Complexité du calcul de bases de Gröbner pour les systèmes quasi-homogènes

Jean-Charles Faugère[1], Mohab Safey El Din[1] et Thibaut Verron[1,2]

[1]Équipe-projet POLSYS (INRIA/UPMC/LIP6)
[2]École Normale Supérieure, Paris

On s'intéresse au problème de la résolution de systèmes polynomiaux. Plus précisément, soit K un corps et $(f_1, \ldots, f_n) \subset K[X_1, \ldots, X_n]$ une famille de polynômes, on cherche à décrire l'ensemble des racines communes des polynômes f_j. Ce problème est riche en applications, qu'elles soient théoriques (géométrie algorithmique, équations implicites) ou pratiques (cryptographie, robotique). L'outil que l'on utilise pour la résolution est le calcul d'une base de Gröbner du système. Ce calcul est difficile en général (par exemple, l'existence de solutions à un système polynomial est un problème NP-dur sur un corps fini), mais on peut souvent exploiter des informations supplémentaires sur la structure des systèmes afin d'en améliorer la complexité.

On considère ici la structure quasi-homogène. Plus précisément, on dira qu'un polynôme $f \in K[X_1, \ldots, X_n]$ est quasi-homogène de degré pondéré d s'il existe $(w_1, \ldots, w_n) \in \mathbb{Z}_{>0}^n$ tels que le polynôme $f(X_1^{w_1}, \ldots, X_n^{w_n})$ est homogène de degré d. Des polynômes avec cette structure sont susceptibles d'apparaître dans de nombreuses applications, par exemple dans des systèmes issus de la physique, où l'on voudrait tenir compte de la dimension des grandeurs, ou dans des problèmes plus théoriques, lorsqu'on introduit une variable pour représenter un polynôme homogène.

Dans cet exposé, on montre comment on peut utiliser les algorithmes adaptés aux systèmes homogènes pour calculer une base de Gröbner d'un système de polynômes quasi-homogènes $F = (f_1, \ldots, f_n)$. Sous des hypothèses de généricité, le système n'a qu'un nombre fini de solutions, qui est donné par la borne de Bézout pondérée $\prod_{i=1}^n \frac{d_i}{w_i}$ (où d_i est le degré pondéré de f_i). On montre aussi que le degré maximal atteint par les polynômes que l'on doit calculer est borné par la borne de Macaulay pondérée $\sum_{i=1}^n (d_i - w_i) + \max\{w_i\}$. Ces résultats s'obtiennent en étudiant la série de Hilbert de l'idéal.

On analyse la complexité des algorithmes F_5 et FGLM pour cette stratégie. L'analyse de la complexité de l'algorithme F_5 se fait en étudiant l'algorithme F_5-matriciel, qui modélise les réductions polynomiales par la réduction sous forme échelon de sous-matrices de la matrice de Macaulay de l'idéal. Au final, on montre que la complexité du calcul de base de Gröbner pour un système quasi-homogène est améliorée d'un facteur $(\prod_{i=1}^n w_i)^\omega$, par rapport à la complexité du calcul pour un système homogène de mêmes degrés.