Corps finis

ABOU YASSIN Jad

13 juin 2019

Table des matières

1 Résultats fondamentaux sur les corps finis **2**
1.1 Existence et unicité d'un corps fini de cardinal puissance d'un nombre premier . . . 2
1.2 Extensions des corps finis . . . 4
1.3 Clôture algébrique d'un corps fini . . . 4
1.3.1 Corps de rupture . . . 4
1.3.2 Limite inductive . . . 5
1.4 Groupe multiplicatif d'un corps fini . . . 6
1.4.1 Cyclicité du groupe multiplicatif d'un corps fini . . . 6
1.4.2 Forme trace d'une extension de corps . . . 7
1.4.3 L'ordre maximal d'un élément de $GL_n(\mathbb{F}_q)$ est $q^n - 1$. 8
1.5 L'anneau $\mathbb{F}_q[X]$ . . . 8
1.5.1 Décomposition des polynômes irréductibles . . . 8
1.5.2 Polynômes primitifs . . . 8

2 Suites récurrentes linéaires homogènes à coefficient dans $\mathbb{F}_q$ **9**
2.1 Définition . . . 9
2.1.1 Suites ultimement périodiques . . . 9
2.1.2 Suites récurrentes linéaires . . . 9
2.2 Construction de suites récurrentes linéaires homogènes périodiques à coefficients dans $\mathbb{F}_q$ de période maximale . . . 10
2.2.1 Ultime périodicité des éléments de E_a . . . 10
2.2.2 Représentation matricielle des éléments de E_a . . . 10
2.2.3 Constructions d'éléments de E_a de prériode $2^r - 1$ . . 11

3 Simulation du hasard : comportement pseudo-aléatoire **13**
3.1 Qu'est-ce qu'une suite pseudo-aléatoire ? . . . 13
3.2 Test des fréquences . . . 13
3.3 Test des blocs . . . 14
3.4 Test de la corrélation . . . 15

4 Implémentation informatique **16**
4.1 Vocabulaire et représentation 17
4.2 Codage du LFSR en Python 17
4.3 Codage des fonctions de test 19
4.3.1 Test des fréquences 19
4.3.2 Test des blocs 19
4.3.3 Test de la corrélation 20
4.4 Applications 21
4.4.1 Générateur d'entiers aléatoires 22
4.4.2 Cryptage et décryptage d'un message 23

5 Conclusion **24**

Résumé

Les corps finis possèdent un grand nombre d'applications pratiques. Ils sont utilisés par exemple pour générer des nombres pseudo-aléatoires informatiquement. Pourtant des objets de nature déterministe, grâce aux suites récurrentes linéaires, on peut obtenir des résultats de nature probabiliste.

Les suites récurrentes linéaires homogènes à coefficients dans un corps fini sont une manière de générer des suites présentant des propriétés de nature probabiliste. Mais leur construction est entièrement déterministe. On a ainsi un transport du caractère déterministe de la construction vers le caractère probabiliste des résultats.

1 Résultats fondamentaux sur les corps finis

1.1 Existence et unicité d'un corps fini de cardinal puissance d'un nombre premier

On sait que, si p est un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps fini de cardinal p. On le note $\mathbb{F}_p$.

Soit $\mathbb{K}$ un corps fini. Sa caractéristique est donc un nombre premier p, car sinon son sous-corps premier serait isomorphe à $\mathbb{Q}$. Ainsi, sous sous-corps premier est isomorphe à $\mathbb{F}_p$. Ainsi, l'extension $\mathbb{K}/\mathbb{F}_p$ est finie. Si on note $n = [\mathbb{K} : \mathbb{F}_p]$ son degré, on obtient alors que $\mathbb{K}$ est isomorphe en tant que $\mathbb{F}_p$-espace vectoriel à $(\mathbb{F}_p)^n$.

Ainsi, $\mathbb{K}$ est de cardinal p^n et son groupe multiplicatif $(\mathbb{K}^*, \times)$ est d'ordre $p^n - 1$. On a donc

$$\forall x \in \mathbb{K}, \quad x^{p^n-1} = 1$$

De ce fait, tout élément de $\mathbb{K}$ est racine du polynôme $X^{p^n} - X$, qui est de degré le cardinal de $\mathbb{K}$. On a donc :

$$X^{p^n} - X = \prod_{x \in \mathbb{K}} (X - x)$$

On obtient en particulier que $\mathbb{K}$ est un corps de décomposition du polynôme $X^{p^n} - X$ sur $\mathbb{F}_p$.

Définition 1. *Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ non nul. Soit $\mathbb{L}$ une extension de $\mathbb{K}$ vérifiant :*

- *P est scindé sur $\mathbb{L}$*
- *Tout sur-corps de $\mathbb{K}$ contenant les racines de P est un sur-corps de $\mathbb{L}$. Ceci équivaut à dire que les racines de P engendrent $\mathbb{L}$ sur $\mathbb{K}$.*

On dit alors que $\mathbb{L}$ est un corps de décomposition de P sur K.

Réciproquement, soit $\mathbb{K}$ un corps de décomposition de $P = X^{p^n} - X$ sur $\mathbb{F}_p$. Le polynôme dérivée de P est -1 qui est constant non nul, donc P n'a aucune racine multiple (car si $Q^2 \mid P$, alors $Q \mid P'$). Ainsi, l'ensemble $\mathcal{R}$ des racines de P est de cardinal p^n. On a de plus

$$\forall (x, y) \in \mathbb{K}, \quad (x+y)^p = x^p + y^p$$

car p divise $\binom{p}{k}$ si $1 \leq k \leq p-1$. Plus précisément, ceci permet de montrer que l'application suivante

$$\begin{array}{rccc} \sigma : & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & x & \longmapsto & x^p \end{array}$$

est un automorphisme de corps (σ est bijectif car, par intégrité de $\mathbb{K}$, le seul élément qui élevé à la puissance p est nul est 0). On l'appelle l'automorphisme de Frobenius. En l'itérant n fois et en se restreignant aux éléments de $\mathcal{R}$, on obtient

$$\forall (x, y) \in \mathcal{R}, \quad (x+y)^{p^n} = x^{p^n} + y^{p^n}$$

En particulier, cela montre que $\mathcal{R}$ est un sous-corps de $\mathbb{K}$. Par minimalité du corps de décomposition, on obtient que $\mathbb{K} = \mathcal{R}$

On obtient ainsi que les corps finis de cardinal p^n sont les corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$.

Proposition 1. *Tous les corps de décomposition de P sur $\mathbb{F}_p$ sont isomorphes.*

Preuve 1. *Soit $\mathbb{L}$ un autre corps de décomposition de P sur $\mathbb{F}_p$. $\mathbb{K}$ étant un corps de décomposition, $\mathbb{L}$ est un sur-corps de $\mathbb{K}$. On a donc un morphisme de corps injectif φ de $\mathbb{K}$ dans $\mathbb{L}$. Les racines de P dans $\mathbb{L}$ sont dans l'image de φ car ce sont les images des racines de P dans $\mathbb{K}$. Or, l'image de $\mathbb{K}$ par φ est un corps. La minimalité de $\mathbb{L}$ en tant que corps de décomposition donne que l'image de φ est $\mathbb{L}$. Donc φ est un isomorphisme.*

Corollaire 1. *Si p est un nombre premier et $n \in \mathbb{N}^*$, alors deux corps de cardinal p^n sont isomorphes*

Corollaire 2. *Soit Ω un sur-corps algébriquement clos de $\mathbb{F}_p$. Alors Ω contient un unique sous-corps de cardinal p^n, qui est l'ensemble des racines dans Ω du polynôme $X^{p^n} - X$*

Ainsi, s'il n'y a pas d'ambiguïté, on notera $\mathbb{F}_{p^n}$ « le » corps fini de cardinal p^n.

1.2 Extensions des corps finis

Théorème 1. *Soit $\mathbb{K}$ un corps fini de cardinal p^n. Alors les sous-corps de $\mathbb{K}$ sont exactement les*

$$\mathbb{K}' = \left\{x \in \mathbb{K},\ x^{p^d} = x\right\}$$

où $d \in \mathbb{N}$ divise n, et un tel corps est de cardinal p^d

Preuve 2. *Soit $\mathbb{K}'$ un sous-corps de $\mathbb{K}$. On note $\mathbb{F}_p$ le sous-corps premier de $\mathbb{K}$ (on sait que les corps $\mathbb{F}_{p^n}$ sont uniques à isomorphisme près). On a alors, si $d = [\mathbb{K}' : \mathbb{F}_p]$ et $q = [\mathbb{K} : \mathbb{K}']$, $dq = n$. Ainsi, d divise n.*

On obtient de la même manière que lors de la construction des corps finis $\mathbb{F}_{p^n}$ que $\mathbb{K}'$ est de cardinal p^d et que les éléments de $\mathbb{K}'$ sont exactement les racines du polynôme $X^{p^d} - X$.

Réciproquement, si d est un diviseur de n, la construction des corps finis $\mathbb{F}_{p^n}$ dit que $\mathbb{K}'$ ainsi défini est un sous-corps de $\mathbb{K}$. Montrons que $|\mathbb{K}'| = p^d$.

d divise n, donc $p^d - 1$ divise $p^n - 1$, car on a q tel que

$$p^n - 1 = p^{dq} - 1 = (p^d - 1)(p^{d(q-1)} + \cdots + 1)$$

On obtient ainsi que $X^{p^d-1} - 1$ divise $X^{p^n-1} - 1$ et donc que $X^{p^d} - X$ divise $X^{p^n} - X$. Or, $X^{p^n} - X$ est scindé à racines simples sur $\mathbb{K}$, donc $X^{p^d} - X$ l'est aussi. Ainsi, l'ensemble de ses racines dans $\mathbb{K}$ est de cardinal p^d d'où le résultat.

1.3 Clôture algébrique d'un corps fini

1.3.1 Corps de rupture

Définition 2. *Un corps de rupture d'un polynôme P irréductible sur $\mathbb{K}$ est une extension simple de $\mathbb{K}$ par une racine de P.*

Autrement dit, $\mathbb{K}'$ est un corps de rupture de P sur $\mathbb{K}$ s'il existe $\mathbb{L}$ un sur-corps de $\mathbb{K}$ contenant une racine α de P tel que $\mathbb{K}' = \mathbb{K}(\alpha)$.

Proposition 2. *Si P est un polynôme irréductible de $\mathbb{K}[X]$ de degré d, alors l'anneau quotient $\mathbb{K}[X]/(P)$ est un corps de rupture de P sur $\mathbb{K}$ et*

$$[\mathbb{K}[X]/(P) : \mathbb{K}] = d$$

Preuve 3. *L'anneau quotient $\mathbb{K}[X]/(P)$ est celui de $\mathbb{K}[X]$ par l'idéal engendré par P, (P), qui est principal car $\mathbb{K}$ est un corps.*

Soit A un élément de $\mathbb{K}[X]$ dont sa classe dans l'anneau quotient est non nulle. On a donc $A \notin P\mathbb{K}[X]$. Ainsi, on a :

$$A\mathbb{K}[X] + P\mathbb{K}[X] = \mathbb{K}[X]$$

car $A\mathbb{K}[X] + P\mathbb{K}[X] = B\mathbb{K}[X]$ puisque $\mathbb{K}[X]$ est principal et comme P est irréductible et que $B \mid P$, alors B est un inversible de $\mathbb{K}[X]$, donc $B\mathbb{K}[X] = \mathbb{K}[X]$

On dispose donc de $U, V \in \mathbb{K}[X]$ tels que $AU + PV = 1_{\mathbb{K}[X]}$. En passant aux classes dans $\mathbb{K}[X]/(P)$, on obtient que

$$\overline{A}\ \overline{U} = 1_{\mathbb{K}[X]/(P)}$$

Donc $\overline{A}$ est inversible dans $\mathbb{K}[X]/(P)$, donc $\mathbb{K}[X]/(P)$ est un corps.

$\mathbb{K}[X]/(P)$ est un sur-corps de $\mathbb{K}$, car les éléments de $\mathbb{K}$ sont les classes des polynômes constants de $\mathbb{K}[X]$, et il contient une racine de P. En effet, soit α la classe de X dans $\mathbb{K}[X]/(P)$, on a

$$P(\alpha) = P(\overline{X}) = \overline{P(X)} = \overline{0}$$

On a de plus $\mathbb{K}[X]/(P) = \mathbb{K}(\alpha)$ et $(1, \alpha, \alpha^2, \ldots, \alpha^{d-1})$ est une base de $\mathbb{K}(\alpha)$. Donc $\mathbb{K}[X]/(P)$ est un corps de rupture de P sur $\mathbb{K}$ de degré d.

1.3.2 Limite inductive

Proposition 3. *Soit $n \in \mathbb{N}$. Alors*

$$\mathbb{F}_{p^{n!}} \subset \mathbb{F}_{p^{(n+1)!}}$$

Preuve 4. *Le résultat est immédiat car $n!$ divise $(n+1)!$ donc $\mathbb{F}_{p^{(n+1)!}}$ contient un (unique) sous-corps isomorphe à $\mathbb{F}_{p^{n!}}$*

On définit Ω comme étant l'union croissante suivante :

$$\Omega = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}$$

Remarque. Ω ainsi défini est appelé limite inductive de la suite de plongements

$$\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^2} \hookrightarrow \mathbb{F}_{p^6} \hookrightarrow \ldots \hookrightarrow \mathbb{F}_{p^{n!}} \hookrightarrow \ldots$$

Proposition 4. *Ω est une clôture algébrique de $\mathbb{F}_p$*

Preuve 5. *Comme Ω est une réunion croissante d'extensions algébriques de $\mathbb{F}_p$, alors Ω est une extension algébrique de $\mathbb{F}_p$. Montrons que Ω est algébriquement clos. Soit $P \in \Omega[X]$ irréductible de degré d. On sait que $\mathbb{F}_{p^{n!}}[X]/(P)$ est un corps de rupture de P sur $\mathbb{F}_{p^{n!}}$ de degré d. On a donc $\mathbb{F}_{p^{n!}}[X]/(P)$ isomorphe à $\mathbb{F}_{p^{n!d}}$ par unicité à isomorphisme près des corps finis.*

Soit $m \in \mathbb{N}$ tel que $n!d \mid m$. On a donc

$$\mathbb{F}_{p^{n!}}[X]/(P) \hookrightarrow \mathbb{F}_{p^{m!}}$$

Comme P a une racine dans $\mathbb{F}_{p^{n!}}[X]/(P)$, il en a une dans $\mathbb{F}_{p^{m!}}$, et donc une dans Ω. D'où Ω est algébriquement clos.

Dans toute la suite, on note $\overline{\mathbb{F}_p} = \Omega$, q une puissance de p. On a donc $\mathbb{F}_q$ l'unique sous-corps de cardinal q de $\overline{\mathbb{F}_p}$, qui est

$$\mathbb{F}_q = \left\{ x \in \overline{\mathbb{F}_p},\ x^q = x \right\}$$

1.4 Groupe multiplicatif d'un corps fini

1.4.1 Cyclicité du groupe multiplicatif d'un corps fini

Théorème 2. *Soit $\mathbb{K}$ un corps fini, alors son groupe multiplicatif $(\mathbb{K}^*, \times)$ est cyclique.*

Si p est premier et $n \in \mathbb{N}^*$, on a

$$(\mathbb{F}_{p^n}^*, \times) \simeq (\mathbb{Z}/(p^n - 1)\mathbb{Z}, +)$$

En particulier, $(\mathbb{F}_{p^n}^*, \times)$ possède $\varphi(p^n - 1)$ générateurs.

Preuve 6. *Soit e l'exposant de $(\mathbb{K}^*, \times)$. On va d'abord montrer qu'il existe un élément x de $(\mathbb{K}^*, \times)$ qui est d'ordre e. Soit x dans $(\mathbb{K}^*, \times)$ d'ordre maximal qu'on note a, et y dans $(\mathbb{K}^*, \times)$ d'ordre b. Si p est premier, on écrit*

$$\begin{cases} a &= p^\alpha r & \alpha \in \mathbb{N},\ r \in \mathbb{N}^*,\ p \nmid r \\ b &= p^\beta s & \beta \in \mathbb{N},\ s \in \mathbb{N}^*,\ p \nmid s \end{cases}$$

On a donc x^{p^α} d'ordre r et y^s d'ordre p^β. Comme $r \wedge p^\beta = 1$, leur produit est d'ordre $p^\beta r$. Mais $a = p^\alpha r$ est maximal, donc $\beta \leq \alpha$.

En faisant de même pour tout p premier, on obtient que l'ordre de tout élément de $(\mathbb{K}^*, \times)$ divise l'ordre de x. Donc x est d'ordre e.

Ainsi, les éléments de $(\mathbb{K}^*, \times)$ annulent le polynôme $X^e - 1$. Si n est le cardinal de $(\mathbb{K}^*, \times)$, on a donc $e \geq n$. Mais e est l'ordre d'un élément de $(\mathbb{K}^*, \times)$ donc $e \leq n$. Finalement, $e = n$ et $(\mathbb{K}^*, \times)$ est cyclique.

1.4.2 Forme trace d'une extension de corps

Ce qui précède permet de définir la forme trace d'une extension finie de corps et d'en exhiber quelques propriétés.

Définition 3. *Soit $\mathbb{K}$ un corps et $\mathbb{L}/\mathbb{K}$ une extension finie de degré n. Si α est un élément de $\mathbb{L}$, on définit la trace de $\mathbb{L}$ sur $\mathbb{K}$ de α comme étant la trace de l'application linéaire :*

$$\begin{array}{rccc} \varphi_\alpha : & \mathbb{L} & \longrightarrow & \mathbb{L} \\ & x & \longmapsto & \alpha x \end{array}$$

Car $\mathbb{L}$ a une structure de $\mathbb{K}$-espace vectoriel de dimension n. On la note $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$.

Définition 4. *Si $\mathbb{K}$ est un corps et $\mathbb{L}/\mathbb{K}$ une extension finie, on définie la forme trace de $\mathbb{L}$ sur $\mathbb{K}$ comme étant l'application :*

$$\begin{array}{rccc} Tr : & \mathbb{L}\times\mathbb{L} & \longrightarrow & \mathbb{K} \\ & (x,y) & \longmapsto & Tr_{\mathbb{L}/\mathbb{K}}(xy) \end{array}$$

Proposition 5. *La forme trace de $\mathbb{F}_{q^r}/\mathbb{F}_q$ n'est pas dégénérée, c'est-à-dire que*

$$\begin{cases} \forall x \in \mathbb{F}_{q^r}^*,\ \exists y \in \mathbb{F}_{q^r}, & Tr(x,y) \neq 0 \\ \forall y \in \mathbb{F}_{q^r}^*,\ \exists x \in \mathbb{F}_{q^r}, & Tr(x,y) \neq 0 \end{cases}$$

Preuve 7. *On sait que le groupe $(\mathbb{F}_{q^n}^*, \times)$ est cyclique. Soit x un générateur de ce groupe. L'application*

$$\begin{array}{rccc} \varphi_x : & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_{q^n} \\ & y & \longmapsto & xy \end{array}$$

est un endomorphisme du $\mathbb{F}_q$-espace vectoriel de dimension n $\mathbb{F}_{q^n}$. Sa matrice dans la base $e = (1_{\mathbb{F}_{q^n}}, x, x^2, \ldots, x^{n-1})$ est une matrice compagnon, que l'on note C, qui est celle du polynôme minimal de x dans $\mathbb{F}_q$ qu'on note $\Pi_{\mathbb{F}_q,x}$. Comme C est une matrice compagnon, $\Pi_{\mathbb{F}_q,x}$ est aussi son polynôme caractéristique, et donc la trace de cet endomorphisme est l'opposé du coefficient en X^{n-1} de $\Pi_{\mathbb{F}_q,x}$, c'est donc la somme des racines $(x_1, \ldots, x_n)$ de $\Pi_{\mathbb{F}_q,x}$ (Nous montrerons plus tard pourquoi ces racines sont distinctes).

Or, $(\varphi_x)^k = \varphi_{x^k}$, dont sa matrice dans la base e est C^k. Son polynôme caractéristique est donc de trace $\sum_{i=1}^n x_i^k$.

Or, $det(V(x_1, \ldots, x_n)) \neq 0$ car les x_i pour $1 \leq i \leq n$ sont deux à deux distincts. Ainsi, il y a au moins un k dans $[\![0, n-1]\!]$ tel que $\sum_{i=1}^n x_i^k \neq 0$ (sinon, on pourrait former une colonne nulle).

Ainsi, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x^k) \neq 0$, donc la forme linéaire $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ est non identiquement nulle. Si x_0 est tel que $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x_0) \neq 0$, alors pour tout y dans $\mathbb{F}_{q^n}^*$, on a :

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x_0) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x_0 y^{-1} y) = Tr(x_0 y^{-1}, y) \neq 0$$

Donc la forme trace n'est pas dégénérée.

1.4.3 L'ordre maximal d'un élément de $GL_n(\mathbb{F}_q)$ est $q^n - 1$

Montrons d'abord que $q^n - 1$ est supérieur à tous les ordres d'éléments de $GL_n(\mathbb{F}_q)$. Soit C dans $GL_n(\mathbb{F}_q)$. On sait que la dimension de la $\mathbb{F}_q$-algèbre $\mathbb{F}_q[C]$ a pour dimension le degré du polynôme minimal de C qui est de degré inférieur à n. Son cardinal est donc majoré par q^n, donc celui de son groupe multiplicatif est majoré par $q^n - 1$. Ainsi, l'ordre de C est inférieur à $q^n - 1$.

Soit C la matrice compagnon exhibée dans la preuve de la non-dégénérescence de la forme trace de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Alors C est d'ordre $q^n - 1$ dans $GL_n(\mathbb{F}_q)$. En effet, si c'était faux, on aurait $0 < k < q^n - 1$ tel que $C^k = I_n$. Or, $x^k = 1_{\mathbb{F}_{q^n}} C^k = 1_{\mathbb{F}_{q^n}}$, ce qui est absurde car x est d'ordre $2^r - 1$.

1.5 L'anneau $\mathbb{F}_q[X]$

1.5.1 Décomposition des polynômes irréductibles

Proposition 6. *Soit P un polynôme unitaire irréductible de $\mathbb{F}_q[X]$. Si x est une racine de P dans $\overline{\mathbb{F}_p}$, on a alors*

$$\mathbb{F}_q(x) = \mathbb{F}_{q^n} \quad et \quad P = \prod_{i=0}^{n-1} (X - x^{q^i})$$

Ainsi, les racines de P dans $\overline{\mathbb{F}_p}$ sont simples. De plus, si $P \neq X$, ces racines sont non nulles et ont toutes le même ordre dans le groupe multiplicatif $(\mathbb{F}_{q^n}^*, \times)$.

Preuve 8. *Tout d'abord, on sait que $\mathbb{F}_{q^n}$ est l'unique sous-corps de $\overline{\mathbb{F}_p}$ de degré n sur $\mathbb{F}_q$. Comme $\mathbb{F}_q(x)$ est un tel corps, c'est donc $\mathbb{F}_{q^n}$.*

Ensuite, on a, si $y \in \overline{\mathbb{F}_p}$, $(P(y))^p = P(y^p)$, puisque comme p est premier, il divise tous les coefficients multinomiaux différents de 1. En itérant ceci r fois (où $q = p^r$) puis k fois, on obtient que $(P(y))^{q^k} = P(y^{q^k})$ si $k \in \mathbb{N}$. Ainsi, les x^{q^i}, pour $0 \leq i \leq n-1$, sont racines de P. (Cela vient en fait du fait que $\sigma(P(X)) = P(\sigma(X))$)

S'il existait $0 \leq i < j \leq n-1$ tels que $x^{q^i} = x^{q^j}$, par injectivité de σ^{q^i}, on aurait $x = x^{q^{j-i}}$, ce qui n'est pas possible puisqu'alors x appartiendrait à $\mathbb{F}_{q^{j-i}}$ ce qui contredit le fait que $\mathbb{F}_q(x) = \mathbb{F}_{q^n}$.

Enfin, comme les q^k pour $0 \leq k \leq n-1$ sont premiers à $q^n - 1$ et donc à l'ordre de x dans $(\mathbb{F}_{q^n}^*, \times)$ (car ce dernier divise $q^n - 1$), alors les x^{q^k} sont tous des générateurs de $< x >$, et donc ont tous le même ordre.

1.5.2 Polynômes primitifs

Définition 5. *Soit $P \in \mathbb{F}_q[X]$ irréductible unitaire de degré $n \geq 0$ et différent de X. Par la proposition précédente, les racines de P dans $\overline{\mathbb{F}_p}$ ont toutes le même ordre dans $\mathbb{F}_{q^n}^*$. Cet ordre est appelé l'ordre de P.*

On dit que P est primitif sur $\mathbb{F}_q$ si P est d'ordre q^n-1, c'est à dire si les racines de P dans $\overline{\mathbb{F}_p}$ engendrent $(\mathbb{F}_{q^n}^*, \times)$.

En particulier, il y a $\dfrac{\varphi(q^n-1)}{n}$ polynômes primitifs de degré n sur $\mathbb{F}_q$.

2 Suites récurrentes linéaires homogènes à coefficient dans $\mathbb{F}_q$

2.1 Définition

2.1.1 Suites ultimement périodiques

Définition 6. *On dit qu'une suite $(x_n)_{n\geq 0}$ d'un ensemble quelconque X est ultimement périodique lorsqu'il existe d dans $\mathbb{N}^*$ et N dans $\mathbb{N}$ tels que :*

$$\forall n \geq N, \quad x_{n+d} = x_n$$

Autrement dit, $(x_n)_{n\geq 0}$ est ultimement périodique s'il existe N dans $\mathbb{N}$ tel que $(x_n)_{n\geq N}$ soit périodique.
d est appelé une période de la suite $(x_n)_n$.

Si $(x_n)_n$ est une telle suite, et si δ est sa plus petite période, alors toutes les périodes de $(x_n)_n$ sont des multiples de δ. On appelle δ la période de $(x_n)_n$.

2.1.2 Suites récurrentes linéaires

Soit $\mathbb{K}$ un corps.

Définition 7. *Soit $r \in \mathbb{N}^*$ et $(u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$. On dit que la suite $(u_n)_n$ est une suite récurrente linéaire homogène d'ordre r s'il existe $(a_0, \ldots, a_{r-1}) \in \mathbb{K}^r$ tel que :*

$$\forall n \in \mathbb{N}, \quad u_{n+r} = \sum_{k=0}^{r-1} a_k u_{n+k}$$

Si $a = (a_0, \ldots, a_{r-1}) \in \mathbb{K}^r$, on pose E_a comme étant l'ensemble des suites $(u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ telles que :

$$\forall n \in \mathbb{N}, \quad u_{n+r} = \sum_{k=0}^{r-1} a_k u_{n+k}$$

On a alors la proposition suivante :

Proposition 7. *E_a est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$ et l'application*

$$\begin{array}{rccc} \varphi : & E_a & \longrightarrow & \mathbb{K}^r \\ & (u_n)_{n\in\mathbb{N}} & \longmapsto & (u_0, \ldots, u_{r-1}) \end{array}$$

est un isomorphisme. En particulier, E_a est de dimension finie r.

2.2 Construction de suites récurrentes linéaires homogènes périodiques à coefficients dans $\mathbb{F}_q$ de période maximale

Dans toute cette partie, on fixe $r \in \mathbb{N}^*$ et $a = (a_0, \ldots, a_{r-1}) \in {\mathbb{F}_q}^r$

2.2.1 Ultime périodicité des éléments de E_a

Lemme 1. *Toute suite de E_a est ultimement périodique de période majorée par $q^r - 1$*

Preuve 9. *Soit $(u_n)_{n\in\mathbb{N}} \in E_a$.*

Si $(u_n)_n$ est nulle à partir d'un certain rang, alors elle ultimement périodique de période 1, inférieur à $q^r - 1$.

Sinon, on a :

$$\forall n \in \mathbb{N}, \quad (u_n, u_{n+1}, \ldots, u_{n+r-1}) \neq (0, 0, \ldots, 0)$$

Ainsi, par le principe des tiroirs, on a $0 \leq i < j \leq q^r - 1$ tels que :

$$(u_i, u_{i+1}, \ldots, u_{i+r-1}) = (u_j, u_{j+1}, \ldots, u_{j+r-1})$$

car il y a $q^r - 1$ r-uplets non nuls et q^r éléments dans $[\![0, q^r - 1]\!]$.
Ainsi, on a pour tout $n \geq i$, $u_{n+j-i} = u_n$.
$(u_n)_n$ est donc ultimement périodique et $j - i$ en est une période.
Or, $j - i \leq q^r - 1$, d'où le résultat.

Nous allons maintenant construire de telles suites de période maximales, c'est-à-dire de période $q^r - 1$.

2.2.2 Représentation matricielle des éléments de E_a

Par l'isomorphisme φ, on associe de manière unique à $(u_n)_{n\in\mathbb{N}} \in E_a$ le vecteur ligne :

$$U_0 = (u_0, u_1, \ldots, u_{r-1})$$

Si $n \in \mathbb{N}$, on pose :

$$U_n = (u_n, u_{n+1}, \ldots, u_{n+r-1})$$

On pose également $P = X^r - \sum_{i=0}^{r-1} a_i X^i$ et C sa matrice compagnon :

$$C = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & 0 & a_{r-2} \\ 0 & 0 & \ldots & 1 & a_{r-1} \end{pmatrix}$$

On obtient alors par un calcul immédiat que :

$$\forall n \in \mathbb{N}, \quad U_{n+1} = U_n C$$

Donc

$$\forall n \in \mathbb{N}, \quad U_n = U_0 C^n$$

On obtient aussi que :

$$(U_n)_{n\geq 0} \text{ est d-périodique } \Leftrightarrow (u_n)_{n\geq 0} \text{ est d-périodique}$$

2.2.3 Constructions d'éléments de E_a de prériode $2^r - 1$

Lemme 2. *Si $a_0 \neq 0$, alors toute suite de E_a est périodique de période divisant l'ordre de C dans $GL_r(\mathbb{F}_q)$.*

Preuve 10. *Comme a_0 est non nul, C est inversible, car $det(C) = (-1)^{r+1}a_0$. Or, $GL_r(\mathbb{F}_q)$ est un groupe fini, on pose alors e l'ordre de C dans $GL_r(\mathbb{F}_q)$. On a :*

$$\forall n \in \mathbb{N}, \quad C^{n+e} = C^n$$

Ainsi, si $(u_n)_{n\in\mathbb{N}} \in E_a$, e est une période de la suite $(U_n)_{n\in\mathbb{N}}$. Donc la période de $(U_n)_{n\in\mathbb{N}}$ divise e.

Montrons que ${\mathbb{F}_q}^r = (0, 0, \ldots, 0, 1)\mathbb{F}_q[C]$:
Si $k \in [\![0, r-1]\!]$ et $(e_1, \ldots, e_r)$ est la base canonique de ${\mathbb{F}_q}^r$, alors on obtient par une récurrence finie immédiate :

$$(0, ..., 0, 1)C^k = e_{r-k} + L, \quad L \in Vect\{e_{r-k+1}, \ldots, e_r\}$$

Ainsi, $(e_r C^k)_{0\leq k\leq r-1}$ est une base de ${\mathbb{F}_q}^r$.
Donc ${\mathbb{F}_q}^r = (0, 0, \ldots, 0, 1)\mathbb{F}_q[C]$.

En particulier, l'endomorphisme

$$\begin{array}{ccc} {\mathbb{F}_q}^r & \longrightarrow & {\mathbb{F}_q}^r \\ L & \longmapsto & LC \end{array}$$

est cyclique.

Définition 8. *On dit que le vecteur $L \in {\mathbb{F}_q}^r$ est C-cyclique si*

$${\mathbb{F}_q}^r = L\mathbb{F}_q[C]$$

C'est-à-dire lorsque $(LC^k)_{0\leq k\leq r-1}$ est une base de ${\mathbb{F}_q}^r$

Proposition 8. *Si P est irréductible, alors tout vecteur non nul L de ${\mathbb{F}_q}^r$ est C-cyclique.*

Preuve 11. *Soit π_C le polynôme minimal de C. Comme C est une matrice compagnon, on a $\pi_C = P$.*
On sait que $\mathbb{F}_q[C]$ est un anneau commutatif, montrons que c'est un corps. Soit $A \in \mathbb{F}_q[C]$. On a $Q \in \mathbb{F}_q[X]$ de degré inférieur à $r-1$ tel que $A = Q(C)$. On a les équivalences suivantes :

$$\begin{aligned} A \text{ est inversible} &\Leftrightarrow \exists B \in \mathbb{F}_q[C], \quad AB = I_r \\ &\Leftrightarrow \exists R \in (\mathbb{F}_q)_{r-1}[X], \quad Q(C)R(C) = I_r \\ &\Leftrightarrow \exists R \in (\mathbb{F}_q)_{r-1}[X], \quad \pi_C \mid (QR - 1) \\ &\Leftrightarrow \exists R, S \in (\mathbb{F}_q)_{r-1}[X], \quad \pi_C S = QR - 1 \\ &\Leftrightarrow \pi_C \wedge Q = 1 \end{aligned}$$

La dernière équivalence provient de l'identité de Bézout.
Comme $P = \pi_C$ est irréductible sur $\mathbb{F}_q$, alors tout élément non nul de $\mathbb{F}_q[C]$ est inversible.
Donc $\mathbb{F}_q[C]$ est un corps.

Soit $L \in (\mathbb{F}_q)^r \backslash \{0\}$. On dispose de $L_0 \in (\mathbb{F}_q)^r$ C-cyclique. On a donc $A \in \mathbb{F}_q[C]$ tel que $L = L_0 A$ donc $L_0 = LA^{-1}$.
Donc $L\mathbb{F}_q[C] = (LA^{-1})(A\mathbb{F}_q[C]) = L_0\mathbb{F}_q[C] = (\mathbb{F}_q)^r$. Ainsi, tout vecteur non nul de $(\mathbb{F}_q)^r$ est C-cyclique.

Les propositions suivantes établissent l'existence de suites récurrentes linéaires homogènes d'ordre r périodiques de période $q^r - 1$.

Proposition 9. *Soit $(u_n)_{n\in\mathbb{N}} \in E_a$ et $U_0 = (u_0, \ldots, u_{r-1})$. Si U_0 est un vecteur C-cyclique, alors la période de $(u_n)_n$ est l'ordre de C dans $GL_r(\mathbb{F}_q)$.*

Preuve 12. *Soit e l'ordre de C dans $GL_r(\mathbb{F}_q)$ et $(u_n)_{n\in\mathbb{N}} \in E_a$ non identiquement nulle. Soit d la période de $(u_n)_n$. On sait que $d \mid e$. On a donc*

$$\begin{aligned} U_d = U_0 &\Leftrightarrow U_0 C^d = U_0 \\ &\Leftrightarrow U_0(C^d - I_r) = 0 \\ &\Leftrightarrow C^d = I_r \\ &\Leftrightarrow e \mid d \end{aligned}$$

En effet, $C^d - I_r \in \mathbb{F}_q[C]$ qui est un corps et $U_0 \neq 0$.
Ainsi, on a $e = d$ et donc $(u_n)_n$ est e-périodique.

On a vu dans la première partie que l'ordre maximal d'un élément de $GL_r(\mathbb{F}_q)$ est $q^r - 1$ et que c'est atteint pour une certaine matrice compagnon. De ceci et de ce qui précède, on en déduit que :

Corollaire 3. *Si C est d'ordre $q^r - 1$ dans $GL_r(\mathbb{F}_q)$ et $U_0 \neq 0$, alors la suite $(u_n)_{n\in\mathbb{N}}$ est périodique de période $q^r - 1$*

Si P est un polynôme primitif, alors ses racines sont génératrices de $(\mathbb{F}_{q^r}, \times)$. La construction des matrices d'ordre maximal dans $GL_r(\mathbb{F}_q)$ donne que la matrice compagnon de P est d'ordre $q^r - 1$. On obtient ainsi le résultat suivant :

Proposition 10. *Si P est un polynôme primitif sur $\mathbb{F}_q$ et $U_0 \neq 0$, alors $(u_n)_{n\in\mathbb{N}}$ est périodique de période $q^r - 1$*

On obtient ainsi une construction de suites récurrentes linéaires homogènes à coefficients dans $\mathbb{F}_q$ de période maximale grâce à la connaissance d'un polynôme primitif sur $\mathbb{F}_q$, la période de cette suite étant $q^{\deg(P)} - 1$.

3 Simulation du hasard : comportement pseudo-aléatoire

Dans toute cette partie, on fixe $r \in \mathbb{N}^*$, $q = 2$ et $a = (a_0, \ldots, a_{r-1}) \in (\mathbb{F}_2)^r$ tel que, si $P = X^r - \sum_{k=0}^{r-1} a_k X^k$, alors P est un polynôme primitif sur $\mathbb{F}_2$. Ce qui précède montre alors que toute suite non identiquement nulle de E_a est $2^r - 1$-périodique.

3.1 Qu'est-ce qu'une suite pseudo-aléatoire ?

Du fait de leur construction, les éléments de E_a ne sont pas aléatoires, car entièrement déterminés par leurs r premiers termes.

Une suite pseudo-aléatoire possède un comportement difficilement prévisible si on ne connait pas la graine, qui est la condition initiale. En particulier, connaître u_n ne permet pas facilement de prédire ce que sera u_{n+1}.

En plus de cela, une suite pseudo-aléatoire sera ici uniforme, c'est-à-dire que chaque terme apparaît dans la suite avec la même « probabilité », c'est-à-dire avec la même fréquence. Si c'est le cas, on dit que la suite passe le test des fréquences.
Plus généralement, chaque k-uplet devrait avoir également la même probabilité d'apparaître : il s'agit du test des blocs.

Finalement, il est souhaitable que ces suites soient le moins corrélées que possible à leurs translatées. Autrement dit, le ième terme de la suite $(u_n)_{n\in\mathbb{N}}$ ne doit donner aucune information sur ce que le ième terme de la suite $(u_{n+j})_{n\in\mathbb{N}}$ peut être.

3.2 Test des fréquences

La suite $(U_n)_{n\in\mathbb{N}}$ étant périodique de période $2^r - 1$, les U_i pour $0 \leq i \leq 2^r - 2$ sont deux à deux distincts et différents de zéro. Or, il existe exactement $2^r - 1$ élément dans ${\mathbb{F}_2}^r \backslash \{0\}$. Ainsi, pour tout vecteur $e = (e_0, \ldots, e_{r-1}) \in {\mathbb{F}_2}^r$ non nul, il existe un unique n dans $[\![0, 2^r - 2]\!]$ tel que :

$$(u_n, \ldots, u_{n+r-1}) = e$$

Cela montre alors que $(u_n)_{n\in\mathbb{N}}$ passe le test des fréquences :

Proposition 11. *L'ensemble des incides n de $[\![0, 2^r - 2]\!]$ tel que $u_n = 1$ (respectivement $u_n = 0$) est de cardinal 2^{r-1} (respectivement $2^{r-1} - 1$)*

La démonstration sera faite pour le test des blocs, il s'agit du cas d'un bloc de taille 1.

Le test des fréquences est le test le plus simple et le plus intuitif : on veut que chaque terme ait la même (ou presque car $2^r - 1$ est impair) probabilité d'apparaître dans la suite. Cependant, la suite suivante passe le test des fréquences, il faut donc d'autres tests plus avancés.

$$111111110000000111111110000000111111110000000\ldots$$

3.3 Test des blocs

Plus généralement, on a le résultat suivant :

Proposition 12. *Soit $s \in [\![1, r]\!]$ et $e = (e_0, \ldots, e_{s-1})$. Alors le nombre d'indices $n \in [\![0, 2^r - s - 1]\!]$ tels que*

$$(u_n, \ldots, u_{n+s-1}) = e$$

est

$$\begin{cases} 2^{r-s} & \text{si } e \neq 0 \\ 2^{r-s} - 1 & \text{si } e = 0 \end{cases}$$

Preuve 13. *Il y a dans ${\mathbb{F}_2}^r$ exactement 2^{r-s} vecteurs $x = (x_0, \ldots, x_{r-1})$ tels que*

$$(x_0, \ldots, x_{s-1}) = e$$

En effet, ce sont exactement les éléments de

$$\{(e_0, \ldots, e_{s-1}, x_s, \ldots, x_{r-1}), \quad (x_s, \ldots, x_{r-1}) \in {\mathbb{F}_2}^{r-s}\}$$

Si de plus e est nul, on retire le vecteur nul de l'ensemble précédent, ce qui donne un ensemble à $2^{r-s} - 1$ éléments.

Comme chaque vecteur non nul de ${\mathbb{F}_2}^r$ apparait une et une seule fois dans $(U_n)_{0 \leq n \leq 2^r - 2}$, on a le résultat.

Ce test renforce le test des fréquences car alors la suite

$$111111110000000111111110000000111111110000000\ldots$$

ne verifie pas ce test. En effet, le bloc 101 n'apparaît jamais alors que 000 apparaît 5 fois dans une période.

3.4 Test de la corrélation

Comme chaque vecteur non nul de ${\mathbb{F}_2}^r$ apparait une unique fois dans chaque période de $(U_n)_n$, le choix du vecteur U_0 ne fait que décaler la suite. Or, il est souhaitable que, si U_0 et U'_0 sont dans ${\mathbb{F}_2}^r$ non nuls, alors le ième terme de la suite $u = (u_0, u_1, \dots)$ ne permet pas de savoir quel sera le ième terme de la suite $u' = (u'_0, u'_1 \dots)$.

Définition 9. *Soient $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ deux suites d-périodiques quelconques.*

On définit la corrélation du couple $((x_n)_n, (y_n)_n)$ comme étant l'entier

$$c = |\{i \in [\![0, d-1]\!],\ x_i = y_i\}| - |\{i \in [\![0, d-1]\!],\ x_i \neq y_i\}|$$

On a $c \in [\![-d, d]\!]$ et c a la parité de d.

Nous allons montrer le résultat suivant

Proposition 13. *Soit $1 \leq j \leq 2^r - 2$. Alors la corrélation du couple $((u_n)_{n\in\mathbb{N}}, (u_{n+j})_{n\in\mathbb{N}})$ est de -1*

Remarque : Il n'est pas possible de faire mieux car la corrélation est de la parité de $2^r - 1$ qui est impair.

Pour le prouver, nous allons utiliser un autre point de vue des éléments de E_a.

Proposition 14. *Soit $P \in \mathbb{F}_q[X]$ un polynôme irréductible de degré r et x une racine de P dans $\overline{\mathbb{F}_p}$. On note Tr la forme trace de l'extension $\mathbb{F}_{q^r}/\mathbb{F}_q$. Alors les éléments de E_a sont les suites de la forme*

$$(Tr(x^n, y))_{n\in\mathbb{N}}$$

pour y dans $\mathbb{F}_{q^n}$.

Preuve 14. *Si y est dans $\mathbb{F}_{q^n}$, alors $(Tr(x^n, y))_{n\in\mathbb{N}}$ est dans E_a. En effet, si $n \in \mathbb{N}$, on a $x^{n+r} = \sum_{i=0}^{n-1} a_i x^{n+i}$ (car $P(x) = 0$). On conclut par linéarité à gauche de la forme trace.*

On pose :

$$\begin{array}{rccc} \Phi : & \mathbb{F}_{q^r} & \longrightarrow & E_a \\ & y & \longmapsto & (Tr(x^n, y))_{n\in\mathbb{N}} \end{array}$$

Par linéarité à droite de la forme trace, Φ est $\mathbb{F}_q$-linéaire. On va montrer que Φ est injective pour conclure que Φ est bijective par égalité des dimensions. Ceci provient du fait que la forme trace n'est pas dégénérée, donc seule l'image de $y = 0$ donne la suite nulle.

Grâce à cette nouvelle représentation des éléments de E_a, on démontre le test de la corrélation

Preuve 15. *Soit x une racine de P. On a y dans $\mathbb{F}_{2^r}^*$ tel que*

$$\forall n \in \mathbb{N}, \quad u_n = Tr(x^n, y)$$

La corrélation du couple $(u_n)_{n\geq 0}, (u_{n+j})_{n\geq 0})$ est égale à

$$\begin{aligned}
\sum_{n=0}^{2^r-2} (-1)^{Tr(x^n,y)} (-1)^{Tr(x^{n+j},y)} &= \sum_{n=0}^{2^r-2} (-1)^{Tr(x^n,y)+Tr(x^{n+j},y)} \\
&= \sum_{n=0}^{2^r-2} (-1)^{Tr(x^n+x^{n+j},y)} \\
&= \sum_{n=0}^{2^r-2} (-1)^{Tr(x^n(1+x^j),y)}
\end{aligned}$$

Si $z = (1 + x^j)y$, on a $z \neq 0$ (car x est d'ordre $2^r - 1$ qui est impair donc $1 + x^j \neq 0$). Comme x est un générateur de $\mathbb{F}_{2^r}^*$ comme racine d'un polynôme primitif de degré r sur $\mathbb{F}_2$, on a que :

$$\{zx^n,\ 0 \leq n \leq 2^r - 1\} = \mathbb{F}_{2^r}^*$$

Or, $T = Tr_{\mathbb{F}_{2^r}/\mathbb{F}_2}$ est un morphisme surjectif de $(\mathbb{F}_{2^r}, +)$ vers $\mathbb{F}_2$. On a donc, si y est dans $\mathbb{F}_{2^r}$ de trace 1 :

$$\begin{aligned}
|T^{-1}(1)| &= \sum_{x\in\mathbb{F}_{2^r}} 1_{T(x)=1} \\
&= \sum_{x\in\mathbb{F}_{2^r}} 1_{T(x+y)=1} \\
&= \sum_{x\in\mathbb{F}_{2^r}} 1_{T(x)=0} \\
&= |T^{-1}(0)|
\end{aligned}$$

D'où le résultat.

4 Implémentation informatique

En informatique, il est très utile de disposer de générateurs de nombres aléatoires. En effet, ces derniers sont très utiles dans divers domaines comme la cryptographie, la simulation ou la transmission de données. Cependant, il n'est pas possible d'en générer algorithmiquement (par définition même d'un algorithme qui est déterministe). Il est possible d'utiliser diverses sources externes (le temps, les fluctuations des propriétés de certains composants, etc.) mais ce n'est pas toujours possible et c'est souvent assez lent.

Ainsi, les générateurs de nombres pseudo-aléatoires, c'est-à-dire des suites de nombres étant générées algorithmiquement (par le processeur par exemple) mais qui présentent des comportements semblables à une suite aléatoire, sont très intéressants, car bien que moins fiables qu'un générateur de nombre aléatoire, ils sont beaucoup plus rapides et efficaces.

4.1 Vocabulaire et représentation

Nous avons précédemment construit des suites ayant un tel comportement. En informatique, on les appelle des registres à décalage à rétroaction linéaire (*Linear feedback shift registers* en anglais, ou LFSR). Ils sont représentés par des diagrammes de la forme suivante :

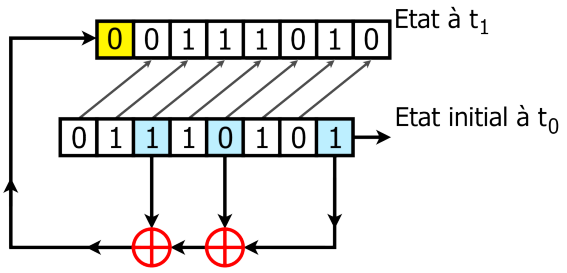


FIGURE 1 – Représentation et fonctionnement d'un LFSR

Ici, un état n représente le r-uplet U_n. Ces derniers peuvent être implémentés informatiquement ou électroniquement de manière très simple, ce qui en font des générateurs pseudo-aléatoires très utilisés.

4.2 Codage du LFSR en Python

Nous allons utiliser le langage Python pour implémenter un LFSR.

Le polynôme P, primitif, sera représenté par une liste de taille r de la manière suivante :

$$X^r - \sum_{k=0}^{r-1} a_k X^k \leftrightarrow [a_0, \ldots, a_{r-1}]$$

Nous allons travailler avec la suite $(U_n)_n$ afin de construire une période de la suite $U = (u_n)_n$.

La fonction qui, à partir d'un polynôme primitif et d'un vecteur de ${\mathbb{F}_2}^r$, renvoie une période de la suite U s'écrit de manière simple comme ci-dessous :

Ici, on travaille dans $\mathbb{Z}$ lors des calculs, puis on réduit modulo 2. Cela est identique à faire les calculs directement dans $\mathbb{F}_2$ car la réduction modulo 2 est un morphisme de groupe.

```python
def lfsr(U_0, C):
    ### Initialisation ###
    U = U_0.copy()
    r = len(U_0)

    ### Itération ###
    while len(U) == r or U[-r:] != U_0:
        u_n = 0
        for i in range(r):
            u_n += C[i] * U[i + len(U) - r]

        u_n = u_n % 2
        U.append(u_n)

    ### Fin de l'algorithme ###
    return U[:-r]
```

FIGURE 2 – Code de la fonction lfsr

Essayons le code : Prenons $P = X^2 + X + 1$ qui est un polynôme primitif de degré deux sur $\mathbb{F}_2$ (d'ailleurs, le seul, car X^2 et $X^2 + 1$ ne le sont pas) et $U_0 = (0, 1)$.

Faisons-le d'abord à la main : on a $u_2 = u_0 \times 1 + u_1 \times 1 = 0 \times 1 + 1 \times 1 = 1$

On a alors :	$U = (0, 1, 1, u_3, \dots)$	et	$U_1 = (1, 1)$
Ensuite :	$u_3 = u_2 \times 1 + u_1 \times 1 = 1 + 1 = 0$		
Donc :	$U = (0, 1, 1, 0, u_4, \dots)$	et	$U_2 = (1, 0)$
Ensuite :	$u_4 = u_3 \times 1 + u_2 \times 1 = 0 + 1 = 1$		
Donc :	$U = (0, 1, 1, 0, 1, u_5, \dots)$	et	$U_3 = (0, 1)$

On a $U_3 = U_0$, on obtient alors une période de U qui est $(0, 1, 1)$

Voici le résultat de l'algorithme :

```
>>> U_0 = [0, 1]
>>> C   = [1, 1]
>>> U   = lfsr(U_0, C)
>>> print(U)
[0, 1, 1]
```

FIGURE 3 – Application du code pour $P = X^2 + X + 1$

On retrouve bien la période que nous avons obtenue. Il est maintenant possible de générer des périodes beaucoup plus grandes avec des polynômes primitifs dans $\mathbb{F}_2$ de degrés de plus en plus élevés. Essayons avec

$$P = X^9 + X^5 + 1$$

qui est primitif [1] sur $\mathbb{F}_2$. D'après la première partie, nous devons avoir une

1. Une liste de plusieurs polynômes primitifs sur $\mathbb{F}_2$ est disponible ici : https ://en.wikipedia.org/wiki/Linear-feedback_shift_register#Some_polynomials_for_maximal_LFSRs

période de taille $2^9 - 1 = 511$. Nous prenons U_0 quelconque.

```
>>> U_0 = [0, 1, 1, 0, 1, 0, 0, 0, 1]
>>> C   = [1, 0, 0, 0, 0, 1, 0, 0, 0]
>>> U   = lfsr(U_0, C)
>>> print(len(U))
511
```

FIGURE 4 – Application du code pour $P = X^9 + X^5 + 1$

4.3 Codage des fonctions de test

Nous allons maintenant implémenter les trois tests explicités dans la partie précédente et les vérifier sur les suites générées.

4.3.1 Test des fréquences

Il s'agit du test le plus simple à implémenter grâce à la fonction *count*. On vérifie simplement s'il y a $2^{r-1} - 1$ zéros et 2^{r-1} uns.

```
def test_freq(U, r):
        return U.count(1) == 2**(r-1) and U.count(0) == 2**(r-1) - 1
```

FIGURE 5 – Code de la fonction du test des fréquences

Essayons-le sur une suite générée par la fonction *lfsr* et sur une autre quelconque.

```
>>> C   = [1, 0, 0, 1]
>>> U_0 = [0, 0, 0, 1]
>>> U   = lfsr(U_0, C)
>>>
>>> V = [ randint(0, 1) for _ in range(15) ]
>>> test_freq(U, 4)
True
>>> test_freq(V, 4)
False
```

FIGURE 6 – Test des fréquences

4.3.2 Test des blocs

Nous allons écrire deux fonctions auxiliaires, la première, *nbBloc* renvoie le nombre d'occurence d'un k-uplet e dans la suite U, en faisant attention de compter ceux qui sont « à cheval » entre deux périodes. La seconde, *plusUn*, permet de passer d'un k-uplet au suivant selon l'ordre lexicographique.

Finalement, la fonction *test_bloc* va vérifier si, pour tout s entre 1 et r et e un s-uplet, il y a exactement 2^{r-s} occurences de e dans U (et une de moins si e est nul)

```
def nbBloc(U, e):
        k = len(e)
        n = 0
        #On orrige le défaut de périodicité en ajoutant le début de U à sa fin
        V = U + U[:k]
        for i in range(len(U)):
                if e == V[i: i+k]:
                        n += 1
        return n

def plusUn(L):
        retenue = True
        i = len(L) - 1
        while retenue and i >= 0:
                retenue = L[i] == 1
                L[i] = 1 - L[i]
                i -= 1
        return not retenue

def test_bloc(U, r):
        for s in range(1, r+1):
                L = [0 for _ in range(s)]
                if nbBloc(U, L) != 2**(r-s)-1 :
                        return False
                while plusUn(L):
                        if nbBloc(U, L) != 2**(r-s) :
                                return False
        return True
```

FIGURE 7 – Code des fonctions *nbBloc*, *plusUn*, *test_bloc*

De même que pour le test des fréquences, essayons le test des blocs sur une suite générée par l'algorithme et une autre quelconque.

```
>>> U_0 = [0, 1, 0, 1, 0, 1, 0]
>>> C   = [1, 0, 0, 0, 0, 0, 1]
>>> U   = lfsr(U_0, C)
>>>
>>> V   = [ randint(0, 1) for _ in range(len(U)) ]
>>>
>>> r = len(C)
>>> test_bloc(U, r)
True
>>> test_bloc(V, r)
False
```

FIGURE 8 – Test des blocs

4.3.3 Test de la corrélation

Ce dernier test est également simple à implémenter. Nous allons d'abord créer une fonction *correlation* qui renvoie la corrélation entre la suite $(u_n)_n$ et la suite $(u_{u+j})_n$ où $j \in [\![1, 2^r - 2]\!]$ est donné en argument.

Ensuite, il ne reste plus qu'à vérifier que pour tout $j \in [\![1, 2^r - 2]\!]$, cette corrélation vaut -1.

```
#On double U pour être sûr que n+j soit un indice existant
def correlation(U, j):
        V = 2*U
        a, b = 0, 0
        for i in range(len(U)):
                if V[i] == V[i+j]:
                        a += 1
                else:
                        b += 1
        return a-b

def test_correlation(U, r):
        j = 1
        while j <= 2**r - 2:
                if correlation(U, j) != -1:
                        return False
                j += 1
        return True
```

FIGURE 9 – Code des fonctions *correlation* et *text_correlation*

Comme précédemment, on peut tester la corrélation pour la suite U et une autre suite quelconque

```
>>> C   = [1, 0, 0, 1, 0]
>>> U_0 = [1, 1, 1, 0, 1]
>>> U   = lfsr(U_0, C)
>>>
>>> V   = [ randint(0, 1) for _ in range(len(U)) ]
>>>
>>> r = len(C)
>>> test_correlation(U, r)
True
>>> test_correlation(V, r)
False
```

FIGURE 10 – Test de la corrélation

Nous avons ainsi implémenté un générateur pseudo-aléatoire sous la forme d'un LFSR en Python, et vérifié que les suites obtenues vérifient bien les propriétés voulues.

4.4 Applications

Terminons par quelques applications simples d'un générateur pseudo-aléatoire

4.4.1 Générateur d'entiers aléatoires

Nous avons utilisé à plusieurs reprises la fonction *randint* du module *random* afin de générer des suites quelconques. Nous allons implémenter une telle fonction.

Par soucis de simplicité, cette fonction ne prendra pas d'argument et renverra un entier entre 1 et $2^r - 1$ ou r est un entier non nul défini par une fonction d'initialisation.

Pour cela, nous allons d'abord écrire une fonction permettant le passage d'un r-uplet de 0 et de 1 représentant un entier en binaire à son écriture décimale et vice-versa. Ensuite, nous allons créer la fonction d'initialisation qui va générer la suite U à partir d'un vecteur initial U_0 choisi par la fonction *time*, ce qui le rend dans la pratique imprévisible. De cette suite U, la fonction *entierAlea* génèrera un nombre pseudo-aléatoire à chaque appel.

```
from time import time

def binVersDec(L):
        x = 0
        for e in L:
                x *= 2
                x += e
        return x

def decVersBin(x, r):
        L = [ 0 for _ in range(r) ]
        for i in range(r-1, -1, -1):
                L[i] = x%2
                x //= 2
        return L
```

FIGURE 11 – Les fonctions de conversion de binaire à décimal

La fonction *entierAlea* utilise comme variable globales U, r et k. Seul k est à préciser comme variable globale car la fonction le modifie. k est l'indice du terme courant dans la suite $(U_n)_n$.

```
def init(C):
        r = len(C)
        U_0 = [0]*r
        while U_0 == [0]*r:
                U_0 = decVersBin(int(time()*100), r)
        return (lfsr(U_0, C), r)


def entierAlea():
        global k
        V = U + U[:r]
        x = binVersDec(V[k:k+r])
        k += 1
        k %= 2**r-1
        return x
```

Après initialisation, voici les 20 premiers termes que donne *entierAlea*. Si on initialise à nouveau, ces termes sont différents car U_0 est différent à chaque initialisation.

```
>>> C   = [1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1]
>>>
>>> U, r = init(C)
>>> k = 0
>>> print([ entierAlea() for _ in range(20) ])
[1389, 2779, 5559, 2926, 5853, 3515, 7031, 5870, 3548, 7097, 6003, 3814, 7629,
7066, 5941, 3691, 7382, 6573, 4954, 1717]
>>>
>>>
>>> U, r = init(C)
>>> k = 0
>>> print([ entierAlea() for _ in range(20) ])
[4112, 32, 64, 128, 256, 512, 1024, 2048, 4096, 1, 3, 6, 13, 27, 55, 111, 222,
444, 889, 1778]
```

FIGURE 12 – Génération de nombres pseudo-aléatoires grâce à la fonction *entierAlea*

4.4.2 Cryptage et décryptage d'un message

Nous allons créer un code permettant de crypter un message. Pour cela, on récupère le code unicode de chaque caractère (représenté sur 8 bit) et on applique l'opération ou exclusif à chaque bit avec un terme de la suite U. La même opération permet de retrouver le caractère d'origine (car dans $\mathbb{F}_2$, on a $(x+y)+y=x$). La suite U étant entièrement déterminée par le vecteur U_0, en supposant C fixé et connu, il s'agit alors de la clé de cryptage.

```
def crypter(U_0, message):
        r = len(U_0)
        L = [ decVersBin(ord(e), 8) for e in message ]
        U = lfsr(U_0, C)
        for i in range(len(L)):
                for k in range(len(L[i])):
                        L[i][k] ^= U[i+k]
        return "".join([ chr(binVersDec(e)) for e in L])
```

FIGURE 13 – La fonction de (dé)cryptage

Vérifions maintenant que le message est bien crypté

```
>>> C   = [1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1]
>>> r = len(C)
>>> U_0 = decVersBin(int(time()*100), r)
>>>
>>> message = "Registre à décalage à rétroaction linéaire"
>>> message = crypter(U_0, message)
>>> print(message)
ß¥Ø+ÖG/¿Z¦éxÍ¨\§Å5Ë%Ë+ç3J$ôÝ    ¹Ó&
>>> message = crypter(U_0, message)
>>> print(message)
Registre à décalage à rétroaction linéaire
```

FIGURE 14 – Cryptage et décryptage d'un message

Le message crypté est bien incompréhensible ! Ainsi, seule la connaissance de U_0 permet de crypter et de décrypter le message.

5 Conclusion

Les registres à décalage à rétroaction linéaire sont un outil très performant afin de générer des suites pseudo-aléatoires, et leurs utilisations sont très variées.

Nous les avons construits grâce aux suites récurrentes linéaires homogènes dans $\mathbb{F}_2$ et nous avons établi différentes propriétés vérifiées par ce genre de suites qui font que leur comportement est pseudo-aléatoire. Dans la pratique, il sont très faciles à mettre en place comme nous l'avons fait, il suffit de connaître un polynôme primitif de $\mathbb{F}_2$ de degré r pour faire un LFSR à r bits. Ils peuvent fonctionner sur des dispositifs de faible puissance de calcul, voire même être implémenté de manière électronique de façon simple. Tout ceci fait que les LFSR sont utilisés dans beaucoup de domaines, par exemple, presque tous les protocoles de communication utilisent un LFSR afin d' « homogénéiser » le flux de bit envoyé, puisqu'une disproportion de 1 et de 0 peut entraîner des difficultés à l'utilisation de codes correcteurs, très présents dans la transmission de données.

Cependant, ils sont de moins en moins utilisés dans la cryptographie et dans la sécurité. En effet, du fait de leur caractère déterministe et linéaire, il existe des méthodes permettant de retrouver la graine U_0 et donc de casser un cryptage fait avec ce système. Il existe d'autres variantes, comme des NLFSR (*non linear feedback shift registers*), qui corrigent ce défaut.

Dans tous les cas, aucun algorithme ne peut produire une suite parfaitement aléatoire. Dans certaines applications, il est donc toujours nécessaire de disposer d'un générateur de nombre aléatoire, qui souvent est un périphérique utilisant diverses sources fluctuantes comme entrée : pression athmosphérique, courant dans une résistance, température, etc.