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	Professeur à l'Ecole Polytechnique.
Jean-Paul COMET	Professeur à l'Université de Nice Sophia Antipolis
Juan-Pablo ORTEGA	Professeur à l'Université de St. Gallen–Suisse

Examinateurs :

Sylvain CONTASSOT-VIVIER	Professeur à l'Université de Lorraine
Raphaël COUTURIER	Professeur à l'Univ. Bourgogne Franche-Comté
Christophe GUYEUX	Professeur à l'Univ. Bourgogne Franche-Comté

Réseau booléen (définition)

- Une fonction $f : \mathbb{B}^{\mathsf{N}} \to \mathbb{B}^{\mathsf{N}}$, $x = (x_1, \ldots, x_{\mathsf{N}}) \mapsto (f_1(x), \ldots, f_{\mathsf{N}}(x))$
- 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* $S = \left(s^t\right)^{t\in\mathbb{N}}$, modification de l'élément s^t de x^t

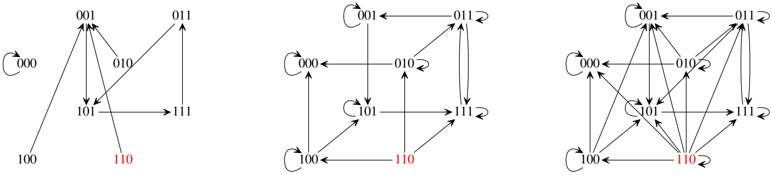
$$x^{t+1} = (x_1^{t+1}, \ldots, x_n^{t+1}) \text{ où } x_i^{t+1} = \begin{cases} f_i(x^t) \text{ si } i = s^t \\ x_i^t \text{ sinon.} \end{cases}$$

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

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

3 schémas $\leadsto$ 3 graphes d'itérations

Graphes des itérations de $(x_1, x_2, x_3) \mapsto ((\overline{x_1} + \overline{x_2}).x_3, x_1.x_3, x_1 + x_2 + x_3)$.

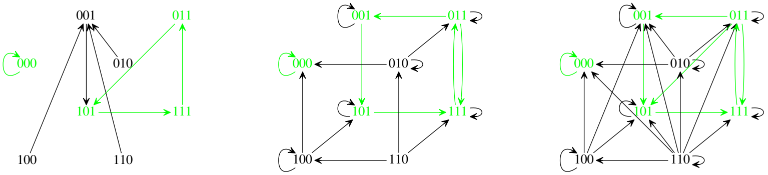


(a) GIS(f) (b) GIU(f) (c) GIG(f)

Attracteurs

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

Attracteurs de $(x_1, x_2, x_3) \mapsto ((\overline{x_1} + \overline{x_2}).x_3, x_1.x_3, x_1 + x_2 + x_3)$.



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

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

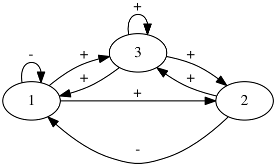
(f) $A_1 = \{000\}$ et $A_2 = \{001, 101, 111, 011\}$

Dépendance entre éléments

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

Graphes des interractions de $(x_1,x_2,x_3) \mapsto ((\overline{x_1}+\overline{x_2}).x_3, x_1.x_3, x_1+x_2+x_3)$.

$$f' = \begin{pmatrix} \frac{(x_1+\overline{x_2}).x_3-(\overline{x_1}+\overline{x_2}).x_3}{\overline{x_1}-x_1} & \frac{(\overline{x_1}+x_2).x_3-(\overline{x_1}+\overline{x_2}).x_3}{\overline{x_2}-x_2} & \dots \\ \frac{\overline{x_1}.x_3-x_1.x_3}{\overline{x_1}-x_1} & 0 & \dots \\ \frac{(\overline{x_1}+x_2+x_3)-(x_1+x_2+x_3)}{\overline{x_1}-x_1} & \dots & \dots \end{pmatrix}$$



Mode asynchrone

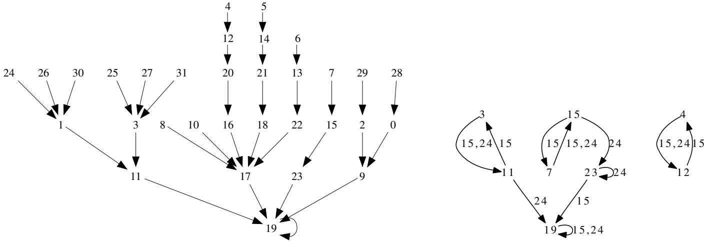
- Deux modes :
  - *synchrone* : chaque élément attend la valeur des élements dont il dépend ;
  - *asynchrone* : chaque élément met à jour sa valeur sans attendre.
- $(D^t)^{t\in\mathbb{N}}$: suite de matrices de taille N $\times$ N t.q.

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

- $x_i^{t+1} = \begin{cases} f_i(x_1^{D^t_{i1}}, \ldots, x_{\mathrm{N}}^{D^t_{i\mathrm{N}}}) \text{ si } i \in s^t \\ x_i^t \text{ sinon} \end{cases}$

Un exemple motivant

$$g(x_1, x_2, x_3, x_4, x_5) = (x_1.\overline{x_2} + \overline{x_1}.x_2, \overline{x_1 + x_2}, x_3.\overline{x_1}, x_5, \overline{x_3} + x_4)$$



(g) GIS(g) (h) GIU(g) (extrait)

FIGURE – Graphes des itérations synchrones

- Avec $D^t = t$ sauf $D^t_{12} = t - 1$ 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

Problématique

- Peut-on prédire le comportement de réseaux bouléens (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 bouléens 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.

Plan

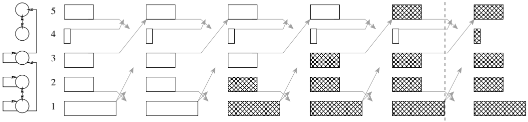
Un peu de Synchronisme

- *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 : $i\mathcal{R}j$ si i et j dans la même CFC du graphe des interactions.

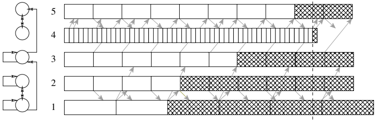
([BCVC10])

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.

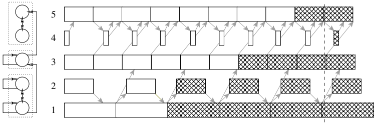
Mode mixte avec g



(a) Parallèle synchrone



(b) Asynchrone



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

FIGURE – Graphes des itérations de g

Convergence par la pratique

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

Du système booléen au modèle PROMELA

- 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 : $\diamond(\Box \texttt{Xp} = \texttt{X})$.

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

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

Plan

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

Plan

Plan

Synthèse scientifique

- Peut-on prédire le comportement de réseaux bouléens (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 bouléens 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.

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.

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.

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