Sujet de thèse

Algorithme incrémentaux pour le Calcul des Bases de Gröbner avec paramètres et implantation.

L'un des axes de recherche prioritaire de l'équipe POLSYS (INRIA/UPMC) est le calcul efficace des bases de Gröbner pour la résolution des systèmes polynomiaux. Ces méthodes sont utilisées dans de nombreuses applications (mécanismes, robotique, cryptographie, …) et l'efficacité des algorithmes est primordiale pour mener a bien les calculs.

Pour l'étude de certains mécanismes (conditions de mobilité et d'assemblage par exemple) il s'agit dans un premier temps de les modéliser par des équations polynomiales. Chacune de ces équations fait intervenir des variables de positions et des paramètres (ou encore variables d'usinage). Dans un deuxième temps, on utilise des algorithmes de calcul des bases de Gröbner pour *éliminer* les variables de positions afin d'obtenir des expressions algébriques ne dépendant que des paramètres. Pour certaines applications les algorithmes actuels ne permettent pas de mener à bien les calculs. Les objectifs de cette thèse sont les suivants :

- Proposer des versions tronquées (ou incrémentaux) des algorithmes existants (F4 ou F5) qui permettent d'arrêter prématurément les calculs (lorsque, en cours de calcul, on a produit assez d'équations).
- Réaliser une implantation en langage C d'un tel algorithme de calcul de base de Gröbner. Le candidat pourra s'appuyer sur une implantation existante (logiciel FGb [3]) de l'algorithme F4 et se concentrera sur la partie « génération de matrices » de ces algorithmes et pourra utiliser des librairies d'algèbre linéaire dédiées existantes (comme [3] ou [4]).

Le sujet de thèse proposé s'inscrit dans un projet de recherche collaboratif établi entre Dassault-Systèmes, l'équipe POLSYS.

[1] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1-3):61-88, June 1999.

[2] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, ISSAC '02, pages 75-83, New York, NY, USA, 2002. ACM.

[3] Jean-Charles Faugère. FGb: A Library for Computing Gröbner Bases. In Komei Fukuda, Joris Hoeven, Michael Joswig, and Nobuki Takayama, editors, *Mathematical Software - ICMS 2010*, volume 6327 of *Lecture Notes in Computer Science*, pages 84-87, Berlin, Heidelberg, September 2010. Springer Berlin / Heidelberg.

[4] Jean-Charles Faugère and Sylvain Lachartre. Parallel Gaussian Elimination for Gröbner bases computations in finite fields. In M. Moreno-Maza and J.L. Roch, editors, *Proceedings of the 4th International Workshop on Parallel and Symbolic Computation*, PASCO '10, pages 89-97, New York, NY, USA, July 2010. ACM.

Contact: Jean-Charles Faugère
(INRIA)