Étude de la multiplication binaire et approches dynamiques pour la factorisation de nombres

Sylvain Contassot-Vivier et Nazim Fatès

Janvier 2014

Résumé : Le but de ce projet est d'étudier la faisabilité d'un système dynamique basé sur la multiplication binaire et de recenser différentes stratégies à explorer dans un but de factorisation de nombres entiers.

Équipe de recherche :	AlGorille et MaIA
Unité de recherche :	Loria – Nancy
Encadrants :	Sylvain Contassot-Vivier <http://www.loria.fr/~contasss/> et Nazim Fatès <http://www.loria.fr/~fates/>
Niveau :	Licence

Contexte

Ce stage concerne la conception d'algorithmes à l'aide de systèmes dynamique discrets. Si la compréhension de tels systèmes a largement consisté en l'étude empirique ou analytique de comportements [1], un domaine reste largement inexploré: celui de la résolution de problèmes algorithmiques particuliers.

Partant d'un cas précis, ce stage cherchera à dégager des méthodes originales de conception de systèmes dynamiques pour la résolution de problèmes informatiques. L'application choisie consiste en la résolution du problème de la factorisation de nombres entiers. L'objectif n'est pas tant de parvenir à trouver des solutions efficaces que de nous confronter à un problème suffisamment difficile pour constituer un bon point de départ pour notre approche. En particulier, l'une des questions clés sera de déterminer si l'utilisation du hasard peut *aider* à converger vers une solution [2].

Description

Les systèmes dynamiques discrets que nous considérons sont un ensemble d'éléments simples en interaction locale, et dont les états appartiennent à un ensemble fini et généralement réduit. L'état global du système (la collection des états de chaque élément) évolue à des temps discrets en appliquant une fonction locale sur tout ou partie des éléments ; on dit qu'un tel système *converge* lorsque son état ne change plus au cours du temps.

L'objectif du stage est de modéliser la multiplication binaire à l'aide de composants simples et d'étudier la dynamique du système. Le défi consiste à faire en sorte que le système se stabilise lorsque l'on atteint une factorisation du nombre entier "cible". Pour cela, on pourra par exemple partir de nombres initialement choisis au hasard et faire évoluer le système selon un réseau de propagation de contraintes. Une réflexion devra donc être conduite sur l'accessibilité des états du système et la façon de le mettre à jour (synchronisme des transitions, asynchronisme déterministe ou aléatoire, etc.)

Compétences requises

Ce travail combinera programmation et analyse mathématique. Des connaissances en théorie des systèmes dynamiques, automates cellulaires, systèmes multi-agents sont bienvenues. Les simulations seront effectuées en Java de préférence mais l'utilisation d'autres langages de programmation est aussi possible.

References

[1] J.M. Bahi, S. Contassot-Vivier, Basins of attraction in fully asynchronous discrete-time discrete-state dynamic networks. IEEE Transactions on Neural Networks, 2006, 17(2), pages 397-408.

[2] N. Fatès, Stochastic Cellular Automata Solve the Density Classification Problem with an Arbitrary Precision - When randomness helps computing *Theory of Computing Systems*, vol. 53(2), 2013, p. 223-242, http://hal.inria.fr/inria-00608485/