Résolution de Systèmes Algébriques Creux

Équipe d'accueil : SALSA (`http://www-salsa.lip6.fr/`) équipe commune INRIA/UPMC.
Lieu : Le stage se déroulera au Laboratoire d'Informatique de Paris 6 (LIP6) sur le campus de Jussieu.
Adresse : 4, place Jussieu, F-75252 Paris Cedex 05.
Encadrants :

- J.-C. Faugère (`Jean-Charles.Faugere@inria.fr`)
- L. Perret (`ludovic.Perret@lip6.fr`)

1 Description

Le stage se situe en calcul scientifique (Computer Algebra en anglais). L'objet est plus précisément la résolution de systèmes non-linéaires (ou algébriques). En effet, la résolution de nombreux problèmes (cryptologie, optimisation, géométrie algorithmique,...) peuvent se ramener à l'étude des solutions de systèmes algébriques. Les bases de Gröbner constituent souvent la méthode générale la plus appropriée pour cette étude [1, 2, 4]. L'algorithme de Buchberger constitue la méthode historique pour calculer ces bases. Des algorithmes de nouvelles générations, à savoir F_4 et F_5 [3, 4], permettent aujourd'hui de calculer relativement efficacement ces bases de Gröbner.

Les systèmes polynomiaux provenant d'applications présentent de nombreuses spécificités. Ils sont de très grande taille (plusieurs centaines ou milliers d'équations et de variables pour des applications en cryptographie) ce qui rend leur résolution très difficile en pratique. Toutefois, ils possèdent le plus souvent une forte structure. Dans ce stage, on souhaite s'intéresser aux systémes "*creux*".

Le stage débutera par un travail de bibliographie pour se familiariser avec les bases de Gröbner. A priori, les algorithmes de bases de Gröbner n'ont pas de statégie spécifique pour les systèmes "*creux*" . On propose donc d'étudier un algorithme dédié permettant de résoudre des systèmes "*creux*" [7]. On demande ensuite d'implanter cet algorithme dans un système de Calcul Formel comme Maple ou Magma [1] et comparer les performances de cet algorithme avec les bases de Gröbner. Finalement, on pourra étudier la possibilité d'incorporer des idées de [7] pour améliorer la rsolution des systèmes "*creux*" avec des bases de Gröbner.

Références

[1] B. Buchberger. *Gröbner Bases : an Algorithmic Method in Polynomial Ideal Theory.* Recent trends in multidimensional systems theory. Reider ed. Bose, 1985.

[2] D. A. Cox, J.B. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms : an Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer-Verlag. New York, 1992.

1. `http://magma.maths.usyd.edu.au/magma/`

[3] J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Basis :* F_4. Journal of Pure and Applied Algebra, vol. 139, pp. 61–68, 1999.

[4] J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Casis without Reduction to Zero :* F_5. Proceedings of ISSAC, pp. 75–83. ACM press, July 2002.

[5] Claude E. Shannon. *A Mathematical Theory of Communication.* Bell System Technical Journal, Vol. 27, pp. 379–423, 1948.

[6] B. Schneier. *Applied Cryptography.* Second Edition, John Wiley & Sons, 1996.

[7] Igor Semaev. *Sparse Algebraic Equations over Finite Fields*. SIAM J. Comput. 39(2) : 388-409 (2009). Preliminary version available at `http://eprint.iacr.org/2010/140`.