Générateurs de nombres pseudo-aléatoires

François Vieille - Suzanne Bay - Simon Amiot

12 javembre 2012

Chapitre 1

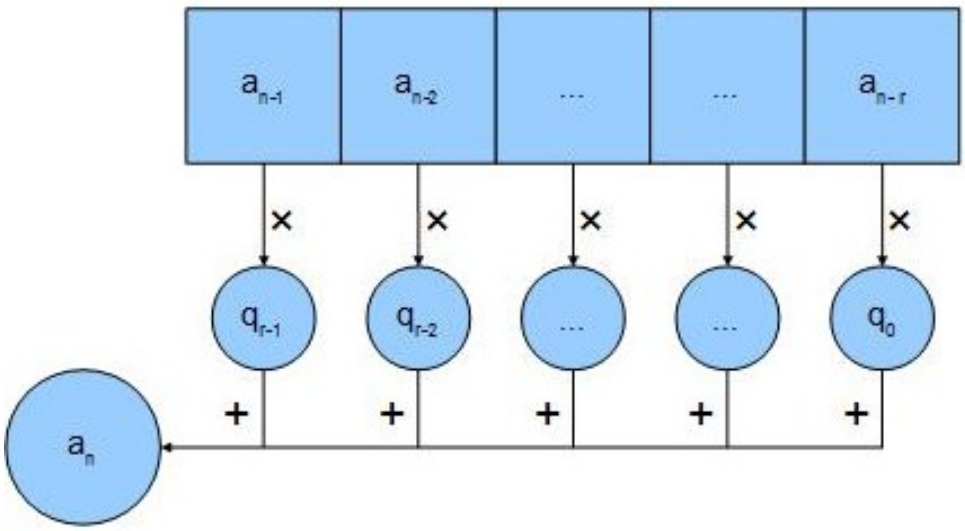
Registre à decalage

1.1 Présentation et exemple

1.1.1 Définition et propriétés des registres à décalages

Les registres à décalages permettent de générer des séquences de caractères qui ont d'excellentes propriétés pour synchroniser l'écoute d'un récépteur. Les registres à décalages sont des appareils éléctroniques qui génèrent un signal pseudo-aléatoire, et ce sont les propriétés de ce signal qui permettent au récepteur GPS d'identifier, avec exactitude, de quel satellite provient le signal et même de mesurer le temps de parcours du signal en se synchronisant au signal reçu du satellite.

Dans le cadre de l'utilisation du GPS, on utilise un registre à décalage permettant de créer un signal périodique de période $2^r - 1$. De plus, il sera très mal corrélé avec toute translation de lui-même, et avec les autres signaux n'ayant pas les mêmes entrées. Rappelons que les signaux produits par les registres à décalage sont des suites de 0 et de 1. Le registre utilisé pour le GPS fait partie de la famille des registres à décalage à rétroaction linéaire (LFSR). Ce sont des générateurs de nombres pseudo-aléatoires constitués d'un registre à décalage et d'une fonction de rétroaction linéaire, c'est-à-dire une fonction qui prend en entrée n termes consécutifs $\{a_{n-r}, a_{n-r+1}, \ldots, a_{n-1}\}$ d'une suite , et renvoie $\{a_{n-r+1}, a_{n-r+2}, \ldots, a_n\}$ avec $a_n = g(a_{n-r}, a_{n-r+1}, \ldots, a_{n-1})$, la fonction g caractérise totalement la fonction de rétroaction linéaire. Voilà comment fonctionne le registre à décalage :



Le n-uplet $q = (q_0, q_1, \ldots, q_{r-1}) \in \{0,1\}^r$ est appelé le quotient du registre, il est fixé et est propre à un satellite donné. Le n-uplet $a = (a_0, a_1, \ldots, a_{r-1}) \in \{0,1\}^r$ est appelé la graine du générateur. Le registre génére une suite pseudo-aléatoire de la manière suivante :

- Il prend les r premiers termes de la suite $a_0, a_1, \ldots, a_{r-1}$ non tous nuls.
- Pour calculer le terme suivant, le registre fait le calcul suivant :

$$a_r \equiv a_0 q_0 + a_1 q_1 + \cdots + a_{r-1} q_{r-1} \pmod 2.$$

- Puis on décale chaque entrée vers la droite, c'est-à-dire qu'on remplace les $a_0, a_1, \ldots, a_{r-1}$ par $a_1, a_2, \ldots, a_r$ dans la première étape.
- Et on itère le procédé.

Définition 1.1. *Une suite $\{a_n\}_{n\geq 0}$ est périodique s'il existe un entier $M > 0$ tel que, pour tout $n \in \mathbb{N}, a_n = a_{n+M}$. Le nombre $N > 0$ minimum ayant cette propriété est appelé la période de la suite.*

Comme ce procédé est parfaitement déterministe et que la graine comporte un nombre fini (exactement r) de termes, la suite générée est périodique. Sa période est inférieur ou égale à 2^r , car il y exactement 2^r éléments distincts dans $\{0,1\}^n$ et donc au maximum 2^r suites distinctes de longueur r. Et de plus, le r-uplet nul n'est jamais générée, car si on a $a_{n-r} = \cdots = a_{n-1} = 0$, alors pour tout $m \leq n$, on a $a_m = 0$, ce qui veut dire

que la graine est nulle, absurde. D'où la période d'une suite générée par un registre est inférieur ou égale à $2^r - 1$.

Pour avoir des propriétés intéressantes, c'est-à-dire une période maximale, il est nécessaire de bien choisir le quotient et la graine. Pour cela, on utilise la théorie des corps finis ainsi que des résultats sur les éléments primitifs de corps.

Nous ne regardons jamais toute la suite, mais une fenêtre de $M = 2^r - 1$ nombres consécutifs $\{a_n\}_m^{m+M-1}$, que nous pouvons appeler $B = \{b_1, \ldots, b_M\}$. Nous voulons la comparer avec une autre fenêtre $C = \{c_1, \ldots, c_M\}$ de la forme $\{a_n\}_p^{p+M-1}$. Par exemple, la suite B est envoyée par le satellite, et la suite C est une permutation cyclique de la même suite générée par le récepteur. Pour déterminer le décalage entre les deux, le récepteur translate d'une entrée la suite qu'il génère (en faisant $p \mapsto p + 1$) de manière répétée jusqu'à ce qu'elle soit identique à B.

1.1.2 Exemple d'un registre à décalage à retroaction linéaire

Cette partie nécessite d'avoir lu la partie 2 et 3 pour bien comprendre la démarche de l'exemple.

Exemple (Exemple d'un registre à décalage à 6 cases)**.** *Nous allons donc travailler dans le corps* $\mathbb{F}_{2^6}$*.*

Première étape : Il s'agit de trouver un polynôme primitif $p(x)$ *de* $\mathbb{F}_{2^6}$*, c'est-à-dire un polynôme* $p(x)$ *irréductible de degré* 6 *tel que* x *soit une racine primitive de* $\mathbb{F}_2/p(x)$*.*

Prenons $p(x) = x^6 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$*. Dans un premier temps, nous allons montrer que* $p(x)$ *est irréductible.*

Pour montrer l'irréductibilité de $p(x)$*, il faut déjà s'assurer qu'il n'a pas de racine dans* $\mathbb{F}_2$*. Pour cela, il suffit juste de calculer* $p(0)$ *et* $p(1)$ *:*

$$p(0) = 1 \quad et \quad p(1) = 1.$$

Maintenant, il faut montrer que $p(x)$ *n'est pas le produit de deux polynômes irréductibles.*

Supposons $p(x) = s_1(x)s_2(x)$ *(à coefficient modulo* 2*). Tout d'abord, ni* $s_1(x)$*, ni* $s_2(x)$ *n'est de degré* 1*, car sinon* $p(x)$ *aurait des racines dans* $\mathbb{F}_2$*. D'où* $1 < deg(s_1(x)), deg(s_2(x)) < 5$*.*

Les polynômes irréductibles qui vérifient ces conditions sont :

$$\begin{aligned} s_1(x) &= x^2+x+1 \\ s_2(x) &= x^3+x^2+1 \\ s_3(x) &= x^3+x+1 \\ s_4(x) &= x^4+x^3+1 \\ s_5(x) &= x^4+x+1 \\ s_6(x) &= x^4+x^3+x^2+x+1. \end{aligned}$$

Et $\forall \quad i,j \in \{1,\ldots,6\}$, $p(x) \neq s_i(x)s_j(x)$.
Donc $p(x)$ *est irréductible.*

Deuxième étape : Dans un deuxième temps, nous allons montrer que x *est un racine primitive du corps* $\mathbb{F}_2/p(x)$. *Pour cela, il suffit de montrer que* $x^{2^6-1} = x^{63} = 1$ *et que* x^3, x^7, x^9 *et* $x^{21} \neq 1$ *(car si* m *l'ordre de* x, *alors* $\forall p \in \mathbb{N} \mid x^p = 1$, p *est un multiple de* m*).*

$$\begin{aligned} x^{63} &= (x^6)^{10} \times x^3 \\ &= ((x^4+x^3+x+1)^2)^5 \times x^3 \\ &= (x^8+x^6+x^2+1)^5 \times x^3. \end{aligned}$$

Or $x^8 = x^2(x^4+x^3+x+1) = x^6+x^5+x^3+x^2 = x^5+x^4+x^2+x+1$.
D'où,

$$\begin{aligned} x^{63} &= (\overbrace{x^5+x^4+x^2+x+1}^{x^8}+\overbrace{x^4+x^3+x+1}^{x^6}+x^2+1)^5 \times x^3 \\ &= (x^5+x^3+1)^5 \times x^3 \\ &= (x^{10}+x^6+1)^2(x^5+x^3+1)x^3 \\ &= (x^5+x^3+x+1)^2(x^5+x^3+1)x^3 \\ &= (x^{10}+x^6+x^2+1)(x^5+x^3+1)x^3 \\ &= (x^5+x^3+x^2+x+1)(x^5+x^3+1)x^3 \\ &= (x^{10}+x^7+x^5+x^4+x^2+x+1)x^3 \\ &= (x^7+x^6+x^4+x^3+x^2+x^7+x^5+x^4+x^2+x+1)x^3 \\ &= (x^5+x^4+x^3+x+1+x^3+x+1)x^3 \\ &= x^8+x^7 \\ &= x^5+x^4+x^2+x+1+x^5+x^4+x^2+x \\ &= 1. \end{aligned}$$

Et on a bien,

$$\begin{aligned} 1 &\neq x^3 \quad \textit{trivial} \\ 1 &\neq x^7 = x^5 + x^4 + x^2 + x \\ 1 &\neq x^9 = x^6 + x^5 + x^3 + x^2 + x = x^5 + x^4 + x^2 + 1 \\ 1 &\neq x^{21} = (x^4 + x^3 + x + 1)^3 \times x^3 = x^3 + x^2 + x. \end{aligned}$$

Donc x est bien une racine primitive du corps $\mathbb{F}_2/p(x)$ et ainsi le polynôme $p(x)$ est primitif.
On peut prendre $(q_0, q_1, q_2, q_3, q_4, q_5) = (1, 1, 0, 1, 1, 0)$, les coefficients de $p(x)$.

– *Troisième étape : Il faut désormais choisir les conditions initiales, la graine. Pour cela il suffit de prendre un polynôme non nul b quelconque et de prendre les a_i tel que*

$$\begin{aligned} a_0 &= T(b) \\ \forall\, i \in \{1, 5\},\ a_i &= T(x^i b). \end{aligned}$$

Prenons $b = x^3 + 1$ (On aurait aussi bien pu prendre $b = 1$ pour se faciliter la tâche). On a alors :

$$\begin{aligned} a_0 &= T(b) = T(x^3 + 1) = 0 \\ a_1 &= T(xb) = T(x^4 + x) = 0 \\ a_2 &= T(x^5 + x^2) = 1 \\ a_3 &= T(x^6 + x^3) = T(x^4 + x + 1) = 0 \\ a_4 &= T(x^5 + x^2 + x) = 1 \\ a_5 &= T(x^6 + x^3 + x^2) = T(x^4 + x^2 + x + 1) = 0. \end{aligned}$$

Le choix de la graine $(a_5, a_4, a_3, a_2, a_1, a_0) = (0, 1, 0, 1, 0, 0)$ (ou des conditions initiales) est fait. Voyons ce que donne la suite :

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

On peut s'apercevoir que sur les $63 = 2^6 - 1$ *premiers termes de la suite, il n'y a aucun* 6*-uplet qui se répète. Et les* 21 *derniers termes* $a_{63} = a_{63+0}, \ldots, a_{83} = a_{63+20}$ *de la suite sont exactement les termes* $a_0, \ldots, a_{20}$*. On obtient bien une suite de période* $2^6 - 1 = 63$*.*

1.1.3 Propriétés de ce générateur et généralisation

Il s'avère que les LFSR ont des propriétés statistiques très intéressantes. Par exemple, dans l'exemple ci-dessus, on s'aperçoit que sur une période $(63 = 2^6 - 1)$, le 1 apparaît 32 fois et le 0 apparaît 31 fois. Regardons les sous-suites de deux entrées :

00 est sortie 15 fois,
01 est sortie 16 fois,
10 est sortie 16 fois,
11 est sortie 16 fois.

De même pour les suites de $3, 4, 5$ et 6 entrées, on obtient les stats suivantes :

3 entrées : 000 sort 7 fois, et les autres $(001, 010, 011, 100, \ldots)$ 8 fois.
4 entrées : 0000 sort 3 fois, et les autres 4 fois.
5 entrées : 00000 sort 1 fois, et les autres 2 fois.
6 entrées : 000000 ne sort jamais, et tous les autres sortent une fois.

Pouvons-nous continuer avec des sous-suites de 7 symboles ? Non, notre registre n'a que 6 cases, si bien que chaque fois que les 6 premiers symboles sont déterminés, le septième et les suivants le sont aussi. Nous pouvons expliquer pourquoi les sous-suites n'ayant que des 0 apparaissent moins souvent : nous ne pouvons nous permettre d'avoir une sous-suite de la forme 0000 parce que la rêgle de fonctionnement du registre à décalage forcerait tous les symboles suivants de la suite à être zéros.

Cet exemple montre que ce registre a de bonnes propriétés statistiques tant qu'on ne considère pas des sous-suites trop longues (ici, on se limite à des sous-suites de 6 symboles). Ceci n'est pas un hasard, et nous le montrerons dans le chapitre 2 (REF ATTENDUE).

Si l'on veut pouvoir bénéficier des bonnes propriétés de ce registre pour des sous-suites plus longues, il faudra prendre un nombre r de cases assez grand. Nous allons décrire le fonctionnement du registre à décalage sous une

autre forme qui prêtera à des généralisations. Á un instant donné, que l'on

appellera l'instant j, les entrées dans les cases sont $a_j, \ldots, a_{j+r-1}$. Réécrivons ces entrées sous la forme $x_{j,0}, \ldots, x_{j,r-1}$, où $x_{j,i} = a_{i+j}$. L'avantage de cette écriture est que l'indice j indique l'instant et l'indice i, la case où se trouve le symbole. Appelons X_j, le vecteur-colonne dont les entrées sont $x_{j,0}, \ldots, x_{j,r-1}$, c'est-à-dire les symboles apparaissent dans les cases à l'instant j. Soit A la matrice

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ q_0 & q_1 & q_2 & q_3 & \cdots & q_{r-1} \end{pmatrix}$$

où toutes les opérations sont effectuées modulo 2. Alors, le vecteur représentant les symboles des cases à l'instant $j+1$ est donné par

$$X_{j+1} = AX_j.$$

Le grand avantage de cette nouvelle présentation est la suivante. Supposons que l'on veuille passer directement de X_j à X_{j+k} sans calculer les étapes intermédiaires. On a $X_{j+k} = A^k X_j$. Donc, si on calcule la matrice A^k, on peut automatiser le calcul de X_{j+k} en fonction de X_j. Le fait de pouvoir automatiser avec des calculs raisonnables le passage de X_j à X_{j+k} est une propriété recherchée dans les bons générateurs de nombres aléatoires.

On voit qu'on peut obtenir d'autres générateurs de nombres aléatoires en gardant l'étape de récurrence et en permettant d'autres formes de matrice A.

1.2 Théorie sur les corps finis

1.2.1 Qu'est-ce qu'un corps fini ?

Définition 1.2 (Définition d'un corps)**.** *Un corps $(A, +, \times)$ est une structure algébrique vérifiant les propriétés suivantes :*

1. *$+$ est une loi de composition interne associative dans A*
2. *$+$ est une loi de composition interne commutative dans A*
3. *$\times$ est une loi de composition interne associative dans A*

4. $\times$ *est distributive sur* $+$
5. $+$ *admet un élément neutre* 0_{A} *dans* A
6. $\times$ *admet un élément neutre* 1_{A} *dans* A
7. *tous les éléments de* A *sont inversibles pour* $+$
8. *tous les éléments de* $A \setminus \{0_{\mathrm{A}}\}$ *sont inversibles pour* $\times$

Ce qui équivaut à :

1. $(A, +, \times)$ *est un anneau*
2. *le groupe des inversibles de* A *est* $A^X = A \setminus \{0_A\}$

Définition 1.3. *Un corps A est dit fini si le nombre d'éléments dans A est fini .*

Exemple 1.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *muni de l'addition et de la multiplication sont des corps. Cependant ils ne sont pas finis. Toutefois, $\mathbb{Z}$ n'en est pas un, car 1 est le seul élément non nul inversible pour la multiplication dans $\mathbb{Z}$.*

Exemple 1.2. $\mathbb{Z}/p\mathbb{Z}$ *est un corps si et seulement si p est premier. De plus, $\mathbb{Z}/p\mathbb{Z}$ est fini quelque soit p.*

On note $\mathbb{F}_p$ l'anneau $\mathbb{Z}/p\mathbb{Z}$.

Preuve de l'exemple 1.3 : ($\Leftarrow$) Supposons p premier.

Soit a un représentant de $\overline{a} \neq \overline{0}$ dans le même système de représentant que p. Comme p premier, on a que $pgcd(a, p) = 1$. Ainsi, on obtient la relation de Bézout suivante :

$$\exists (u, v) \in \mathbb{Z} \quad | \quad au + pv = 1. \tag{1.1}$$

D'où, en reprenant l'équation (1.1) modulo p, on obtient

$$\exists (\overline{u}, \overline{v}) \in \mathbb{Z}/p\mathbb{Z} \quad | \quad \overline{au + bv} = \overline{a}\,\overline{u} + \overline{p}\,\overline{v} = \overline{a}\,\overline{u} = \overline{1}.$$

D'où $\overline{a}$ est inversible, d'inverse $\overline{u}$ dans $\mathbb{Z}/p\mathbb{Z}$. Ceci vaut pour tout $\overline{a}$ appartenant à $\mathbb{Z}/p\mathbb{Z}$.

Donc $\mathbb{Z}/p\mathbb{Z}$ est un corps.

($\Rightarrow$) On raisonne par contraposée. On suppose que p n'est pas premier et on veut montrer que $\mathbb{Z}/p\mathbb{Z}$ n'est pas un corps.

Il existe a, b entiers compris entre 2 et $p - 1$ tel que $ab = p$. Ce qui donne dans $\mathbb{Z}/p\mathbb{Z}$,

$$\overline{a}\overline{b} = \overline{p} = \overline{0}.$$

Or un corps est intègre. D'où $\mathbb{Z}/p\mathbb{Z}$ n'est pas intègre implique que $\mathbb{Z}/p\mathbb{Z}$ n'est pas un corps.
D'où le résultat.

□

Exemple 1.3. *Soit $p(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. L'ensemble $\mathbb{F}_2/p(x)$ est un corps fini.*

En effet, $A = \mathbb{F}_2/p(x) = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$.

$\overline{1}$ est inversible d'inverse lui-même, et $\overline{x}$ $(\overline{x+1}) = \overline{x^2+x} = \overline{1}$. Donc $\overline{x}$ a pour inverse $\overline{x+1}$, et réciproquement.

1.2.2 Corps de polynomes

Définition 1.4. *Un polynôme irréductible est un polynôme qui n'est ni inversible ni produit de deux polynômes non inversibles.*

Proposition 1.1. *(i) Soit $p(x)$ un polynome de degré n . Le quotient $\mathbb{F}/p(x)$ peut être identifié à $\{q(x) \in \mathbb{F}[x]$ tel que degré $q < n\}$ muni de l'addition et de la multiplication modulo $p(x)$.*

(ii) $\mathbb{F}/p(x)$ est un corps si et seulement si $p(x)$ est irréductible sur $\mathbb{F}$.

Démonstration. (i) Il s'agit de montrer que $\{q(x) \in \mathbb{F}[x]$ tel que degré $q < n\}$ muni de l'addition et de la multiplication modulo $p(x)$ est un anneau fini, et qu'on peut identifier chaque élément de $\mathbb{F}/p(x)$ à un élément de $\{q(x) \in \mathbb{F}[x]$ tel que degré $q < n\}$.
On va chercher à montrer que $A = \{q(x) \in \mathbb{F}[x]$ tel que degré $q < n\}$ est un sous-anneau de $\mathbb{F}[x]$.

- On a déja que $A \subset \mathbb{F}[x]$.
- De plus, il est évident que $1 \in A$.
- Soit $Q(x), R(x) \in A$, on sait que l'inverse de $R(x)$ pour l'addition dans $\mathbb{F}[x]$ est $-R(x)$.
  D'où $Q(x)(R(x))^{-1} = -Q(x)R(x)$.
  On sait que $-Q(x)R(x) \in \mathbb{F}[x]$ car $\mathbb{F}[x]$ est un anneau.
  Soit $deg(-Q(x)R(x)) < n$, et dans ce cas $Q(x)(R(x))^{-1} \in A$.
  Soit $deg(-Q(x)R(x)) \geq n$.
  On fait la division euclidienne de $-Q(x)R(x)$ par $p(x)$ et on obtient :

$$-Q(x)R(x) = p(x)D(x) + r(x) \quad avec \quad deg(r(x)) < n$$

Ainsi $Q(x)(R(x))^{-1} = -Q(x)R(x) = r(x)$ avec la multiplication modulo $p(x)$. Or $r(x) \in \mathbb{F}[x]$ et $deg(r(x)) < n$, donc $r(x) \in A$.
Donc $Q(x)(R(x))^{-1}$.

Donc $A = \{q(x) \in \mathbb{F}[x] \text{ tel que degré } q < n\}$ est un sous-anneau de $\mathbb{F}[x]$. De plus, on a A fini, car $\mathbb{F}$ l'est et qu'on ne prend que les polynômes de degré $< n$. Enfin, chaque classe d'équivalence de $\mathbb{F}/p(x)$ a un représentant dans A et réciproquement, chaque élément $q(x)$ peut être identifié à $\overline{q(x)}$ élément de $\mathbb{F}/p(x)$.

(ii) ($\Leftarrow$) Supposons $p(x)$ est irréductible, il s'agit de montrer que $\mathbb{F}/p(x)$ est un corps.
Soit $\overline{q(x)} \in \mathbb{F}/p(x)$, $\overline{q(x)} \neq \overline{0}$. Montrons que $\overline{q(x)}$ a un inverse pour la loi $\times$.
Prenons $\phi_q : \overline{s(x)} \mapsto \overline{s(x)}\ \overline{p(x)}$ définie de $\mathbb{F}/p(x)$ dans lui-même. Soit $\overline{s_1(x)}, \overline{s_2(x)} \in \mathbb{F}/p(x) \mid \phi(\overline{s_1(x)}) = \phi(\overline{s_2(x)})$.
D'où $\overline{s_1(x)}\ \overline{p(x)} = \overline{s_2(x)}\ \overline{p(x)}$ si et seulement si $(\overline{s_1(x)} - \overline{s_2(x)})\overline{p(x)} = \overline{0}$.
Par (i), on identifie $\overline{s_1(x)}, \overline{s_2(x)}, \overline{p(x)}$ à $s_1(x), s_2(x)$ et $p(x)$.
Et on obtient qu'il existe un polynôme $b(x)$ appartenant à $\mathbb{F}[x]$ tel que $(s_1(x) - s_2(x))p(x) = b(x)q(x)$.
Or $q(x)$ irréductible, d'où soit $p(x)$, soit $s_1(x) - s_2(x)$ est un multiple de $q(x)$. Mais $\overline{q(x)} \neq \overline{0}$ donc $\overline{s_1(x)} - \overline{s_2(x)} = \overline{0}$.
Donc $\overline{s_1(x)} = \overline{s_2(x)}$, et ϕ injective.
Or $\mathbb{F}/p(x)$ est fini, donc ϕ est surjective. D'où il existe $\overline{s(x)}$ tel que $\phi_q(\overline{s(x)}) = \overline{1}$, c'est-à-dire $\overline{s(x)}\ \overline{q(x)} = \overline{1}$.
Donc $\mathbb{F}/p(x)$ est un corps.

($\Rightarrow$) Supposons que $\mathbb{F}/p(x)$ est un corps.
On raisonne par l'absurde, on suppose que $p(x)$ n'est pas irréductible, il existe $b(x), c(x)$ deux polynômes non nuls de $\mathbb{F}[x]$ tel que $p(x) = b(x)c(x)$ avec nécessairement $1 < deg(b(x)) < n$ et $1 < deg(c(x)) < n$.
$\mathbb{F}/p(x)$ est un corps, il est donc intègre. Or $\overline{0} = \overline{p(x)} = \overline{b(x)}\ \overline{c(x)}$.
Et pourtant $\overline{b(x)}, \overline{c(x)} \neq \overline{0}$ car polynômes non nuls tel que $1 < deg(b(x)), deg(c(x)) < n$, absurde.
Donc $p(x)$ est irréductible.

□

1.2.3 racines primitives d'un corps finis

Définition 1.5. *Un élément non nul d'un corps tel que tous les autres éléments non nuls peuvent être obtenus de celui-ci par exponentiation est appelé élément primitif ou racine primitive .*

Théorème 1.1. *Tout corps finis $\mathbb{F}_{p^r}$ possède une racine primitive c'est-à-dire qu'il existe un élément non nul α dont l'ensemble des puissances coïncide avec l'ensemble des éléments non nuls de $\mathbb{F}_{p^r}$:*

$$\mathbb{F}_{p^r} \setminus \{0\} = \{\alpha, \alpha^2, \ldots, \alpha^{p^r-1} = 1\}$$

Démonstration. Les éléments non nuls de $\mathbb{F}_{p^r}$ forment un groupe multiplicatif G dont le nombre d'éléments est $p^r - 1$. Chaque élément non nul y engendre un sous-groupe fini $H = \{y^i \mid i \in \mathbb{N}\}$.($H$ est fini puisque sous-groupe de G fini).Le théorème de Lagrange nous dit que le cardinal de H divise le cardinal de G. De plus, comme H est fini, il existe s minimum tel que $y^s = 1$ (tout élément de H a un ordre). Ce s, appelé l'ordre de y, est égal au nombre d'éléments de H. Donc, y est racine du polynôme $x^s - 1 = 0$. Comme $s \mid p^r - 1$, alors y est racine du polynôme $R(x) = x^{p^r-1} - 1$. On vient donc de montrer que tout élément de G est racine du polynôme $R(x) = x^{p^r-1} - 1$. Supposons maintenant qu'il existe m, un diviseur strict de $p^r - 1$ tel que l'ordre de tout élément de G divise m. Alors tout élément de G est racine du polynôme $x^m - 1 = 0$. Contradiction car ce polynôme a, au plus, m racines. Donc, il existe des y_i d'ordre $m_i, i = 1 \ldots n$, tel que le plus petit commun multiple des m_i soit égal à $p^r - 1$. Alors, le produit $y_1 \ldots y_n = \alpha$ est d'ordre $p^r - 1$. □

1.3 Utilité des corps finis dans le registre à décalage

1.3.1 Corrélation

Définition 1.6. *On appellera corrélation entre les deux suites B et C de longueur M le nombre d'entrées i où $b_i = c_i$ moins le nombre d'entrées i où $b_i \neq c_i$. On la notera $Cor(B, C)$.*

Proposition 1.2. *La corrélation entre les deux suites est donnée par :*

$$Cor(B,C) = \sum_{i=1}^{M} (-1)^{b_i}(-1)^{c_i}$$

Démonstration. Le nombre $Cor(B,C)$ est calculé ainsi : chaque fois que $b_i = c_i$ on doit additionner 1. Chaque fois que $b_i \neq c_i$ on doit soustraire 1. Rappelons que les b_i et les c_i ne prennent que les valeurs 0 ou 1. Si $b_i = c_i$, alors soit $(-1)^{b_i} = (-1)^{c_i} = 1$, soit $(-1)^{b_i} = (-1)^{c_i} = -1$. Dans les deux cas, $(-1)^{b_i}(-1)^{c_i} = 1$. De même, si $b_i \neq c_i$ exactement un des nombres $(-1)^{b_i}$ et $(-1)^{c_i}$ vaut 1, et l'autre vaut -1. Donc $(-1)^{b_i} = (-1)^{c_i} = -1$. □

Voici le théorème que nous allons chercher à prouver dans toute cette partie :

Théorème 1.2. *Étant donné un registre à décalage avec un quotient $q = (q_{r-1}, ..., q_1, q_0) \in \{0,1\}^r$ et des conditions initiales $a_0, a_1, \ldots, a_{r-1} \in \{0,1\}^r$ tel que la suite générée par le registre est périodique de longueur $2^r - 1$. On considère deux fenêtres de cette suite de même longueur $M = 2^r - 1$, soit $B = \{a_n\}_{n=m}^{n=m+M-1}$ et $C = \{a_n\}_{n=p}^{n=p+M-1}$ avec $p > m$. Si M ne divise pas $p - m$ alors*

$$Cor(B,C) = -1$$

C'est-à-dire que le nombre de bits en désaccord est toujours un de plus que le nombre de bits en accord .

Ce théorème nous dit, dans un premier temps, que l'on peut choisir un quotient et des conditions initiales tel que la suite générée soit de période maximale, égale à $2^r - 1$. Le théorème suivant va servir de base pour la prochaine partie.

Théorème 1.3.
1. *$\mathbb{F}_{2^r}$ muni de l'addition des polynômes modulo 2 et de cette multiplication est un corps.*
2. *Il existe un élément α tel que les éléments non nuls de $\mathbb{F}_{2^r}$ sont précisement les α^i, $i = 0 \ldots 2^r - 2$, c'est-à-dire*

$$\mathbb{F}_{2^r} \setminus \{0\} = \{1, \alpha, \alpha^2, \ldots, \alpha^{2^r-2}\}$$

A cause de cette propriété, α est appelé racine primitive du corps et satisfait à $\alpha^{2^r-1} = 1$

3. *$\{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ sont linéairement indépendants comme éléments de l'espace vectoriel $\mathbb{F}_2^r$ sur $\mathbb{F}_2$ (qui est isomorphe à notre corps $\mathbb{F}_{2^r}$).*
4. *Une racine primitive α du corps $\mathbb{F}_{2^r}$ est racine d'un polynôme irréductible sur $\mathbb{F}_2$*
$$Q(x) = x^r + q_{r-1}x^{r-1} + \cdots + q_1 x + q_0$$
Le corps construit avec le polynôme Q est isomorphe au corps construit avec le polynôme P.

Démonstration. 1. La preuve est identique à la preuve du fait que $\mathbb{F}_p$ est un corps si p premier (voir exemple 1.1). On utilise pour cela l'algorithme d'Euclide pour les polynômes qui permet de trouver le plus grand diviseur communs de deux polynômes.

2. Il suffit de prendre $p = 2$ dans le théorème 1.1.
3. Nous admettrons que les éléments $\{1, \alpha, \ldots, \alpha^{r-1}\}$ sont linéairement indépendants dans l'espace $\mathbb{F}_2^r$ qui est isomorphe à $\mathbb{F}_{2^r}$.
4. Les vecteurs $\{1, \alpha, \ldots, \alpha^r\}$ sont linéairement dépendants car un ensemble de $r+1$ vecteurs dans un espace de dimension r est toujours linéairement dépendant. Comme les vecteurs $\{1, \alpha, \ldots, \alpha^{r-1}\}$ sont linéairement indépendants, il existe des coefficients $q_0, q_1, \ldots, q_{r-1}$ tels que $\alpha^r = q_0 + q_1\alpha + \cdots + q_{r-1}\alpha^{r-1}$. Donc, α est racine du polynôme $Q(x) = x^r + q_{r-1}x^{r-1} + \ldots + q_1 x + q_0$. Ce polynôme est irréductible sur $\mathbb{F}_2$. Sinon, α serait racine d'un polynôme de degré inférieur à r, ce qui serait en contradiction avec le fait que $\{1, \alpha, \ldots, \alpha^{r-1}\}$ sont linéairement indépendants dans $\mathbb{F}_2^r$.

□

1.3.2 Primitivité et trace

Définition 1.7. *Un polynôme $Q(x)$ à coefficients dans $\mathbb{F}_2$ est dit primitif s'il est irréductible et si le polynôme x est racine primitive du corps $\mathbb{F}/Q(x)$ construit à partir du polynôme $Q(x)$.*

Définition 1.8. *La fonction trace du corps $\mathbb{F}_{2^r}$ est la fonction $T : \mathbb{F}_{2^r} \to \mathbb{F}_2$ définie par $T(b_{r-1}x^{r-1} + \cdots + b_1 x + b_0) = b_{r-1}$*

Proposition 1.3. *La fonction T est linéaire et surjective. Elle prend la valeur 0 sur exactement la moitié des éléments de $\mathbb{F}_{2^r}$ et la valeur 1 sur l'autre moitié.*

Démonstration. 1. Linéarité de T :

Soit A, B tel que $A(x) = a_{r-1}x^{r-1} + \cdots + a_1x + a_0$ et $B(x) = b_{r-1}x^{r-1} + \cdots + b_1x + b_0$ avec $a_0, \ldots, a_{r-1}, b_0, \ldots, b_{r-1} \in \{0, 1\}$. Alors $T(A) = a_{r-1}$ et $T(B) = b_{r-1}$. Et on a

$$\begin{aligned} T(A+B) &= T((a_{r-1}+b_{r-1})x^{r-1} + \cdots + (a_1+b_1)x + (a_0+b_0)) \\ &= a_{r-1} + b_{r-1} \\ &= T(A) + T(B) \end{aligned}$$

De plus, pour tout α élément de $\mathbb{F}_2$,

$$\begin{aligned} T(\alpha A) &= T(\alpha a_{r-1}x^{r-1} + \cdots + \alpha a_1x + \alpha a_0) \\ &= \alpha a_{r-1} \\ &= \alpha T(A) \end{aligned}$$

D'où la linéarité de T.

2. Surjectivité de T :

L'espace d'arrivée de T est le corps à deux éléments $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$. Or pour $A(x) = x^{r-1}$ et $B(x) = 1$ deux éléments de $\mathbb{F}_{2^r}$, on a $T(A) = \overline{1}$ et $T(B) = \overline{0}$. D'où $\{\overline{0}, \overline{1}\} \subseteq Im(T)$. Or $Im(T) \subseteq \mathbb{F}_2 = \{\overline{0}, \overline{1}\}$ donc $Im(T) = \mathbb{F}_2$.

Donc T est surjective.

3. Répartition des 0 et des 1 : Il y a exactement 2^{r-1} polynômes de degré $r-1$ et 2^{r-1} polynômes de degré $< r-1$ dans $\mathbb{F}_{2^r}$. Or T prend la valeur 1 pour les polynômes de degré $r-1$ et 0 pour les autres. D'où T prend la valeur 1 sur la moitié des éléments de $\mathbb{F}_{2^r}$ et 0 sur l'autre moitié.

□

La remarque suivante indique comment choisir les $q_0, \ldots, q_{r-1}$ et les $a_0, \ldots, a_{r-1}$, dans un générateur LFSR, pour obtenir une période maximale.

Remarque. *Nous choisissons un polynôme $P(x)$ primitif de degré r sur $\mathbb{F}_2$*

$$P(x) = x^r + q_{r-1}x^{r-1} + \cdots + q_1x + q_0$$

qui nous permet de construire le corps $\mathbb{F}_{2^r}$. Les q_i du registre à décalage sont les coefficients du polynôme $P(x)$. Pour construire de bonnes conditions initiales, on prend un r-tuples $b = (b_0, ..., b_{r-1}) \in \mathbb{F}_2^r \setminus \{0\}$ que l'on identifie au

polynôme $b_{r-1}x^{r-1} + \cdots + b_1 x + b_0$. *On prend comme éléments initiaux*

$$\begin{aligned} a_0 &= T(b), \\ a_1 &= T(xb), \\ &\vdots \\ a_{r-1} &= T(x^{r-1}b). \end{aligned}$$

Voila comment calculer a_1.

$$\begin{aligned} a_1 = T(bx) &= T(b_{r-1}x^r + b_{r-2}x^{r-1} + \cdots + b_0 x) \\ &= T(b_{r-1}(q_{r-1}x^{r-1} + \cdots + q_1 x + q_0) + b_{r-2}x^{r-1} + \cdots + b_0 x) \\ &= T((b_{r-1}q_{r-1} + b_{r-2})x^{r-1} + \cdots) \\ &= b_{r-1}q_{r-1} + b_{r-2}. \end{aligned}$$

Un calcul similaire permet de calculer $a_2, \ldots, a_{r-1}$. *Les formules deviennent vite énormes mais le calcul se fait très bien dans des exemples numériques quand on remplace les* b_i *et les* q_i *par des valeurs* 0 *ou* 1.

1.3.3 Preuve du théorème 1.2

Maintenant, il faut montrer que, pour ce choix de quotient et ce choix des conditions initiales, la suite est périodique et sa période est $M = 2^r - 1$. Et il faut montrer que la corrélation entre deux suites vaut -1, si elles ne sont pas décalées d'un multiple de M.

Proposition 1.4. *Choisissons pour les* q_i *d'un registre à décalage les coefficients d'un polynôme primitif de degré* r *sur* $\mathbb{F}_2$

$$P(x) = x^r + q_{r-1}x^{r-1} + \cdots + q_1 x + q_0.$$

Soit $b = b_{r-1}x^{r-1} + \cdots + b_1 x + b_0$. *On prend comme éléments initiaux* $(a_0, a_1, \ldots, a_{r-1})$ *vu dans la remarque précédente. Alors, la suite générée par le registre à décalage est la suite* $\{a_n\}$, *avec* $a_n = T(x^n b)$. *Elle est périodique, et sa période divise* $2^r - 1$.

Démonstration. On utilise que $P(x) = 0$, c'est-à-dire le fait que $x^r = q_{r-1}x^{r-1} + \cdots + q_1 x + q_0$.

Alors,

$$\begin{aligned} T(x^r b) &= T((q_{r-1}x^{r-1} + \cdots + q_1 x + q_0)b) \\ &= q_{r-1}T(x^{r-1}b) + \cdots + q_1 T(xb) + q_0 T(b) \\ &= q_{r-1}a_{r-1} + \cdots + q_1 a_1 + q_0 a_0 \\ &= a_r. \end{aligned}$$

Supposons maintenant, par induction, que les éléments de la suite générée vérifient tous $a_i = T(x^i b)$ pour $i \leq n-1$. Alors ,

$$\begin{aligned} T(x^n b) &= T(x^r x^{n-r} b) \\ &= T((q_{r-1}x^{r-1} + \cdots + q_1 x + q_0)x^{n-r} b) \\ &= q_{r-1}T(x^{n-1}b) + \cdots + q_1 T(x^{n-r+1}b) + q_0 T(x^{n-r}b) \\ &= q_{r-1}a_{n-1} + \cdots + q_1 a_1 + q_0 a_{n-r} \\ &= a_n. \end{aligned}$$

Donc, la multiplication par x correspond exactement à l'action du registre à décalage. On voit que la suite est périodique de période $2^r - 1$ puisque $x^{2^r-1} = 1$. □

La proposition suivante et sa preuve démontre la partie corrélation du théorème 1.2.

Proposition 1.5. *Si* $B = \{a_n\}_{n=m}^{n=m+M-1}$ *et* $C = \{a_n\}_{n=p}^{n=p+M-1}$, *alors* $Cor(B, C) = -1$ *si* M *ne divise pas* $p - m$.

Démonstration. On peut supposer $m \leq p$,

$$\begin{aligned}
Cor(B,C) &= \sum_{i=0}^{M-1}(-1)^{a_{m+i}}(-1)^{a_{p+i}} \\
&= \sum_{i=0}^{M-1}(-1)^{T(x^{m+i}b)}(-1)^{T(x^{p+i}b)} \\
&= \sum_{i=0}^{M-1}(-1)^{T(x^{m+i}b)+T(x^{p+i}b)} \\
&= \sum_{i=0}^{M-1}(-1)^{T(x^{m+i}b+x^{p+i}b)} \\
&= \sum_{i=0}^{M-1}(-1)^{T(bx^{m+i}(1+x^{p-m}))} \\
&= \sum_{i=0}^{M-1}(-1)^{T(x^{m+i}\beta)}
\end{aligned}$$

où $\beta = b(1+x^{p-m})$. On sait que, dans notre corps, x est une racine primitive et donc, que $x^M = 1$ et que $x^N \neq 1$ si $1 \leq N < M$. On en déduit que $x^N = 1$ si et seulement si M divise N. Si M divise $p-m$, alors $x^{p-m} = 1$ et $\beta = b(1+1) = 0$. Dans ce cas, $Cor(B,C) = M$. Si M ne divise pas $p-m$, le polynôme $(1+x^{p-m})$ n'est pas le polynôme nul ; ainsi $\beta = b(1+x^{p-m})$ est non nul comme élément de $\mathbb{F}_{2^r}$, puisqu'il est le produit de deux éléments non nuls du corps. Donc β est de la forme x^k où $k \in \{0,\ldots,2^r-2\}$, ce qui entraîne que l'ensemble $\{\beta x^{i+m}, 0 \leq i \leq M-1\}$ forme une permutation de $\mathbb{F}_{2^r} \setminus \{0\} = \{1, x, x^2, \ldots, x^{2^r-2}\}$. La fonction trace T prend la valeur 1 sur la moitié des éléments de $\mathbb{F}_{2^r}$ et 0 sur l'autre moitié. Comme elle prend la valeur 0 en 0, elle prend la valeur 0 sur $2^{r-1}-1$ des éléments de $\mathbb{F}_{2^r} \setminus \{0\}$ et la valeur 1 sur 2^{r-1} des éléments de $\mathbb{F}_{2^r} \setminus \{0\}$.

D'où $Cor(B,C) = -1$ □

Le corollaire suivant et sa preuve achève la démonstration du théorème 1.2.

Corollaire 1.1. *La période de la suite pseudo-aléatoire générée par le registre à décalage est exactement $M = 2^r - 1$.*

Démonstration. Si la période était égale à $K < M$ alors la suite coïnciderait avec sa translatée de K composantes, et les deux auraient une corrélation égale à M, en contradiction avec la proposition 1.5. □

Le Théorème 1.2 est démontré.