TP10 : Invariants de similitudes et LFSR

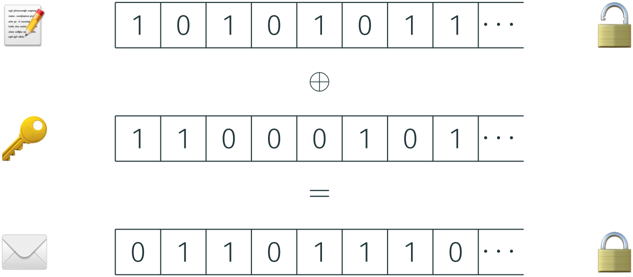
Résumé du TP

Bertrand Meyer

4 mai 2020

Contexte cryptographique

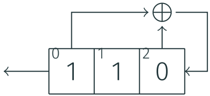
Mécanisme :



Besoin crucial :
Une suite chiffrante aléatoire en apparence mais facile à convenir.

L'ingrédient : le LFSR

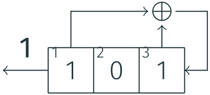
Dispositif électronique qui crache des bits.



L’ingrédient : le LFSR

Dispositif électronique qui crache des bits.

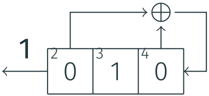
Étape 0



L'ingrédient : le LFSR

Dispositif électronique qui crache des bits.

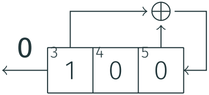
Étape 1



L'ingrédient : le LFSR

Dispositif électronique qui crache des bits.

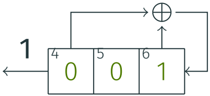
Étape 2



L’ingrédient : le LFSR

Dispositif électronique qui crache des bits.

Étape 3



Contenu des registres

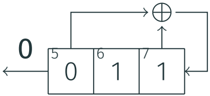
$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}^4} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

- 🤔 La suite produite est géométrique : $\rightarrow$ puissance de matrice.

L’ingrédient : le LFSR

Dispositif électronique qui crache des bits.

Étape 4



Polynôme de connexion $\chi = x^3 + x^2 + 1$

Contenu des registres

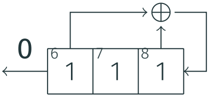
$$\begin{pmatrix}0\\1\\1\end{pmatrix} = \underbrace{\begin{pmatrix}0&1&0\\0&0&1\\1&0&1\end{pmatrix}^5}_{\text{Transposée de la matrice compagnon de } \chi} \begin{pmatrix}1\\1\\0\end{pmatrix}$$

- 🤔 La suite produite est géométrique : $\rightarrow$ puissance de matrice.

L’ingrédient : le LFSR

Dispositif électronique qui crache des bits.

Étape 5



Polynôme de connexion $\chi = x^3 + x^2 + 1$

$$[\ 1\ 1\ 0\ 1\ 0\ \mathbf{0}\ 1\,]^{\infty}$$

Contenu des registres

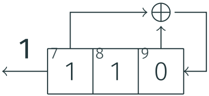
$$\begin{pmatrix}1\\1\\1\end{pmatrix} = \underbrace{\begin{pmatrix}0 & 1 & 0\\0 & 0 & 1\\1 & 0 & 1\end{pmatrix}^{6}}_{\substack{\text{Transposée de la matrice}\\ \text{compagnon de } \chi}} \begin{pmatrix}1\\1\\0\end{pmatrix}$$

- 🤔 La suite produite est géométrique : $\rightarrow$ puissance de matrice.
- 🌠 Période longue souhaitée : polynôme primitif de $\mathbb{F}_2[x]$

L’ingrédient : le LFSR

Dispositif électronique qui crache des bits.

Étape 6



Polynôme de connexion $\chi = x^3 + x^2 + 1$

$[\ 1\ 1\ 0\ 1\ 0\ 0\ \mathbf{1}]^\infty$

Contenu des registres

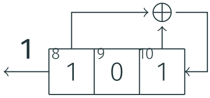
$$\begin{pmatrix}1\\1\\0\end{pmatrix} = \underbrace{\begin{pmatrix}0&1&0\\0&0&1\\1&0&1\end{pmatrix}^7}_{\text{Transposée de la matrice compagnon de } \chi} \begin{pmatrix}1\\1\\0\end{pmatrix}$$

- 🤔 La suite produite est géométrique : $\rightarrow$ puissance de matrice.
- 🌠 Période longue souhaitée : polynôme primitif de $\mathbb{F}_2[x]$

L’ingrédient : le LFSR

Dispositif électronique qui crache des bits.

Étape 7



Polynôme de connexion $\chi = x^3 + x^2 + 1$

$$[\ \mathbf{1}\ 1\ 0\ 1\ 0\ 0\ 1]^\infty$$

Contenu des registres

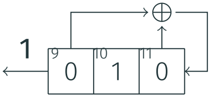
$$\begin{pmatrix}1\\0\\1\end{pmatrix} = \underbrace{\begin{pmatrix}0 & 1 & 0\\0 & 0 & 1\\1 & 0 & 1\end{pmatrix}^8}_{\text{Transposée de la matrice compagnon de } \chi} \begin{pmatrix}1\\1\\0\end{pmatrix}$$

- 🤔 La suite produite est géométrique : $\rightarrow$ puissance de matrice.
- 🌠 Période longue souhaitée : polynôme primitif de $\mathbb{F}_2[x]$

L'ingrédient : le LFSR

Dispositif électronique qui crache des bits.

Étape 8



Polynôme de connexion $\chi = x^3 + x^2 + 1$

$[\ 1\ \mathbf{1}\ 0\ 1\ 0\ 0\ 1]^{\infty}$

Contenu des registres

$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}^{9}}_{\text{Transposée de la matrice compagnon de } \chi} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

- 🤔 La suite produite est géométrique : $\rightarrow$ puissance de matrice.
- 🌠 Période longue souhaitée : polynôme primitif de $\mathbb{F}_2[x]$
- ⚠️ Un LFSR seul est facilement prévisible : $\rightarrow$ algorithme de Berlekamp-Massey

Réduction des endomorphismes

Décompositions de modules

Décomposition d'un A-module

Un module de type fini sur un anneau principal A est toujours de la forme

$$\underbrace{A^r}_{\text{partie libre}} \oplus \underbrace{A/d_1A \oplus A/d_2A \oplus \cdots \oplus A/d_sA}_{\text{partie de torsion}}$$

avec $d_1 | d_2$, $d_2 | d_3$, …et $d_{s-1} | d_s$.

Composantes p-primaires

On peut extraire de chaque A/d_iA la partie de d_i puissance de p (p premier).

Exemple

Un module sur $\mathbb{Z}$

$$\mathbb{Z}/5\mathbb{Z} \quad \oplus \quad \mathbb{Z}/10\mathbb{Z} \quad \oplus \quad \mathbb{Z}/150\mathbb{Z}$$

Exemple

Un module sur $\mathbb{Z}$

$$\begin{array}{cccccc} & \mathbb{Z}/5\mathbb{Z} & \oplus & \mathbb{Z}/10\mathbb{Z} & \oplus & \mathbb{Z}/150\mathbb{Z} \\ = & (\mathbb{Z}/5\mathbb{Z}) & \oplus & (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}) & \oplus & (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}3\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}) \end{array}$$

Exemple

Un module sur $\mathbb{Z}$

$$
\begin{array}{lcccccc}
 & \mathbb{Z}/5\mathbb{Z} & \oplus & \mathbb{Z}/10\mathbb{Z} & \oplus & \mathbb{Z}/150\mathbb{Z} \\
= & (\mathbb{Z}/5\mathbb{Z}) & \oplus & (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}) & \oplus & (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}3\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}) \\
= & \underbrace{(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})}_{\text{composante 2-primaire}} & \oplus & \underbrace{(\mathbb{Z}/3\mathbb{Z})}_{\text{composante 3-primaire}} & \oplus & \underbrace{(\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5^2\mathbb{Z})}_{\text{composante 5-primaire}}
\end{array}
$$

Exemple
Un module sur $\mathbb{Z}$

$$
\begin{array}{cccccc}
 & \mathbb{Z}/5\mathbb{Z} & \oplus & \mathbb{Z}/10\mathbb{Z} & \oplus & \mathbb{Z}/150\mathbb{Z} \\
= & (\mathbb{Z}/5\mathbb{Z}) & \oplus & (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}) & \oplus & (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}3\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}) \\
= & \underbrace{(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})}_{\text{composante 2-primaire}} & \oplus & \underbrace{(\mathbb{Z}/3\mathbb{Z})}_{\text{composante 3-primaire}} & \oplus & \underbrace{(\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5^2\mathbb{Z})}_{\text{composante 5-primaire}}
\end{array}
$$

Composante 2-primaire de type $(1, 1)$

Composante 3-primaire de type (1)

Composante 5-primaire de type $(1, 1, 2)$

Soit $\mathbf{u}$ un endomorphisme de $\mathbb{K}^n$.

Exemple

$$\mathbf{u} = \begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix}$$

Polynômes d'endomorphisme

Soit $\mathbf{u}$ un endomorphisme de $\mathbb{K}^n$.

On peut former des polynômes en $\mathbf{u}$

Exemple

$$\mathbf{u} = \begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix}$$

$$\mathbf{u}^3 - 2\mathbf{u} - 6 = \begin{pmatrix} 7 & -16 \\ 16 & -9 \end{pmatrix}$$

Soit $\mathbf{u}$ un endomorphisme de $\mathbb{K}^n$.

On peut former des polynômes en $\mathbf{u}$ et définir une multiplication

$$\cdot : \mathbb{K}[x] \times \mathbb{K}^n \to \mathbb{K}^n.$$

Exemple

$$\mathbf{u} = \begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix}$$

$$\mathbf{u}^3 - 2\mathbf{u} - 6 = \begin{pmatrix} 7 & -16 \\ 16 & -9 \end{pmatrix}$$

$$\begin{aligned} \left(x^3 - 2x - 6\right) \cdot \begin{pmatrix} 5 \\ -2 \end{pmatrix} &= \begin{pmatrix} 7 & -16 \\ 16 & -9 \end{pmatrix} \begin{pmatrix} 5 \\ -2 \end{pmatrix} \\ &= \begin{pmatrix} 67 \\ 98 \end{pmatrix} \end{aligned}$$

Soit $\mathbf{u}$ un endomorphisme de $\mathbb{K}^n$.

On peut former des polynômes en $\mathbf{u}$ et définir une multiplication

$$\cdot : \mathbb{K}[x] \times \mathbb{K}^n \to \mathbb{K}^n.$$

On voit désormais $\mathbb{K}^n$ comme un $\mathbb{K}[x]$-module.

Exemple

$$\mathbf{u} = \begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix}$$

$$\mathbf{u}^3 - 2\mathbf{u} - 6 = \begin{pmatrix} 7 & -16 \\ 16 & -9 \end{pmatrix}$$

$$\begin{aligned} \left(x^3 - 2x - 6\right) \cdot \begin{pmatrix} 5 \\ -2 \end{pmatrix} &= \begin{pmatrix} 7 & -16 \\ 16 & -9 \end{pmatrix} \begin{pmatrix} 5 \\ -2 \end{pmatrix} \\ &= \begin{pmatrix} 67 \\ 98 \end{pmatrix} \end{aligned}$$

Lemme :
En tant que $\mathbb{K}[x]$-module, $\mathbb{K}^n$ coïncide avec

$$\mathbb{K}^n \simeq \mathbb{K}[x]^n / \mathrm{Im}(\mathbf{u} - x \cdot \mathbf{I}).$$

Invariants de similitude

Lemme :
En tant que $\mathbb{K}[x]$-module, $\mathbb{K}^n$ coïncide avec

$$\mathbb{K}^n \simeq \mathbb{K}[x]^n/\mathrm{Im}(\mathbf{u} - x \cdot \mathbf{I}).$$

C'est un module de torsion :

$$\mathbb{K}[x]/p_1 \oplus \mathbb{K}[x]/p_2 \oplus \cdots \oplus \mathbb{K}[x]/p_s \text{ avec } p_1|p_2|\cdots|p_s \in \mathbb{K}[x].$$

Invariants de similitude

Lemme :
En tant que $\mathbb{K}[x]$-module, $\mathbb{K}^n$ coïncide avec

$$\mathbb{K}^n \simeq \mathbb{K}[x]^n / \mathrm{Im}(\mathbf{u} - x \cdot \mathbf{I}).$$

C'est un module de torsion :

$$\mathbb{K}[x]/p_1 \oplus \mathbb{K}[x]/p_2 \oplus \cdots \oplus \mathbb{K}[x]/p_s \text{ avec } p_1 | p_2 | \cdots | p_s \in \mathbb{K}[x].$$

Les $(p_i)_{i \leq s}$ s'appellent les invariants de similitudes.

Invariants de similitude

Lemme :
En tant que $\mathbb{K}[x]$-module, $\mathbb{K}^n$ coïncide avec

$$\mathbb{K}^n \simeq \mathbb{K}[x]^n / \mathrm{Im}(\mathbf{u} - x \cdot \mathbf{I}).$$

C'est un module de torsion :

$$\mathbb{K}[x]/p_1 \oplus \mathbb{K}[x]/p_2 \oplus \cdots \oplus \mathbb{K}[x]/p_s \text{ avec } p_1 | p_2 | \cdots | p_s \in \mathbb{K}[x].$$

Les $(p_i)_{i \leq s}$ s'appellent les invariants de similitudes.

- On peut calculer les $(p_i)_{i \leq s}$ par forme normale de Smith.

Invariants de similitude

Lemme :
En tant que $\mathbb{K}[x]$-module, $\mathbb{K}^n$ coïncide avec

$$\mathbb{K}^n \simeq \mathbb{K}[x]^n / \mathrm{Im}(\mathbf{u} - x \cdot \mathbf{I}).$$

C'est un module de torsion :

$$\mathbb{K}[x]/p_1 \oplus \mathbb{K}[x]/p_2 \oplus \cdots \oplus \mathbb{K}[x]/p_s \text{ avec } p_1 | p_2 | \cdots | p_s \in \mathbb{K}[x].$$

Les $(p_i)_{i \leq s}$ s'appellent les invariants de similitudes.

- On peut calculer les $(p_i)_{i \leq s}$ par forme normale de Smith.
- p_s est le polynôme minimal $\pi_{\mathbf{u}}$ de $\mathbf{u}$.

Invariants de similitude

Lemme :
En tant que $\mathbb{K}[x]$-module, $\mathbb{K}^n$ coïncide avec

$$\mathbb{K}^n \simeq \mathbb{K}[x]^n / \mathrm{Im}(\mathbf{u} - x \cdot \mathbf{I}).$$

C'est un module de torsion :

$$\mathbb{K}[x]/p_1 \oplus \mathbb{K}[x]/p_2 \oplus \cdots \oplus \mathbb{K}[x]/p_s \text{ avec } p_1 | p_2 | \cdots | p_s \in \mathbb{K}[x].$$

Les $(p_i)_{i \leq s}$ s'appellent les invariants de similitudes.

- On peut calculer les $(p_i)_{i \leq s}$ par forme normale de Smith.
- p_s est le polynôme minimal $\pi_{\mathbf{u}}$ de $\mathbf{u}$.
- $p_1 p_2 \cdots p_s$ est le polynôme caractéristique $\chi_{\mathbf{u}}$ de $\mathbf{u}$.

Invariants de similitude

Lemme :
En tant que $\mathbb{K}[x]$-module, $\mathbb{K}^n$ coïncide avec

$$\mathbb{K}^n \simeq \mathbb{K}[x]^n / \mathrm{Im}(\mathbf{u} - x \cdot \mathbf{I}).$$

C'est un module de torsion :

$$\mathbb{K}[x]/p_1 \oplus \mathbb{K}[x]/p_2 \oplus \cdots \oplus \mathbb{K}[x]/p_s \text{ avec } p_1 | p_2 | \cdots | p_s \in \mathbb{K}[x].$$

Les $(p_i)_{i \leq s}$ s'appellent les invariants de similitudes.

- On peut calculer les $(p_i)_{i \leq s}$ par forme normale de Smith.
- p_s est le polynôme minimal $\pi_{\mathbf{u}}$ de $\mathbf{u}$.
- $p_1 p_2 \cdots p_s$ est le polynôme caractéristique $\chi_{\mathbf{u}}$ de $\mathbf{u}$.
- Les deux polynômes annulent $\mathbf{u}$.

Décomposition de Frobenius

Dans une base adaptée à la somme directe

$$\mathbb{K}^n \simeq \mathbb{K}[x]/p_1 \oplus \mathbb{K}[x]/p_2 \oplus \cdots \oplus \mathbb{K}[x]/p_s,$$

l'endomorphisme **u** admet pour matrice

$$\left(\begin{array}{c|c|c|c} \mathsf{C}(p_1) & 0 & \cdots & 0 \\ \hline 0 & \mathsf{C}(p_2) & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & 0 \\ \hline 0 & \cdots & 0 & \mathsf{C}(p_s) \end{array}\right),$$

dite forme de Frobenius.

Dans une base adaptée à la somme directe

$$\mathbb{K}^n \simeq \mathbb{K}[x]/p_1 \oplus \mathbb{K}[x]/p_2 \oplus \cdots \oplus \mathbb{K}[x]/p_s,$$

l'endomorphisme **u** admet pour matrice

$$\left(\begin{array}{c|c|c|c}
\mathsf{C}(p_1) & 0 & \cdots & 0 \\ \hline
0 & \mathsf{C}(p_2) & \ddots & \vdots \\ \hline
\vdots & \ddots & \ddots & 0 \\ \hline
0 & \cdots & 0 & \mathsf{C}(p_s)
\end{array}\right),$$

dite forme de Frobenius.

Un endomorphisme est dit cyclique si $s = 1$.

Blocs de Jordan

On appelle bloc de Jordan la matrice

$$J_{\lambda,k} = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \lambda & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix} \in \mathbb{K}^{k\times k}$$

- $J_{\lambda,k}$ n'est pas diagonalisable si $k > 1$,
- Polynôme caractéristique $\chi_{J_{\lambda,k}}(x) = (x-\lambda)^k$,
- Polynôme minimal $\pi_{J_{\lambda,k}}(x) = (x-\lambda)^k$.
- les puissances de $J_{\lambda,k}$ se calculent facilement.

Il existe une base de $\mathbb{K}^n$ dans laquelle la matrice de u est diagonale par bloc

$$\left(\begin{array}{cccc|ccc|c|ccc}
J_{\lambda_{1},n_{1,1}} & & & & & & & & & & \\
 & J_{\lambda_{1},n_{2,1}} & & & & & & & & & \\
 & & \ddots & & & & & & & & \\
 & & & J_{\lambda_{1},n_{s,1}} & & & & & & & \\ \hline
 & & & & J_{\lambda_{2},n_{1,2}} & & & & & & \\
 & & & & & \ddots & & & & & \\
 & & & & & & J_{\lambda_{2},n_{s,2}} & & & & \\ \hline
 & & & & & & & \ddots & & & \\ \hline
 & & & & & & & & J_{\lambda_{k},n_{1,k}} & & \\
 & & & & & & & & & \ddots & \\
 & & & & & & & & & & J_{\lambda_{k},n_{s,k}}
\end{array}\right)$$

où λ_j est racine du polynôme p_i d'ordre $n_{i,j}$.

La composante $(x-\lambda_j)$-primaire de $\mathbb{K}^n$ est de type $(n_{1,j}, n_{2,j}, \ldots, n_{s,j})$.

Conséquences

- La décomposition de Jordan généralise la diagonalisation,
- Elle fonctionne toujours.
- u est diagonalisable
  ssi π_u n'a que des racines simples
  ssi tous les blocs de Jordan sont de taille 1.

Exemple détaillé (présentation du cas)

Soit $\mathbf{u}$ l'endomorphisme de ${\mathbb{F}_7}^{12}$ de matrice

$$[\mathsf{u}]_{\mathcal{B}} = \begin{pmatrix} 3 & 6 & 1 & 6 & 1 & 3 & 6 & 3 & 1 & 6 & 2 & 0 \\ 1 & 3 & 5 & 6 & 4 & 2 & 6 & 4 & 0 & 3 & 3 & 6 \\ 0 & 2 & 3 & 0 & 3 & 3 & 6 & 0 & 0 & 2 & 6 & 1 \\ 5 & 1 & 2 & 6 & 0 & 1 & 4 & 6 & 0 & 0 & 4 & 0 \\ 5 & 2 & 5 & 2 & 2 & 5 & 0 & 4 & 1 & 1 & 1 & 6 \\ 3 & 5 & 0 & 1 & 1 & 0 & 1 & 6 & 6 & 3 & 6 & 5 \\ 4 & 2 & 1 & 1 & 6 & 4 & 1 & 5 & 1 & 0 & 6 & 5 \\ 5 & 1 & 2 & 5 & 1 & 1 & 4 & 0 & 4 & 1 & 0 & 1 \\ 0 & 2 & 2 & 0 & 6 & 6 & 5 & 4 & 5 & 4 & 0 & 0 \\ 1 & 3 & 1 & 1 & 1 & 1 & 4 & 1 & 4 & 5 & 5 & 4 \\ 0 & 6 & 4 & 5 & 1 & 4 & 2 & 6 & 3 & 5 & 3 & 2 \\ 3 & 3 & 0 & 1 & 4 & 1 & 0 & 5 & 2 & 3 & 5 & 5 \end{pmatrix} \in {\mathbb{F}_7}^{12 \times 12}$$

dans la base canonique $\mathcal{B}$ de ${\mathbb{F}_7}^{12}$.

Exemple détaillé

On met $[\mathbf{u}]_{\mathcal{B}} - x \cdot \mathbf{I} \in \mathbb{F}_7[x]^{12\times 12}$ sous forme normale de Smith

$$\begin{pmatrix}
3-x & 6 & 1 & 6 & 1 & 3 & 6 & 3 & 1 & 6 & 2 & 0 \\
1 & 3-x & 5 & 6 & 4 & 2 & 6 & 4 & 0 & 3 & 3 & 6 \\
0 & 2 & 3-x & 0 & 3 & 3 & 6 & 0 & 0 & 2 & 6 & 1 \\
5 & 1 & 2 & 6-x & 0 & 1 & 4 & 6 & 0 & 0 & 4 & 0 \\
5 & 2 & 5 & 2 & 2-x & 5 & 0 & 4 & 1 & 1 & 1 & 6 \\
3 & 5 & 0 & 1 & 1 & -x & 1 & 6 & 6 & 3 & 6 & 5 \\
4 & 2 & 1 & 1 & 6 & 4 & 1-x & 5 & 1 & 0 & 6 & 5 \\
5 & 1 & 2 & 5 & 1 & 1 & 4 & -x & 4 & 1 & 0 & 1 \\
0 & 2 & 2 & 0 & 6 & 6 & 5 & 4 & -x & 4 & 0 & 0 \\
1 & 3 & 1 & 1 & 1 & 1 & 4 & 1 & 4 & 5-x & 5 & 4 \\
0 & 6 & 4 & 5 & 1 & 4 & 2 & 6 & 3 & 5 & 3-x & 2 \\
3 & 3 & 0 & 1 & 4 & 1 & 0 & 5 & 2 & 3 & 5 & 5-x
\end{pmatrix} \in \mathbb{F}_7[x]^{12\times 12}$$

Exemple détaillé (forme normale de Smith)

On obtient la forme normale de Smith $\Delta \in \mathbb{F}_7[x]^{12\times 12}$ de $[\mathbf{u}]_{\mathcal{B}} - x \cdot \mathbf{I}$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^2+3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^4+2x^3+2x^2+6x+4 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^6+4x^5+5x^4+x^3+2x+3
\end{pmatrix}$$

Exemple détaillé (forme normale de Smith)

On obtient la forme normale de Smith $\Delta \in \mathbb{F}_7[x]^{12\times 12}$ de $[\mathbf{u}]_{\mathcal{B}} - x \cdot \mathbf{I}$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^2+3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^4+2x^3+2x^2+6x+4 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^6+4x^5+5x^4+x^3+2x+3
\end{pmatrix}$$

et les invariants de similitude

$$p_1 = x^2 + 3 \in \mathbb{F}_7[x],$$

Exemple détaillé (forme normale de Smith)

On obtient la forme normale de Smith $\Delta \in \mathbb{F}_7[x]^{12\times 12}$ de $[\mathbf{u}]_{\mathcal{B}} - x \cdot \mathbf{I}$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^2+3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^4+2x^3+2x^2+6x+4 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^6+4x^5+5x^4+x^3+2x+3
\end{pmatrix}$$

et les invariants de similitude

$$\begin{aligned}
p_1 &= x^2+3 \in \mathbb{F}_7[x], \\
p_2 &= x^4+2x^3+2x^2+6x+4 \in \mathbb{F}_7[x],
\end{aligned}$$

Exemple détaillé (forme normale de Smith)

On obtient la forme normale de Smith $\Delta \in \mathbb{F}_7[x]^{12\times 12}$ de $[\mathbf{u}]_{\mathcal{B}} - x \cdot \mathbf{I}$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^2 + 3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^4 + 2x^3 + 2x^2 + 6x + 4 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^6 + 4x^5 + 5x^4 + x^3 + 2x + 3
\end{pmatrix}$$

et les invariants de similitude

$$\begin{aligned}
p_1 &= x^2 + 3 \in \mathbb{F}_7[x], \\
p_2 &= x^4 + 2x^3 + 2x^2 + 6x + 4 \in \mathbb{F}_7[x], \\
p_3 &= x^6 + 4x^5 + 5x^4 + x^3 + 2x + 3 \in \mathbb{F}_7[x].
\end{aligned}$$

Exemple détaillé (forme normale de Smith)

On obtient la forme normale de Smith $\Delta \in \mathbb{F}_7[x]^{12\times 12}$ de $[\mathbf{u}]_{\mathcal{B}} - x \cdot \mathbf{I}$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^2+3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^4+2x^3+2x^2+6x+4 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^6+4x^5+5x^4+x^3+2x+3
\end{pmatrix}$$

et les invariants de similitude

$$\begin{aligned}
p_1 &= x^2+3 \in \mathbb{F}_7[x], \\
p_2 &= x^4+2x^3+2x^2+6x+4 \in \mathbb{F}_7[x], \\
p_3 &= x^6+4x^5+5x^4+x^3+2x+3 \in \mathbb{F}_7[x].
\end{aligned}$$

Notez que $p_1 | p_2$ et que $p_2 | p_3$.

Exemple détaillé (décomposition de Frobenius)

Il existe une base $\mathcal{F}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de l'endomorphisme u prend la forme, dite de Frobenius,

$$[\mathsf{u}]_{\mathcal{F}} = \left(\begin{array}{c|c|c} & & \\ \hline & & \\ \hline & & \end{array}\right) \in {\mathbb{F}_7}^{12\times 12},$$

Exemple détaillé (décomposition de Frobenius)

Il existe une base $\mathcal{F}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de l'endomorphisme $\mathbf{u}$ prend la forme, dite de Frobenius,

$$[\mathrm{u}]_{\mathcal{F}} = \left(\begin{array}{cc|c|c} 0 & 4 & & \\ 1 & 0 & & \\ \hline & & & \\ & & & \\ \hline & & & \\ & & & \end{array}\right) \in {\mathbb{F}_7}^{12 \times 12},$$

compte tenu des trois polynômes

$$p_1 \quad = \quad x^2 - 4,$$

et leur matrice compagnon.

Exemple détaillé (décomposition de Frobenius)

Il existe une base $\mathcal{F}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de l'endomorphisme $\mathbf{u}$ prend la forme, dite de Frobenius,

$$[\mathrm{u}]_{\mathcal{F}} = \left(\begin{array}{cc|cccc|c} 0 & 4 & & & & & \\ 1 & 0 & & & & & \\ \hline & & 0 & 0 & 0 & 3 & \\ & & 1 & 0 & 0 & 1 & \\ & & 0 & 1 & 0 & 5 & \\ & & 0 & 0 & 1 & 5 & \\ \hline & & & & & & \\ & & & & & & \\ & & & & & & \end{array}\right) \in {\mathbb{F}_7}^{12\times 12},$$

compte tenu des trois polynômes

$$\begin{aligned} p_1 &= x^2 - 4, \\ p_2 &= x^4 - (5x^3 + 5x^2 + x + 3), \end{aligned}$$

et leur matrice compagnon.

Exemple détaillé (décomposition de Frobenius)

Il existe une base $\mathcal{F}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de l'endomorphisme $\mathbf{u}$ prend la forme, dite de Frobenius,

$$[\mathrm{u}]_{\mathcal{F}} = \left(\begin{array}{cc|cccc|cccccc}
0 & 4 & & & & & & & & & & \\
1 & 0 & & & & & & & & & & \\
\hline
 & & 0 & 0 & 0 & 3 & & & & & & \\
 & & 1 & 0 & 0 & 1 & & & & & & \\
 & & 0 & 1 & 0 & 5 & & & & & & \\
 & & 0 & 0 & 1 & 5 & & & & & & \\
\hline
 & & & & & & 0 & 0 & 0 & 0 & 0 & 4 \\
 & & & & & & 1 & 0 & 0 & 0 & 0 & 5 \\
 & & & & & & 0 & 1 & 0 & 0 & 0 & 0 \\
 & & & & & & 0 & 0 & 1 & 0 & 0 & 6 \\
 & & & & & & 0 & 0 & 0 & 1 & 0 & 2 \\
 & & & & & & 0 & 0 & 0 & 0 & 1 & 3
\end{array}\right) \in {\mathbb{F}_7}^{12\times 12},$$

compte tenu des trois polynômes

$$\begin{aligned}
p_1 &= x^2 - 4, \\
p_2 &= x^4 - (5x^3 + 5x^2 + x + 3), \\
p_3 &= x^6 - (3x^5 + 2x^4 + 6x^3 + 5x + 4),
\end{aligned}$$

et leur matrice compagnon.

Exemple détaillé (décomposition de Frobenius)

Il existe une base $\mathcal{F}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de l'endomorphisme $\mathbf{u}$ prend la forme, dite de Frobenius,

$$[\mathrm{u}]_{\mathcal{F}} = \left(\begin{array}{cc|cccc|cccccc} 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 5 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 \end{array}\right) \in {\mathbb{F}_7}^{12\times 12},$$

compte tenu des trois polynômes

$$\begin{aligned} p_1 &= x^2 - 4, \\ p_2 &= x^4 - (5x^3 + 5x^2 + x + 3), \\ p_3 &= x^6 - (3x^5 + 2x^4 + 6x^3 + 5x + 4), \end{aligned}$$

et leur matrice compagnon.

Exemple détaillé (décomposition de Jordan)

Après factorisation des invariants de similitude,

$$\begin{aligned} p_1 &= (x-2)(x-5) \\ p_2 &= (x-2)^2(x-3)(x-5) \\ p_3 &= (x-2)^3(x-3)^2(x-5). \end{aligned}$$

il existe une base $\mathcal{J}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de u prend la forme, dite de Jordan,

$$[\mathrm{u}]_{\mathcal{J}} = \left(\begin{array}{c|c|c|c|c|c|c|c} & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \end{array}\right) \in {\mathbb{F}_7}^{12\times 12}.$$

Exemple détaillé (décomposition de Jordan)

Après factorisation des invariants de similitude,

$$\begin{aligned} p_1 &= (x-2)(x-5) \\ p_2 &= (x-2)^2(x-3)(x-5) \\ p_3 &= (x-2)^3(x-3)^2(x-5). \end{aligned}$$

il existe une base $\mathcal{J}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de **u** prend la forme, dite de Jordan,

$$[\mathbf{u}]_{\mathcal{J}} = \begin{pmatrix} 2 & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \end{pmatrix} \in {\mathbb{F}_7}^{12\times 12}.$$

Exemple détaillé (décomposition de Jordan)

Après factorisation des invariants de similitude,

$$\begin{aligned} p_1 &= (x-2)(x-5) \\ p_2 &= (x-2)^2(x-3)(x-5) \\ p_3 &= (x-2)^3(x-3)^2(x-5). \end{aligned}$$

il existe une base $\mathcal{J}$ de $\mathbb{F}_7{}^{12}$ telle que la matrice de $\mathbf{u}$ prend la forme, dite de Jordan,

$$[\mathrm{u}]_{\mathcal{J}} = \left(\begin{array}{c|cc|ccc|c|cc|c|c|c}
2 & & & & & & & & & & & \\ \hline
 & 2 & 1 & & & & & & & & & \\
 & 0 & 2 & & & & & & & & & \\ \hline
 & & & & & & & & & & & \\
 & & & & & & & & & & & \\
 & & & & & & & & & & & \\ \hline
 & & & & & & & & & & & \\ \hline
 & & & & & & & & & & & \\
 & & & & & & & & & & & \\ \hline
 & & & & & & & & & & & \\ \hline
 & & & & & & & & & & & \\ \hline
 & & & & & & & & & & &
\end{array}\right) \in \mathbb{F}_7{}^{12\times 12}.$$

Exemple détaillé (décomposition de Jordan)

Après factorisation des invariants de similitude,

$$\begin{aligned} p_1 &= (x-2)(x-5) \\ p_2 &= (x-2)^2(x-3)(x-5) \\ p_3 &= (x-2)^3(x-3)^2(x-5). \end{aligned}$$

il existe une base $\mathcal{J}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de u prend la forme, dite de Jordan,

$$[\mathsf{u}]_{\mathcal{J}} = \left(\begin{array}{c|cc|ccc|c|cc|c|c|c} 2 & & & & & & & & & & & \\ \hline & 2 & 1 & & & & & & & & & \\ & 0 & 2 & & & & & & & & & \\ \hline & & & 2 & 1 & 0 & & & & & & \\ & & & 0 & 2 & 1 & & & & & & \\ & & & 0 & 0 & 2 & & & & & & \\ \hline & & & & & & & & & & & \\ \hline & & & & & & & & & & & \\ & & & & & & & & & & & \\ \hline & & & & & & & & & & & \\ \hline & & & & & & & & & & & \\ \hline & & & & & & & & & & & \end{array}\right) \in {\mathbb{F}_7}^{12\times 12}.$$

Après factorisation des invariants de similitude,

$$\begin{aligned} p_1 &= (x-2)(x-5) \\ p_2 &= (x-2)^2(x-3)(x-5) \\ p_3 &= (x-2)^3(x-3)^2(x-5). \end{aligned}$$

il existe une base $\mathcal{J}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de u prend la forme, dite de Jordan,

$$[\mathsf{u}]_{\mathcal{J}} = \left(\begin{array}{c|cc|ccc|c|cc|c|c|c} 2 & & & & & & & & & & & \\ \hline & 2 & 1 & & & & & & & & & \\ & 0 & 2 & & & & & & & & & \\ \hline & & & 2 & 1 & 0 & & & & & & \\ & & & 0 & 2 & 1 & & & & & & \\ & & & 0 & 0 & 2 & & & & & & \\ \hline & & & & & & 3 & & & & & \\ \hline & & & & & & & & & & & \\ & & & & & & & & & & & \\ \hline & & & & & & & & & & & \\ \hline & & & & & & & & & & & \\ \hline & & & & & & & & & & & \end{array}\right) \in {\mathbb{F}_7}^{12\times 12}.$$

Après factorisation des invariants de similitude,

$$
\begin{aligned}
p_1 &= (x-2)(x-5) \\
p_2 &= (x-2)^2(x-3)(x-5) \\
p_3 &= (x-2)^3(x-3)^2(x-5).
\end{aligned}
$$

il existe une base $\mathcal{J}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de $\mathbf{u}$ prend la forme, dite de Jordan,

$$
[\mathrm{u}]_{\mathcal{J}} = \left(\begin{array}{c|cc|ccc|c|cc|c|c|c}
2 & & & & & & & & & & & \\ \hline
 & 2 & 1 & & & & & & & & & \\
 & 0 & 2 & & & & & & & & & \\ \hline
 & & & 2 & 1 & 0 & & & & & & \\
 & & & 0 & 2 & 1 & & & & & & \\
 & & & 0 & 0 & 2 & & & & & & \\ \hline
 & & & & & & 3 & & & & & \\ \hline
 & & & & & & & 3 & 1 & & & \\
 & & & & & & & 0 & 3 & & & \\ \hline
 & & & & & & & & & & & \\ \hline
 & & & & & & & & & & & \\ \hline
 & & & & & & & & & & &
\end{array}\right) \in {\mathbb{F}_7}^{12\times 12}.
$$

Exemple détaillé (décomposition de Jordan)

Après factorisation des invariants de similitude,

$$\begin{aligned} p_1 &= (x-2)(x-5) \\ p_2 &= (x-2)^2(x-3)(x-5) \\ p_3 &= (x-2)^3(x-3)^2(x-5). \end{aligned}$$

il existe une base $\mathcal{J}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de u prend la forme, dite de Jordan,

$$[\mathrm{u}]_{\mathcal{J}} = \left(\begin{array}{c|cc|ccc|c|cc|c|c|c}
2 & & & & & & & & & & & \\ \hline
 & 2 & 1 & & & & & & & & & \\
 & 0 & 2 & & & & & & & & & \\ \hline
 & & & 2 & 1 & 0 & & & & & & \\
 & & & 0 & 2 & 1 & & & & & & \\
 & & & 0 & 0 & 2 & & & & & & \\ \hline
 & & & & & & 3 & & & & & \\ \hline
 & & & & & & & 3 & 1 & & & \\
 & & & & & & & 0 & 3 & & & \\ \hline
 & & & & & & & & & 5 & & \\ \hline
 & & & & & & & & & & & \\ \hline
 & & & & & & & & & & &
\end{array}\right) \in {\mathbb{F}_7}^{12\times 12}.$$

Exemple détaillé (décomposition de Jordan)

Après factorisation des invariants de similitude,

$$
\begin{aligned}
p_1 &= (x-2)(x-5)\\
p_2 &= (x-2)^2(x-3)(x-5)\\
p_3 &= (x-2)^3(x-3)^2(x-5).
\end{aligned}
$$

il existe une base $\mathcal{J}$ de ${\mathbb{F}_7}^{12}$ telle que la matrice de u prend la forme, dite de Jordan,

$$
[\mathrm{u}]_{\mathcal{J}} = \left(\begin{array}{c|cc|ccc|c|cc|c|c|c}
2 & & & & & & & & & & & \\ \hline
 & 2 & 1 & & & & & & & & & \\
 & 0 & 2 & & & & & & & & & \\ \hline
 & & & 2 & 1 & 0 & & & & & & \\
 & & & 0 & 2 & 1 & & & & & & \\
 & & & 0 & 0 & 2 & & & & & & \\ \hline
 & & & & & & 3 & & & & & \\ \hline
 & & & & & & & 3 & 1 & & & \\
 & & & & & & & 0 & 3 & & & \\ \hline
 & & & & & & & & & 5 & & \\ \hline
 & & & & & & & & & & 5 & \\ \hline
 & & & & & & & & & & &
\end{array}\right) \in {\mathbb{F}_7}^{12\times 12}.
$$

Exemple détaillé (décomposition de Jordan)

Après factorisation des invariants de similitude,

$$
\begin{aligned}
p_1 &= (x-2)(x-5)\\
p_2 &= (x-2)^2(x-3)(x-5)\\
p_3 &= (x-2)^3(x-3)^2(x-5).
\end{aligned}
$$

il existe une base $\mathcal{J}$ de $\mathbb{F}_7{}^{12}$ telle que la matrice de **u** prend la forme, dite de Jordan,

$$
[\mathrm{u}]_{\mathcal{J}} = \left(\begin{array}{c|cc|ccc|c|cc|c|c|c}
2 & & & & & & & & & & & \\ \hline
 & 2 & 1 & & & & & & & & & \\
 & 0 & 2 & & & & & & & & & \\ \hline
 & & & 2 & 1 & 0 & & & & & & \\
 & & & 0 & 2 & 1 & & & & & & \\
 & & & 0 & 0 & 2 & & & & & & \\ \hline
 & & & & & & 3 & & & & & \\ \hline
 & & & & & & & 3 & 1 & & & \\
 & & & & & & & 0 & 3 & & & \\ \hline
 & & & & & & & & & 5 & & \\ \hline
 & & & & & & & & & & 5 & \\ \hline
 & & & & & & & & & & & 5
\end{array}\right) \in \mathbb{F}_7{}^{12\times 12}.
$$

Exemple détaillé (décomposition de Jordan)

Après factorisation des invariants de similitude,

$$\begin{aligned} p_1 &= (x-2)(x-5) \\ p_2 &= (x-2)^2(x-3)(x-5) \\ p_3 &= (x-2)^3(x-3)^2(x-5). \end{aligned}$$

il existe une base $\mathcal{J}$ de $\mathbb{F}_7{}^{12}$ telle que la matrice de **u** prend la forme, dite de Jordan,

$$[\mathrm{u}]_{\mathcal{J}} = \left(\begin{array}{c|cc|ccc|c|cc|c|c|c}
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5
\end{array}\right) \in \mathbb{F}_7{}^{12\times 12}.$$

Notons que **u** n'est pas diagonalisable.

Exemple détaillé

Le polynôme minimal π_{u} de l'endomorphisme u est

$$\begin{aligned}\pi_{\mathsf{u}} = p_3 &= (x-2)^3(x-3)^2(x-5)\\ &= x^6+4x^5+5x^4+x^3+2x+3.\end{aligned}$$

Exemple détaillé

Le polynôme minimal $\pi_{\mathbf{u}}$ de l'endomorphisme **u** est

$$\begin{aligned}\pi_{\mathbf{u}} = p_3 &= (x-2)^3(x-3)^2(x-5)\\ &= x^6+4x^5+5x^4+x^3+2x+3.\end{aligned}$$

Le polynôme caractéristique $\chi_{\mathbf{u}}$ de l'endomorphisme **u** est

$$\begin{aligned}\chi_{\mathbf{u}} = p_1p_2p_3 &= (x-2)^6(x-3)^3(x-5)^3\\ &= x^{12}-x^{11}+4x^{10}+x^9+x^8-x^7-x^6\\ &\qquad +3x^5+5x^4+5x^3+3x^2+x+1.\end{aligned}$$

Exemple détaillé

Le polynôme minimal $\pi_{\mathbf{u}}$ de l'endomorphisme $\mathbf{u}$ est

$$\begin{aligned}\pi_{\mathbf{u}} = p_3 &= (x-2)^3(x-3)^2(x-5)\\ &= x^6+4x^5+5x^4+x^3+2x+3.\end{aligned}$$

Le polynôme caractéristique $\chi_{\mathbf{u}}$ de l'endomorphisme $\mathbf{u}$ est

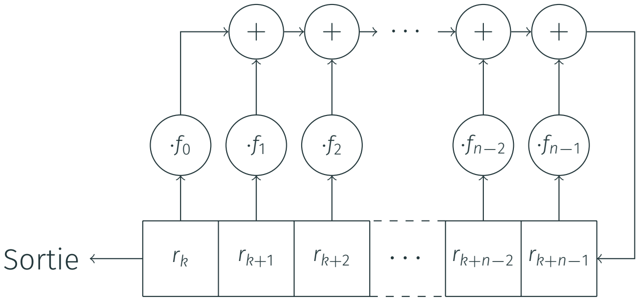
$$\begin{aligned}\chi_{\mathbf{u}} = p_1p_2p_3 &= (x-2)^6(x-3)^3(x-5)^3\\ &= x^{12}-x^{11}+4x^{10}+x^9+x^8-x^7-x^6\\ &\qquad +3x^5+5x^4+5x^3+3x^2+x+1.\end{aligned}$$

${\mathbb{F}_7}^{12}$ vu comme $\mathbb{F}_7[x]$-module admet

- une composante $(x-2)$-primaire de type $(1,2,3)$,
- une composante $(x-3)$-primaire de type $(1,2)$,
- une composante $(x-5)$-primaire de type $(1,1,1)$,

Le fonctionnement d’un LFSR

Le dispositif



produit une suite récurrente linéaire

$$\forall k \in \mathbb{N}, \qquad r_{k+n} = f_0 r_k + f_1 r_{k+1} + \cdots + f_{n-1} r_{k+n-1}$$

déterminée par son germe.

Pour l'étudier

Polynôme caractéristique (ou de rétroaction) :

$$\chi(x) = x^n - f_{n-1}x^{n-1} - \cdots - f_1 x - f_0$$

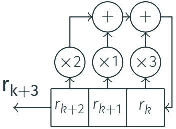
Polynôme de connection :

$$c(x) = x^n \cdot \chi(1/x) = 1 - f_{n-1}x - \cdots - f_1 x^{n-1} - f_0 x^n.$$

Terme général :

$$\begin{pmatrix} r_k \\ r_{k+1} \\ \vdots \\ r_{k+n-1} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 & & \\ 0 & \ddots & \ddots & \\ & & 0 & 1 \\ f_0 & f_1 & & f_{n-1} \end{pmatrix}^k}_{\text{C : transposée de la matrice compagnon de } \chi} \begin{pmatrix} r_0 \\ r_1 \\ \vdots \\ r_{n-1} \end{pmatrix}$$

Exemple



Dans $\mathbb{F}_5$

Polynôme caractéristique $\chi = x^3 + 2x^2 + 4x + 3 \in \mathbb{F}_5[x]$

Polynôme de connection $c = 3x^3 + 4x^2 + 2x + 1 \in \mathbb{F}_5[x]$

Suite vectorielle géométrique :

$$\begin{pmatrix} r_{k+1} \\ r_{k+2} \\ r_{k+3} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 1 & 3 \end{pmatrix}}_{C} \begin{pmatrix} r_k \\ r_{k+1} \\ r_{k+2} \end{pmatrix}.$$

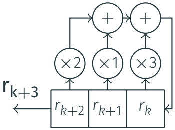
Calcul explicite

Par un calcul de puissance sur la forme de Jordan de $\mathbf{C}$, la suite $(r_k)_{k\in\mathbb{N}}$ est une combinaison linéaire des suites

$$\left(k^d\lambda^k\right)_{k\in\mathbb{N}}$$

où λ est racine de χ et d est strictement inférieur à la multiplicité de λ comme racine de χ.

Exemple



Dans $\mathbb{F}_5$

Polynôme caractéristique $\chi = x^3 + 2x^2 + 4x + 3 \in \mathbb{F}_5[x]$

Les racines de χ sont 1, 3 et 4. La matrice **C** a pour forme de Jordan

$$J = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

La suite $(r_k)_{k\in\mathbb{N}}$ est une combinaison linéaire des suites

$$(1)_{k\in\mathbb{N}}, \quad \left(3^k\right)_{k\in\mathbb{N}}, \quad \left((-1)^k\right)_{k\in\mathbb{N}}.$$

Période

Périodicité des polynômes de $\mathbb{F}_q[X]$

L'ordre multiplicatif de la matrice C est un multiple de la période de la suite $(r_k)_{k\in\mathbb{N}}$, puisque

$$(r_{k+i})_{i<n} = \mathsf{C}^k \, (r_{k+i})_{i<n} \, .$$

Périodicité des polynômes de $\mathbb{F}_q[x]$

L'ordre multiplicatif de la matrice C est un multiple de la période de la suite $(r_k)_{k\in\mathbb{N}}$, puisque

$$(r_{k+i})_{i<n} = \mathsf{C}^k\,(r_{k+i})_{i<n}\,.$$

Comme la matrice $\mathsf{C}^\top$ est aussi la matrice de la multiplication par x dans $\mathbb{F}_q[x]/\langle\chi\rangle$, l'ordre de C égale le plus petit entier t tel que $x^t \equiv 1 \mod \chi$ (ou encore période de χ).

L'ordre multiplicatif de la matrice C est un multiple de la période de la suite $(r_k)_{k\in\mathbb{N}}$, puisque

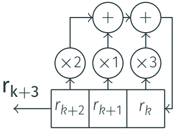
$$(r_{k+i})_{i<n} = \mathsf{C}^k \, (r_{k+i})_{i<n} \, .$$

Comme la matrice $\mathsf{C}^\top$ est aussi la matrice de la multiplication par x dans $\mathbb{F}_q[x]/\langle\chi\rangle$, l'ordre de C égale le plus petit entier t tel que $x^t \equiv 1 \mod \chi$ (ou encore période de χ).

Cas optimal

Le polynôme χ de degré n de $\mathbb{F}_q[x]$ est primitif; sa période est $q^n - 1$. Il est également irréductible (*cf.* cours sur les corps finis).

Exemple



Dans $\mathbb{F}_5$

Polynôme caractéristique $\chi = x^3 + 2x^2 + 4x + 3 \in \mathbb{F}_5[x]$

$$\mathsf{C} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \mathsf{J} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

L'ordre de C est 4 : facile à voir sur sa forme de Jordan J que $\mathsf{J}, \mathsf{J}^2, \mathsf{J}^3 \neq \mathsf{I}$ mais $\mathsf{J}^4 = \mathsf{I}$.

La période de χ est 4 car $x, x^2, x^3 \not\equiv 1 \mod \chi$ mais $x^4 \equiv 1 \mod \chi$.

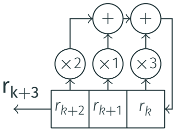
Le polynôme χ n'est pas primitif car son ordre n'est pas 124.

La période du polynôme caractéristique χ peut être atteinte comme période du LFSR grâce un bon choix du germe. On peut d’ailleurs décrire entièrement l’ensemble des périodes obtenues (voir notes).

Cas intéressant pour la cryptographie

Un LFSR produit une suite de période maximale si et seulement si son polynôme caractéristique χ est primitif et le germe est non nul.

Exemple



Dans $\mathbb{F}_5$

Polynôme caractéristique $\chi = (x-1)(x+1)(x-2) \in \mathbb{F}_5[x]$

$C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 1 & 3 \end{pmatrix}$ d'ordre 4

Le LFSR produit des suites de période :

- 1 par exemple avec germe 000, 111, $\lambda\lambda\lambda$. (5 possibilités)
- 2 par exemple avec germe 101, $\lambda\mu\lambda$. (2×5 possibilités)
- 4 par exemple avec germe 033, $\lambda\mu\nu$ avec $\lambda \neq \nu$. (4×25 possibilités).

On peut résumer par la notation

$$5(1) \oplus 5(2) \oplus 25(4).$$

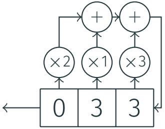
Ce LFSR n'est pas maximal.

L’algorithme de Berlekamp-Massey

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

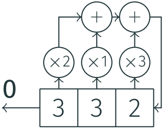
$R(x) =$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

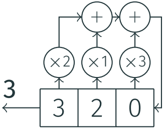
$R(x) = \mathbf{0}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0														

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x$

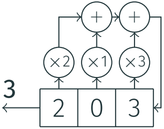
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3													

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x + 3x^2$

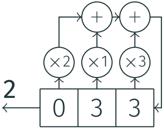
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3												

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x + 3x^2 + 2x^3$

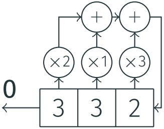
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2											

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x + 3x^2 + 2x^3 + \mathbf{0}x^4$

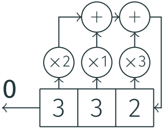
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0										

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x + 3x^2 + 2x^3 + 3x^5$

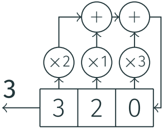
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0	3									

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x + 3x^2 + 2x^3 + 3x^5 + 3x^6$

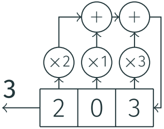
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0	3	3								

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

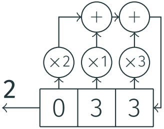
$R(x) = 3x + 3x^2 + 2x^3 + 3x^5 + 3x^6 + 2x^7$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0	3	3	2							

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

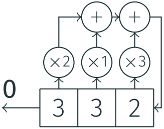
$R(x) = 3x + 3x^2 + 2x^3 + 3x^5 + 3x^6 + 2x^7$**0**

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0	3	3	2	0						

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x + 3x^2 + 2x^3 + 3x^5 + 3x^6 + 2x^7 + 3x^9$

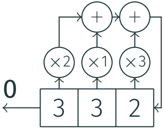
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0	3	3	2	0	3					

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x + 3x^2 + 2x^3 + 3x^5 + 3x^6 + 2x^7 + 3x^9 + 3x^{10}$

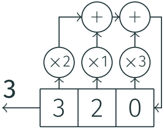
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0	3	3	2	0	3	3				

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x + 3x^2 + 2x^3 + 3x^5 + 3x^6 + 2x^7 + 3x^9 + 3x^{10} + 2x^{11}$

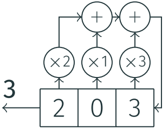
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0	3	3	2	0	3	3	2			

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x + 3x^2 + 2x^3 + 3x^5 + 3x^6 + 2x^7 + 3x^9 + 3x^{10} + 2x^{11} + \mathbf{0}x^{12}$

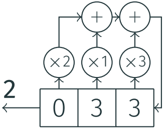
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0	3	3	2	0	3	3	2	0		

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

$R(x) = 3x + 3x^2 + 2x^3 + 3x^5 + 3x^6 + 2x^7 + 3x^9 + 3x^{10} + 2x^{11} + 3x^{13}$

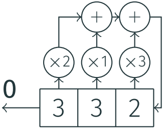
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0	3	3	2	0	3	3	2	0	3	

$R(x)$ possède une infinité de termes, qui encode toute la suite.

Série formelle

Soit la série formelle

$$R(x) = \sum_{k=0}^{\infty} r_k x^k \in \mathbb{F}[[x]]$$



Dans $\mathbb{F}_5$

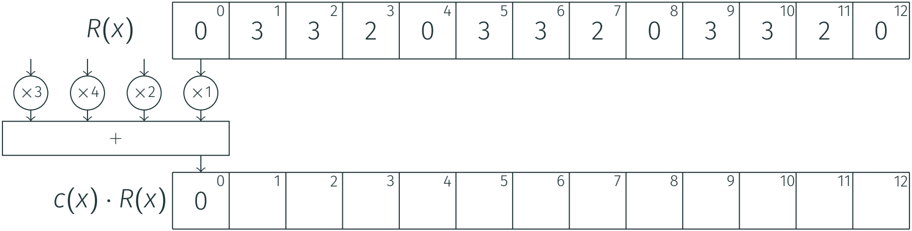
$R(x) = 3x + 3x^2 + 2x^3 + 3x^5 + 3x^6 + 2x^7 + 3x^9 + 3x^{10} + 2x^{11} + 3x^{13} + O(x^{14})$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	3	3	2	0	3	3	2	0	3	3	2	0	3	3

$R(x)$ possède une infinité de termes, qui encode toute la suite.

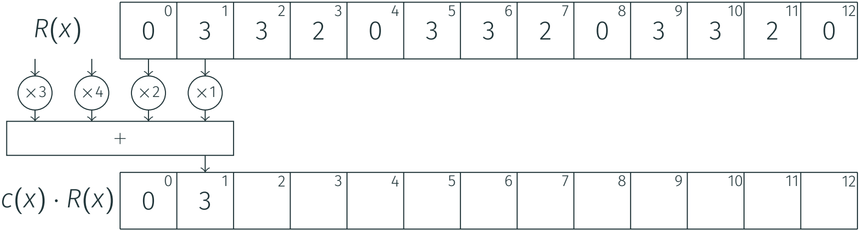
Le polynôme de connection $c(x)$

Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est



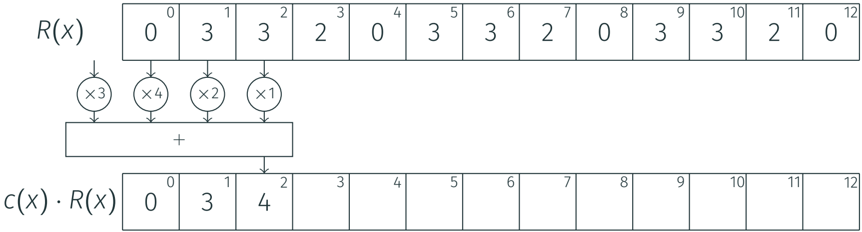
Le polynôme de connection $c(x)$

Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est

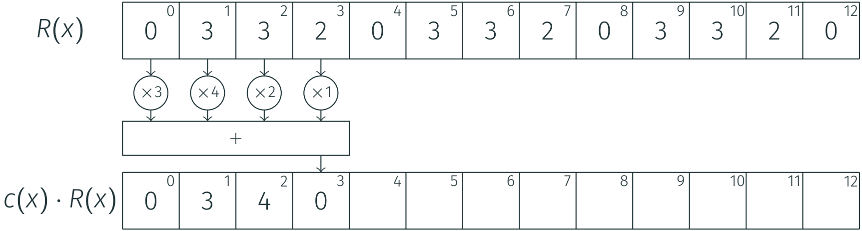


Le polynôme de connection $c(x)$

Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est

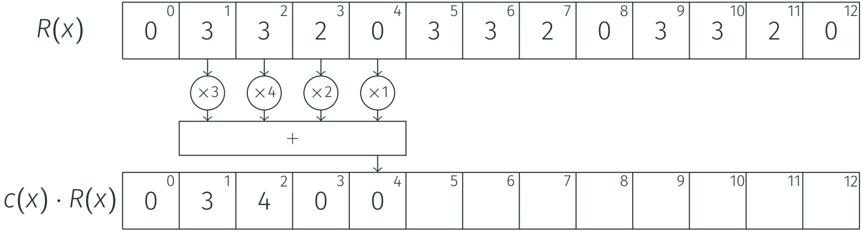


Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est



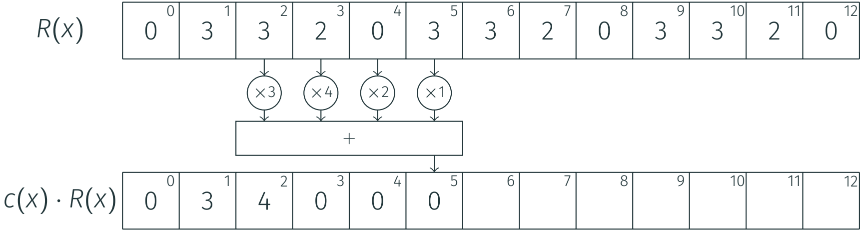
Le polynôme de connection $c(x)$

Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est



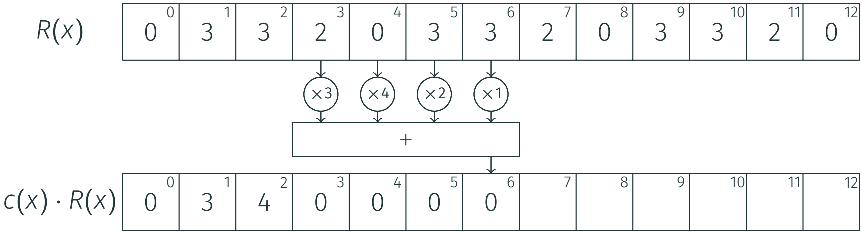
Le polynôme de connection $c(x)$

Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est



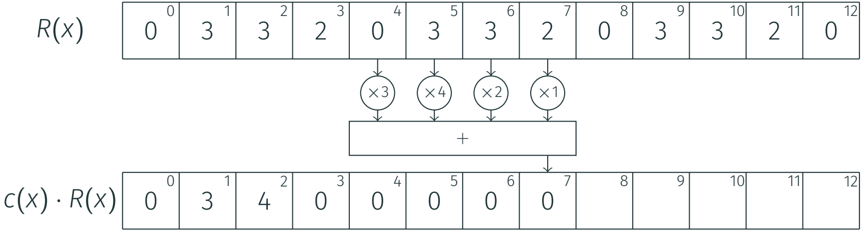
Le polynôme de connection $c(x)$

Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est



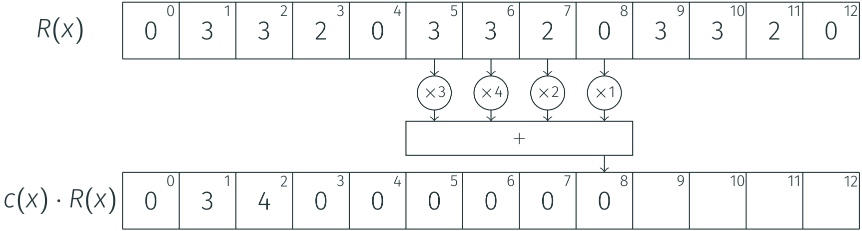
Le polynôme de connection $c(x)$

Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est



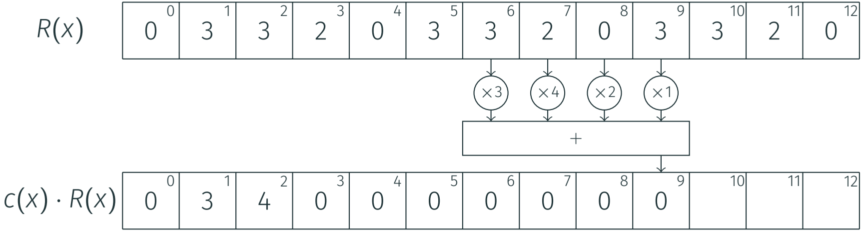
Le polynôme de connection $c(x)$

Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est

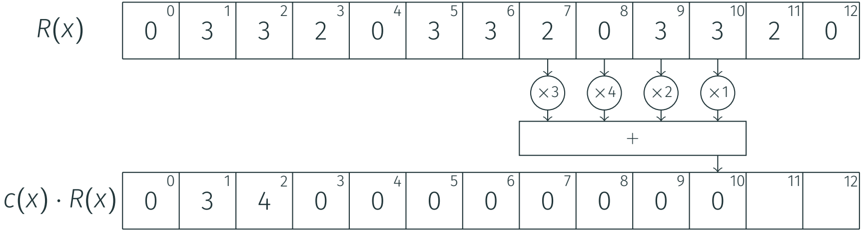


Le polynôme de connection $c(x)$

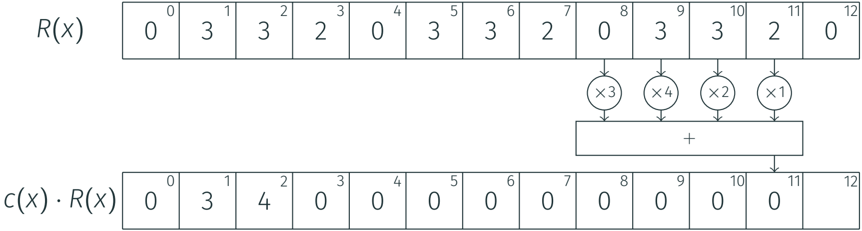
Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est



Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est

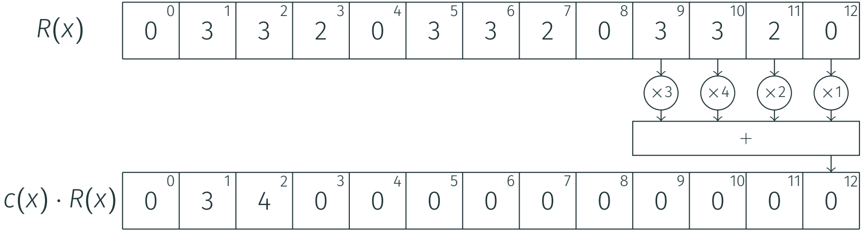


Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est

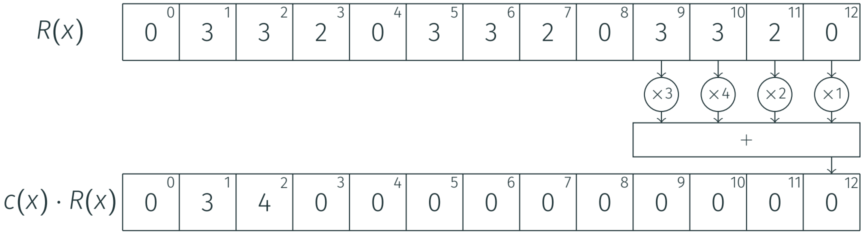


Le polynôme de connection $c(x)$

Le produit $c(x) \cdot R(x)$, où $c(x) = 3x^3 + 4x^2 + 2x + 1$, est

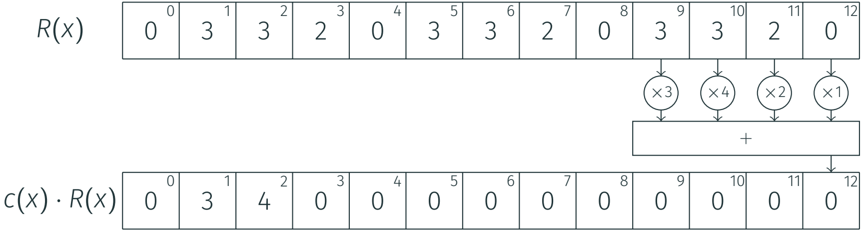


Le produit $c(x) \cdot R(x)$ est un polynôme de degré $< n$.



Le polynôme de connection $c(x)$

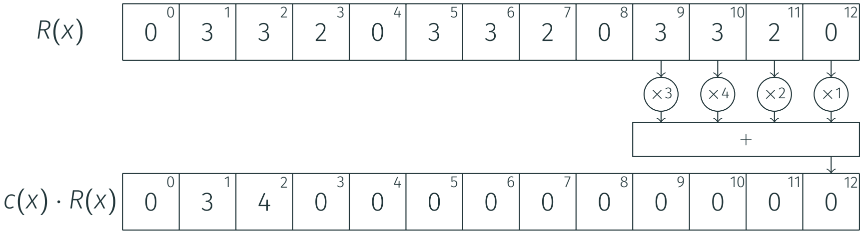
Le produit $c(x) \cdot R(x)$ est un polynôme de degré $< n$.



Donc $R(x)$ est une fraction rationnelle.

$$R(x) = \frac{p(x)}{c(x)} = \frac{4x^2 + 3x}{3x^3 + 4x^2 + 2x + 1}.$$

Le produit $c(x) \cdot R(x)$ est un polynôme de degré $< n$.



Donc $R(x)$ est une fraction rationnelle.

$$R(x) = \frac{p(x)}{c(x)} = \frac{4x^2 + 3x}{3x^3 + 4x^2 + 2x + 1}.$$

Trouver le polynôme de connection $c(x)$ est un problème d'algèbre linéaire à $2n$ inconnues.

Remarque annexe

Une manipulation algébrique fait le lien entre la série formelle et le terme général avec les puissances

$$\begin{aligned}
R(x) &= \frac{4x^2+3x}{3x^3+4x^2+2x+1} \\
&= \frac{2}{1-x}+\frac{1}{1-3x}+\frac{2}{1-4x} \\
&= 2\sum_{k=0}^{\infty} x^k + \sum_{k=0}^{\infty}(3x)^k + 2\sum_{k=0}^{\infty}(4x)^k \\
&= \sum_{k=0}^{\infty}\left(\underbrace{2+3^k+2\cdot(-1)^k}_{r_k}\right)x^k
\end{aligned}$$

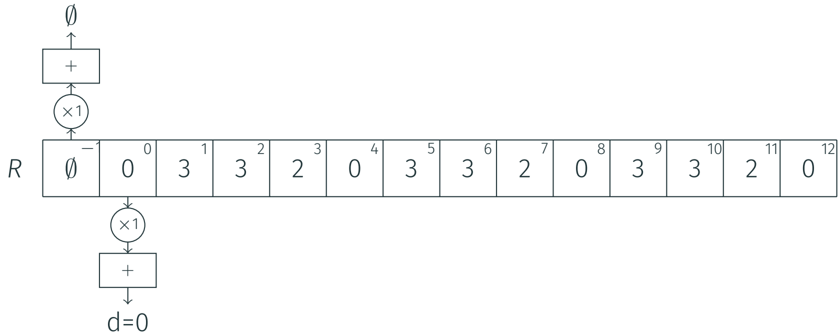
Principe de l’algorithme de Berlekamp-Massey

L’algorithme de Berlekamp-Massey calcule intelligemment le polynôme de connection $c(x)$ à partir de 2n termes consécutifs de la suite.

Au fur et à mesure qu’il lit la suite, il corrige une valeur provisoire du polynôme de connection $c(x)$ en utilisant la dernière occurence non-nulle d’une version antérieure de $c(x)$ (stockée ci-après dans $c^*(x)$).

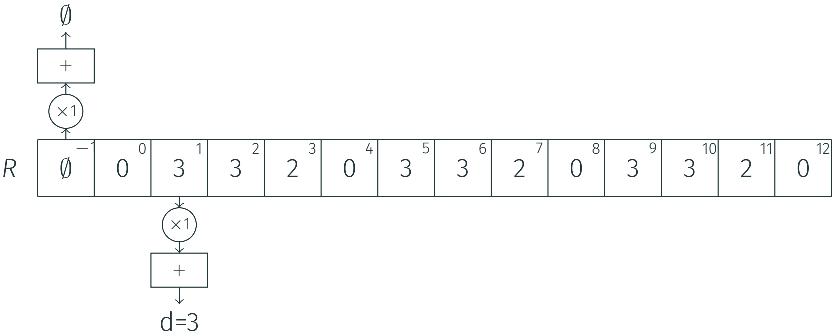
Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 1 \qquad c^*(x) = 1$



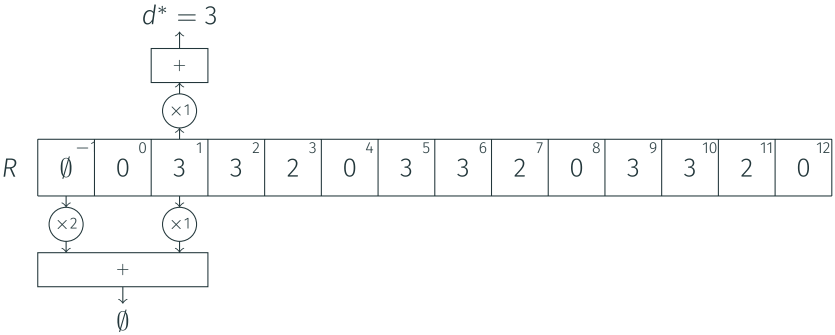
Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 1 \qquad c^*(x) = 1$

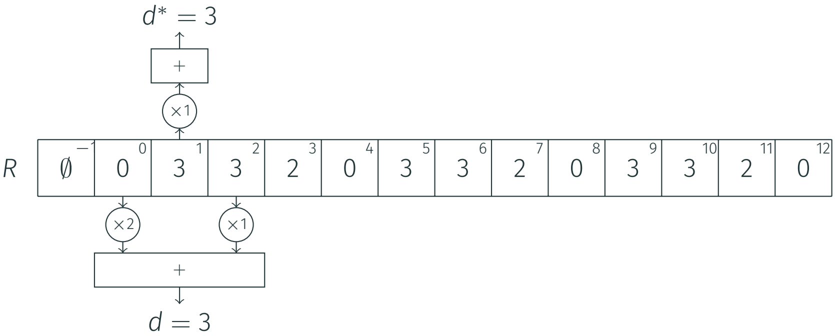


Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 1 - 3x^2 \qquad c^*(x) = 1$

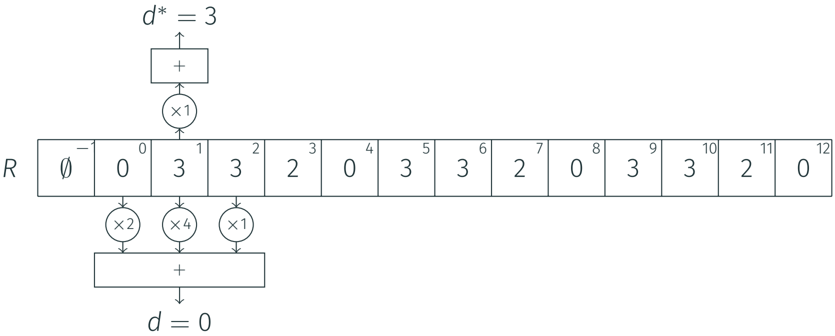


$c(x) = 2x^2 + 1 \qquad c^*(x) = 1$



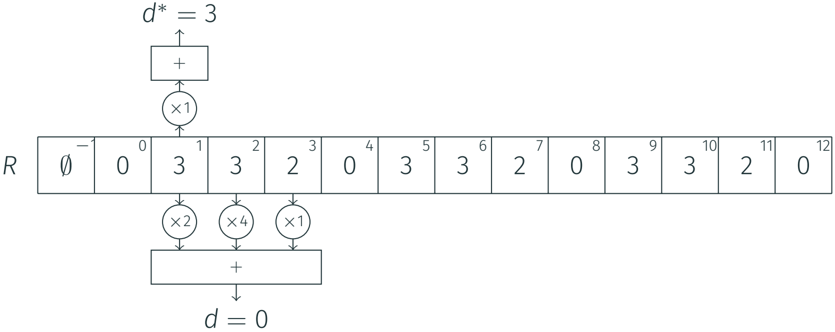
Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 2x^2 + 4x + 1 \qquad c^*(x) = 1$



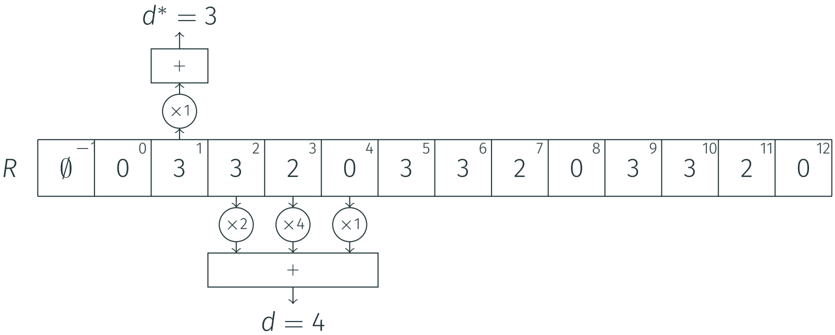
Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 2x^2 + 4x + 1 \qquad c^*(x) = 1$



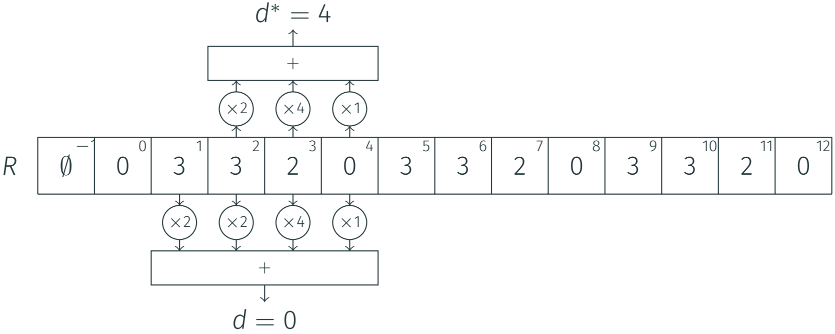
Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 2x^2 + 4x + 1 \qquad c^*(x) = 1$

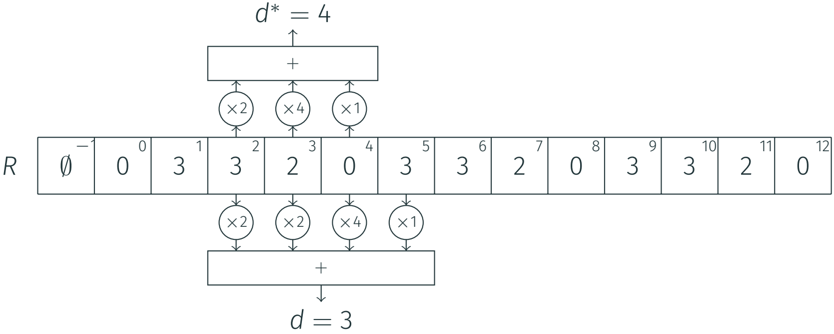


Déroulement de l’algorithme de Berlekamp-Massey

$c(x) = 2x^2 + 4x + 1 - 3x^3 \qquad c^*(x) = 2x^2 + 4x + 1$

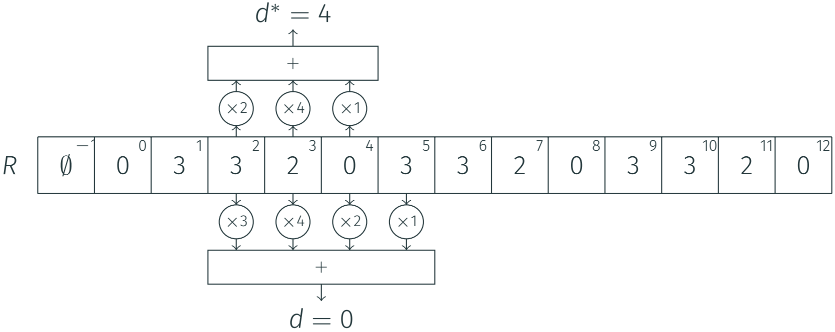


$c(x) = 2x^3 + 2x^2 + 4x + 1 \qquad c^*(x) = 2x^2 + 4x + 1$



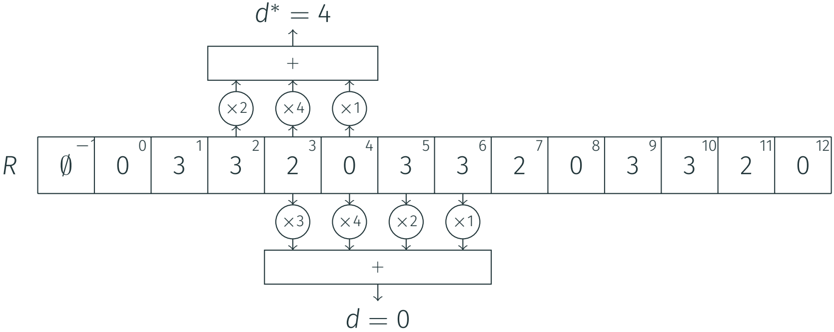
Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 2x^3 + 2x^2 + 4x + 1 - x \cdot (2x^2 + 4x + 1)$ $\qquad$ $c^*(x) = 2x^2 + 4x + 1$



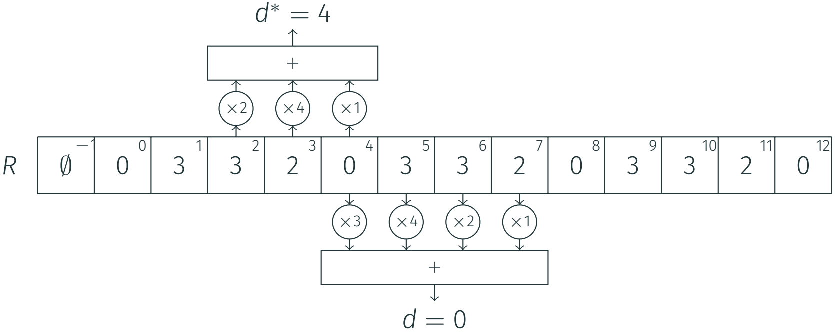
Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 3x^3 + 4x^2 + 2x + 1 \qquad c^*(x) = 2x^2 + 4x + 1$



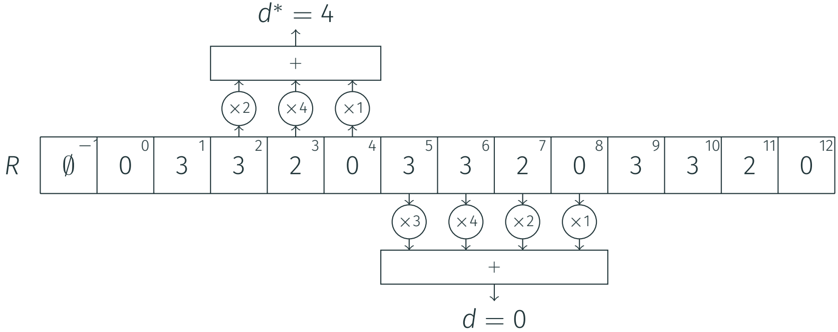
Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 3x^3 + 4x^2 + 2x + 1 \qquad c^*(x) = 2x^2 + 4x + 1$



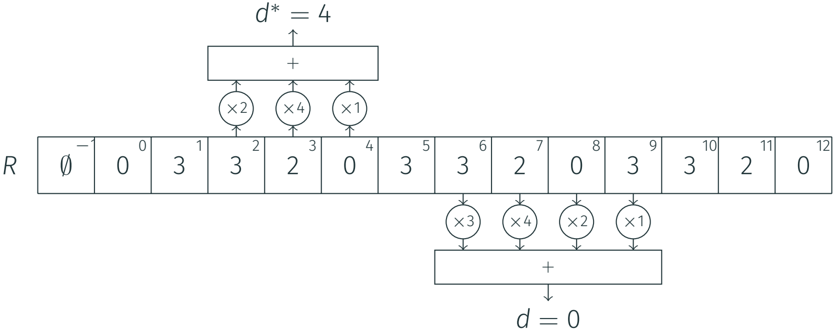
Déroulement de l'algorithme de Berlekamp-Massey

$$c(x) = 3x^3 + 4x^2 + 2x + 1 \qquad c^*(x) = 2x^2 + 4x + 1$$



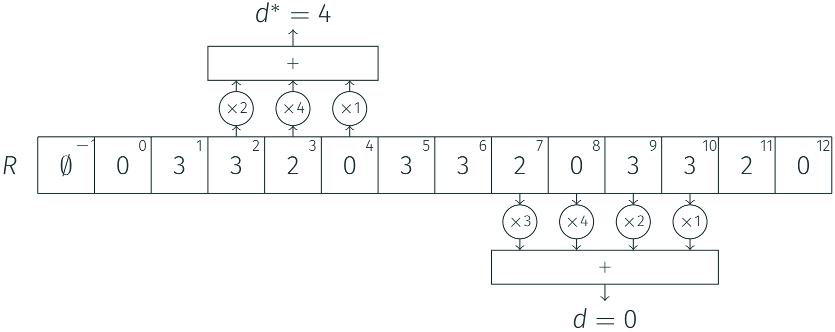
Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 3x^3 + 4x^2 + 2x + 1 \qquad c^*(x) = 2x^2 + 4x + 1$



Déroulement de l'algorithme de Berlekamp-Massey

$c(x) = 3x^3 + 4x^2 + 2x + 1 \qquad c^*(x) = 2x^2 + 4x + 1$



L'algorithme a obtenu le bon polynôme de connection.

Conséquence cryptographique

À cause de Berlekamp Massey, si on utilise des LFSR pour générer une suite pseudo-aléatoire à des fins cryptographique, il est toujours nécessaire de combiner plusieurs LFSR de manière non-linéaire pour obtenir une suite robuste.