

# Modèles discrets pour la sécurité informatique : des méthodes itératives à l'analyse vectorielle.

Jean-François COUCHOT  
Soutenance d'HDR : le 30/01/16

Rapporteurs :

Olivier BOURNEZ  
Jean-Paul COMET  
Juan-Pablo ORTEGA

Professeur à l'Ecole Polytechnique.  
Professeur à l'Université de Nice Sophia Antipolis  
Professeur à l'Université de St. Gallen-Suisse

Examineurs :

Sylvain CONTASSOT-VIVIER  
Raphaël COUTURIER  
Christophe GUYEUX

Professeur à l'Université de Lorraine  
Professeur à l'Univ. Bourgogne Franche-Comté  
Professeur à l'Univ. Bourgogne Franche-Comté



## Réseau booléen (définition)

- Une fonction  $f : \mathbb{B}^N \rightarrow \mathbb{B}^N, x = (x_1, \dots, x_N) \mapsto (f_1(x), \dots, f_N(x))$
- Un schéma de mise à jour de la suite  $(x^t)^{t \in \mathbb{N}}$  des configurations :
  - *Parallèle synchrone* :  $x^{t+1} = f(x^t)$ .
  - *Unaire* : à partir de la *stratégie unaire*  $S = (s^t)^{t \in \mathbb{N}}$ , modification de l'élément  $s^t$  de  $x^t$

$$x^{t+1} = (x_1^{t+1}, \dots, x_n^{t+1}) \text{ où } x_i^{t+1} = \begin{cases} f_i(x^t) & \text{si } i = s^t \\ x_i^t & \text{sinon.} \end{cases}$$

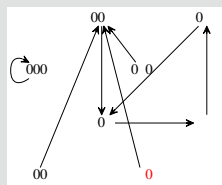
- *Généralisé* : à partir de la *stratégie généralisée*  $(s^t)^{t \in \mathbb{N}}$ , à chaque itération  $t$ , modification des éléments de  $x^t$  dans  $s^t \subset \{1, \dots, n\}$

$$x^{t+1} = (x_1^{t+1}, \dots, x_n^{t+1}) \text{ où } x_i^{t+1} = \begin{cases} f_i(x^t) & \text{si } i \in s^t \\ x_i^t & \text{sinon} \end{cases}$$

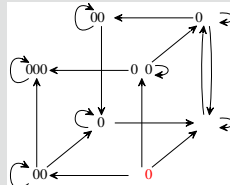
## 3 schémas $\rightsquigarrow$ 3 graphes d'itérations

### Graphes des itérations de

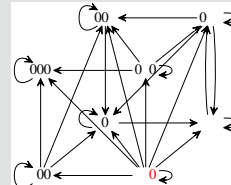
$$(X_1, X_2, X_3) \mapsto ((\overline{X_1} + \overline{X_2}) \cdot X_3, X_1 \cdot X_3, X_1 + X_2 + X_3).$$



(a) GIS(f)



(b) GIU(f)



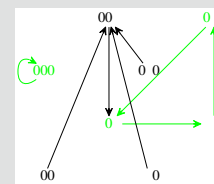
(c) GIG(f)

## Attracteurs

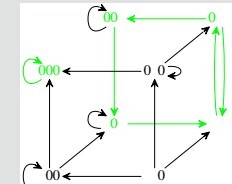
- $x$  point fixe de  $f$  si  $x = f(x)$
- $A$  attracteurs du graphe si
  - pour tout arc  $x \rightarrow y$ , si  $x \in A$ , alors  $y \in A$  et
  - $A$  : le plus petit au sens de l'inclusion

### Attracteurs de

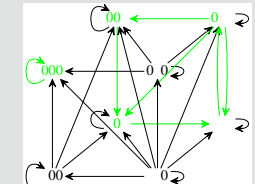
$$(X_1, X_2, X_3) \mapsto ((\overline{X_1} + \overline{X_2}) \cdot X_3, X_1 \cdot X_3, X_1 + X_2 + X_3).$$



(d)  $A_1 = \{000\}$  et  $A_2 = \{011, 101, 111\}$



(e)  $A_1 = \{000\}$  et  $A_2 = \{001, 101, 111, 011\}$



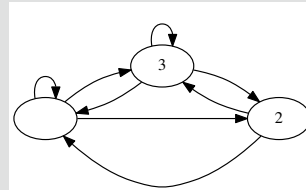
(f)  $A_1 = \{000\}$  et  $A_2 = \{001, 101, 111, 011\}$

# Dépendance entre éléments

- Mat. de  $\{-1, 0, 1\}^{N^2}$  des « dérivées partielles »  $f'_{ij} = \frac{f_i(\bar{x}^j) - f_i(x)}{\bar{x}_j - x_j}$ .
- Représentée par un *graphe des interactions* orienté :
  - Sommets :  $\{1, \dots, N\}$
  - Arcs :  $j \xrightarrow{s} i$  si  $\exists x \in \mathbb{B}^N$  tq.  $f'_{ij}(x) = s$ ,  $s \in \{-1, 1\}$

## Graphes des interactions de $(X_1, X_2, X_3) \mapsto ((\bar{X}_1 + \bar{X}_2) \cdot X_3, X_1 \cdot X_3, X_1 + X_2 + X_3)$ .

$$f' = \begin{pmatrix} \frac{(\bar{x}_1 + \bar{x}_2) \cdot x_3 - (\bar{x}_1 + \bar{x}_2) \cdot x_3}{x_1 - x_1} & \frac{(\bar{x}_1 + \bar{x}_2) \cdot x_3 - (\bar{x}_1 + \bar{x}_2) \cdot x_3}{x_2 - x_2} & \frac{(\bar{x}_1 + \bar{x}_2) \cdot x_3 - (\bar{x}_1 + \bar{x}_2) \cdot x_3}{x_3 - x_3} & \dots \\ \frac{\bar{x}_1 \cdot x_3 - x_1 \cdot x_3}{x_1 - x_1} & 0 & \dots & \dots \\ \frac{(\bar{x}_1 + \bar{x}_2 + x_3) - (x_1 + x_2 + x_3)}{x_1 - x_1} & \dots & \dots & \dots \end{pmatrix}$$



# Un exemple motivant

## $g(x_1, x_2, x_3, x_4, x_5) = (x_1 \cdot \bar{x}_2 + \bar{x}_1 \cdot x_2, x_1 + x_2, x_3 \cdot \bar{x}_1, x_5, \bar{x}_3 + x_4)$

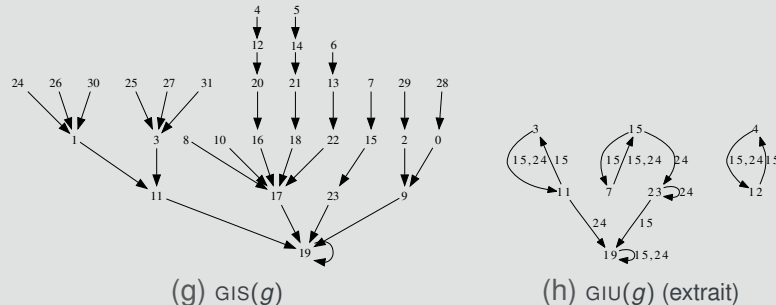


FIGURE – Graphes des itérations synchrones

- Avec  $D^t = t$  sauf  $D_{12}^t = t - 1$  pour  $t$  impair,  $g$  oscille entre  $(0, 0, 0, 1, 1)$  et  $(0, 1, 0, 1, 1)$
- Schéma parallèle : converge en synchrone, diverge en asynchrone

# Mode asynchrone

- Deux modes :
  - *synchrone* : chaque élément attend la valeur des éléments dont il dépend ;
  - *asynchrone* : chaque élément met à jour sa valeur sans attendre.
- $(D^t)^{t \in \mathbb{N}}$  : suite de matrices de taille  $N \times N$  t.q.

$$D_{ij}^t = \text{date où } x_j \text{ est disponible au composant } i$$

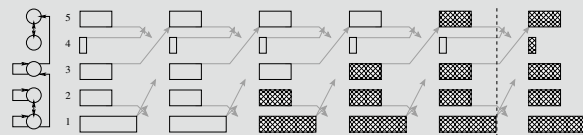
$$x_i^{t+1} = \begin{cases} f_i(x_1^{D_{i1}^t}, \dots, x_N^{D_{iN}^t}) & \text{si } i \in S^t \\ x_i^t & \text{sinon} \end{cases}$$

# Problématique

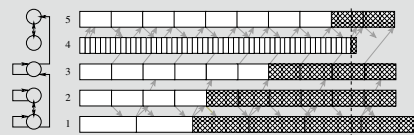
- Peut-on prédire le comportement de réseaux booléens (Sec. 2)
  - Théorique : **conditions théoriques** nécessaires/suffisantes de convergence/divergence ?
  - Pratique : vérification par simulation (**exhaustive ?**)
- Itérations divergentes  $\leftrightarrow$  **comportement chaotique** (Sec. 3) ?
  - Caractérisation des réseaux booléens chaotiques.
  - Génération et prédiction.
- Générateurs de nombres pseudo-aléatoires (Sec. 4) :
  - Caractérisation d'un PRNG chaotique.
  - Générations et qualité.
- Du Chaos au masquage d'information (Sec. 5).
  - D'un point de vue chaotique.
  - D'un point de vue analyse vectorielle discrète.

1. Introduction : iterations de réseaux booléens
2. Réseaux booléens : des preuves de convergences
3. Des systèmes dynamiques discrets au chaos
4. Applications à la génération de nombres pseudo-aléatoires
5. Application au masquage d'information
6. Conclusion

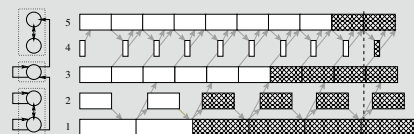
## Mode mixte avec $g$



(a) Parallèle synchrone



(b) Asynchrone



(c) Mixte tq.  $\langle 1 \rangle = \{1, 2\}$ ,  $\langle 3 \rangle = \{3\}$ ,  $\langle 4 \rangle = \{4, 5\}$ .

- *Mode mixte* [ABCVS05] : regroupement des nœuds qui pourraient introduire des cycles.
  - A l'intérieur de chaque groupe : mode synchrone.
  - A l'extérieur de chaque groupe : mode asynchrone.
- Relation de synchronisation :  $iRj$  si  $i$  et  $j$  dans la même CFC du graphe des interactions.

### ( [BCVC10] )

Soit  $f$  possédant un unique point fixe  $x^*$  et une stratégie pseudo-périodique  $s$ . Si les itérations synchrones convergent vers  $x^*$  pour cette stratégie, alors les itérations mixtes à délai uniforme convergent aussi vers  $x^*$  pour cette stratégie.

## Convergence par la pratique

- Conditions suffisantes de convergence : facile à appliquer, domaine restreint
- Recherche d'une métrique décroissante minorée : difficile
- Simulations :
  - Non exhaustives pour les schémas généralisés et asynchrones.
  - Verdict  $\leftrightarrow$  vérité ssi divergence (contre-exemple).
- Souhait : exploiter un outil qui traiterai toutes les transitions
  - explosion combinatoire : par abstraction, quotientage, ordre partiel...
  - Model checker : SPIN [Hol03].
  - Correction et complétude de la démarche.

- Points clefs de la traduction :
  - Stratégie : pseudo périodicité garantie par le choix indéterministe de SPIN.
  - Délais (bornés par construction) : oubli de certaines valeurs grâce à l'indéterminisme de SPIN.
- Convergence universelle :  $\diamond(\Box x_p = x)$ .

## (Correction et complétude de la traduction vers Promela [Cou10])

Soit  $\phi$  un modèle de système dynamique discret et  $\psi$  sa traduction PROMELA. Les itérations de  $\phi$  sont universellement convergentes si et seulement si  $\psi$  vérifie la propriété LTL sous hypothèse d'équité faible.

- Bilan :
  - Preuve automatique de convergence de modèles indpt. schéma/mode.
  - Ne passe pas à l'échelle.

# Rappels sur les itérations chaotiques

## Definition (Chaos selon Devaney)

$k$  continue sur  $(\mathcal{X}, d)$  est chaotique si elle est transitive, régulière et fortement sensible aux conditions initiales.

- *Transitivité* : pour chaque point, chacun de ses voisinages a un futur pouvant contenir tout point de l'espace.
- *Régularité* : l'ensemble de ses points périodiques est dense dans  $\mathcal{X}$ .
- *Forte sensibilité aux cond. initiales* : pour chaque point, chacun de ses voisinages a un point dont un futur est éloigné.

1. Introduction : iterations de réseaux booléens
2. Réseaux booléens : des preuves de convergences
3. Des systèmes dynamiques discrets au chaos
4. Applications à la génération de nombres pseudo-aléatoires
5. Application au masquage d'information
6. Conclusion

# Espace pour itérations chaotiques (unaires)

- Vers une fonction de  $\mathcal{X}_U = \mathbb{B}^N \times \llbracket 1; N \rrbracket^N$  dans lui même [Guy10] :
  - $F_{f_U} : \mathbb{B}^N \times \llbracket 1; N \rrbracket^N \rightarrow \mathbb{B}^N, (x, i) \mapsto (x_1, \dots, x_{i-1}, f_i(x), x_{i+1}, \dots, x_N)$
  - $\sigma : \llbracket 1; N \rrbracket^N \rightarrow \llbracket 1; N \rrbracket^N$  t.q.  $\forall t \in \mathbb{N}, \sigma(s)_t = s_{t+1}$
  - $G_{f_U}$  définie par  $G_{f_U}(x, s) = (F_{f_U}(x, s_0), \sigma(s))$
- Distance  $d : d((x, s), (x', s')) = d_H(x, x') + d_S(s, s')$

## (Fonctions t.q. $G_{f_U}$ est chaotique [BCG12])

Soit  $f : \mathbb{B}^N \rightarrow \mathbb{B}^N$ . Les itérations de la fonction  $G_{f_U}$  sont chaotiques si et seulement si  $\text{GIU}(f)$  est fortement connexe.

# Espace pour itérations chaotiques (généralisées)

- Vers une fonction de  $\mathcal{X}_g = \mathbb{B}^N \times (\mathcal{P}(\llbracket 1; N \rrbracket))^N$  dans lui-même :
  - $F_{f_g} : \mathbb{B}^N \times \mathcal{P}(\llbracket 1; N \rrbracket) \rightarrow \mathbb{B}^N$  par  $F_{f_g}(x, s)_i = \begin{cases} f_i(x) & \text{si } i \in s; \\ x_i & \text{sinon.} \end{cases}$
  - $\sigma : (\mathcal{P}(\llbracket 1; N \rrbracket))^N \rightarrow (\mathcal{P}(\llbracket 1; N \rrbracket))^N$  t.q.  $\forall t \in \mathbb{N}, \sigma(s)_t = s_{t+1}$
  - $G_{f_g}$  définie par  $G_{f_g}(x, S) = (F_{f_g}(x, s_0), \sigma(S))$ ,
- Distance  $d : d((x, s), (x', s')) = d_H(x, x') + d'_S(s, s')$

## (Fonctions t.q. $G_{f_g}$ est chaotique)

Soit  $f : \mathbb{B}^N \rightarrow \mathbb{B}^N$ . Les itérations de la fonction  $G_{f_g}$  sont chaotiques si et seulement si  $GIG(f)$  est fortement connexe.

# Générer un graphe GIU fortement connexe

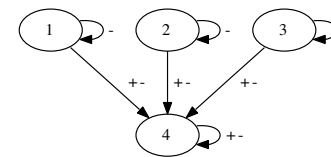
- Méthode naïve : suppressions successives aléatoires d'arcs de  $GIU(\neg)$ .
- Cond. suffisantes sur le graphe d'interactions.

## (Fonctions avec GIU fort. connexe [BCGR11])

Soit  $f$  une fonction de  $\mathbb{B}^N$  vers lui-même telle que  $\Gamma(f)$  :

- N'a pas de cycle de longueur supérieure ou égale à deux.
- Chacun des sommets avec une boucle + a aussi une boucle -.
- Chacun des sommets est accessible depuis un sommet avec une boucle -.

Alors,  $GIU(f)$  est fortement connexe.



$\rightsquigarrow \begin{cases} 34226 \text{ fonctions} \\ 520 \text{ non isomorphes} \end{cases}$

# Plan

- Introduction : itérations de réseaux booléens
- Réseaux booléens : des preuves de convergences
- Des systèmes dynamiques discrets au chaos
- Applications à la génération de nombres pseudo-aléatoires
- Application au masquage d'information
- Conclusion

# PRNG par itérations unaires

**Input:** une fonction  $f$ , un nombre d'itérations  $b$ , une configuration initiale  $x^0$  (N bits)

**Output:** une configuration  $x$  (N bits)

$x \leftarrow x^0$ ;

**for**  $i = 1, \dots, b$  **do**

$s \leftarrow \text{Random}(N)$ ;

$x \leftarrow F_{f_u}(x, s)$ ;

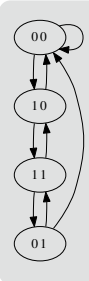
**end**

return  $x$ ;

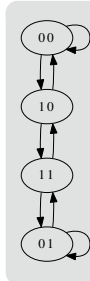
- $\text{Random}$  : un PRNG (N bits).
- Remarques :
  - $b = 1 \rightsquigarrow$  itérations (chaotiques) de  $F_{f_u}$
  - Quid de l'uniformité de la sortie ?

## (Uniformité de la sortie [BCGR11])

Soit  $f : \mathbb{B}^N \rightarrow \mathbb{B}^N$ , GIU( $f$ ) son graphe d'itérations,  $\check{M}$  sa matrice d'adjacence. Si GIU( $f$ ) est fortement connexe, alors la sortie du générateur de nombres pseudo-aléatoires suit une loi qui tend vers la distribution uniforme ssi  $\frac{1}{N} \check{M}$  est doublement stochastique.



- $g(x_1, x_2) = (\bar{x}_1, x_1 \bar{x}_2)$
- $M_g = \frac{1}{2} \begin{pmatrix} 1010 \\ 1001 \\ 1001 \\ 0110 \end{pmatrix}$
- $\pi_g = (\frac{4}{10}, \frac{1}{10}, \frac{3}{10}, \frac{2}{10})$



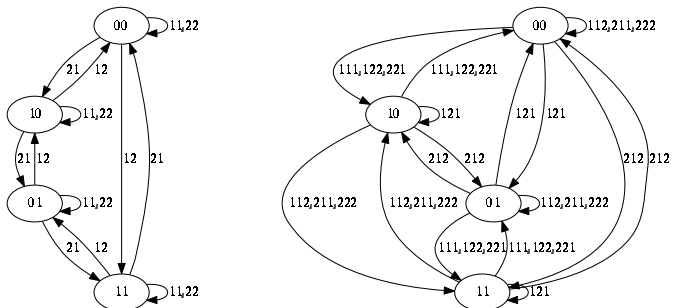
- $h(x_1, x_2) = (\bar{x}_1, x_1 \bar{x}_2 + \bar{x}_1 x_2)$
- $M_h = \frac{1}{2} \begin{pmatrix} 1010 \\ 0101 \\ 1001 \\ 0110 \end{pmatrix}$
- $\pi_h = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$

# Espace pour itérations chaotiques ( $b$ )

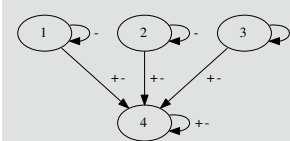
- Vers une fonction de  $\mathcal{X}_u = \mathbb{B}^N \times \llbracket 1; N \rrbracket^N$  dans lui-même [CCVHG16]:
  - $F_{f_u} : \mathbb{B}^N \times \llbracket 1; N \rrbracket \rightarrow \mathbb{B}^N, (x, i) \mapsto (x_1, \dots, x_{i-1}, f_i(x), x_{i+1}, \dots, x_N)$
  - $\sigma : \llbracket 1; N \rrbracket^N \rightarrow \llbracket 1; N \rrbracket^N$  t.q.  $\forall t \in \mathbb{N}, \sigma(s)_t = s_{t+1}$
  - $G_{f_u, b}$  définie par  $G_{f_u, b}(x, s) = (F_{f_u}(\dots(F_{f_u}(x, s_0), \dots), s_{b-1}), \sigma^b(s))$
- Distance  $d((x, s), (x', s')) = d_H(x, x') + d'_S(s, s')$

## (Fonctions t.q. $G_{f_u, b}$ est chaotique [CCVHG16])

La fonction  $G_{f_u, b}$  est chaotique sur  $(\mathcal{X}_u, d)$  si et seulement si le graphe d'itérations  $GIU_b(f)$  est fortement connexe.



- Seules 16 vérifient les hypothèses du théorème précédent.
- $b$  : nombre d'itérations suffisant pour une déviation p.r. la distribution uniforme inf. à  $10^{-4}$ .



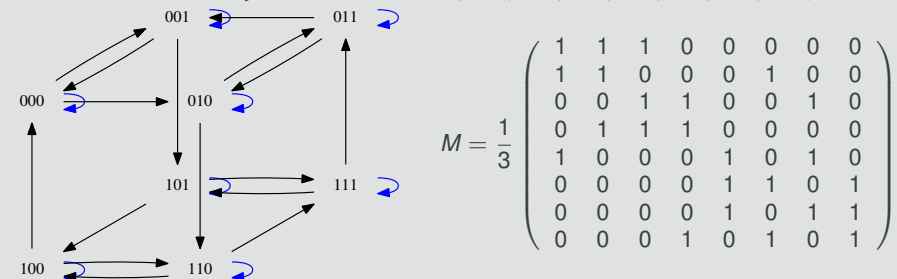
| Nom                | Définition   | $b$      |
|--------------------|--|----------|
| $\mathcal{F}_1$    | 14, 15, 12, 13, 10, 11, 8, 9, 6, 7, 4, 5, 2, 3, 1, 0 | 206      |
| $\vdots$           | $\vdots$   | $\vdots$ |
| $\mathcal{F}_9$    | 14, 15, 12, 13, 10, 11, 9, 8, 7, 6, 5, 4, 3, 2, 0, 1 | 42       |
| $\vdots$           | $\vdots$   | $\vdots$ |
| $\mathcal{F}_{16}$ | 14, 15, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1, 0 | 206      |

- Succès de tous les PRNGs issus de ces fonctions aux tests du National Institute of Standards and Technology (NIST).

- Erreur de raisonnement :
  - Générateur prouvé chaotique pour  $b = 1$ !
  - Pas compatible avec la pratique :  $b > 42$  nécessaire pour suivre une loi uniforme (à  $10^{-4}$  près).
  - Etendre la théorie!**

# GIU fortement connexe par construction

- CLPFD : approche de type « générer, tester ».
- $f^*(x_1, x_2, x_3) = (x_2 \oplus x_3, \bar{x}_1 x_3 + x_1 \bar{x}_2, \bar{x}_1 x_3 + x_1 x_2)$  : très faible  $b$ .
- $f^*$  : 3-cube ss le cycle hamiltonien 000, 100, 101, 001, 011, 111, 110, 010, 000.



## (N-cube privé d'un cycle hamiltonien [CHG+14])

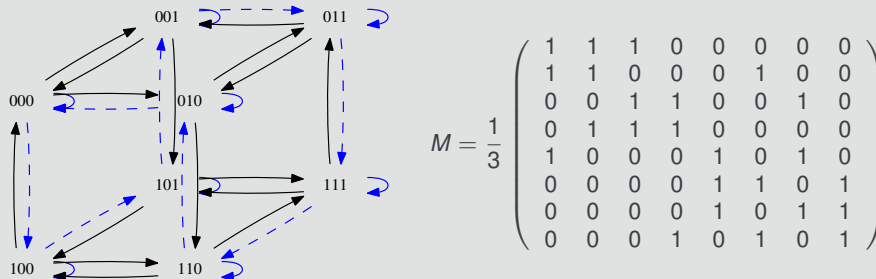
Dans un N-cube, dans lequel un cycle hamiltonien a été enlevé :

- La matrice de Markov engendrée est doublement stochastique.
- Le graphe GIU correspondant est fortement connexe.



## GIU fortement connexe par construction

- CLPFD : approche de type « générer, tester ».
- $f^*(x_1, x_2, x_3) = (x_2 \oplus x_3, \overline{x_1 x_3} + x_1 \overline{x_2}, \overline{x_1 x_3} + x_1 x_2)$  : très faible  $b$ .
- $f^*$  : 3-cube ss le cycle hamiltonien 000, 100, 101, 001, 011, 111, 110, 010, 000.



$$M = \frac{1}{3} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

### ( N-cube privé d'un cycle hamiltonien [CHG<sup>+</sup>14])

Dans un N-cube, dans lequel un cycle hamiltonien a été enlevé :

- La matrice de Markov engendrée est doublement stochastique.
- Le graphe GIU correspondant est fortement connexe.

## Evaluation de l'écart / distribution uniforme

### (Temps de mixage sans chemin hamiltonien [CCVHG16])

On considère un N-cube dans lequel un chemin hamiltonien a été supprimé et la fonction de probabilités  $p$  définie sur l'ensemble des arcs comme suit :

$$p(e) \begin{cases} = \frac{1}{2} + \frac{1}{2N} \text{ si } e = (v, v) \text{ avec } v \in \mathbb{B}^N, \\ = \frac{1}{2N} \text{ sinon.} \end{cases}$$

La chaîne de Markov associée converge vers la distribution uniforme et

$$t_{\text{mix}}(\varepsilon) \leq \lceil \log_2(\varepsilon^{-1}) \rceil 4(8N^2 + 4N \ln(N + 1))$$

- Remarques sur la preuve :
  - Itérations paresseuses  $\neq$  algorithme.
  - Hypothèse très faible : suppressions d'un arc entrant et d'un arc sortant par nœud.
  - Pratiquement :  $4(8N^2 + 4N \ln(N + 1)) \rightsquigarrow 4(2N \ln(2N + 8))$ .

## Codes de Gray équilibrés

- Intuition de convergence rapide vers la distribution uniforme : supprimer un cycle hamiltonien équilibré (chaque bit nié autant de fois).
- Extension de *Robinson-Cohn* [ZS04] : preuve de l'existence (sans construction) de cycle hamiltonien équilibré.

### (Constr. de cycles hamiltonien équilibré [CCVHG16])

Il existe une séquence (et construction de celle-ci) dans de l'extension de l'algorithme de Robinson-Cohn telle que le cycle est équilibré.

- Pratique : grande famille de cycles hamiltonien équilibrés ( $N \leq 16$ ).

## Et les itérations généralisées ?

**Input:** une fonction  $f$ , un nombre d'itérations  $b$ , une configuration initiale  $x^0$  (N bits)

**Output:** une configuration  $x$  (N bits)

$x \leftarrow x^0$ ;

$k \leftarrow b$ ;

**for**  $i = 1, \dots, k$  **do**

$s \leftarrow \text{Set}(\text{Random}(2^N))$ ;

$x \leftarrow F_{f_g}(x, s)$ ;

**end**

**return**  $x$ ;

### (Uniformité de la sortie ds le cas généralisé)

Soit  $f : \mathbb{B}^N \rightarrow \mathbb{B}^N$  et  $\tilde{M}$  sa matrice d'adjacence. Si  $\text{GIU}(f)$  est fortement connexe, alors la sortie du PRNG suit une loi qui tend vers la distribution uniforme si et ssi  $\frac{1}{2^N} \tilde{M}$  est une matrice doublement stochastique.

## Nombre moyen d'appels à un générateur binaire par bit généré

| Itérations   | 4    | 5    | 6    | 7    | 8    |
|--------------|------|------|------|------|------|
| Unaires      | 19.0 | 22.3 | 23.7 | 25.3 | 27.0 |
| Généralisées | 17   | 13   | 11   | 10   | 9    |

- Fréquence des configurations non accessibles en 1 itération :
  - Unaire :  $1 - \frac{n-1}{2^n}$  (croissant).
  - généralisée :  $1/2$  (constant), mais décroissance de la fréquence des bits constants.
- Test de NIST : succès dans tous les cas.

1. Introduction : iterations de réseaux booléens
2. Réseaux booléens : des preuves de convergences
3. Des systèmes dynamiques discrets au chaos
4. Applications à la génération de nombres pseudo-aléatoires
5. Application au masquage d'information
6. Conclusion


# Plan

1. Introduction : iterations de réseaux booléens
2. Réseaux booléens : des preuves de convergences
3. Des systèmes dynamiques discrets au chaos
4. Applications à la génération de nombres pseudo-aléatoires
5. Application au masquage d'information
6. Conclusion


# Synthèse scientifique


- Peut-on prédire le comportement de réseaux booléens (Sec. 2)
  - Théorique : **conditions théoriques** nécessaires/suffisantes de convergence/divergence ?
  - Pratique : vérification par simulation (**exhaustive ?**)
- Itérations divergentes ↔ **comportement chaotique** (Sec. 3) ?
  - Caractérisation des réseaux booléens chaotiques.
  - Génération et prédiction.
- Générateurs de nombres pseudo-aléatoires (Sec. 4) :
  - Caractérisation d'un PRNG chaotique.
  - Générations et qualité.
- Du Chaos au masquage d'information (Sec.5).
  - D'un point de vue chaotique.
  - D'un point de vue analyse vectorielle discrète.




 A. Abbas, J. M. Bahi, S. Contassot-Vivier, and M. Salomon.  
**Mixing synchronism / asynchronism in discrete-state discrete-time dynamic networks.**

In *4th Int. Conf. on Engineering Applications and Computational Algorithms, DCDIS'2005*, pages 524–529, Guelph, Canada, July 2005.  
ISSN 1492-8760.


 Jacques Bahi, Jean-François Couchot, and Christophe Guyeux.  
**Steganography : a class of secure and robust algorithms.**  
*The Computer Journal*, 55(6) :653–666, 2012.

 Jacques Bahi, Jean-François Couchot, Christophe Guyeux, and Adrien Richard.  
**On the link between strongly connected iteration graphs and chaotic boolean discrete-time dynamical systems.**


In *FCT'11, 18th Int. Symp. on Fundamentals of Computation Theory*, volume 6914 of *LNCS*, pages 126–137, Oslo, Norway, August 2011.

 J. M. Bahi, S. Contassot-Vivier, and J.-F. Couchot.  
**Convergence results of combining synchronism and asynchronism for discrete-state discrete-time dynamic network.**


Research Report RR2010-02, LIFC - Laboratoire d'Informatique de l'Université de Franche Comté, May 2010.


 Jean-François Couchot, Sylvain Contassot-Vivier, Pierre-Cyrille Héam, and Christophe Guyeux.  
**Random walk in a n-cube without hamiltonian cycle to chaotic pseudorandom number generation : Theoretical and practical considerations.**

*International Journal of Bifurcation and Chaos*, 2016.  
Accepted on Oct 2016.

 Jean-François Couchot, Pierre-Cyrille Héam, Christophe Guyeux, Qianxue Wang, and Jacques Bahi.  
**Pseudorandom number generators with balanced gray codes.**

In *Secrypt 2014, 11th Int. Conf. on Security and Cryptography*, pages 469–475, Vienna, Austria, August 2014.


 J.-F. Couchot.  
**Formal Convergence Proof for Discrete Dynamical Systems.**  
Research Report RR2010-03, LIFC - Laboratoire d'Informatique de l'Université de Franche Comté, May 2010.

 Christophe Guyeux.  
***Le désordre des itérations chaotiques et leur utilité en sécurité informatique.***

Thèse de Doctorat, LIFC, Université de Franche-Comté, 13 décembre 2010.

Rapporteurs : Pascale Charpin, Directrice de Recherche, INRIA-Rocquencourt ; Eric Filiol, Professeur, ESIEA-Laval ; Pierre Spitéri, Professeur Emérite, IRIT-ENSEEIH.  
Examineurs : Michel de Labachellerie, Directeur de recherche CNRS, Université de Franche-Comté ; Laurent Larger, Professeur, Université de Franche-Comté ; Jean-Claude Miellou, Professeur, Université de Franche-Comté ; Congduc Pham, Professeur, Université de Pau. Directeur : Jacques M. Bahi, Professeur, Université de Franche-Comté.

 Gerard J. Holzmann.  
***The SPIN Model Checker : Primer and Reference Manual.***  
Addison-Wesley, Pearson Education, 2003.

 A. J. van Zanten and I. N. Suparta.  
**Totally balanced and exponentially balanced gray codes.**

