Réseaux d'automates additifs

Enrico Formenti, Christophe Papazian, Pierre-Alain Scribot

I3S - MC3

Motivations

Définition

On note $\mathbb{B} = \{0, 1\}$. Un réseau de n automates booléens (RAB) est défini par :

$$F : \mathbb{B}^n \to \mathbb{B}^n$$

Motivations

Définition

On note $\mathbb{B} = \{0, 1\}$. Un réseau de n automates booléens (RAB) est défini par :

$$F : \mathbb{B}^n \to \mathbb{B}^n$$

Exemple

$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$ avec :

$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$

Motivations

Définition

On note $\mathbb{B} = \{0, 1\}$. Un réseau de n automates booléens (RAB) est défini par :

$$F : \mathbb{B}^n \to \mathbb{B}^n$$

Exemple

$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$ avec :

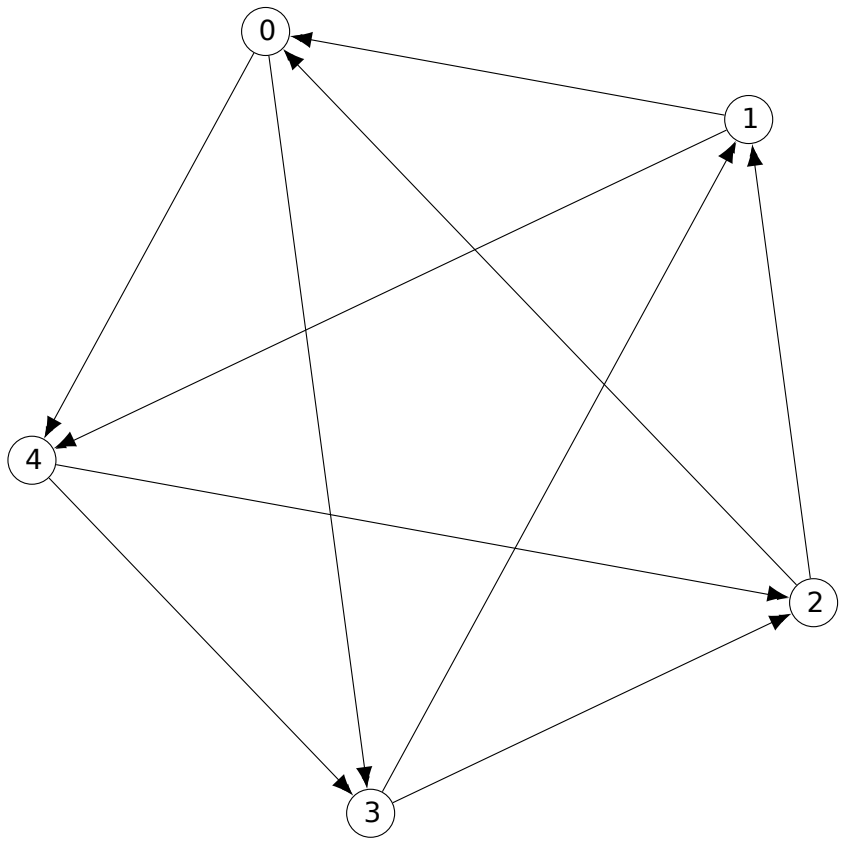
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



Motivations

Définition

On note $\mathbb{B} = \{0, 1\}$. Un réseau de n automates booléens (RAB) est défini par :

$$F : \mathbb{B}^n \to \mathbb{B}^n$$

Exemple

$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$ avec :

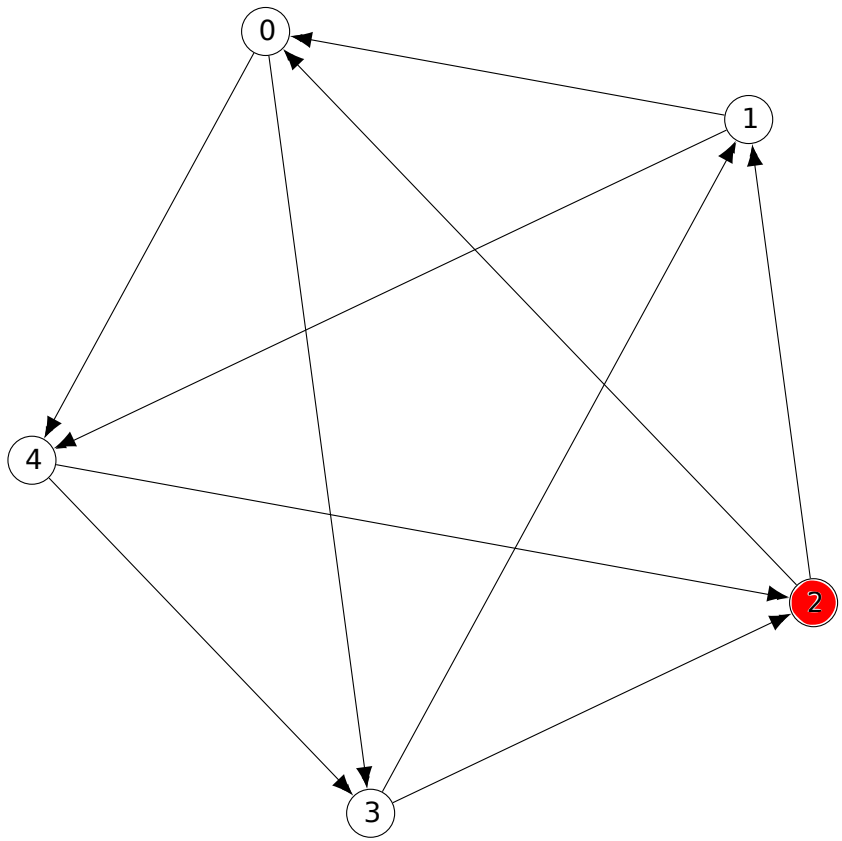
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



Motivations

Définition

On note $\mathbb{B} = \{0, 1\}$. Un réseau de n automates booléens (RAB) est défini par :

$$F : \mathbb{B}^n \to \mathbb{B}^n$$

Exemple

$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$ avec :

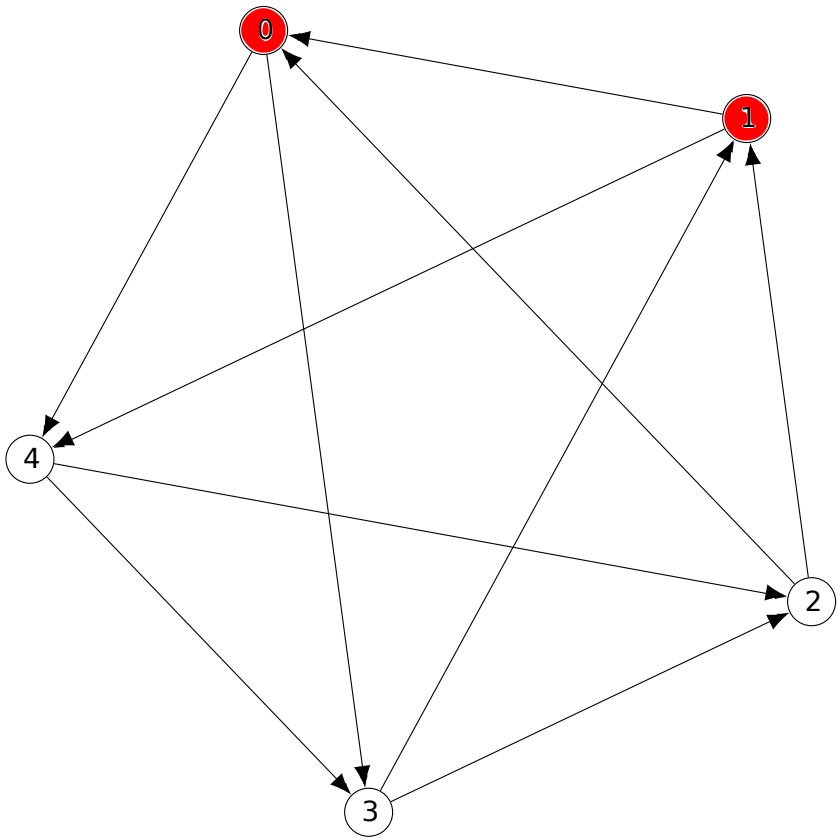
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



Motivations

Définition

On note $\mathbb{B} = \{0, 1\}$. Un réseau de n automates booléens (RAB) est défini par :

$$F : \mathbb{B}^n \to \mathbb{B}^n$$

Exemple

$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$ avec :

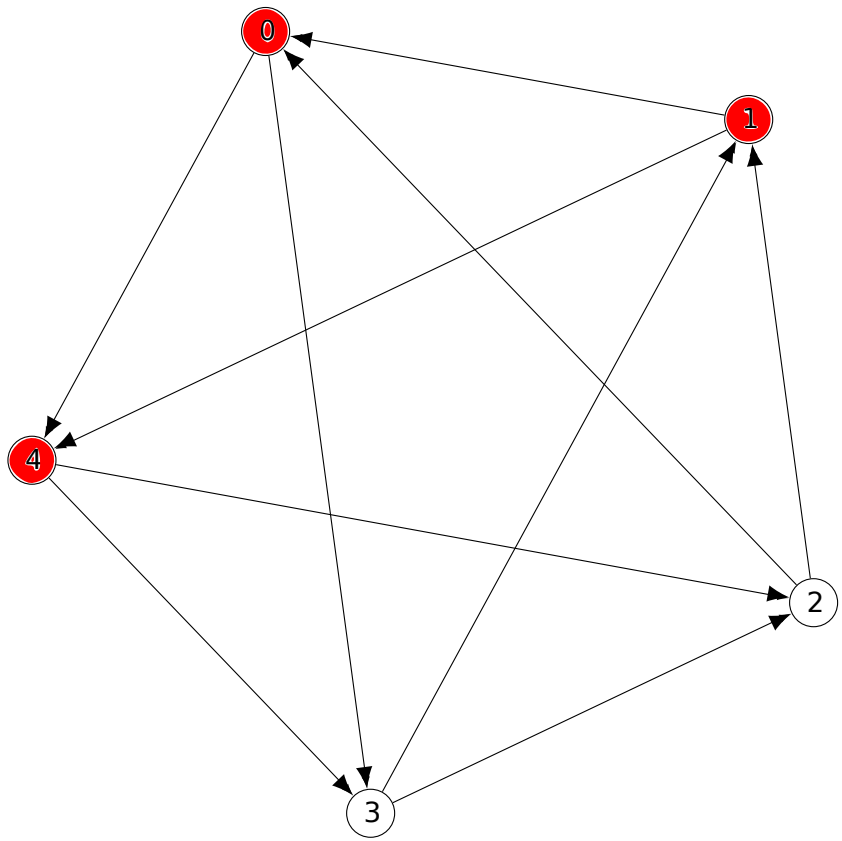
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



Motivations

Définition

On note $\mathbb{B} = \{0, 1\}$. Un réseau de n automates booléens (RAB) est défini par :

$$F : \mathbb{B}^n \to \mathbb{B}^n$$

Exemple

$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$ avec :

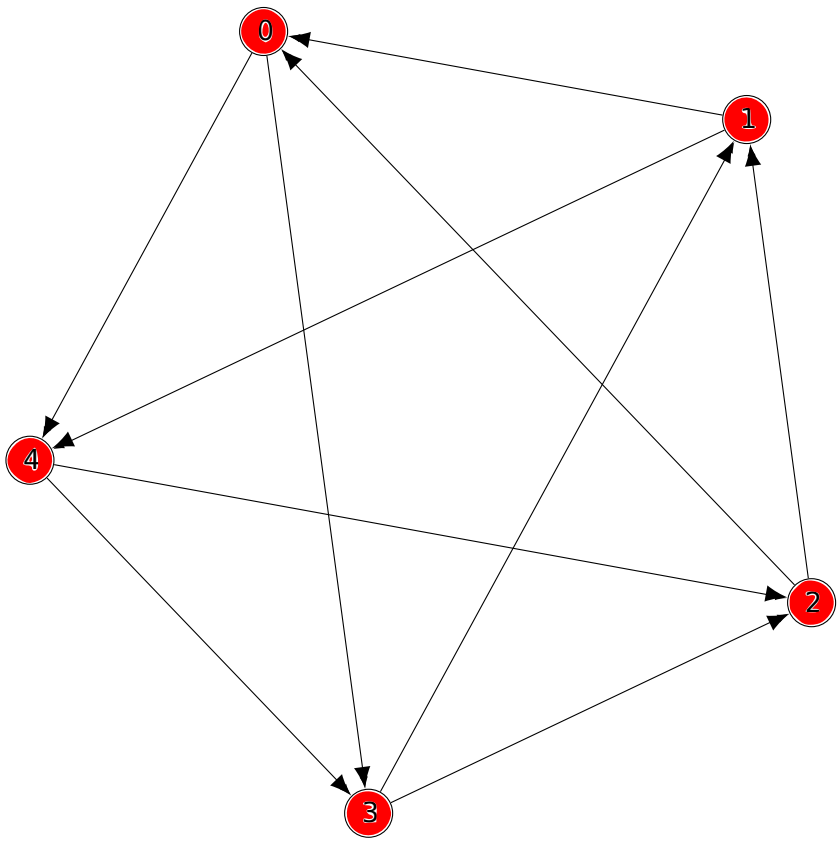
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



Motivations

Définition

On note $\mathbb{B} = \{0, 1\}$. Un réseau de n automates booléens (RAB) est défini par :

$$F : \mathbb{B}^n \to \mathbb{B}^n$$

Exemple

$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$ avec :

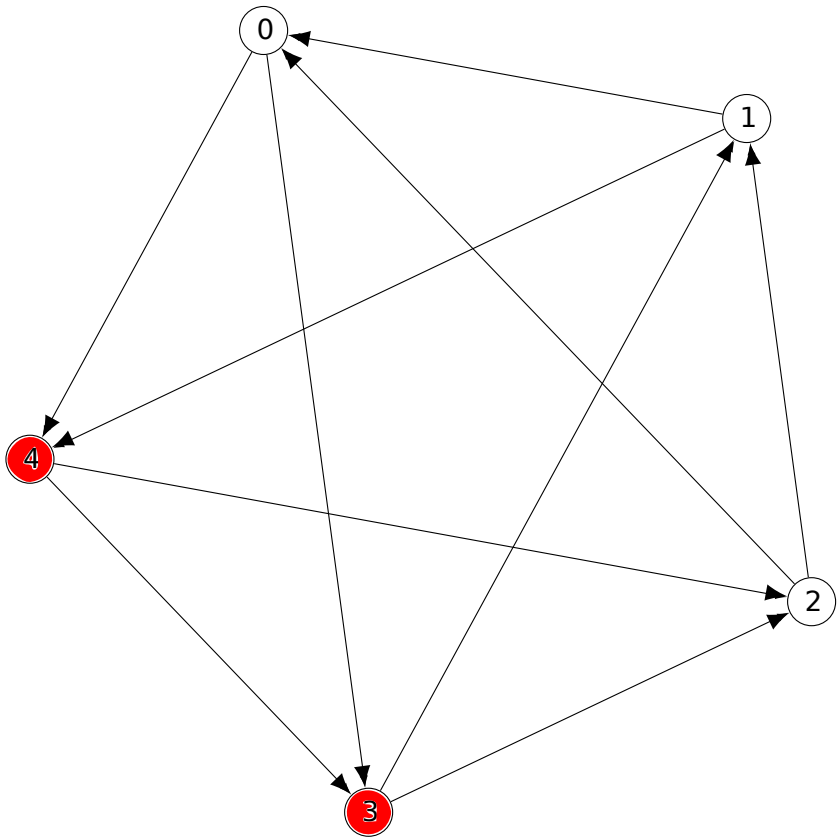
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

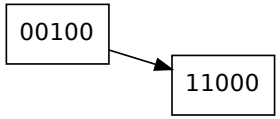
$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



00100

$$n = 5 \ , \ F = (f_0, f_1, f_2, f_3, f_4)$$
$$f_0(x) = x_1 \oplus x_2$$
$$f_1(x) = \neg(x_2 \wedge x_3)$$
$$f_2(x) = \neg x_3 \wedge x_4$$
$$f_3(x) = x_0 \wedge x_4$$
$$f_4(x) = x_0 \vee x_1$$



$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$

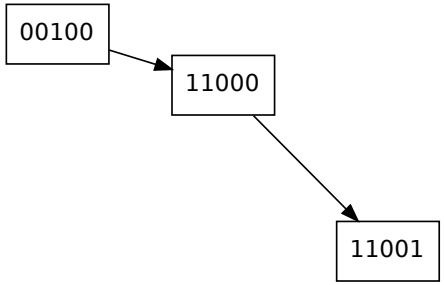
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$

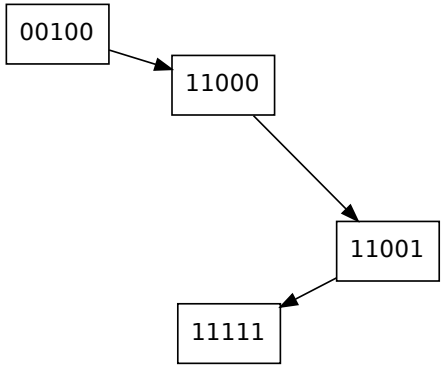
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$

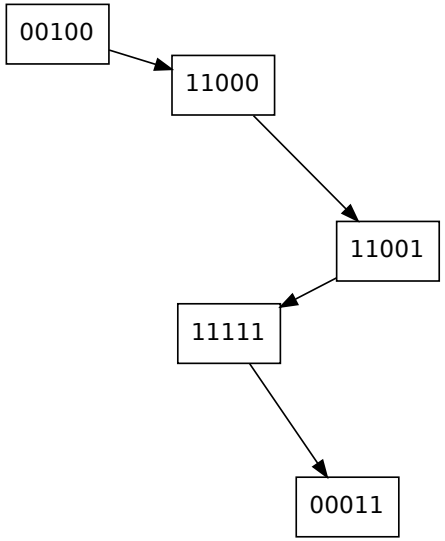
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$

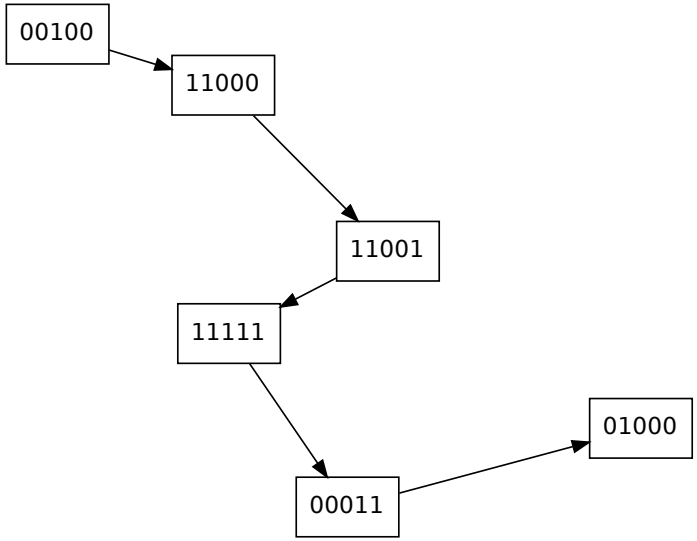
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$

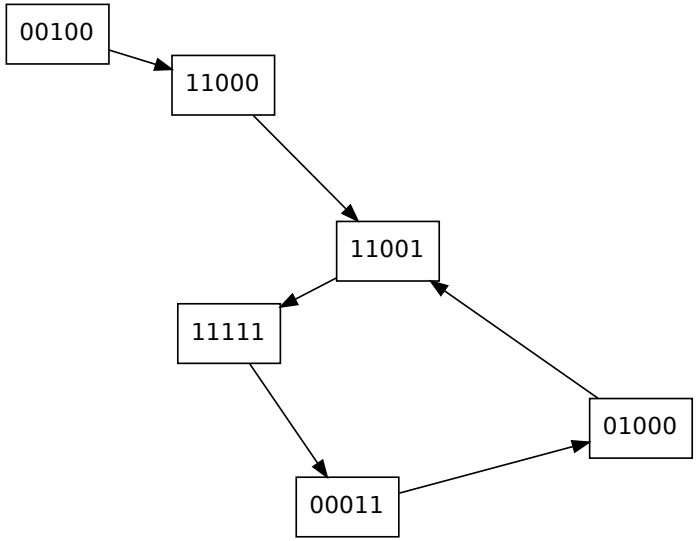
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$

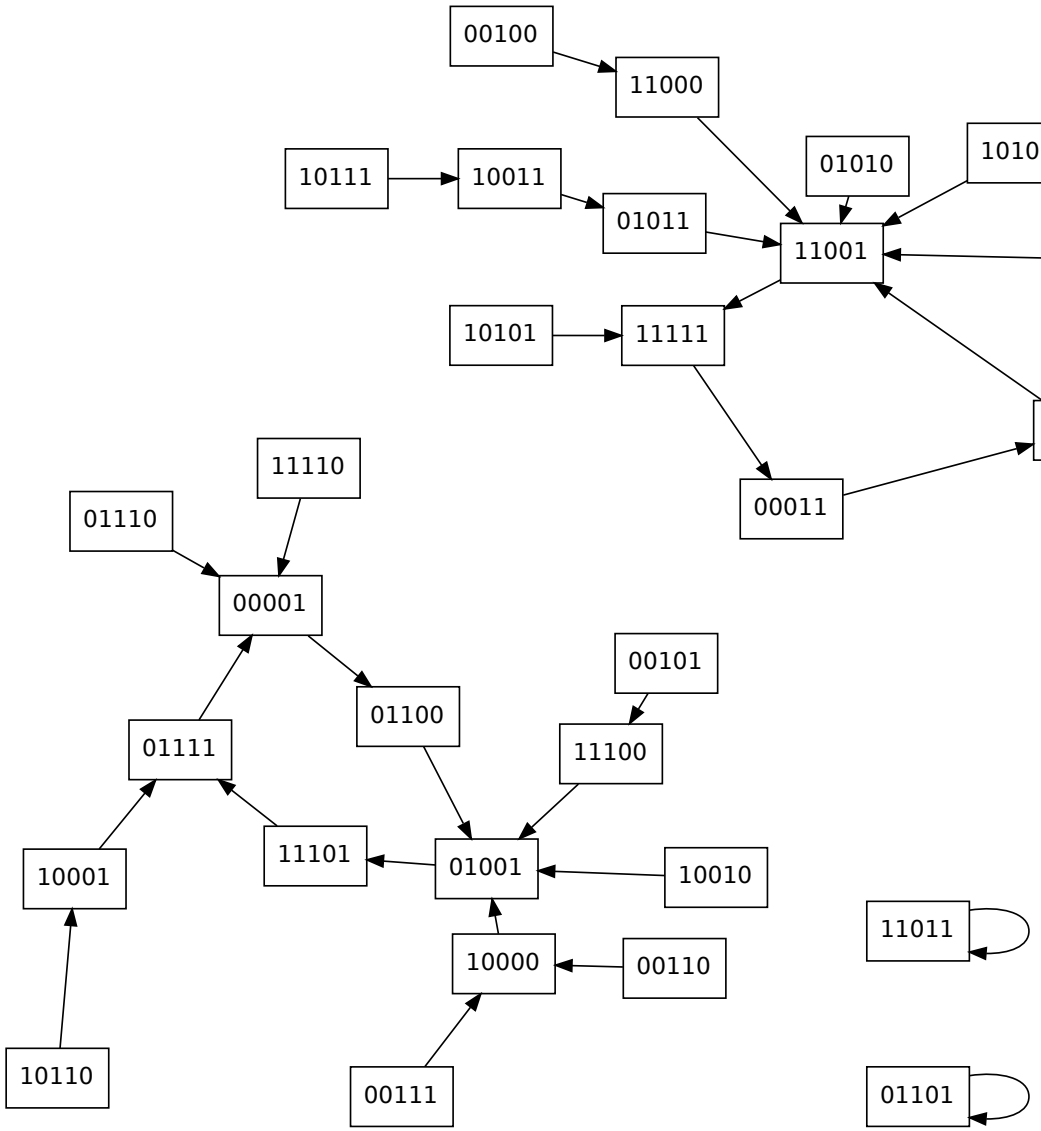
$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$



$n = 5$, $F = (f_0, f_1, f_2, f_3, f_4)$

$f_0(x) = x_1 \oplus x_2$

$f_1(x) = \neg(x_2 \wedge x_3)$

$f_2(x) = \neg x_3 \wedge x_4$

$f_3(x) = x_0 \wedge x_4$

$f_4(x) = x_0 \vee x_1$

Dynamique

Configurations récurrentes

$$\mathcal{R} = \{x \in \mathbb{B}^n \mid \exists t > 0, F^t(x) = x\}$$

Dynamique

Configurations récurrentes

$$\mathcal{R} = \{x \in \mathbb{B}^n \mid \exists t > 0, F^t(x) = x\}$$

Période

$$\forall x \in \mathcal{R}, \pi(x) = \min\{t \in \mathbb{N}^* \mid F^t(x) = x\}$$

Dynamique

Configurations récurrentes

$$\mathcal{R} = \{x \in \mathbb{B}^n \mid \exists t > 0, F^t(x) = x\}$$

Période

$$\forall x \in \mathcal{R}, \pi(x) = \min\{t \in \mathbb{N}^* \mid F^t(x) = x\}$$

Configurations transitoires

$$\mathcal{T} = \{x \in \mathbb{B}^n \mid \forall t > 0, F^t(x) \neq x\}$$

Dynamique

Configurations récurrentes

$$\mathcal{R} = \{x \in \mathbb{B}^n \mid \exists t > 0, F^t(x) = x\}$$

Période

$$\forall x \in \mathcal{R}, \pi(x) = \min\{t \in \mathbb{N}^* \mid F^t(x) = x\}$$

Configurations transitoires

$$\mathcal{T} = \{x \in \mathbb{B}^n \mid \forall t > 0, F^t(x) \neq x\}$$

Temps de convergence

$$\forall x \in \mathcal{T}, \lambda(x) = \min\{t \in \mathbb{N}^* \mid F^t(x) \in \mathcal{R}\}$$

Réseaux additifs

Cas booléen

Toutes les fonctions locales de transition sont des XOR : chaque automate fait la somme modulo 2 des ses entrées

Réseaux additifs

Cas booléen

Toutes les fonctions locales de transition sont des XOR : chaque automate fait la somme modulo 2 des ses entrées

Cas général

Les automates prennent leur états dans un anneau fini : chaque automate réalise une combinaison linéaire des ses entrées.
Ex : $\mathbb{Z}/m\mathbb{Z}$.

Réseaux additifs

Cas booléen

Toutes les fonctions locales de transition sont des XOR : chaque automate fait la somme modulo 2 des ses entrées

Cas général

Les automates prennent leur états dans un anneau fini : chaque automate réalise une combinaison linéaire des ses entrées.
Ex : $\mathbb{Z}/m\mathbb{Z}$.

Cas intermédiaire

Les automates prennent leur états dans un corps fini.
Ex : $\mathbb{F}_p$ où p est un nombre premier.

Expression algébrique

La fonction globale du réseau d'un réseau additif sur $\mathbb{F}_p$ s'écrit :

$$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$$

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{pmatrix} \mapsto \begin{pmatrix} \sum a_{0,j}\ u_j \\ \sum a_{1,j}\ u_j \\ \vdots \\ \sum a_{n-1,j}\ u_j \end{pmatrix}$$

Expression algébrique

La fonction globale du réseau d'un réseau additif sur $\mathbb{F}_p$ s'écrit :

$$F : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$$

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{pmatrix} \mapsto \begin{pmatrix} \sum a_{0,j}\ u_j \\ \sum a_{1,j}\ u_j \\ \vdots \\ \sum a_{n-1,j}\ u_j \end{pmatrix}$$

F est donc un endomorphisme de $\mathbb{F}_p^n$, et peut s'écrire sous forme d'une matrice A à coefficients dans $\mathbb{F}_p$:

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,0} & a_{n-1,1} & \cdots & a_{n-1,n-1} \end{pmatrix}$$

Expression algébrique

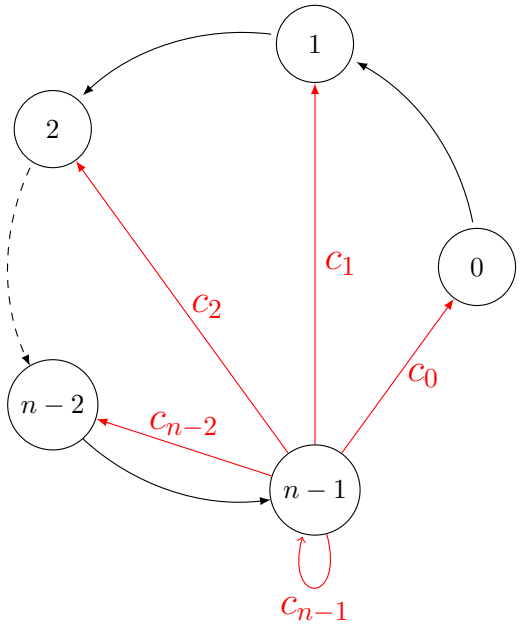
Supposons d'abord que A soit sous forme de *matrice compagnon* :

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}$$

Expression algébrique

Supposons d'abord que A soit sous forme de *matrice compagnon* :

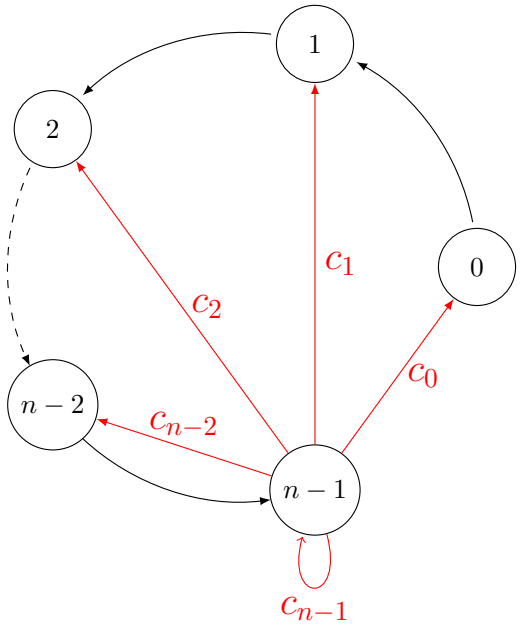
$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}$$



Expression algébrique

Supposons d'abord que A soit sous forme de *matrice compagnon* :

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}$$



Son polynôme caractéristique (aussi son polynôme minimal) est :

$$P(X) = X^n - \sum_{i=0}^{n-1} c_i X^i$$

Itérer : multiplier par A

$$A.u = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix} . \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{n-1} \end{pmatrix} = \begin{pmatrix} 0 + c_0 u_{n-1} \\ u_0 + c_1 u_{n-1} \\ u_1 + c_2 u_{n-1} \\ \vdots \\ u_{n-2} + c_{n-1} u_{n-1} \end{pmatrix}$$

Itérer : multiplier par A

$$A.u = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix} . \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{n-1} \end{pmatrix} = \begin{pmatrix} 0 + c_0 u_{n-1} \\ u_0 + c_1 u_{n-1} \\ u_1 + c_2 u_{n-1} \\ \vdots \\ u_{n-2} + c_{n-1} u_{n-1} \end{pmatrix}$$

En posant $U(X) = \sum_{i=0}^{n-1} u_i X^i$, on observe que :

$$\begin{aligned} X.U(X) \mod P(X) &= \sum_{i=0}^{n-1} u_i X^{i+1} = \left(\sum_{i=0}^{n-2} u_i X^{i+1} \right) + u_{n-1} X^n \\ &= \left(\sum_{i=0}^{n-2} u_i X^{i+1} \right) + \left(u_{n-1} \sum_{i=0}^{n-1} c_i X^i \right) \end{aligned}$$

Itérer : multiplier par A

$$A.u = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix} . \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{n-1} \end{pmatrix} = \begin{pmatrix} 0 + c_0 u_{n-1} \\ u_0 + c_1 u_{n-1} \\ u_1 + c_2 u_{n-1} \\ \vdots \\ u_{n-2} + c_{n-1} u_{n-1} \end{pmatrix}$$

En posant $U(X) = \sum_{i=0}^{n-1} u_i X^i$, on observe que :

$$\begin{aligned} X.U(X) \mod P(X) &= \sum_{i=0}^{n-1} u_i X^{i+1} = \left(\sum_{i=0}^{n-2} u_i X^{i+1} \right) + u_{n-1} X^n \\ &= \left(\sum_{i=0}^{n-2} u_i X^{i+1} \right) + \left(u_{n-1} \sum_{i=0}^{n-1} c_i X^i \right) \end{aligned}$$

Itérer : multiplier par X dans $\mathbb{F}_p[X]/P(X)$

Soit :

$$\Phi \quad : \quad \mathbb{F}_p^n \quad \to \quad \mathbb{F}_p[X]/P(X)$$

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{pmatrix} \quad \mapsto \quad \sum_{i=0}^{n-1} u_i X^i$$

Φ est bijective, et le diagramme suivant commute :

$$\begin{array}{ccc} \mathbb{F}_p^n & \xrightarrow{\Phi} & \mathbb{F}_p[X]/P(X) \\ \downarrow F & & \downarrow \mu_X \\ \mathbb{F}_p^n & \xrightarrow{\Phi} & \mathbb{F}_p[X]/P(X) \end{array}$$

avec $\mu_X(Q(X)) = X.Q(X)$

Dynamique dans $\mathbb{F}_p[X]/P(X)$

Si $P(X)$ est irréductible (et $\neq X$), $\mathbb{F}_p[X]/P(X)$ est un corps, tous ses éléments $\neq 0$ sont inversibles, et toutes les configurations sont récurrentes, de même période π :

$$\forall U \in \mathbb{F}_p[X]/P(X), \quad \pi(U) = \min\{t \in \mathbb{N}^* \mid X^t.U = U\}$$

Dynamique dans $\mathbb{F}_p[X]/P(X)$

Si $P(X)$ est irréductible (et $\neq X$), $\mathbb{F}_p[X]/P(X)$ est un corps, tous ses éléments $\neq 0$ sont inversibles, et toutes les configurations sont récurrentes, de même période π :

$$\forall U \in \mathbb{F}_p[X]/P(X), \quad \pi(U) = \min\{t \in \mathbb{N}^* \mid X^t.U = U\}$$

$$\forall U \neq 0, \pi(U) = \boxed{\pi = \min\{t \in \mathbb{N}^* \mid X^t = 1\}}$$

Dynamique dans $\mathbb{F}_p[X]/P(X)$

Si $P(X)$ est irréductible (et $\neq X$), $\mathbb{F}_p[X]/P(X)$ est un corps, tous ses éléments $\neq 0$ sont inversibles, et toutes les configurations sont récurrentes, de même période π :

$$\forall U \in \mathbb{F}_p[X]/P(X), \quad \pi(U) = \min\{t \in \mathbb{N}^* \mid X^t.U = U\}$$

$$\forall U \neq 0, \pi(U) = \boxed{\pi = \min\{t \in \mathbb{N}^* \mid X^t = 1\}}$$

0 étant un point fixe, on a donc k orbites de taille π, avec :

$$\boxed{k \times \pi = p^n - 1}$$

$\longrightarrow$ Il "suffit" de trouver l'ordre de X parmi les diviseurs de $p^n - 1$

Dynamique dans $\mathbb{F}_p[X]/P(X)$

Supposons $P = Q^s$, où Q est irréductible ($\neq X$), et $s > 1$.

Dynamique dans $\mathbb{F}_p[X]/P(X)$

Supposons $P = Q^s$, où Q est irréductible ($\neq X$), et $s > 1$.

- Si $Q \nmid U$, alors $\text{pgcd}(U, Q^s) = 1$ et U est inversible : sa période est l'ordre de X dans $\mathbb{F}_p[X]/P(X)$.

Dynamique dans $\mathbb{F}_p[X]/P(X)$

Supposons $P = Q^s$, où Q est irréductible ($\neq X$), et $s > 1$.

- Si $Q \nmid U$, alors $\text{pgcd}(U, Q^s) = 1$ et U est inversible : sa période est l'ordre de X dans $\mathbb{F}_p[X]/P(X)$.
- Si $U = V.Q^g$ avec $g < s$ et $Q \nmid V$, sa période est l'ordre de X dans $\mathbb{F}_p[X]/Q(X)^{s-g}$

Dynamique dans $\mathbb{F}_p[X]/P(X)$

Supposons $P = Q^s$, où Q est irréductible ($\neq X$), et $s > 1$.

- Si $Q \nmid U$, alors $\text{pgcd}(U, Q^s) = 1$ et U est inversible : sa période est l'ordre de X dans $\mathbb{F}_p[X]/P(X)$.
- Si $U = V.Q^g$ avec $g < s$ et $Q \nmid V$, sa période est l'ordre de X dans $\mathbb{F}_p[X]/Q(X)^{s-g}$

Thm

Si X est d'ordre t dans $\mathbb{F}_p[X]/Q(X)$, $Q(X)$ irréductible, alors X est d'ordre $tp^{\lceil \log_p(s) \rceil}$ dans $\mathbb{F}_p[X]/Q(X)^s$

Transitoires ?

$$F \text{ bijective } \Leftrightarrow \mathcal{R} = \mathbb{F}_p^n \Leftrightarrow \det(A) \neq 0 \Leftrightarrow c_0 \neq 0$$

Transitoires ?

$$F \text{ bijective } \Leftrightarrow \mathcal{R} = \mathbb{F}_p^n \Leftrightarrow \det(A) \neq 0 \Leftrightarrow c_0 \neq 0$$

Autrement dit, il n'y a de transitoires que si $c_0 = 0$. Mais $P(X)$ est irréductible et de terme constant nul ssi $P(X) = X$.

Transitoires ?

$$F \text{ bijective } \Leftrightarrow \mathcal{R} = \mathbb{F}_p^n \Leftrightarrow \det(A) \neq 0 \Leftrightarrow c_0 \neq 0$$

Autrement dit, il n'y a de transitoires que si $c_0 = 0$. Mais $P(X)$ est irréductible et de terme constant nul ssi $P(X) = X$.

Si $P = Q^s$ avec Q irréductible, le seul cas possible est donc $P(X) = X^s$. Matriciellement, cela signifie que A est une matrice $s \times s$ de la forme :

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

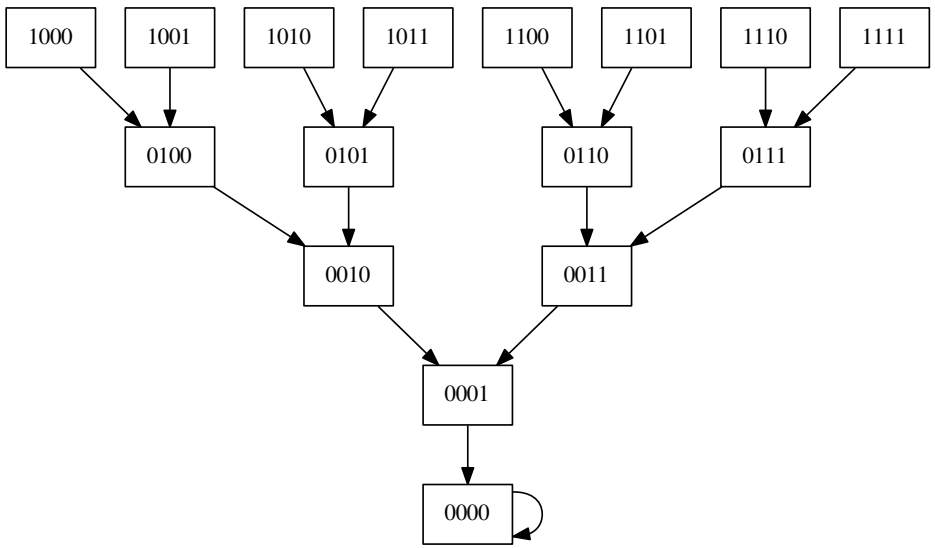
Transitoires ?

$$F \text{ bijective } \Leftrightarrow \mathcal{R} = \mathbb{F}_p^n \Leftrightarrow \det(A) \neq 0 \Leftrightarrow c_0 \neq 0$$

Autrement dit, il n'y a de transitoires que si $c_0 = 0$. Mais $P(X)$ est irréductible et de terme constant nul ssi $P(X) = X$.

Si $P = Q^s$ avec Q irréductible, le seul cas possible est donc $P(X) = X^s$. Matriciellement, cela signifie que A est une matrice $s \times s$ de la forme :

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

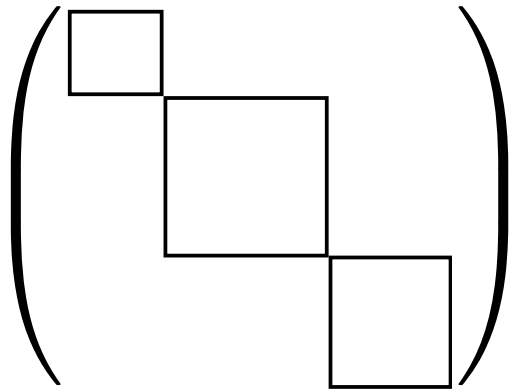


Matrice quelconque

$$A = \begin{pmatrix} & \dots & \end{pmatrix}$$

On part d'une matrice A quelconque : c'est la transposée de la matrice d'adjacence du graphe d'interaction (les arcs étant étiquetés par les coefficients $a_{i,j}$).

Matrice quelconque

A' = 

1er changement de base : *Lemme des noyaux*. On cherche B telle que $A' = B^{-1}AB$ soit bloc-diagonale, chaque bloc correspondant à un facteur Q^s (Q irréductible) du polynôme caractéristique $P(X)$ de A.

Matrice quelconque

$$A'' = \left(\begin{array}{ccc} \square & & \\ & \square & \\ & & \square \end{array} \right)$$

2è changement de base : *Forme normale de Frobenius*. Pour chaque bloc A'_i, on cherche C_i telle que $A''_i = C_i^{-1} A'_i C_i$ soit bloc-diagonale, chaque bloc étant une matrice compagnon.

Matrice quelconque

$$A'' = \begin{pmatrix} \square & & & & \\ & \square & & & \\ & & \square & & \\ & & & \square & \\ & & & & \square \end{pmatrix}$$

Il ne reste plus qu'à calculer la dynamique de chaque bloc (dont le polynôme associé est de la forme $Q^{s'}, s' \leqslant s$), puis à recomposer la dynamique globale par produit cartésien.

Lemme des noyaux

Thm

Soit ϕ un endomorphisme d'un espace vectoriel E, P_1 et P_2 deux polynômes premiers entre eux. Alors :

$$\ker P_1P_2(\phi) = \ker P_1(\phi) \oplus \ker P_2(\phi)$$

De plus, les restrictions à $\ker P_1P_2(\phi)$ des projections sur un noyau parallèlement à l'autre sont des polynômes en ϕ.

Décomposition en forme de Frobenius

Endomorphisme cyclique

Un endomorphisme ϕ d'un $\mathbb{K}$-espace vectoriel E (de dimension n) est *cyclique* si $\exists x \in E \mid \mathcal{B}_x = \{\phi^k(x), k = 0, \ldots, n-1\}$ soit une base de E. Dans ce cas, la matrice de ϕ dans $\mathcal{B}_x$ est une matrice compagnon.

Décomposition en forme de Frobenius

Endomorphisme cyclique

Un endomorphisme ϕ d'un $\mathbb{K}$-espace vectoriel E (de dimension n) est *cyclique* si $\exists x \in E \mid \mathcal{B}_x = \{\phi^k(x), k = 0, \ldots, n-1\}$ soit une base de E. Dans ce cas, la matrice de ϕ dans $\mathcal{B}_x$ est une matrice compagnon.

Thm

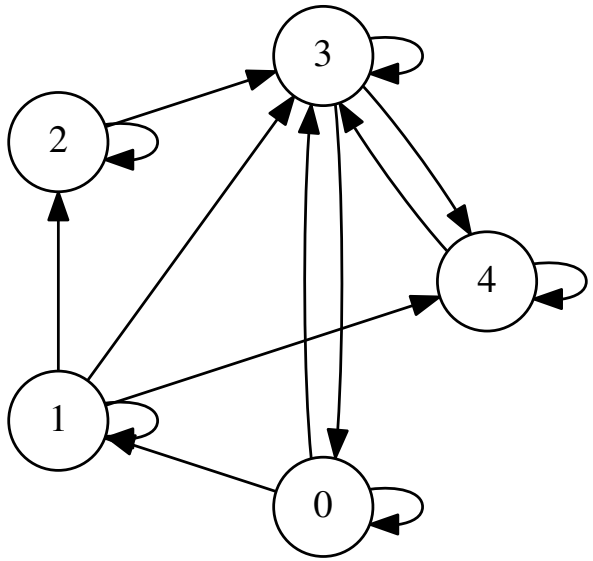
Soit ϕ un endomorphisme de E. Il existe une suite $F_1, \ldots, F_r$ de sous-espaces vectoriels de E, tous stables par ϕ, telle que :

- $E = F_1 \oplus F_2 \oplus \ldots \oplus F_r$
- *Pour tout i de $\{1, \ldots, r\}$, la restriction ϕ_i de ϕ à F_i est un endomorphisme cyclique de F_i.*
- *Si P_i désigne le polynôme minimal de ϕ_i, alors $P_{i+1} \mid P_i$ pour tout i de $\{1, \ldots, r-1\}$.*

$P_1, \ldots, P_r$ est la suite des invariants de similitude.

Un exemple sur $\mathbb{B}^5$

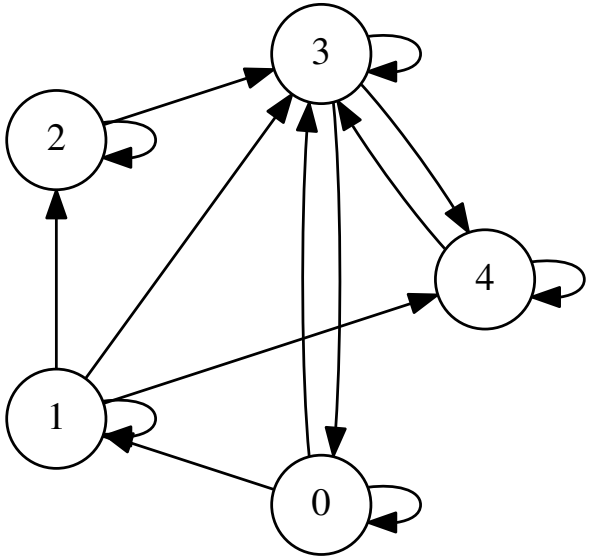
$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$



$$P(X) = X^5 + X^4 + X^3 + X^2 + X = X(X+1)^2(X^2+X+1)$$

Un exemple sur $\mathbb{B}^5$

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

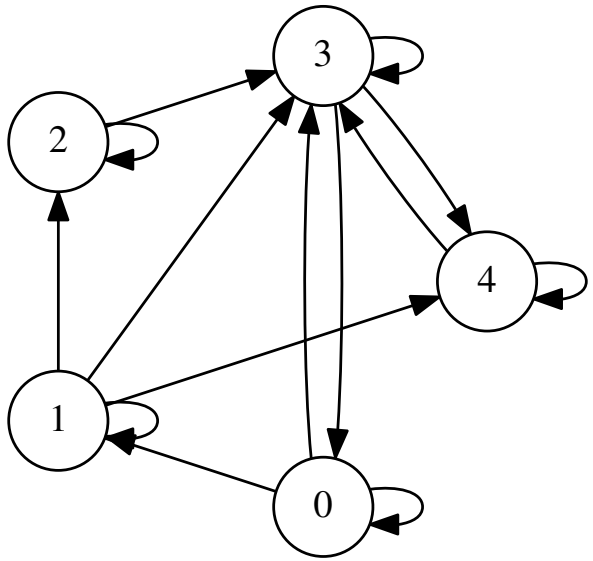


$P(X) = X^5 + X^4 + X^3 + X^2 + X = X(X+1)^2(X^2+X+1)$

$P(X) = P_1 P_2 P_3$ avec P_1, P_2, P_3 premiers entre eux.

Un exemple sur $\mathbb{B}^5$

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$



$P(X) = X^5 + X^4 + X^3 + X^2 + X = X(X+1)^2(X^2+X+1)$
$P(X) = P_1 P_2 P_3$ avec P_1, P_2, P_3 premiers entre eux.

On a, par le lemme des noyaux :

$$\ker((P_1 P_2 P_3)(A)) = \ker(P_1(A)) \oplus \ker(P_2(A)) \oplus \ker(P_3(A))$$

Un exemple sur $\mathbb{B}^5$

$\ker(P_1(A)) = \ker(A) = \text{Vect}\{(1,1,1,1,0)\}$
$\ker(P_2(A)) = \ker((A+I)^2) = \text{Vect}\{(0,1,1,0,0),(0,1,0,0,1)\}$
$\ker(P_3(A)) = \ker(A^2+A+I) = \text{Vect}\{(1,0,1,1,0),(0,1,1,1,1)\}$

On obtient ainsi :

$$B = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Un exemple sur $\mathbb{B}^5$

$\ker(P_1(A)) = \ker(A) = \text{Vect}\{(1,1,1,1,0)\}$
$\ker(P_2(A)) = \ker((A+I)^2) = \text{Vect}\{(0,1,1,0,0),(0,1,0,0,1)\}$
$\ker(P_3(A)) = \ker(A^2+A+I) = \text{Vect}\{(1,0,1,1,0),(0,1,1,1,1)\}$

On obtient ainsi :

$$B = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \Longrightarrow A' = B^{-1}AB = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Un exemple sur $\mathbb{B}^5$

$$\ker(P_1(A)) = \ker(A) = \text{Vect}\{(1,1,1,1,0)\}$$
$$\ker(P_2(A)) = \ker((A+I)^2) = \text{Vect}\{(0,1,1,0,0),(0,1,0,0,1)\}$$
$$\ker(P_3(A)) = \ker(A^2+A+I) = \text{Vect}\{(1,0,1,1,0),(0,1,1,1,1)\}$$

On obtient ainsi :

$$B = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \Longrightarrow A' = B^{-1}AB = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Un exemple sur $\mathbb{B}^5$

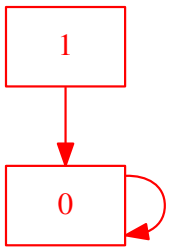
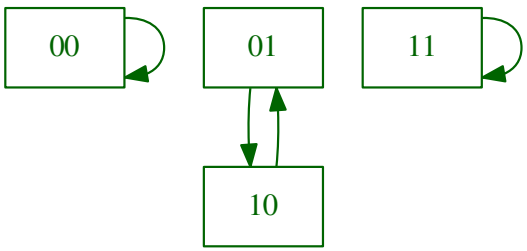
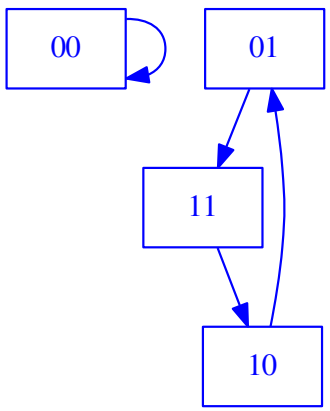
$\ker(P_1(A)) = \ker(A) = \text{Vect}\{(1,1,1,1,0)\}$
$\ker(P_2(A)) = \ker((A+I)^2) = \text{Vect}\{(0,1,1,0,0),(0,1,0,0,1)\}$
$\ker(P_3(A)) = \ker(A^2+A+I) = \text{Vect}\{(1,0,1,1,0),(0,1,1,1,1)\}$

On obtient ainsi :

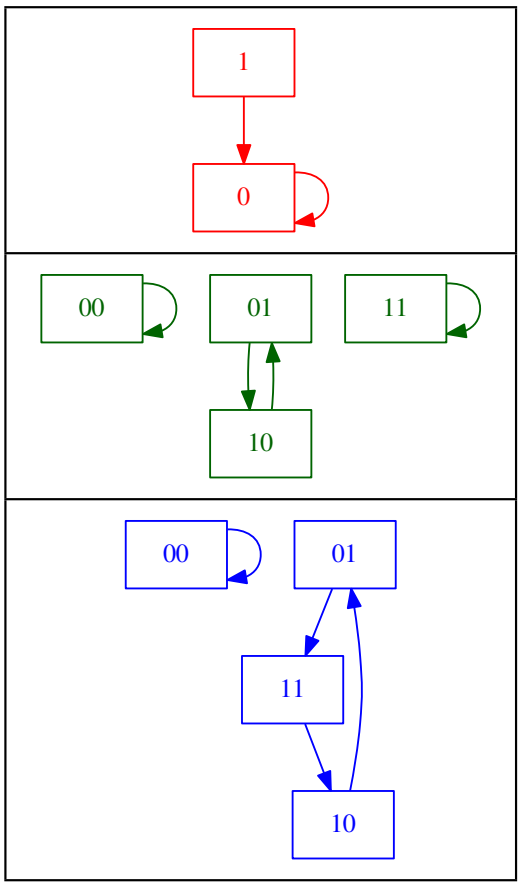
$$B = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \Longrightarrow A' = B^{-1}AB = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

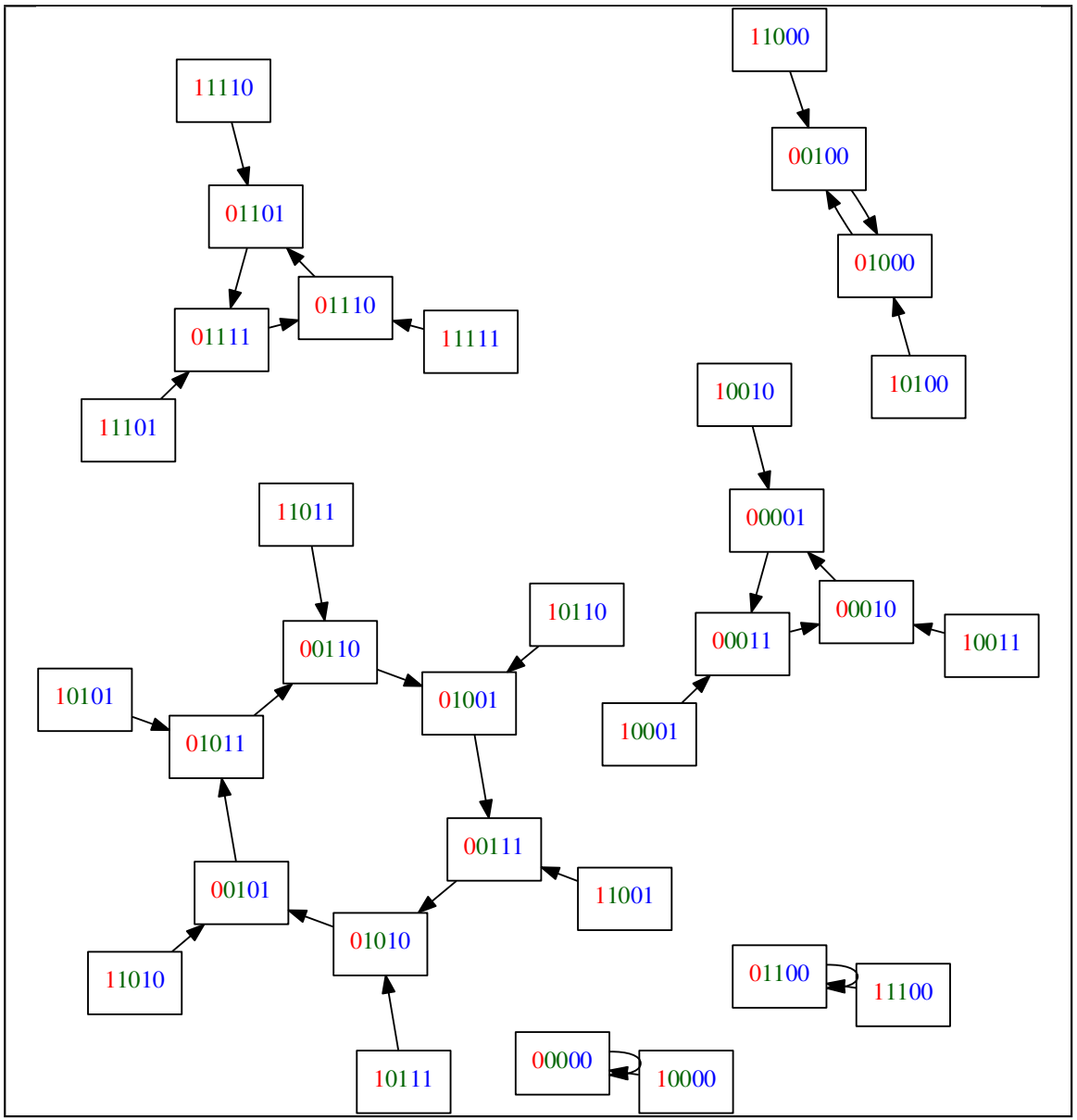
NB : Pour cet exemple, les matrices obtenues sont déjà sous forme de Frobenius.

Un exemple sur $\mathbb{B}^5$

Polynôme	ordre de X	Dynamique
X	∞	
$(X+1)^2$	2	
X^2+X+1	3	

Un exemple sur $\mathbb{B}^5$





Remarques

- Deux orbites de tailles t_1 et t_2 se combinent en donnant k orbites de taille t_3 avec $k = \text{pgcd}(t_1, t_2)$ et $t_3 = \text{ppcm}(t_1, t_2)$
- Concernant les transitoires, la succession des deux décompositions fournit une suite de puissances de X : $X^{\lambda_1}, X^{\lambda_2}, \ldots$. En posant $\forall t \in \mathbb{N}^*, q(t) = |\{\lambda_i \mid \lambda_i \geqslant t\}|$ et $s(t) = \sum_i \{\min(t-1, \lambda_i)\}$, on connaît le nombre $\theta(t)$ de configurations de hauteur t :

$$\theta(t) = p^{s(t)}(p^{q(t)} - 1)$$

Complexité

- Décompositions matricielles : $\mathcal{O}(n^3)$ (notamment grâce à l'algorithme de Storjohann pour la décomposition de Frobenius)
- Factorisation polynomiale : $\mathcal{O}(n^3)$ (algorithme de Berlekamp)
- Calcul de l'ordre de X : polynomial si on a connaît les diviseurs de $p^n - 1$, sinon exponentiel

Conclusion et perspectives

- Cas des corps réglé

Conclusion et perspectives

- Cas des corps réglé (mais déjà partiellement fait : B.Elspas, *The Theory of Autonomous Linear Sequential Networks*)

Conclusion et perspectives

- Cas des corps réglé (mais déjà partiellement fait : B.Elspas, *The Theory of Autonomous Linear Sequential Networks*)
- Comprendre ce qu'il se passe dans les anneaux non intègres : il n'y a plus unicité de la factorisation. Par exemple, dans $\mathbb{Z}/8\mathbb{Z}[X]$, on a

$$\begin{aligned} P(X) = X^3 + X^2 + 5 * X + 5 &= (X+1)(X^2+5) \\ &= (X+5)(X^2+4X+1) \end{aligned}$$

  De plus, trouver les facteurs éventuels ne suffit plus : il faut étudier les diviseurs de zéro dans $\mathbb{Z}/8\mathbb{Z}[X]/P(X)$

Conclusion et perspectives

- Cas des corps réglé (mais déjà partiellement fait : B.Elspas, *The Theory of Autonomous Linear Sequential Networks*)
- Comprendre ce qu'il se passe dans les anneaux non intègres : il n'y a plus unicité de la factorisation. Par exemple, dans $\mathbb{Z}/8\mathbb{Z}[X]$, on a

$$\begin{aligned} P(X) = X^3 + X^2 + 5 * X + 5 &= (X+1)(X^2+5) \\ &= (X+5)(X^2+4X+1) \end{aligned}$$

  De plus, trouver les facteurs éventuels ne suffit plus : il faut étudier les diviseurs de zéro dans $\mathbb{Z}/8\mathbb{Z}[X]/P(X)$
- Etudier les différents modes de mise à jour

Conclusion et perspectives

- Cas des corps réglé (mais déjà partiellement fait : B.Elspas, *The Theory of Autonomous Linear Sequential Networks*)
- Comprendre ce qu'il se passe dans les anneaux non intègres : il n'y a plus unicité de la factorisation. Par exemple, dans $\mathbb{Z}/8\mathbb{Z}[X]$, on a

$$\begin{aligned} P(X) = X^3 + X^2 + 5 * X + 5 &= (X+1)(X^2+5) \\ &= (X+5)(X^2+4X+1) \end{aligned}$$

  De plus, trouver les facteurs éventuels ne suffit plus : il faut étudier les diviseurs de zéro dans $\mathbb{Z}/8\mathbb{Z}[X]/P(X)$
- Etudier les différents modes de mise à jour
- Possibilité de linéariser des réseaux non linéaires ?

Merci de votre attention.