Conception vectorielle de FCSR

Marjane abdelaziz

LAGA

08 Juillet 2011

1. Séquences pseudo-aléatoires
2. Registres à rétroaction
3. Valuations
4. Classification des registres et des a.v.d complets
5. Registre linéaire
6. Registre linéaire avec retenue sur $\mathbb{F}_p$
7. Registres vectoriels à rétroaction avec retenue
8. Différents modes de connexion

Généralités sur les séquences

Séquence

Une séquence dans $\mathbb{F}_{p^n}$ est une suite infinie d'éléments dans ce corps, notée $\underline{a} = (a_i)_{i \in \mathbb{N}}$.

Périodicité

On dit qu'une séquence $(a_i)_{i \in \mathbb{N}}$ est ultimement périodique s'il existe $i_0 > 0$ et T entiers tels que :

$$\forall i \geq i_0, \quad a_{i+T} = a_i$$

Si $i_0 = 0$, on dit qu'elle est strictement périodique.

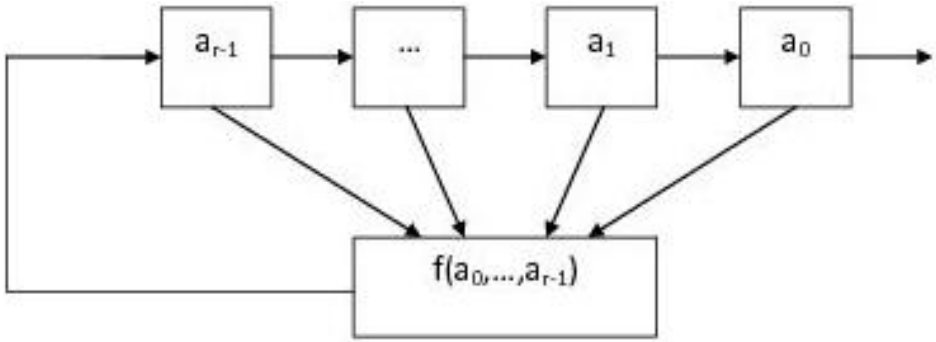
Objectifs

On cherche à générer des séquences binaires (ou sur $\mathbb{F}_{p^n}$) périodiques ayant de bonnes propriétés de pseudo-aléarité :

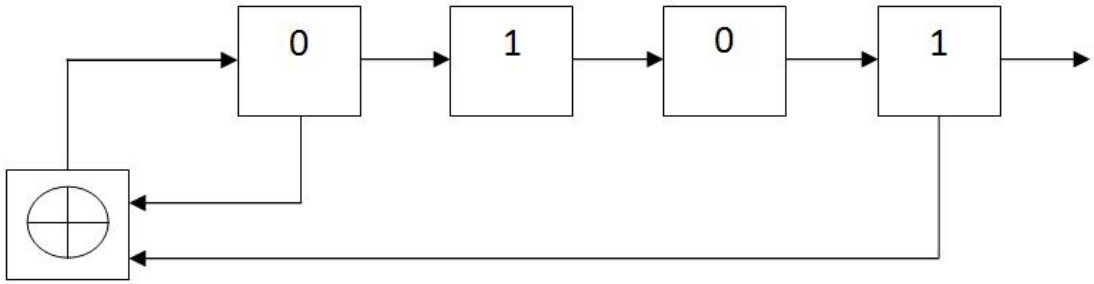
- une grande période.
- la propriété de l'équilibre (nombre de 0 et de 1 dans une période)
- la propriété de répétition (nombre d'apparition d'un mot binaire dans une période).
- une faible inter-correlation : $\mathcal{C}_{\underline{a},\underline{b}}(\tau) = \sum_{i=0}^{i=N-1} (-1)^{a_i + b_{i+\tau}}$.

Description

- Feedback Shift Registers (1950) : modèle classique pour générer des séquences.
- Conception : une taille r, une entrée $(a_0, \ldots, a_{r-1})$ dans le corps fini $\mathbb{F}_{p^n}$, une fonction de retour f booléenne, le calcul du bit suivant $a_r = f(a_0, \ldots, a_{r-1})$, un décalage dans le registre et une sortie a_0.
- La séquence générée est périodique de période $\leq p^{nr}$.



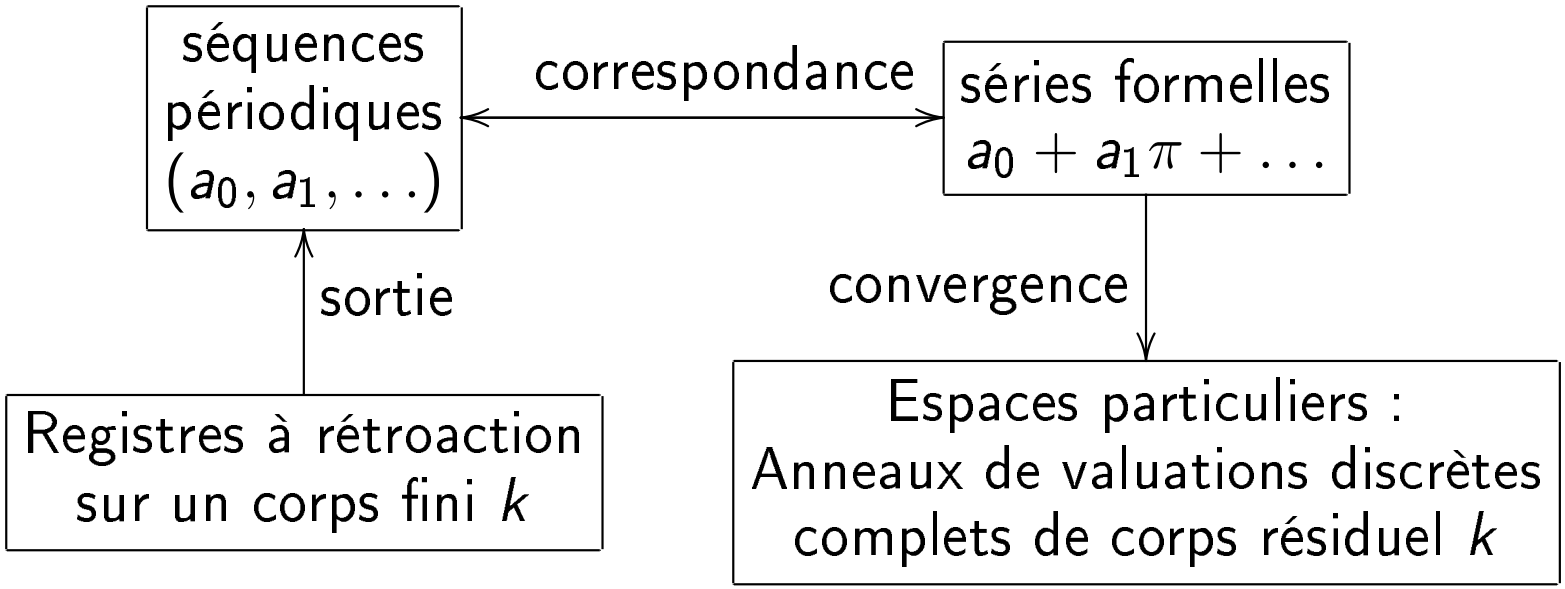
Exemple de Registre



Séquence de sortie (101011001000111101011 0 . . .).
période= 15.

Analyse des séquences de sorties

Idée centrale utilisée pour l'analyse :



Propriétés de $a_0 + a_1\pi + \ldots \Rightarrow$ Propriétés de $(a_0, a_1, \ldots)$.

Définition d'une valeur absolue ultramétrique

Définition

Soit K un corps commutatif. Une valeur absolue est une application $|.| : K \to \mathbb{R}_+$ qui vérifie :

- $|a| = 0 \Leftrightarrow a = 0$,
- pour tout $a, b \in K$, $|ab| = |a|.|b|$ et
- pour tout $a, b \in K, |a + b| \leq |a| + |b|$.

$(K, |.|)$ est appelé corps valué. Si $|.|$ vérifie la condition suivante plus forte

- pour tout $a, b \in K, |a + b| \leq \max(|a|, |b|)$,

alors $|.|$ est appelée valeur absolue non-archimédienne et $(K, |.|)$ est appelé corps valué non-archimédien.

Exemples

- sur $\mathbb{Q}$, la valeur absolue p-adique définie par $|\frac{m}{n}|_p = (\frac{1}{p})^{r-s}$ avec $m = m^{'}p^{r}$ et $n = n^{'}p^{s}$ o ù $p \nmid m^{'}$ et $n^{'}$.
- sur $k(X)$, la valeur absolue X-adique définie par $|\frac{P}{Q}| = \alpha^{r-s}$ $(0 < \alpha < 1)$ avec $P = P^{'}X^{r}$ et $Q = Q^{'}X^{s}$ où $X \nmid P^{'}$ et $Q^{'}$.
- Ces deux valeurs absolues sont ultramétriques.

Groupe des valeurs, Anneau de valuation et Corps résiduel

Définition

Soit $(K, |.|)$ un corps valué.

- L'image de $|.|$ privée de 0 est appelée groupe des valeurs et est notée Γ. C'est un sous groupe multiplicatif de $\mathbb{R}^{>0}$.
- L'ensemble des élements de K de valeur absolue ≤ 1 noté $\mathcal{O}$ est appelé anneau de valuation.

Proposition

$\mathcal{O}$ est un sous anneau local de K. L'ensemble des éléments de K de valeur absolue < 1 noté $\mathcal{M}$ est l'idéal maximal de $\mathcal{O}$. L'ensemble des inversibles de $\mathcal{O}$ est $\mathcal{O} \setminus \mathcal{M}$.

Définition

Le quotient $k = \mathcal{O}/\mathcal{M}$ est appelé corps résiduel.

Valuation discrète

Définition

$|.|$ est appelée valeur absolue discrète si Γ est monogène. Dans ce cas, $(K, |.|)$ est dit corps de valuation discrète et $\mathcal{O}$ est dit anneau de valuation discrète. Une valeur absolue discrète est ultramétrique.

Proposition

Il existe $\pi \in \mathcal{O}$ unique à un inversible près tel que $\forall a \in K$, il existe un entier $v(a)$ tel que $|a| = |\pi|^{v(a)}$.

Définition

π est appelé une uniformisante de $\mathcal{O}$ et $v(a)$ est appelé valuation de a.

Proposition

- $\mathcal{M} = \pi\mathcal{O}$.
- $\mathcal{O}$ est principal et possède un unique idéal premier $\pi\mathcal{O}$.

Complété d'un corps valué

Théorème de Complétion

Soit $(K, |.|)$ un corps valué. Notons $C(K)$ l'ensemble des suites de Cauchy de K et $M(K)$ l'ensemble des suites de K convergentes vers 0.
$C(K)/M(K)$ noté $\hat{K}$ est un corps complet valué avec pour valeur absolue

$$|(a_n)_n| = \lim_{+\infty} |a_n|.$$

K s'injecte dans $\hat{K}$ par l'application "diagonale" $x \longrightarrow (x, x, \ldots)$. K est dense dans $\hat{K}$. $\hat{K}$ est l'unique extension valuée complète de K à isomorphisme près vérifiant ces propriétés. Il y a isomorphisme des groupes des valeurs $\hat{\Gamma} \cong \Gamma$ et isomorphisme des corps résiduels $\hat{k} \cong k$.

Complété d'un corps de valuation discrète

Théorème : Développement de Hensel

Si (K, v) est un corps de valuation discrète alors son complété l'est aussi et ses éléments se développent de manière unique en série convergente à coefficientsdans k : $a = \sum_{-\infty<<n} a_n \pi^n$. $\hat{\mathcal{O}}$ est un anneau de valuation discrète complet. Ses éléments sont indexés par $\mathbb{N}$.

K	$\hat{K}$	$\hat{\mathcal{O}}$	$\hat{\mathcal{M}}$	$\hat{k}$
$(\mathbb{Q}, v_p)$	$\mathbb{Q}_p$	$\mathbb{Z}_p, \sum_n a_n p^n$	$p.\mathbb{Z}_p$	$\mathbb{F}_p$
$(k(X), v_X)$	$k((X))$	$k[[X]], \sum_n a_n X^n$	$X.k[[X]]$	k

Table: Exemples de complété de corps de valuation discrète

Extension et indice de ramification

Définition

Soit $(K', v') \supseteq (K, v)$ une extension finie de corps valués.

- L'ordre du groupe quotient Γ'/Γ est appelé indice de ramification et est noté $[\Gamma' : \Gamma]$.
- La dimension de k' comme k espace vectoriel est appelé degré résiduel et est noté $[k' : k]$.

Théorème

Pour tout extension finie de corps valués, $[\Gamma' : \Gamma].[k' : k] \leq [K' : K]$.
Si K est un corps de valuation discrète complet alors
$[\Gamma' : \Gamma].[k' : k] = [K' : K]$.

Classification des c.v.d. complets de corps rés. parfait

Définition

k est dit corps parfait dans deux cas : si k est de caractéristique 0 ou si l'homomorphisme de Frobenius $x \longrightarrow x^p$ est surjectif dans le cas de caractéristique p. En particulier, tout corps fini est parfait.

Théorème

Soit K un corps de v.d. complet de corps résiduel k parfait. Alors :

- Si $car(K) = car(k)$, alors $K \cong k((X))$ et $\mathcal{O} \cong k[[X]]$.
- si $car(K) = 0$ et $car(k) = p$, alors $\mathbb{Q}_p \subseteq K$. Soit d l'indice de ramification de cette extension. On distingue 2 cas :
  - Si $d = 1$, alors $K \cong Frac(W(k))$ et $\mathcal{O} \cong W(k)$ l'anneau des vecteurs de Witt sur k. K est dit absolument non-ramifié.
  - Si $d > 1$, alors K est une extension de $Frac(W(k))$ de degré d et $\mathcal{O}$ est $W(k)$-module libre de rang d. K est dit ramifié.

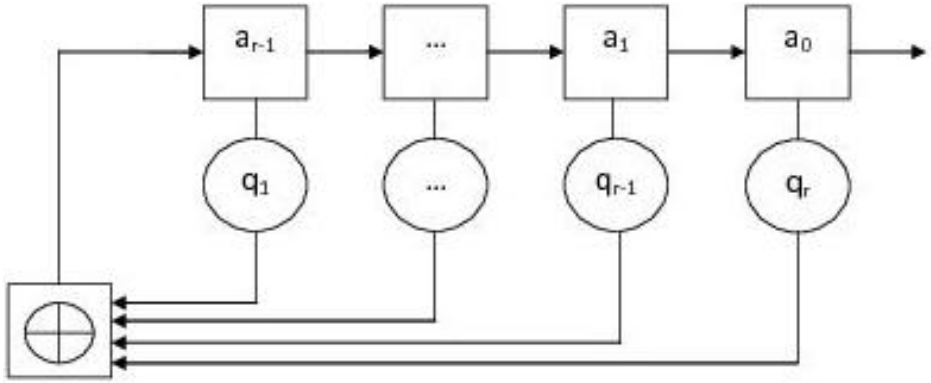
Classification pour le corps résiduel fini

On s'intéresse au cas de corps résiduel fini, car on cherche à générer des séquences périodiques, le plus simple étant de construire des séquences à coefficients dans un ensemble fini.

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

Table: Classification des a.v.ds et des registres à rétroaction.

LFSR ou Registre à décalage et à rétroaction linéaire

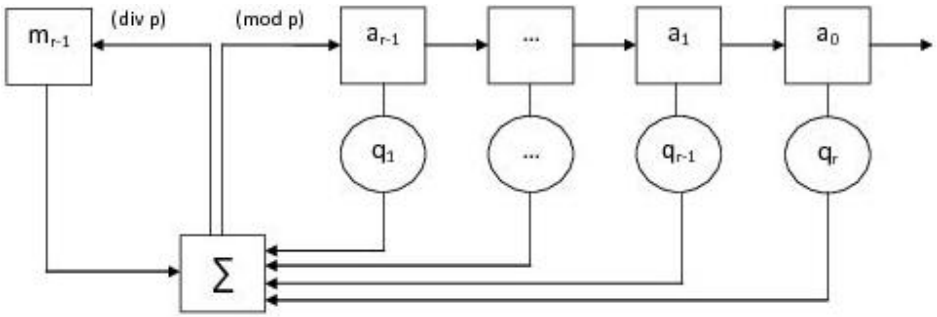


- Le LFSR est étudié et utilisé depuis 1950.
- L'addition se fait sans retenue dans $\mathbb{F}_{p^n}[X]$ et dans $\mathbb{F}_{p^n}[[X]]$.
- Séquence de sortie $\underline{a} = (a_0, a_1, \ldots) \subseteq \mathbb{F}_{p^n}$ associée à la série formelle $a(X) = a_0 + a_1 X + \ldots \in \mathbb{F}_{p^n}[[X]]$.
- $a(X) \in \mathbb{F}_{p^n}(X) \Leftrightarrow \underline{a}$ périodique.

Propriétés des LFSR

Sortie	$\underline{a} = (a_0, a_1, \ldots) \in \mathbb{F}_{p^n}$
coefficients de connexion	$q_1, \ldots, q_r$
polynôme de connexion	$Q(X) = q_r X^r + \ldots + q_1 X - 1$
série formelle associée	$a(X) = a_0 + a_1 X + \ldots \in \mathbb{F}_{p^n}[[X]]$
propriété fondamentale	$a(X) = \frac{P(X)}{Q(X)}$
période	$\mathtt{per}(\underline{a}) \mid \mathtt{ord}_Q(X)$
période maximale m-séquence	$\mathtt{per}(\underline{a}) = p^{nr} - 1$ si $(P, Q) = 1$ et si Q irréductible primitif
Séquence de Gold	si $p = 2$, $n = 1$, per $= 2^r - 1$, r impair $s = 2^k + 1$, $(k, r) = 1$ $\mathcal{C}_{\underline{a},\underline{a}^s}(\tau) = -1, -1 \pm 2^{\frac{r+1}{2}}$

FCSR ou Registre à décalage et à rétroaction avec retenue

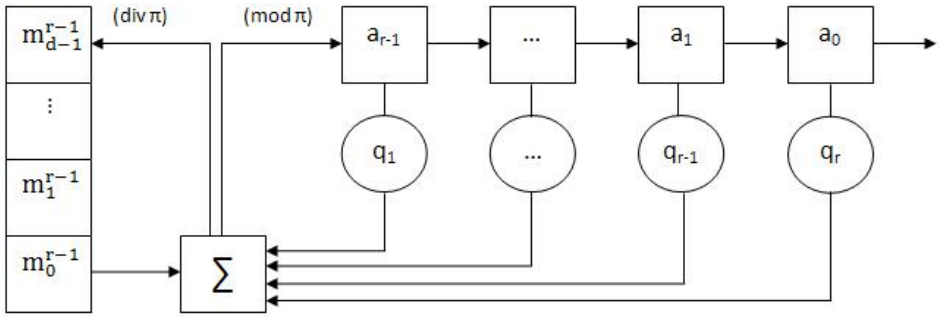


- Le FCSR est introduit par Goresky et Klapper en 1993.
- L'addition se fait avec une retenue dans $\mathbb{Z}$ et dans $\mathbb{Z}_p$.
- Séquence de sortie $\underline{a} = (a_0, a_1, \ldots) \subseteq \mathbb{F}_p$ associée à la série formelle $a = a_0 + a_1 p + \ldots \in \mathbb{Z}_p$.
- $a \in \mathbb{Q} \Leftrightarrow \underline{a}$ périodique.

Propriétés des FCSR

Sortie	$\underline{a} = (a_0, a_1, \ldots) \in \mathbb{F}_p$
coefficients de connexion	$q_1, \ldots, q_r$
entiers de connexion	$q = q_r p^r + \ldots + q_1 p - 1$
entier p-adique associé	$a = a_0 + a_1 p + \ldots \in \mathbb{Z}_p$
propriété fondamentale	$a = \frac{s}{q}$
période	$\mathtt{per}(\underline{a}) \mid \mathtt{ord}_q(p)$
période maximale l-séquence	$\mathtt{per}(\underline{a}) = q - 1$ si $(s, q) = 1$, si q premier et si p racine primitive de q
mémoire	$m \nearrow$ ou $\searrow$ vers $[0, q_1 + \ldots + q_r[$
Séquence de faible inter-corrélation	si $p = 2$, $(e, q-1) = 1$ $\mathcal{C}_{\underline{a},\underline{a}^e}(\tau) = 0, q - 1$

d-FCSR ou Reg. à déc. et à rétroaction avec retenue et saut



- Le d-FCSR est introduit en 1994 par Goresky et Klapper.
- L'addition dans $\mathbb{Z}_p[\pi]$ se fait avec retenue et saut.
- Séquence de sortie $\underline{a} = (a_0, a_1, \ldots) \subseteq \mathbb{F}_p$ associée à la série formelle $a = a_0 + a_1\pi + \ldots \in \mathbb{Z}_p[\pi]$.
- $a \in \mathbb{Q}[\pi] \Leftrightarrow \underline{a}$ périodique.

extension des FCSRs sur $\mathbb{F}_{p^n}$

- Problème : Construire les FCSRs sur $\mathbb{F}_{p^n}$ sans utiliser les vecteurs de Witt ?
- Réponse : Conception vectorielle en considérant l'anneau de $\mathbb{Z}_p[X]/(P(X))$ avec P polynôme irréductible modulo p.
- $\mathbb{Z}_p[X]/(P(X)) \cong W(\mathbb{F}_{p^n})$ est un anneau de valuation discrète complet de corps résiduel $\mathbb{F}_{p^n}$.

Conception du registre

- On garde le même schéma.
- L'état initial et les coefficients de connexion sont dans $\mathbb{F}_p[X]/(P)$.
- La mémoire est dans $\mathbb{Z}[X]/(P)$.
- On relève tous les éléments dans $\mathbb{Z}[X]/(P)$ respectivement par rapport à la base canonique $\mathcal{B} = \{1, \bar{X}, \ldots, \bar{X}^{n-1}\}$.
- On écrit tous les éléments comme des vecteurs.
- Les calculs sont vectoriels et les fonctions $(\texttt{mod}p)$ et $(\texttt{div}p)$ s'appliquent composante par composante.
- le FCSR vectoriel est construit sur le triplet $(\mathbb{F}_p, P(X), \mathcal{B})$.

Definition

vecteur de connexion :

$(\tilde{q}_0, \ldots, \tilde{q}_{n-1})$ où $\tilde{q}_i = \sum_{j=1}^{j=r} q_i^j p^j$ pour tout $0 \leq i \leq n-1$.

entier de connexion :

$q = q_r p^r + \ldots + q_1 p - 1$ est un élément dans $\mathbb{Z}[X]/(P)$ et s'écrit $\tilde{q}_{n-1}\bar{X}^{n-1} + \ldots + \tilde{q}_0 - 1$ par rapport à $\mathcal{B}$.

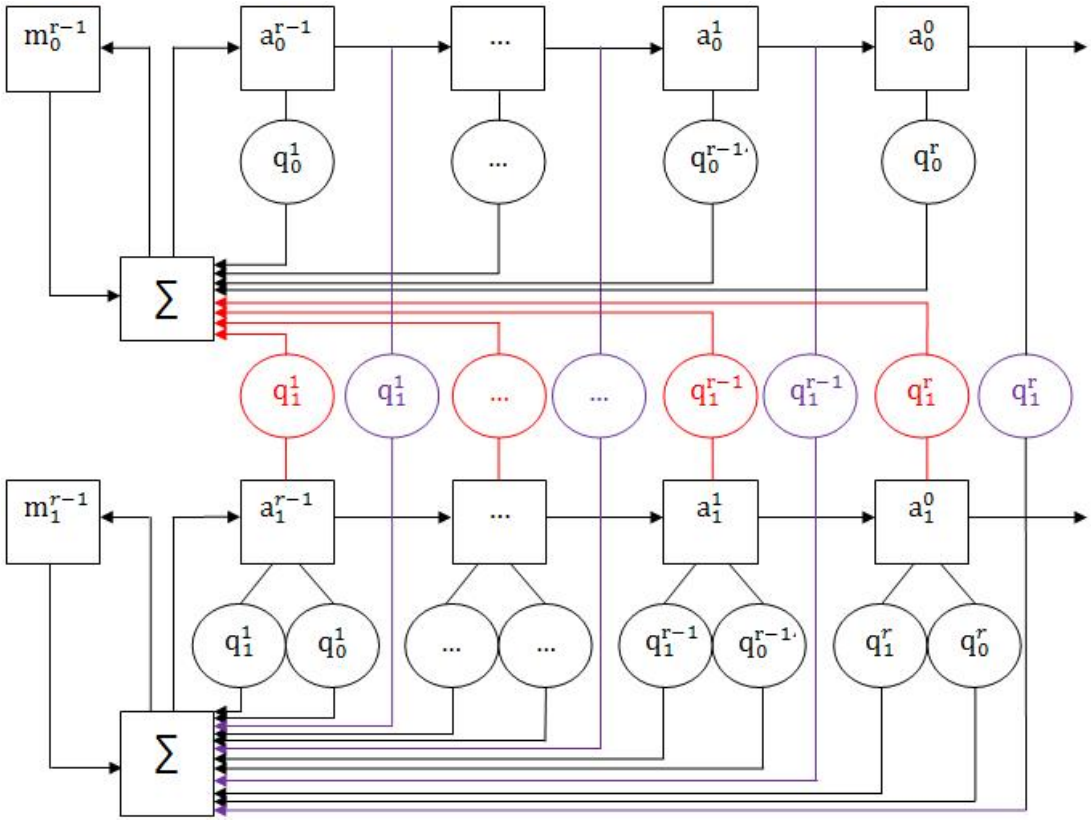
Exemple pour $n = 2$ et $p = 2$.

.

- On considère un FCSR construit sur $(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$.
- L'état initial est de la forme $(a_0^0 + a_1^0\bar{X}, \ldots, a_0^{r-1} + a_1^{r-1}\bar{X})$ dans $\mathbb{F}_2[X]/(X^2 - X - 1)$ et la mémoire initiale $m_0^{r-1} + m_1^{r-1}\bar{X}$ dans $\mathbb{Z}[X]/(X^2 - X - 1)$.
- On calcule $\sigma_0^r = \sum_{i=1}^{i=r} \left(q_1^i a_1^i + q_0^i a_0^i \right) + m_0^{r-1}$ et

  $\sigma_1^r = \sum_{i=1}^{i=r} \left(q_1^i a_1^{r-i} + q_1^i a_0^{r-i} + q_0^i a_1^{r-i} \right) + m_1^{r-1}$.
- On calcule $a_0^r = \sigma_0^r(\mathtt{mod2})$, $a_1^r = \sigma_1^r(\mathtt{mod2})$, $m_0^r = \sigma_0^r(\mathtt{div2})$ et $m_1^r = \sigma_1^r(\mathtt{div2})$.
- On sort a_0, on entre $a_r = a_0^r + a_1^r\bar{X}$ et $m_r = m_0^r + m_1^r\bar{X}$.

Représentation d'un FCSR vectoriel pour $p = 2$ et $n = 2$



Analyse du FCSR vectoriel

La séquence de sortie correspond à n sous-séquences dans $\mathbb{F}_p$.

$$\underline{a} = (a_i)_{i\in\mathbb{N}} = \sum_{j=0}^{j=n-1} (a_j^i)_{i\in\mathbb{N}} \bar{X}^j = \begin{pmatrix} a_0^0 & a_0^1 & a_0^2 & \cdots \\ a_1^0 & a_1^1 & a_1^2 & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ a_{n-1}^0 & a_{n-1}^1 & a_{n-1}^2 & \cdots \end{pmatrix}_{\mathcal{B}}$$

À chaque sous-séquence, on associe son développement p-adique
$\beta_j = a_j^0 + a_j^1 p + \ldots + a_j^i p^i + \ldots$
On obtient un vecteur d'entiers p-adiques $\beta = (\beta_j)_{j=0}^{j=n-1}$.

Analyse du FCSR vectoriel

Le vecteur β vérifie un système linéaire à coefficients entiers avec une matrice $\mathcal{M}$ dont les coefficients diagonaux sont impairs et les autres pairs. Les coefficients sont des combinaisons linéaires des $\tilde{q}_i$.

Definition

$\mathcal{M}$ est appelée matrice de connexion.

Théorème

On se donne un FCSR sur $(\mathbb{F}_p, P, \mathcal{B})$ de matrice de connexion $\mathcal{M}$ et d'entier de connexion q. Soit une séquence de sortie et β son vecteur p-adique associé. Alors

- $\beta \in \frac{1}{|\det \mathcal{M}|}\mathbb{Z}^n$
- $\mathcal{M}$ est la matrice de la transformation linéaire définie comme la multiplication par $-q$ par rapport à la base $\mathcal{B}$.
- $N_{\mathbb{Q}}^{\mathbb{Q}[X]/(P)}(-q) = \det \mathcal{M}$.

Cas quadratique	
Corps	$\mathbb{F}_2[X]/(X^2 - X - 1)$
séquence de sortie	$\underline{a} = (a_1^i)_{i\in\mathbb{N}}\bar{X} + (a_0^i)_{i\in\mathbb{N}}$
vecteur de connection	$(\tilde{q_0}, \tilde{q_1})$
matrice de connection	$\mathcal{M} = \begin{pmatrix} 1-\tilde{q_0} & -\tilde{q_1} \\ -\tilde{q_1} & 1-\tilde{q_0}-\tilde{q_1} \end{pmatrix}$
vecteur rationnel correspondant	$\beta = \left(\frac{\tilde{p_0}}{\tilde{q}}, \frac{\tilde{p_1}}{\tilde{q}}\right)$
forme du déterminant	forme quadratique $u^2 + uv - v^2$ $u = \tilde{q_0} - 1$ et $v = \tilde{q_1}$

Périodicité

- $\tilde{q} = |N(-q)|$ est un entier impair représenté par une n-forme avec pour arguments $\tilde{q}_0 - 1$, $\tilde{q}_1, \ldots$ et $\tilde{q}_{n-1}$.
- Toute séquence générée par un FCSR vectoriel $(\mathbb{F}_2, P, \mathcal{B})$ est périodique.
- La période de $\underline{a}$ est le PPCM des périodes des sous-séquences.
- Soit $\beta = (\frac{p_j}{\tilde{q}})_{j=0}^{j=n-1}$ le vecteur p-adique associé à la séquence de sortie.

  Alors $\mathtt{per}(\underline{a}) = \mathrm{PPCM}_{0 \leq j \leq n-1} \left\{ \mathtt{ord}_{\frac{\tilde{q}}{\gcd(\tilde{q}, p_j)}}(p); p_j \notin \tilde{q}\mathbb{Z} \right\}$
- $\mathtt{per}(\underline{a}) / \mathtt{ord}_{\tilde{q}}(p) / \tilde{q} - 1$
- Cette borne est atteinte si $\tilde{q}$ est un nombre premier représenté par la n-forme dont p est racine primitive modulo $\tilde{q}$ et s'il existe p_j tel que $p_j \notin \tilde{q}\mathbb{Z}$.
- On obtient des l-séquences.

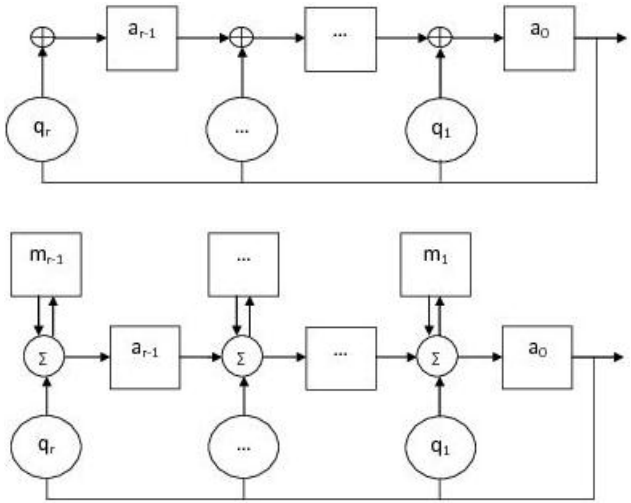
Exemples de périodes maximales

$\tilde{q}$	u,v
11	3,2
59	7,2
101	9,4
701	27,28

$\tilde{q}=$	39741402961906954206160047535539796042005214340820825272689327902761723128526374726419918065389 49
$u=$	199352459131827501532804161134421503646014008796 3
$v=$	199352459131827501532804161134421503646014008786 0

Mode Galois

- On cherche à diversifier le mode de connexion entre les différentes cellules du registre.
- Le mode de Fibonacci est le plus classique mais le moins adapté aux applications cryptographiques.
- Le mode Galois est introduit en 2002 par Goresky et Klapper. Il met à jour simultanément toutes les cellules du registre à chaque top d'horloge.



Mode Ring et Généralisation

- En 2004, Mrugalski introduit pour les LFSRs une généralisation appelée mode Ring. Les connexions sont arbitraires.
- En 2009, Arnault, Berger et al. l'adaptent aux FCSRs.
- La fonction de transition est représentée par une matrice $T = (t_{i,j}) \in \mathcal{M}_{r\times r}(\mathbb{F}_p)$ où chaque coefficient représente la connexion entre la "cellule i" et la "cellule j".
- $$Fib = \begin{pmatrix} 0 & \dots & 0 & q_r \\ 1 & \dots & 0 & q_{r-1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & q_1 \end{pmatrix} \quad Gal = \begin{pmatrix} q_1 & \dots & q_{r-1} & q_r \\ 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix}.$$

Analyse en mode Ring

- L'analyse est identique et les séquences de sorties vérifient les mêmes propriétés.
- La sortie d'un LFSR en mode Ring de matrice de transition T peut être générée par un LFSR en mode Fibonacci de polynôme de connexion $\det(I - XT)$.
- La sortie d'un FCSR en mode Ring de matrice de transition T peut être générée par un FCSR en mode Fibonacci d'entier de connexion $\det(I - pT)$.

Le mode Ring adapté aux VFCSRs

- La matrice de transition $T = (t_{i,j})$ d'un VFCSR est à coefficientsdans $\mathbb{F}_{p^n}$ comme l'état initial.
- On traduit la multiplication par $t_{i,j}$ comme une multiplication vectorielle : $t_{i,j}$ est remplacé par un bloc $n \times n$ à coefficients dans $\mathbb{Z}$ et T par une matrice $\mathcal{T}$ (de bloc) $nr \times nr$
- On écrit tous les éléments comme des vecteurs dans la base $\mathcal{B}$:

$$\begin{aligned} a(t) = &\quad (a_0^0(t), \ldots, a_{n-1}^0(t), \ldots, a_0^{r-1}(t), \ldots, a_{n-1}^{r-1}(t)) \\ m(t) = &\quad (m_0^1(t), \ldots, m_{n-1}^1(t), \ldots, m_0^r(t), \ldots, m_{n-1}^r(t)). \end{aligned}$$

- On calcule $a(t+1) = a(t).\mathcal{T} + m(t)(\mathtt{mod} p)$ et $m(t+1) = a(t).\mathcal{T} + m(t)(\mathtt{div} p)$

Exemple pour le cas $p = 2$ et $n = 2$ de taille $r = 2$

Un VFCR construit sur $(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$ de taille $r = 2$ a pour matrice de transition à coefficients dans $\mathbb{Z}$:

$$\mathcal{T} = \begin{pmatrix} t_0^{1,1} & t_1^{1,1} & t_0^{1,2} & t_0^{1,2} \\ t_1^{1,1} & t_0^{1,1} + t_1^{1,1} & t_1^{1,2} & t_0^{1,2} + t_1^{1,2} \\ t_0^{2,1} & t_1^{2,1} & t_0^{2,2} & t_1^{2,2} \\ t_1^{2,1} & t_0^{2,1} + t_1^{2,1} & t_1^{2,2} & t_0^{2,2} + t_1^{2,2} \end{pmatrix}$$

et pour fonction de transition

$$(a_0^0(t), a_1^0(t), a_0^1(t), a_1^1(t)) \otimes \mathcal{T} \oplus (m_0^1(t), m_1^1(t), m_0^2(t), m_1^2(t)).$$

Comparaison avec les FCSR binaires de taille 4

Registres	différents modèles	valeurs de $\tilde{q} = \lvert\det(I - 2T)\rvert$	périodes max. $\mathtt{ord}_{\tilde{q}}(2) = \tilde{q} - 1$
FCR binaire taille 2	2^4	1,3,5	2,4
FCR binaire taille 4	2^{16}	1,3,5,7,9,$\cdots$,59,61, 63,69,75,77,81,87, 91,99,135	2,4,10,12,18, 28,36,52,58,60
VFCSR-Q en Fib. and Gal. of size 2	2^4	1,5,9,11,19,25,29 ,31,41	4,10,18,28
VFCR-Q of size 2	2^8	1,5,9,11,19,25,29, 31,41,45,49,55,61,99	4,10,18,28,60

Table: Comparaison de périodes maximales avec les FCRs binaires de taille double

Merci !