p$, l'ensemble des entiers p-adiques, peut être construit de façon analogue.

Proposition 6.

$$\sum_{i=0}^{\infty} 2^i \tag{2.15}$$

est une série convergente dans $\mathbb{Q}_2$

Démonstration. En annexe □

Proposition 7. *$\forall p$ premier, $\mathbb{Q}_p$ est un corps.*

Démonstration. En annexe □

Proposition 8. *$\forall p$ premier, $\forall x \in \mathbb{Q}_p$, x est un <u>entier</u> p-adique $\Leftrightarrow v_p(x) \geq 0$.*

Démonstration. En annexe □

Définition 15. *Tout entier p-adique peut s'écrire sous forme d'une suite $(u_n)_{n\geq 1}$ telle que, $\forall n \geq 1$:*

$$u_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ et } u_n \equiv u_{n+1} \pmod{p}^n \tag{2.16}$$

Exemple :

$$\begin{aligned} 51 &= 1 + (1 \cdot 2) + (0 \cdot 2^2) + (0 \cdot 2^3) + (1 \cdot 2^4) + (1 \cdot 2^5) \\ u_n &= (1, 3, 3, 3, 19, 51, 51, \ldots) \end{aligned}$$

Remarque : *Quelques différences "amusantes" entre $\mathbb{Q}_p$ et $\mathbb{R}$*
- Certaines suites peuvent converger dans $\mathbb{R}$ et dans certains $\mathbb{Q}_p$, mais pas vers les mêmes nombres, et diverger dans d'autres $\mathbb{Q}_p$
- Dans $\mathbb{Q}_p$, la suite $(p^n)_{n\in\mathbb{N}}$ converge vers 0
- Toute boule est centrée en tous ses points ; et 2 boules sont soit incluses l'une dans l'autre, soit disjointes

Dans la suite, ce qui nous intéressera sera surtout les entiers 2-adiques.

2.4.3 Calcul dans $\mathbb{Q}_p$

Addition et soustraction

L'addition est analogue à celle dans $\mathbb{R}$, avec les retenues :

$$\begin{array}{cccccccc} & \ldots & 1 & 2 & 3 & 4 & 0 & 1_5 \\ + & \ldots & 1 & 0 & 4 & 3 & 2 & 1_5 \\ \hline & \ldots & 2 & 3 & 3 & 2 & 2 & 2_5 \end{array} \qquad \begin{array}{cccccccc} & \ldots & 4 & 1 & 3 & 5 & 6 & 2_7 \\ + & \ldots & 1 & 0 & 5 & 4 & 1 & 1_7 \\ \hline & \ldots & 5 & 2 & 2 & 3 & 0 & 3_7 \end{array}$$

De même pour la multiplication :

$$\begin{array}{cccccccc} & & & & 3 & 0 & 3 & 2_5 \\ \times & & & & & 2 & 4 & 1_5 \\ \hline & & & & 3 & 0 & 3 & 2_5 \\ + & & 2 & 3 & 1 & 3 & 3 & \cdot_5 \\ + & 1 & 0 & 3 & 1 & 4 & \cdot & \cdot_5 \\ \hline & 1 & 3 & 2 & 1 & 3 & 1 & 2_5 \end{array} \qquad \begin{array}{cccccccc} & & 4 & 1 & 2 & 4 & 0 & 3_7 \\ \times & & & & & 5 & 2 & 1_7 \\ \hline & & & & 2 & 4 & 0 & 3_7 \\ + & & & 4 & 1 & 2 & 6 & \cdot_7 \\ + & 1 & 6 & 0 & 0 & 1 & \cdot & \cdot_7 \\ \hline & 1 & 6 & 4 & 4 & 0 & 6 & 3_7 \end{array}$$

Il est donc aisé de calculer un nombre par rapport à un autre. On pourra par exemple aussi s'en servir pour calculer un nombre négatif $-n$ en multipliant la forme p-adique n par -1.

Par division euclidienne

Cette méthode est utile pour transformer un nombre de $\mathbb{Q}$ en un nombre de $\mathbb{Q}_p$. Elle est surtout utilisée un nombre est sous forme :

$$\frac{1}{1 - p - p^2 - p^3 - \ldots}$$

Prenons par exemple :

$$\frac{-1}{5} = \frac{1}{1 - 2 - 2^2}$$

$$\begin{array}{l|l} \begin{array}{cccccccccc} & 1 & & & & & & & & \\ -(& 1 & - & 2 & - & 2^2 &) & & & \\ \hline & & & 2 & + & 2^2 & & & & \\ & & -(& 2 & - & 2^2 & - & 2^3 &) & \\ \hline & & & & & 2 \cdot 2^2 & + & 2^3 & & \end{array} & \begin{array}{c} 1 - 2 - 2^2 \\ \hline 1 + 2 + 2^4 + 2^5 + \ldots \end{array} \\ \begin{array}{cccccccccc} & & & & & & & = & 2^4 & \\ & & & & & & & -(& 2^4 & - & 2^5 & - & 2^6 &) \\ \hline & & & & & & & & 2^5 & + & 2^6 & & \end{array} & \end{array}$$

Ici, on a donc :

$$\begin{aligned} \frac{-1}{5} &= 1 + 2 + 2^4 + 2^5 + \ldots \\ &= \ldots 11011011_5 \end{aligned}$$

2.5 Auto-corrélation

Définition 16. *L'autocorrélation d'une fonction f, notée $R_f(T)$, est la corrélation entre $f(x)$ et $f(x+T)$.*

Proposition 9. *L'autocorrelation est une fonction symétrique, $R_f(T) = R_f(-T)$, qui atteint son maximum en $R_f(0)$.*

En effet, la corrélation entre deux fonctions identiques est maximale.

Dans le cas d'une suite binaire pseudo-aléatoire, on introduit la notion d'autocorrélation arithmétique. [10]

Définition 17. *Soit $(a_n)_{n\in\mathbb{N}}$ une suite binaire pseudo-aléatoire de période T.*
Étant donné que la corrélation périodique d'ordre k est définie comme suit :

$$C_k(a_n) = \max_{0<d1<d2<\ldots<dk-1<T} |\sum_{n=0}^{T-1}(-1)^{a_n+a_{n+d1}+a_{n+d2}+\in+a_{n+dk-1}}| \tag{2.17}$$

L'autocorrélation, $C_2(a_n)$, sera :

$$C_2(a_n) = \max_{0<d<T} |\sum_{n=0}^{T-1}(-1)^{a_n+a_{n+d}}| \tag{2.18}$$

Exemple : En pratique, si on dispose de la suite suivante : 1011001, de période 7, on écrit d'abord toutes les suites 'décalées' de 1 à 6 crans.

- $d = 1 \Rightarrow 0110011$
- $d = 2 \Rightarrow 1100110$
- $d = 3 \Rightarrow 1001101$
- $d = 4 \Rightarrow 0011011$
- $d = 5 \Rightarrow 0110110$
- $d = 6 \Rightarrow 1101100$

Pour chacune des suites, on somme un "indicateur" pour chaque chiffre, qui vaut -1 s'ils sont différents, et 1 s'ils sont identiques. On fait ensuite une valeur absolue de la somme. On a donc les résultats suivants :

- $d = 1 \Rightarrow 1$
- $d = 2 \Rightarrow 5$
- $d = 3 \Rightarrow 3$
- $d = 4 \Rightarrow 3$
- $d = 5 \Rightarrow 5$
- $d = 6 \Rightarrow 1$

D'où $C_2(a_n) = 5$.

Néanmoins, il existe une autre définition de l'autocorrélation.

Définition 18. *Soient :*

$$X(t) = \sum_{n=0}^{T-1} a_{n+t}2^n \text{ et } \alpha(t) = \sum_{n=0}^{\infty} a_{n+t}2^n \tag{2.19}$$

On définit $s_{n,t}$ tel que :

$$\alpha(n) - \alpha(0) = \sum_{n=0}^{\infty} s_{n,t} 2^n \tag{2.20}$$

Alors l'autocorrélation arithmétique A est définie par :

$$A(t) = C_1(s_{n,t}) = |\sum_{n=0}^{T-1} (-1)^{s_{n,t}}| \tag{2.21}$$

L'autocorrélation est entre autres utilisée pour les suites pseudo-aléatoire afin de mesurer la dépendance entre un bit obtenu et le ou les suivants.

Goresky et Klapper, dans une œuvre différente, ont prouvé que pour $1 < t < T$ fixé, l'autocorrélation arithmétique idéale d'une suite de période T est $\frac{T}{2^T - pgcd(T,t)}$. C'est donc vers cette autocorrélation que devrait tendre une suite pseudo-aléatoire.

Fort heureusement, il a été prouvé pour les m-sequences des LFSR et les l-sequences des FCSR que c'est bel et bien le cas.[7]

2.6 Feedback with Carry Register (FCSR)

Introduisons maintenant le concept de FCSR.

Cette notion est en fait analogue à celle des LFSR, à ceci près qu'ils ont été créés pour "casser" la linéarité des LFSR, grâce à un système de retenue.

Là où les LFSR étaient plutôt modélisés grâce à des suites binaires récurrentes, les FCSR sont généralement modélisés par des développements de Hensel d'un nombre 2-adique.

Voici comment fonctionne un FCSR :
Si $N > 1$ est un entier, alors un N-aire FCSR de longueur r peut être vu comme une suite d'états :

— D'abord, on fixe un état initial :

$$(a; z) = (a_0, a_1, \ldots, a_{r-1}; z)$$

Avec, $\forall i \in \mathbb{N}$, $a_i \in S = \{0, 1, \ldots, N-1\}$

— Ensuite, on calcule :

$$s = q_r a_0 + \ldots + q_1 a_{r-1} + z = \sum_{i=0}^{r-1} (q_{r-i} a_i) + z$$

— Puis, on calcule a_r et z' grâce à l'expression :

$$s = a_r + N z'$$

où $a_r \in S$. Ainsi, on réalise une "division euclidienne" par N.
Et c'est là la différence principale des FCSR : on retient le z', qui sera une "retenue".

— L'état suivant est donc :

$$(a; z) = (a_1, a_2, \ldots, a_r; z')$$

Définition 19. *On nomme entier de connexion, noté q, le nombre :*

$$q = q_r N^r + \ldots + q_1 N - 1 = \sum_{i=1}^{r} (q_i N^i) - 1 \tag{2.22}$$

Si N est premier, la sortie du FCSR est associée à un nombre N-adique a tel que :

$$a = a_0 + a_1 N + a_2 N^2 + \ldots = \sum_{i=0}^{\infty} a_i N^i \tag{2.23}$$

Si la suite produite est périodique, alors il existe un autre moyen de la définir :

Proposition 10. *Si a est une séquence périodique générée par un FCSR, avec un entier de connexion q, alors :*

$$a_i = (cN^{-i} \pmod q) \pmod N \tag{2.24}$$

Proposition 11. *Si a est une séquence périodique générée par un FCSR, avec un entier de connexion q, alors sa période est inférieure à $\varphi(q)$ (la fonction d'Euler de q).*

Définition 20. *Si a est une séquence périodique générée par un FCSR, avec un entier de connexion q, et que sa période est maximale, c'est-à-dire $\varphi(q)$, alors a est appelée une l-sequence.*

Proposition 12. *a est une l-sequence si et seulement si N et q sont premiers entre eux.*

Dans la suite, nous allons nous intéresser à des suites binaires, donc $N = 2$. Étant donné que l'on ne considère que des entiers de connexion $q = p^e$, avec p nombre premier impair et $e \geq 1$, on a toujours N premier avec q.
Par conséquent, le LFSR produira toujours des l-sequences.
Elles produiront donc des suites 2-adiques qui seront périodiques, de période $\varphi(q)$.

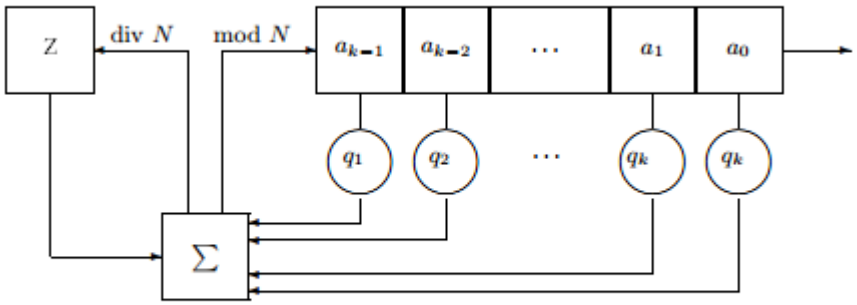


Fig. 2. A Feedback with Carry Shift Register

Exemple : [5]

2.7 Conjecture de Goresky et Klapper

Conjecture 1. *Soit a une l-sequence générée par un FCSR dont l'entier de connexion est p^e, avec p premier.* Goresky *et* Klapper *ont conjecturé que pour $p^e \notin \{5, 9, 11, 13\}$, toutes les décimations de a sont cycliquement distinctes.*

NB : Pour $p > 13$ et $e = 1$, Goresky et Klapper ont prouvé que la quantité de décimations distinctes est élevée, et parfois qu'elles sont toutes distinctes.

Pour pouvoir étudier l'article de Hong Xu et Wen-Feng Qi, nous allons devoir définir une nouvelle notation :

Définition 21. *Soit $f(x)$ un polynôme de $\mathbb{Z}/(p^e)$.*

- *On note $G(f(x), p^e)$ l'ensemble des séquences de $\mathbb{Z}/(p^e)$ générées par $f(x)$.*
- *On note $G'(f(x), p^e)$ les séquences de $G(f(x), p^e)$ qui ne sont pas congrues à 0, modulo p. Autrement dit,*

$$G(f(x), p^e) = \{\underline{u} \in G(f(x), p^e) | \underline{u} \not\equiv \underline{0} \pmod{p}\} \tag{2.25}$$

Avec cette définition, nous allons pouvoir reformuler la conjecture de Goresky et Klapper.

Conjecture 2. *Soit $p^e \notin \{5, 9, 11, 13\}$, avec p premier et $e > 1$, tels que 2 soit une racine primitive modulo p^e. Posons ξ et ζ deux différentes racines primitives modulo p^e. Posons $f(x) = x - \xi$ et $g(x) = x - \zeta$. Alors :*

$$\forall \underline{u} \in G'(f(x), p^e), \forall \underline{v} \in G'(g(x), p^e) : u \not\equiv v \pmod{2}. \tag{2.26}$$

Le but du papier sera donc de vérifier cette conjecture dans certains cas.

Chapitre 3

Décimations des l-séquences

3.1 Structure du papier

Le papier étudié, ***Further Results on the Distinctness of Decimations of l-sequences***, de Hong Xu et Wen-Feng Qi, se base sur les travaux de Goresky et Klapper sur le sujet.

Ici, il s'agit de s'intéresser aux FCSR dont l'entité de connexion est p^e avec $e > 1$, avec l'exception notable de $p^e = 9$. Le but du papier est de prouver que les l-sequences générées par de tels FCSR sont cycliquement distinctes. Dans ce but, le papier est structuré autour de trois grands théorèmes.

Le **Théorème 1** est l'objectif principal du papier. C'est l'extension de la **Conjecture 2** qui avait été posée par Goresky et Klapper avec $p^e \notin \{5, 9, 11, 13\}$.

Pour le prouver, nous allons utiliser deux autres théorèmes : le **Théorème 2** et le **Théorème 3**. Ces deux théorèmes correspondent en fait à une disjonction de cas. Nous allons alors étudier les deux cas, et prouver que les deux sont valides. Dans ce cas, le Théorème 1 sera prouvé.

Enfin, pour justifier ces 2 derniers théorèmes, sont utilisés **5 lemmes**, qui seront détaillés ci-dessous. Ils apporteront des éléments qui serviront dans les preuves des théorèmes 2 et 3.

3.2 Théorèmes

Théorème 1. *Soit $p^e \neq 9$ avec p premier et $e > 1$, tel que 2 est une racine primitive modulo p^e. Si ξ et ζ sont aussi de telles racines distinctes, posons $f(x) = x - \xi$ et $g(x) = x - \zeta$. Alors :*

$$\forall \underline{u} \in G'(f(x), p^e), \forall \underline{v} \in G'(g(x), p^e) : u \not\equiv v \pmod 2. \tag{3.1}$$

Prouver ce théorème revient à prouver le fait que les décimations d'une l-séquence engendrée par le FCSR associé sont cycliquement distinctes.

Pour y parvenir, on introduit les notations $\underline{\alpha} = h_f \underline{u}_0 \pmod p$ et $\underline{\beta} = h_g \underline{u}_0 \pmod p$, avec $h_f(x)$ défini dans la proposition 1 :

Proposition 13. *Soit $f(x)$ un polynôme primitif de degré n sur $\mathbb{Z}/(p^e)$, p premier et $e \in \mathbb{N}^*$. $h_f(x)$ est l'unique polynôme non-nul de $\mathbb{Z}/p\mathbb{Z}$ de degré inférieur à n tel que :*

$$x^{p^{i-1}T_0} \equiv 1 + p^i \cdot h_f(x) \pmod{f(x), p^{i+1}}, i \in \{1, 2, ..., e-1\} \tag{3.2}$$

où $T_0 = p^n + 1$.

Une fois ceci défini, il ne reste plus qu'à énoncer les deux théorèmes en effectuant une simple disjonction des cas. Précisément, nous allons étudier si $\underline{\alpha}$ est congru ou non à $(p-1)\underline{\beta} \pmod p$.

Théorème 2. *Si* $\underline{u}$, $\underline{v}$, $\underline{\alpha}$, $\underline{\beta}$ *sont définis comme précédemment :*

$$\underline{\alpha} \not\equiv (p-1)\underline{\beta} \pmod p \Rightarrow \underline{u} \not\equiv \underline{v} \pmod 2 \tag{3.3}$$

Théorème 3. *Si* $\underline{u}$, $\underline{v}$, $\underline{\alpha}$, $\underline{\beta}$ *sont définis comme précédemment :*

$$\underline{\alpha} \equiv (p-1)\underline{\beta} \pmod p \Rightarrow \underline{u} \not\equiv \underline{v} \pmod 2 \tag{3.4}$$

Prouver les théorèmes 2 et 3 reviendrait donc à prouver le théorème 1. La preuve de ce théorème sera détaillée en **Annexe A**.

3.3 Lemmes utilisés

De nombreux lemmes sont utilisés pour prouver les théorèmes 2 et 3, qui constituent le véritable 'cœur' de la démonstration, le reste du papier n'étant que des préliminaires et éléments afin de la construire.

Lemme 1. *Soit* $f(x)$ *un polynôme primitif de* $\mathbb{Z}/(p)$*, avec* p *premier impair. Alors :*

$$\forall \underline{u}, \underline{v} \in G'(f(x), p), \underline{u} = \underline{v} \Leftrightarrow \underline{u} \equiv \underline{v} \pmod 2 \tag{3.5}$$

Ce lemme est central à l'entité de la démonstration, voire du papier. Il nous permet de comprendre pourquoi le Théorème 1 est équivalent à l'objectif posé par le papier.

Lemme 2. *Soit* p *un nombre premier impair. Soit* $\lambda, \alpha, \beta \in (\mathbb{Z}/(p))^*$*, avec* $\alpha \equiv \lambda\beta \pmod p$*, et* $\delta \in \mathbb{Z}/(p)$ *avec* $\delta \equiv 0 \pmod 2$*. Si* $1 \leq \lambda \leq p-2$*, alors* $\exists j \in \mathbb{N}$*,* $1 \leq j \leq p-1$*, tel que :*

$$(j\alpha \pmod p) \pmod 2 \neq ((j\beta + \delta) \pmod p) \pmod 2 \tag{3.6}$$

Le lemme 2, qui définit α et β, précise le fait qu'il s'agit de m-séquences, engendrées respectivement par $f(x) \pmod p$ et $g(x) \pmod p$, ce qui leur confère des propriétés essentielles pour la suite de la démonstration.

Lemme 3. *Soient* $\underline{u}$,$\underline{v}$ *définis comme précédemment. Si* $\exists t \in \mathbb{N}$ *tel que* $u_{e-1}(t) \not\equiv v_{e-1}(t) \pmod 2$*, alors :*

$$\underline{u} \not\equiv \underline{v} \pmod 2 \tag{3.7}$$

Le lemme 3 donne une propriété essentielle, qui sera par la suite utilisée pour démontrer le Théorème 2 et une partie des cas étudiés dans le Théorème 3.

Lemme 4. *Soient* $\underline{u}$,$\underline{v}$ *et* $\underline{\alpha}$, $\underline{\beta}$ *définis comme précédemment. Si* $\underline{\alpha} \equiv (p-1)\underline{\beta} \pmod p$ *et* $\underline{u}_{e-1} \equiv \underline{v}_{e-1} \pmod p$*, alors :*

$$\underline{u}_{e-1} + \underline{v}_{e-1} \equiv (p-1) \cdot \underline{1} \pmod p \tag{3.8}$$

Le lemme 4 donne enfin une propriété pour le Théorème 3. C'est pourquoi, en recoupant les lemmes 3 et 4, il est possible de couvrir tous les cas étudiés dans le Théorème 3.

Lemme 5. *Soient $f(x)$ et $g(x)$ définis comme précédemment. Si $p < 3$, alors $\nexists \underline{u} \in G'(f(x), p^e$ et $\underline{v} \in G'(g(x), p^e$:*

$$\underline{u}_0 = \underline{v}_0 \tag{3.9}$$

et

$$\underline{u}_1 + \underline{v}_1 \equiv (p-1) \cdot \underline{1} \pmod{p} \tag{3.10}$$

Si $p = 3$ et $e \geqslant 3$, alors $\nexists \underline{u} \in G'(f(x), p^e$ et $\underline{v} \in G'(g(x), p^e$:

$$\underline{u}_0 = \underline{v}_0 \tag{3.11}$$

et

$$\underline{u}_2 + \underline{v}_2 \equiv (p-1) \cdot \underline{1} \pmod{p} \tag{3.12}$$

Le lemme 5 sera très utile pour une disjonction de cas du théorème 3.

Annexe A

Preuves sur les nombres p-adiques

Proposition 14. *La valeur absolue p-adique est une norme que* $\mathbb{Q}$.

Démonstration.
— $\forall p$ premier, si $|x|_p = 0$, alors soit $x = 0$ d'après le prolongement cité ci-dessus,
soit $p^{-v_p(x)} = 0$, ce qui est impossible car $p \neq 0$.
Aussi, si $x = 0$, alors évidemment $|x|_p = 0$. Donc $|x|_p = 0 \Leftrightarrow x = 0$.
— $\forall x, y \in \mathbb{Q}$, $\forall p$ premier, $|x + y|_p = p^{-v_p(x+y)}$
Or, il paraît évident que $v_p(x + y) \geq min(v_p(x), v_p(y))$, par définition de v_p
Donc $-v_p(x + y) \leq sup(-v_p(x), -v_p(y))$
Soit $-v_p(x + y) \leq -v_p(x)$ et $-v_p(x + y) \leq -v_p(y)$
Soit $p^{-v_p(x+y)} \leq p^{-v_p(x)}$ et $p^{-v_p(x+y)} \leq p^{-v_p(y)}$
Donc $|x + y|_p \leq |x|_p$ et $|x + y|_p \leq |y|_p$
Soit au final $|x + y|_p \leq |x|_p + |y|_p$

— $\forall x, y \in \mathbb{Q}$, $\forall p$ premier, $|xy|_p = p^{-v_p(xy)}$
Or, il paraît évident que $v_p(xy) = v_p(x) + v_p(y)$, par définition de v_p
De là, $p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)}$
Soit au final $|xy|_p = |x|_p|y|_p$

□

Proposition 15.

$$\sum_{i=0}^{\infty} 2^i \tag{A.1}$$

est une série convergente dans $\mathbb{Q}_2$

Démonstration. Soit $k \in \mathbb{N}$.

$$\begin{aligned} |\sum_{i=0}^{k} 2^i|_2 &\leq \sum_{i=0}^{k} |2^i|_2 \\ &\leq \sum_{i=0}^{k} \frac{1}{2^i} \\ &\leq 2 \end{aligned}$$

Par conséquent, la série $\sum_{i=0}^{\infty} 2^i$ converge pour la norme 2-adique. De plus,

$$\begin{aligned}
\sum_{i=0}^{\infty} 2^i + \sum_{i=0}^{\infty} 2^i &= 2 \cdot \sum_{i=0}^{\infty} 2^i \\
&= \sum_{i=1}^{\infty} 2^i \\
&= \sum_{i=0}^{\infty} 2^i - 1 \\
\Rightarrow \sum_{i=0}^{\infty} 2^i &= -1
\end{aligned}$$

□

Introduisons un lemme :

Lemme 6. *Un élément de $\mathbb{Z}_p$ est inversible si et seulement si sa variation est nulle.*

Démonstration. Soit $a \in \mathbb{Z}_p$. On peut écrire a sous la forme suivante :

$$a = \sum_{i=0}^{\infty} a_i p^i$$

Posons que sa variation est nulle. Dans ce cas, sa réduction dans $\mathbb{F}_p$ est non nulle, et donc inversible en tant qu'elément de ce corps.
Choisissons $0 < b_0 < p$ tel que $a_0 b_0 \equiv 1 \pmod{p}$.
Alors $\exists k$ tel que $a_0 b_0 = 1 + kp$.
Or, on sait que $\exists \alpha$ tel que $a = a_0 + p\alpha$.
Donc $ab_0 = 1 + kp + p\alpha b_0 = 1 + p\beta$, avec $\beta = (k + \alpha b_0)$
C'est-à-dire que si $(1 + \beta p)$ est inversible
Alors : $ab_0(1 + \beta p)^{-1} = 1$
Soit $a^{-1} = b_0(1 - \beta p)^{-1}$
Or, on peut remarquer que, $\gamma \in \mathbb{Z}$:
$(1 - \gamma p)^{-1} = 1 - \gamma p) + (\gamma p)^2 + \ldots$ Qui est clairement un entier p-adique.
Donc si on prend $\beta = -\gamma$, $(1 + \beta p)$ est inversible, donc a est inversible.

Inversement, si a est inversible, alors sa réduction à $\mathbb{F}_p$ aussi, donc elle est non nulle. Donc $a_0 \neq 0$, donc sa variation est nulle.

□

Proposition 16. *$\forall p$ premier, $\mathbb{Q}_p$ est un corps.*

Démonstration. $\forall p$ premier, $\mathbb{Q}_p \subset \mathbb{R}$.
Nous devons donc prouver que $\mathbb{Q}_p$ est un sous-corps de $(\mathbb{R}, +, \times)$.
On peut remarquer que l'addition et la multiplication ont déjà été évoquées comme héritant de celles de $\mathbb{R}$, et que $\mathbb{Q}_p$ est stable pour celles-ci.
Nous allons donc nous concentrer à prouver que nous pouvons inverser dans $\mathbb{Q}_p$.
$\forall \frac{a}{b} \in \mathbb{Q}_p$, avec $a, b \in \mathbb{Z}_p$, $\exists n_1, n_2, u_1, u_2 \in \mathbb{Z}$ tels que : $a = p^{n_1} u_1$ et $b = p^{n_2} u_2$
Par conséquent,

$$\frac{a}{b} = \frac{p^{n_1} u_1}{p^{n_2} u_2} = p^{n_1 - n_2} \frac{u_1}{u_2}$$

Pour prouver que $\frac{a}{b}$, il suffit $\frac{u_1}{u_2}$ l'est (nous sommes dans $\mathbb{Q}_p$, donc la puissance de p peut être négative). Or, par définition, $v_p(u_1) = v_p(u_2) = 0$.
Donc u_1 et u_2 sont inversibles. Donc $\frac{a}{b}$ l'est aussi. □

Proposition 17. *$\forall p$ premier, $\forall x \in \mathbb{Q}_p$, x est un <u>entier</u> p-adique $\Leftrightarrow v_p(x) \geq 0$.*

Démonstration. Avec ce qui a été fait précédemment, on prouve cette proposition simplement :
<u>$\Rightarrow$:</u> Si $x \in \mathbb{Q}_p$ est un entier, alors $x \in \mathbb{Z}_p$. Mais comme il appartient aussi à $\mathbb{Q}_p$ qui est un corps, x est inversible. Or un entier p-adique inversible est de variation nulle.
<u>$\Leftarrow$:</u> Si $x \in \mathbb{Q}_p$ est de variation positive, alors posons $a, b \in \mathbb{Z}_p$ tels que $x = \frac{a}{b}$, on a $v_p(a) \geq v_(p)$.
Donc, $\exists u_1, u_2 \in \mathbb{Z}_p$ tq :

$$\begin{aligned} \frac{a}{b} &= \frac{p^{v_p(a)}u_1}{p^{v_p(a)}u_2} \\ &= p^{v_p(a)-v_p(b)}\frac{u_1}{u_2} \end{aligned}$$

Mais comme u_2 est de variation nulle, il est inversible, $\exists u_3 \in \mathbb{Z}_p$ tq $(u_2)^{-1} = u_3$. Donc :

$$\frac{a}{b} = u_1 u_3$$

Donc $x \in \mathbb{Z}_p$. □

Annexe B

Preuve du Théorème 3

Penchons-nous par exemple sur la preuve du **Théorème 3**. Il s'agit d'une disjonction de cas, puisant principalement dans le **lemme 3** et le **lemme 4**.
Elle suppose dans un premier temps que :

$$\exists t \in \mathbb{N}, \underline{u}_{e-1}(t) \not\equiv \underline{v}_{e-1}(t) \pmod 2 \tag{B.1}$$

On en déduit, par le **lemme 3**, que $\underline{u} \not\equiv \underline{v} \pmod 2$. Dans un tel cas, la démonstration est déjà terminée.

Dans le cas contraire, on suppose donc la chose suivante :

$$\underline{u}_{e-1} \equiv \underline{v}_{e-1} \pmod 2 \tag{B.2}$$

Du **Lemme 4**, il découle la chose suivante :

$$\underline{u}_{e-1} + \underline{v}_{e-1} \equiv (p-1) \cdot \underline{1} \pmod p \tag{B.3}$$

Il faut pour terminer la preuve, prouver que :

$$(\underline{u} \pmod{p^{e-1}}) \pmod 2 \neq (\underline{v} \pmod{p^{e-1}}) \pmod 2 \tag{B.4}$$

Vu qu'il s'agit de deux suites primitives, on les écrira par facilité de langage $\underline{u}^{(e-1)}$ et $\underline{v}^{(e-1)}$

Le **lemme 3** nous permet de donner que si $\underline{u}_{e-2} \not\equiv \underline{v}_{e-2} \pmod 2$, la démonstration est terminée. On va donc s'intéresser uniquement aux cas où ces nombres sont congrus.

On appelle k le plus grand entier tel que $\forall j \leq k$, $\underline{u}_{e-j} \not\equiv \underline{v}_{e-j} \pmod 2$. Si $k = e$, alors on a particulièrement que $\underline{u}_0 \equiv \underline{v}_0 \pmod 2$, et par le **lemme 1** que $\underline{u}_0(t) = \underline{v}_0(t)$. Ce résultat contredit le **lemme 5**.

Dans le cas contraire, on a que $\underline{u}_{e-k-1} \equiv \underline{v}_{e-k-1} \pmod 2$. Le **lemme 3** nous donne alors que $\underline{u}_{e-k} \not\equiv \underline{v}_{e-k} \pmod 2$. Néanmoins, nous savons aussi que $\forall j \leq k$, $\underline{u}_{e-j} \equiv \underline{v}_{e-k} \pmod 2$.

On a donc une preuve du théorème.

Annexe C

Implémentations en python

Voici un exemple d'implémentation du FCSR en python :

```
#!/usr/bin/python
# coding= utf8

def FCSR(N,q,a,z):
        j=0
        l=(int)(raw_input("Inquiquez le nombre d'éxécutions du FCSR"))
        while l!=0:
                i=0
                s=0
                while i<r :
                        s += q[r-i-1]*a[i+j]
                        i+=1
                s += z
                z=s//N
                a.append(s%N)
                j+=1
                l-=1
        return a

def base_p(x,p):
        b=[]
        while x != 0 :
                b.append(x%p)
                x=x//p
        return b

N =(int)(raw_input("Indiquez N"))
j=(int)(raw_input("Indiquez l'entier de connexion q"))
j=j+1
q=base_p(j,N)
q=q[1:]
r =len(q)
i=0
```

```
a=[]
while 1:
        i+=1
        n =(int)(raw_input("Indiquez a("+str(i)+")"))
        a.append(n)
        if i==r :
                break
z=0

a=FCSR(N,q,a,z)
print a
```

Et voici un exemple d'implémentation d'un test d'autocorrelation sur python :

```
#!/usr/bin/python
# coding= utf8

a=(str)(raw_input("Introduisez la séquence"))
q=[]
for i in a:
        q.append(int(i))
l=len(q)
i=1
k=0
print q
while i<l:
        s=0
        j=0
        while j<l:
                n=q[j]+q[(j+i)%l]
                s+=(-1)**(n)
                j+=1
        if abs(s)>=k:
                k=abs(s)
        i+=1
print k
```

En testant le premier algorithme avec $N = 2$, $q = 5^2 = 25$ et $a = [1, 0, 0, 1]$, en faisant un FCSR d'une longueur de 100, on obtient :
$[1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1,$
$0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1]$
Il y a donc clairement une période : $[1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1]$, qui est bien de longueur $20 = \varphi(25)$.

En entrant cette séquence dans le test d'auto-corrélation, il en ressort 11 :
Cette séquence est donc cycliquement distincte, mais ne possède pas une auto-corrélation idéale.

Bibliographie

[1] Laurent Dubreuil. *Amélioration de l'étalement de spectre par l'utilisation de codes correcteurs d'erreurs*. PhD thesis, Université de Limoges, 2005. pp. 39-48.

[2] Anna Devic et Julian Kellerhals. Les nombres p-adiques. Master's thesis, Ecole Polytechnique Fedérale de Lausanne, 2006.

[3] A. Necer F. Arnault, T.P. Berger. Feedback with carry shift registers synthesis with the euclidean algorithm. 2010.

[4] Wen-Feng Qi Hong Xu. Further results on the distinctness of decimations of l-sequences.

[5] Andrew Klapper. A survey of feedback with carry shift registers.

[6] D. Kohel. Registre à décalage à rétroaction linéaire. `http://iml.univ-mrs.fr/~kohel/tch/M2-CryptoSymetrique/CM/LFSR.pdf`.

[7] A.Klapper M.Goresky. Arithmetic crosscorrelations of feedback with carry register sqequences. *IEEE Trans. Inform. Theory*, vol. IT-43, Juillet 1997.

[8] A.Klapper M.Goresky. Feedback shift registers ; 2-adic span, and combiners with memory. *J. Cryptology*, vol. 10, 1997.

[9] A.Klapper M.Goresky. On the distinctness of decimations of l-sequences, sequences and their applications. 2001.

[10] Arne Winterhof Richard Hofer, László Mérai. Measures of pseudorandomness : Arithmetic autocorrelation and correlation measure. Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences.

[11] Wikiversity. Corps locaux : Introduction, nombres p-adiques. `https://fr.wikiversity.org/wiki/Corps_locaux/Introduction,_nombres_p-adiques`.