Analyse dynamique de l'algorithme LLL

18 Mars 2005

Sujet de thèse proposé par Brigitte Vallée,
Directrice de Recherches au CNRS (GREYC,
Université de Caen) à Antonio VERA

L'algorithme célèbre de réduction des réseaux euclidiens, l'algorithme LLL, [3] est un algorithme de base en théorie algorithmique des nombres et en cryptographie. C'est un outil central dans la cryptanalyse de nombreux schémas cryptographiques [4], notamment dans certaines variantes de RSA. Cet algorithme est à la fois extrèmement utilisé et très mal compris. En particulier, son analyse est encore balbutiante, et les méthodes classiques d'analyse d'algorithmes se heurtent à la structure trop complexe de cet algorithme. Les méthodes dynamiques introduites par le groupe caennais en analyse d'algorithmes peuvent s'avérer sans doute très efficaces dans ce cadre.

Depuis 5 à 6 ans, le groupe caennais prend conscience du rôle très important que peut jouer la théorie des systèmes dynamiques dans l'analyse en moyenne des algorithmes. Il a élaboré un nouveau concept, celui d' analyse dynamique des algorithmes où l'on considère un algorithme et l'ensemble de ses données comme un système dynamique. Les données sont alors les particules du système qui sont soumises au champ créé par les opérations que leur fait subir l'algorithme. A un système dynamique, on associe classiquement, depuis Ruelle, un opérateur appelé opérateur de transfert qui permet de décrire l'évolution du système. L'idée originale du groupe caennais consiste à détourner l'opérateur de transfert de son usage habituel et à le considérer comme un opérateur super-générateur , en ce sens qu'il engendre lui-mème les séries génératrices associées à l'algorithme. Les opérations sur les algorithmes continuent à bien se traduire en opérations sur ces opérateurs générateurs, et la valeur propre dominante de l'opérateur de transfert concentre les propriétés essentielles du système. C'est pourquoi elle va jouer un rôle essentiel, le mème rôle que la singularité dominante dans le cadre classique des séries génératrices, et va ainsi permettre d'appréhender le comportement asymptotique moyen de l'algorithme, mème quand celui-ci est corrélé .

L'algorithme LLL peut ètre vu comme une généralisation multidimensionnelle de l'algorithme d'Euclide, qui fonctionne, lui, en dimension 1. Maintenant que le groupe caennais a presque complètement élucidé les phénomènes dynamiques sous-jacents à l'analyse des algorithmes d'Euclide [5, 6, 1], il veut utiliser son expertise et son expérience de la modélisation dynamique pour passer à des dimensions supérieures.

En dimension 2, c'est l'algorithme de Gauss qui constitue à la fois la première généralisation de l'algorithme d'Euclide, et la brique de base de l'algorithme LLL. Le groupe caennais a déjà obtenu également des résultats précis sur l'analyse de l'algorithme de Gauss, il y a une petite dizaine d'années [2] : il avait décrit le système dynamique sous-jacent à l'algorithme de Gauss, et étudié le manière approfondie le nombre d'itérations de l'algorithme dans le cas

où les entrées sont distribuées uniformément. Le groupe souhaite maintenant revenir à cet algorithme pour résoudre des problèmes plus complexes :

- étude précise d'autres paramètres importants de l'algorithme, comme les quotients , ou les continuants , analyse de la complexité moyenne en bits,
- étude de paramètres importants de la configuration de sortie : défaut d'orthogonalité, et plus généralement distribution de la configuration de sortie.
- prise en compte d'autres modèles aléatoires pour les entrées, car la distribution uniforme des entrées n'est pas un choix légitime pour les applications cryptographiques. En particulier, quelle est l'influence de la distribution des entrées sur le comportement de l'algorithme et la distribution des sorties ?

Cette étude complète de la dimension 2 pourrait débuter lors du stage de Master.

Nous chercherons ensuite à appliquer ces résultats précis de la dimension 2 séparément dans chacune des boites de l'algorithme LLL.

Ensuite, il faut passer à une modélisation globale de l'algorithme LLL pour des dimensions supérieures, et la dimension 3 est une transition entre les petites dimensions (1 et 2) et les dimensions générales. On pourra commencer par décrire le système dynamique sous-jacent à l'algorithme LLL(3), et obtenir une analyse en moyenne de cet algorithme -avec peut-être des hypothèses heuristiques simplificatrices- dans un certain nombre de modèles aléatoires.

Le but ultime est l'étude du cas général de la dimension quelconque : il faut alors obtenir une description du système dynamique sous-jacent à l'algorithme. Ce système est probablement trop complexe pour qu'on puisse le manipuler tel quel, et des hypothèses simplificatrices devront sans doute être prises en compte. Nous chercherons à répondre aux mèmes questions que celles que nous nous sommes posés en dimension 2, et à comparer le comportement de l'algorithme et de ses configurations de sortie dans le cas de distributions d'entrées que l'on rencontre couramment en cryptographie. On pourrait ainsi formellement prouver la faisabilité de nombreuses cryptanalyses, et la thèse permettrait d'obtenir des bornes en moyenne , plus réalistes que les bornes actuelles, garanties par le pire des cas.

Références

[1] DAIREAUX, B. Page web personnelle, rubrique recherche. http ://users.info.unicaen.fr/∼daireaux/.

[2] DAUDÉ, H., FLAJOLET, P., AND VALLÉE, B. An average-case analysis of the gaussian algorithm for lattice reduction. In *Combinatorics, Probability and Computing, Cambridge University Press*, vol. 6. 1997, pp. 397–433.

[3] LENSTRA, A., LENSTRA, H., AND LOVASZ, L. Factoring polynomials with rational coefficients. *Mathematische Annalen 261*, 4 (1982), 515–534.

[4] NGUYEN, P., AND STERN, J. The two faces of lattices in cryptology. In *Proceedings of CALC '01* (2001), no. 2146 in Lecture Notes in Computer Science, pp. 146–180.

[5] VALLÉE, B. Euclidean dynamics. Soumis.

[6] VALLÉE, B. Page web personnelle, rubrique recherche. http ://users.info.unicaen.fr/∼brigitte/.