Résolution de systèmes polynomiaux de dimension zéro par algèbre linéaire rapide.

Jean-Charles Faugère [†] Pierrick Gaudry [‡] Louise Huot [†]
Guénaël Renault [†]

Résumé

Un des problèmes fondamentaux du calcul formel est la résolution de systèmes polynomiaux. Les bases de Gröbner sont un outil puissant pour résoudre ce problème en particulier pour les systèmes à coefficients dans les corps finis. Habituellement, pour résoudre efficacement un système d'équations polynomiales en utilisant les bases de Gröbner, on calcule dans un premier temps la base de Gröbner pour l'ordre du degré lexicographique inverse de l'idéal associé au système à résoudre ; puis en utilisant un algorithme de changement d'ordre on calcule la base de Gröbner lexicographique nous permettant de "lire" les solutions du système.

Depuis les années 1990, il est bien connu que les algorithmes de calcul de bases de Gröbner et les algorithmes de changement d'ordre sont reliés de très près à l'algèbre linéaire. De plus, sous des hypothèses génériques, résoudre un système polynomial de dimension zéro peut se faire en une complexité polynomiale en le nombre de solutions du système. Cependant, en raison de la complexité du changement d'ordre la résolution des systèmes polynomiaux a une complexité cubique en le nombre de solutions. La plupart des problèmes d'algèbre linéaire ont la même complexité que la multiplication de deux matrices carrées denses de taille $n \times n$: $O(n^\omega)$ avec $2 \leq \omega < 2.3727$. Ainsi une question essentielle est donc de décider si la résolution de systèmes de dimension zéro peut se faire en une complexité arithmétique polynomiale en le nombre de solutions avec exposant ω. Le but de cet exposé est de répondre à cette question. Sous des hypothèses génériques, nous montrons que la complexité de résoudre des systèmes polynomiaux engendrant des idéaux radicaux est en $\widetilde{O}(D^\omega)$ où D est le nombre de solutions du système et la notation $\widetilde{O}$ signifie que l'on omet les facteurs logarithmiques.

[†]UPMC, Université Paris 06 ; INRIA, Centre Paris Rocquencourt ; Projet PolSys, LIP6/CNRS ; UMR 7606, France ; Adresses e-mail : Jean-Charles.Faugere@inria.fr, {Louise.Huot,Guenael.Renault}@lip6.fr

[‡]Université de Lorraine ; LORIA, Lorraine ; Projet CARAMEL, LORIA/CNRS ; UMR 7503, France ; Adresse e-mail : Pierrick.Gaudry@loria.fr