

# Interprétation matricielle des suites récurrentes linéaires et des codes quasi-cycliques

Pierre-Louis Cayrel, Christophe Chabot, Abdelkader Necer

Université de Limoges - XLIM - DMI - PI2C

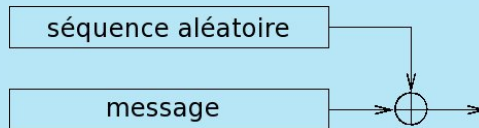
Colloque Franco-Algérien - 14/12/2007

# Sommaire

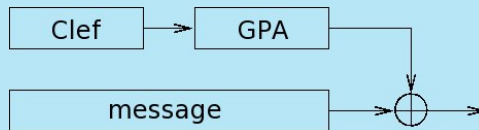
- 1 Motivations
  - Chiffrement à flot
  - Chiffrement par blocs
- 2 SRL classiques
  - Action de  $\mathbb{A}[X]$  sur  $\mathbb{A}^{\mathbb{N}}$
  - Résultats principaux
  - Application aux codes
- 3 SRL à coefficients matriciels
  - Action de  $M_{\ell,\ell}(\mathbb{F}_q)[X]$  sur  $(\mathbb{F}_q^{\ell})^{\mathbb{N}}$
  - Résultats principaux
  - Application aux codes
- 4 Codes quasi-cycliques
  - Action de  $M_{\ell,\ell}(\mathbb{F}_q)[X]$  sur  $(\mathbb{F}_q^{\ell})^m$
  - Résultats principaux
- 5 Conclusion

# Motivations

## ▷ Chiffrement à flot :

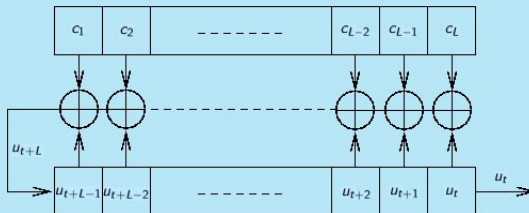


non réaliste → générateur pseudo-aléatoire



## Motivations

### ▷ LFSR (Linear Feedback Shift Register) :



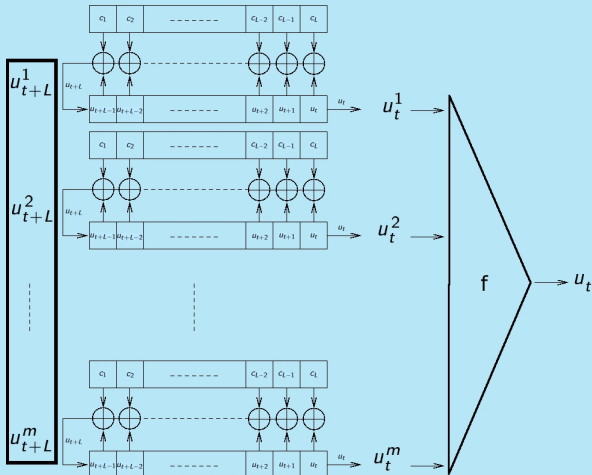
Polynôme de rétroaction :

$$u_{t+L} = c_1 u_{t+L-1} + c_2 u_{t+L-2} + \dots + c_L u_t.$$

→ suite chiffrante = suite récurrente linéaire sur  $\mathbb{F}_2$ .

# Motivations

## ▷ LFSRs combinés :



# Motivations

Polynôme de rétroaction :

$$\begin{pmatrix} u_{t+L}^1 \\ \dots \\ u_{t+L}^m \end{pmatrix} = C_1 \begin{pmatrix} u_{t+L-1}^1 \\ \dots \\ u_{t+L-1}^m \end{pmatrix} + C_2 \begin{pmatrix} u_{t+L-2}^1 \\ \dots \\ u_{t+L-2}^m \end{pmatrix} + \dots + C_L \begin{pmatrix} u_t^1 \\ \dots \\ u_t^m \end{pmatrix}$$

où  $C_i \in M_{m,m}[\mathbb{F}_2]$ .

→ suite chiffrante = suite récurrente linéaire sur  $\mathbb{F}_2^m$ .

## Motivations

### ▷ Chiffrement à base de codes :

*Système de Mc Eliece :*

*Clefs privées :*

$S \in M_{k,k}[\mathbb{F}]$  inversible.

$G \in M_{k,n}[\mathbb{F}]$  génératrice de  $C$ . Le produit  $SGP$ .

$P \in M_{n,n}[\mathbb{F}]$  permutation.

*Clef publique :*

*Chiffrement :*

$$x \longrightarrow xSGP + e$$

*Déchiffrement :*

$$(xSGP + e)P^{-1} = xSG + eP^{-1}.$$

$$\text{décodage} \longrightarrow xS$$

$$\times S^{-1} \longrightarrow x$$

*Cryptanalyse :* retrouver des paramètres du code à partir de la suite chiffrée.

# Suites récurrentes linéaires classiques

Soit  $\mathbb{A}$  un anneau commutatif unitaire.

**Définition :**

Une suite  $(u_n)_{n \in \mathbb{N}}$  d'éléments de  $\mathbb{A}$  est dite récurrente linéaire s'il existe  $a_1, \dots, a_h \in \mathbb{A}$  tels que :

$$u_{n+h} = a_1 u_{n+h-1} + \dots + a_h u_n, \forall n \geq 0.$$

Exemple : la suite de Fibonacci

$$u_0 = 0, u_1 = 1$$

$$u_{n+2} = u_{n+1} + u_n, \forall n \geq 0.$$

## Action de $\mathbb{A}[X]$ sur $\mathbb{A}^{\mathbb{N}}$

▷ Structure de  $\mathbb{A}[X]$ -module sur  $\mathbb{A}^{\mathbb{N}}$  :

$$X * (u_n)_{n \in \mathbb{N}} = (u_{n+1})_{n \in \mathbb{N}}$$

$$\left( \sum_{i=0}^h p_i X^i \right) * (u_n)_{n \in \mathbb{N}} = \left( \sum_{i=0}^h p_i u_{n+i} \right)_{n \in \mathbb{N}}$$

*Exemple :*

$$u = (u_n)_{n \in \mathbb{N}}, v = (v_n)_{n \in \mathbb{N}}, v = (X^2 - X - 1) * u.$$

$$v_n = u_{n+2} - u_{n+1} - u_n, \forall n \geq 0.$$

# Polynômes annulateurs

Soit  $E \subset \mathbb{A}^{\mathbb{N}}$ .

**Définition :**

$$\text{Ann}(E) := \{P \in \mathbb{A}[X] / \forall u \in E, P * u = 0\}$$

Exemple :  $\mathbb{A} = \mathbb{Z}/4\mathbb{Z}, u = (2, 2, \dots)$ ,

$$2, X - 1 \in \text{Ann}(u)$$

## Polynômes caractéristiques

### **Propriété :**

$u$  est une SRL  $\iff$   $\text{Ann}(u)$  est un idéal cofini  
(contient un polynôme unitaire).

### **Définition :**

Tout polynôme unitaire de  $\text{Ann}(u)$  est dit polynôme caractéristique de  $u$ .

Si  $u_{n+h} = a_1 u_{n+h-1} + \dots + a_h u_n, \forall n \geq 0,$

$$f(X) = X^h - a_1 X^{h-1} - \dots - a_h$$

est un polynôme caractéristique de  $u$ .

**Définition :** Si  $f \in \mathbb{A}[X]$ , on note

$$\Omega(f) := \{u \in \mathbb{A}^{\mathbb{N}} / f * u = 0\}.$$

*Exemples :*

$$\begin{aligned}\Omega(X - 1) &= \{\text{suites constantes}\}. \\ \Omega(X^2 - X - 1) &= \{u \in \mathbb{A}^{\mathbb{N}} / u_{n+2} = u_{n+1} + u_n, \forall n \geq 0\}.\end{aligned}$$

Si  $\mathbb{A} = \mathbb{K}$  est un corps,

$\Omega(f)$  est un  $\mathbb{K}$ -e.v. de dimension  $\deg(f)$ .

## Résultats principaux

▷ Maintenant, on suppose que  $\mathbb{A} = \mathbb{K}$  est un corps.

**Théorème :** Soit  $(u_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ , les assertions suivantes sont équivalentes :

▷  $(u_n)_{n \in \mathbb{N}}$  est une suite récurrente linéaire.

▷  $S(X) = \sum u_n X^n \in \mathbb{K}(X)$ .  $\left( S(X) = \frac{P(X)}{Q(X)}, Q(0) \neq 0 \right)$

▷ 
$$\begin{pmatrix} u_n \\ \vdots \\ u_{n+h-1} \end{pmatrix} = M^n \begin{pmatrix} u_0 \\ \vdots \\ u_{h-1} \end{pmatrix}.$$

Si  $P(X) = \sum_{i=0}^h p_i X^i$  est un polynôme caractéristique de  $u$ ,

$$M = \begin{pmatrix} 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \\ -p_1 & -p_2 & \cdots & -p_h \end{pmatrix}$$

## Exposant d'un polynôme

▷ On suppose ici que  $\mathbb{K} = \mathbb{F}_q$  est un corps fini.

$(u_n)_{n \in \mathbb{N}}$  est une SRL  $\iff (u_n)_{n \in \mathbb{N}}$  est périodique.

### **Définition :**

$P \in \mathbb{F}_p[X]$  est dit d'exposant  $e$  si  $P$  divise  $X^e - 1$  et si  $P$  ne divise pas  $X^f - 1$  pour  $f \leq e - 1$ .

### **Théorème :**

Si  $P$  est irréductible de degré  $k$  et d'exposant  $e$ , alors  $e$  divise  $p^k - 1$ .

## Application aux codes

Soit  $f$  d'exposant  $e$ . Notons

$$\mathcal{C}(f) := \{u = (u_0, \dots, u_{e-1}, u_0, \dots, u_{e-1}, \dots) / f * u = 0\}.$$

$\mathcal{C}(f)$  est un code cyclique sur  $\mathbb{F}_q$  engendré par  $g(X)$  avec

$$g(X) = \left( \frac{X^e - 1}{\text{pgcd}(f, X^e - 1)} \right)^*.$$

## Action de $M_{\ell,\ell}(\mathbb{F}_q)$ sur $(\mathbb{F}_q^\ell)^\mathbb{N}$

Considérons ici des suites d'éléments de  $\mathbb{A} = \mathbb{F}_q^\ell$ .

Notons  $M = M_{\ell,\ell}[\mathbb{F}_q]$ .

**Structure de  $M[X]$ -module à gauche sur  $\mathbb{A}^\mathbb{N}$  :**

$$M[X] \times \mathbb{A}^\mathbb{N} \longrightarrow \mathbb{A}^\mathbb{N}$$

$$(P(X), V) \longmapsto P * V := \left( \sum_{i=0}^{\deg(P)} p_i v_{n+i} \right)_{n \in \mathbb{N}}$$

où  $P(X) = \sum_{i=0}^{\deg(P)} p_i X^i$ .

# Suites récurrentes linéaires à coefficients matriciels

## **Définition :**

Une suite  $(u_n)_{n \in \mathbb{N}}$  d'éléments de  $\mathbb{F}_q^\ell$  sera dite récurrente linéaire à coefficients matriciels s'il existe  $A_1, \dots, A_h \in M_{\ell, \ell}[\mathbb{F}_q]$  telles que :

$$u_{n+h} = A_1 u_{n+h-1} + \dots + A_h u_n, \forall n \geq 0.$$

## **Mêmes définitions :**

$$\text{Ann}(E) := \{P \in M[X] / \forall u \in E, P * u = 0\}$$

$$\Omega(f) := \{u \in (\mathbb{F}_q^\ell)^\mathbb{N} / f * u = 0\}.$$

## Résultats principaux

Soit  $(u_n)_{n \in \mathbb{N}}$  une SRL de polynôme caractéristique

$$P(X) = \sum_{i=0}^h A_i X^i. \text{ Alors :}$$

$$G = \begin{pmatrix} 0 & I_\ell & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & I_\ell \\ -A_0 & -A_1 & \cdots & -A_{h-1} \end{pmatrix} \text{ vérifie :}$$

$$\begin{pmatrix} u_n \\ \vdots \\ u_{n+h-1} \end{pmatrix} = G^n \begin{pmatrix} u_0 \\ \vdots \\ u_{h-1} \end{pmatrix}.$$

## Polynôme caractéristique

**Proposition :** Le polynôme caractéristique de  $G$  est donné par la formule :

$$\det(XI_{h\ell} - G) = \det\left(X^h I_\ell + \sum_{i=0}^{h-1} X^i A_i\right).$$

Exemple :  $\ell = 2, h = 3$  sur  $\mathbb{F}_2$

$$\det \left( \begin{pmatrix} X & & & & & \\ & X & & & & \\ & & X & & & \\ & & & X & & \\ & & & & X & \\ & & & & & X \end{pmatrix} - \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \right)$$

$$= \det \begin{pmatrix} X^3 + X^2 + X + 1 & & \\ X^2 + X + 1 & & \\ & X^3 + X^2 + X + 1 & \\ & & 1 \end{pmatrix}$$

***Théorème :***

*Soient  $u \in (\mathbb{F}_q^\ell)^\mathbb{N}$  et  $U(X) \in \mathbb{F}_q^\ell[[X]]$  sa série génératrice.  
 $u$  est une SRL  $\iff U(X)$  est une fraction rationnelle*

***Remarques :***

- $U(X) = \frac{R(X)}{Q(X)}$  avec  $R(X) \in \mathbb{F}_q^\ell[X]$  et  $Q(X) \in M[X]$  avec  $\deg(R) < \deg(Q)$  et  $Q(0)$  inversible.
- $Q(X) * U(X) = R(X)$

## Application aux codes

Soit  $f \in M[X]$  réversible. Alors, il existe  $e \in \mathbb{N}^*$  tel que :

$$f \text{ divise } X^e - 1.$$

Notons  $\mathcal{C}(f) := \{u = (u_0, \dots, u_{e-1}, u_0, \dots, u_{e-1}, \dots) / f * u = 0\}$ .

$\mathcal{C}(f)$  est un code cyclique sur  $\mathbb{F}_q^\ell$

# Codes quasi-cycliques

Soit  $n = m\ell$ . On considère l'identification :

$$\begin{aligned} \phi : \quad & \mathbb{F}_q^{n=m\ell} \longrightarrow (\mathbb{F}_q^\ell)^m =: \mathbb{A}^m \\ & (c_0, \dots, c_{n-1}) \longmapsto ((c_0, \dots, c_{\ell-1}), \dots, (c_{(m-1)\ell}, \dots, c_{n-1})) \end{aligned}$$

$C \subset \mathbb{F}_q^{m\ell}$  est  $\ell$ -quasi-cyclique  $\iff \phi(C) \subset (\mathbb{F}_q^\ell)^m$  est cyclique.

Soit  $M := M_{\ell, \ell}(\mathbb{F}_q)$ .

Structure de  $M[X]$  module à gauche :

$$M[X] \times \mathbb{A}^{\mathbb{N}} \longrightarrow \mathbb{A}^{\mathbb{N}}$$

$$(P(X), V) \longmapsto P * V := \left( \sum_{i=0}^{\deg(P)} p_i v_{n+i} \right)_{n \in \mathbb{N}}$$

$$M[X] \times \mathbb{A}^m \longrightarrow \mathbb{A}^m$$

$$(P(X), c) \longmapsto P * c := \left( \sum_{i=0}^{\deg(P)} p_i c_{(n+i \bmod m)} \right)_{n=0, \dots, m-1}$$

où  $P(X) = \sum_{i=0}^{\deg(P)} p_i X^i$ ,  $V = (v_n)_{n \in \mathbb{N}}$  et  $c = (c_0, \dots, c_{m-1})$ .

## (Re)-Définition :

Soient  $f \in M[X]/\langle X^m - 1 \rangle$  et  $C$  un  $\mathbb{F}_q$ -ss-e.v. de  $\mathbb{A}^m$ .

On note :

- $\Omega(f) := \{x \in \mathbb{A}^m / f * x = 0\}$  ( $\mathbb{F}_q$ -espace vectoriel).
- $Ann(C) := \{P \in M[X]/\langle X^m - 1 \rangle / P * c = 0, \forall c \in C\}$   
(idéal à gauche de  $M[X]/\langle X^m - 1 \rangle$ ).

## Résultats principaux



- $M[X]$  est non commutatif.
- $\text{Ann}(C)$  peut contenir un polynôme de degré minimal non réversible.

### ▷ Résultats négatifs :

- $\text{Ann}(C)$  n'est pas forcément principal.
- En général,  $\Omega(\text{Ann}(C)) \neq C$ .

## Résultats principaux

### ▷ Résultats positifs :

Dans cette section, on considère  $f, Q \in M[X]/\langle X^m - 1 \rangle$  réversibles tels que  $fQ = X^m - 1$ .

$$\dim_{\mathbb{F}_q}(\Omega(f)) = \ell \deg(f).$$

→ Réponse impulsionnelle.

$$\text{Ann}(\Omega(f)) = \langle f \rangle.$$

→  $\text{Ann}(\Omega(f))$  ne contient pas de polynôme de degré inférieur à  $\deg(f)$ .

## Résultats principaux

### Proposition :

$$\Omega(f) = Q * \mathbb{A}^m.$$

- $(Q * e_{i,j})_{i=0,\dots,\deg(f)-1, j=0,\dots,l-1}$  est une famille libre.
- dimension.

### Théorème :

$$\Omega(f)^\perp = \Omega({}^t Q^*).$$

- proposition précédente.
- étaler les calculs...

Codes cycliques :  $X^n - 1 = g(X)h(X)$ ,  $\langle g(X) \rangle^\perp = \langle h^*(X) \rangle$ .

# Conclusion

- SRL classiques :
  - Action de polynômes à coefficients **scalaires**.
  - Polynôme caractéristique.
  - Fraction rationnelle.
  - Exposant.
- SRL à coefficients matriciels :
  - Action de polynômes à coefficients **matriciels**.
  - Polynôme caractéristique.
  - Fraction rationnelle (**dans un autre sens**).
  - Exposant.
- Codes quasi-cycliques :
  - Cas particulier des SRL à coefficients matriciels.
  - Anneau non commutatif → certains problèmes.
  - Caractérisation du dual de  $\Omega(f)$ .