Complexité du calcul de base de Gröbner pour des systèmes semi-réguliers surdéterminés

Magali Bardet
travail en commun avec Jean-Charles Faugère et Bruno Salvy

7 Novembre 2003
Séminaires de calcul formel et de cryptographie, Rennes

Nous nous intéressons au problème de la complexité du calcul d'une base de Gröbner pour des systèmes "suffisamment génériques" et surdéterminés. Par exemple, pour des systèmes dont les coefficients ont été tirés au hasard, ou pour des systèmes dont les générateurs ont des coefficients "indépendants". Notons que l'exemple de Mayr-Meyer, dont la complexité est doublement exponentielle, n'appartient pas à la catégorie des systèmes "suffisamment génériques".

Nous commençons l'exposé par des rappels sur les suites régulières et sur leurs propriétés. Pour un système de m équations à n inconnues avec $m \leq n$, la définition de suite régulière convient comme définition mathématique de "suffisamment générique", et la complexité du calcul d'une base de Gröbner est bien comprise. Pour de telles suites, on connaît leur série de Hilbert et leur régularité, et si la suite est en position de Noether et que l'on utilise l'ordre DRL (Degré Reverse Lexicographique), on peut prévoir exactement le comportement de l'algorithme de calcul de base de Gröbner F5 de Jean-Charles Faugère, et donner la complexité (arithmétique) globale du calcul. De plus, on peut montrer que "presque toute suite" est une suite régulière (l'ensemble des suites régulières est un ouvert de Zariski non vide dans l'ensemble des suites possibles, si on a fixé le nombre de générateurs et leurs degrés, ainsi que le nombre de variables). Cependant, dans de nombreuses applications, les systèmes rencontrés sont surdéterminés, et les études sur les suites régulières ne s'appliquent plus (en particulier, il n'existe plus de suites régulières).

Nous donnons une définition mathématique de "suffisamment générique". Nos définitions de suites semi-régulières et de degré de régularité étendent la notion de suite régulière et de régularité aux suites surdéterminées. Nous montrons que pour des suites semi-régulières, on peut prévoir les tailles exactes de chaque matrice intervenant dans la version matricielle de l'algorithme F5. Cela nous permet de calculer la série de Hilbert, le degré de régularité et le coût (arithmétique) global du calcul de la base de Gröbner, pour tout ordre gradué par le degré. Nous donnons un algorithme qui, étant donnés des entiers $m, n, d_1, \ldots, d_m$ calcul le degré de régularité d'une suite semi-régulière de m polynômes en n variables de degrés respectifs $d_1, \ldots, d_m$. En utilisant des techniques d'analyse asymptotique (séries génératrices, méthodes du point col et des points cols coalescents) nous calculons un développement asymptotique de ce degré en fonction du nombre de variables. Ainsi, pour une suite de $2n$ polynômes quadratiques en n variables à cœfficients entiers, le degré de régularité est $D_{\text{reg}} \sim 0.085786\, n + 1.0415\, n^{1/3} - 1.4697 + 1.7130\, \frac{1}{n^{1/3}} + o\left(\frac{1}{n^{1/3}}\right)$ (ainsi $D_{\text{reg}} \sim n/11.657$ est une bien meilleur borne que la borne de Macaulay $\sim n$ que l'on obtient si l'on ne tient pas compte de la surdétermination). Nous donnons la valeur explicite de chaque cœfficient, et le coût global du calcul est $\binom{n+D_{\text{reg}}-1}{D_{\text{reg}}}^{\omega}$ où ω est le coefficient d'algèbre linéaire. Nous prouvons que pour $m \leq n+1$, "presque toute" suite est une suite semi-régulière, et nous le conjecturons dans les autres cas.

Ces techniques s'appliquent également (moyennant quelques adaptations) au calcul d'une base de Gröbner pour un système modulo deux comportant les équations de corps $x_1^2 - x_1, \ldots, x_n^2 - x_n$ (voir l'exposé du séminaire de Cryptographie l'après-midi). Ce type de système a de nombreuses applications dans le domaine de la cryptographie.