Résolution de systèmes algèbriques en deux variables: Complexité binaire du calcul d'une représentation Univariée Rationnelle

March 30, 2013

La résolution de systèmes algébriques en deux variables est un problème fondamental avec des applications dans divers domaines tel que la geomètrie algorithmique, l'infographie... etc. Souvent, résoudre un système revient à calculer des approximations numériques de ses solutions. Aussi, pour faciliter ce calcul, de nombreux algorithmes de résolution procèdent d'abord par le calcul d'une *représentation univariée* des solutions ou en d'autre termes une application bijective donnant les solutions du système en fonction des racines d'un polynôme univarié. Outre le calcul des solutions, l'avantage d'une telle représentation est de réduire certains opérations sur des système bivarié à des opérations avec des polynômes univariés, un exemple intéressant est le calcul du signe d'un polynôme sur les solutions réelles d'un système. Le but de notre présentation est l'étude et le calcul de telles représentations pour un système de deux polynômes de degré d avec des coefficients entiers de taille τ.

Au coeur, des algorithmes calculant une *représentation univariée* des solutions se trouve le calcul d'une forme linéaire séparante, c'est-à-dire une combinaison linéaire des variables qui prend des valeurs différentes quand elle est évaluée en des solutions (complexes) distinctes du système.

Dans un premier temps, nous présenterons un nouvel algorithme qui calcul une forme linéaire séparante de manière déterministe. Ce dernier combine les propriétés du résultant de deux polynômes avec le calcul modulo des nombres premiers pour obtenir une forme séparante en $\tilde{O}_B(d^8 + d^7\tau)$ opérations binaires. Cette complexité réduit d'un facteur d^2 la meilleure complexité connue pour résoudre ce problème.

Étant donné un système de deux polynômes en deux variables, ainsi qu'une forme linéaire séparant ses solutions, résoudre ce système revient

à calculer une représentation univariée de ces solutions. Une première méthode, introduite par Gonzalez-Vega et El Kahoui [1], consiste à calculer une décomposition triangulaire après changement générique de variables. L'analyse de complexité de cette méthode montre que la représentation ainsi calculée est de taille $O(d^5 + d^4\tau)$. Une seconde méthode, procède en calculant une autre forme de représentation introduite par Rouillier, la Représentation Univariée Rationnelle ou *RUR*. Une borne en $O(d^5 + d^4\tau)$ sur la taille de la *RUR* peut être obtenue en appliquant au cas bivarié les résultats énoncés par Dahan et Schost [2] dans le cas général de n polynômes en n variables. Nous verrons cependant que dans le cas présent, cette borne peut être réduite d'un facteur d. Pour cela, nous montrerons que pour un système de deux polynômes en deux variables, une Représentation Univariée Rationnelle s'exprime de manière simple à l'aide d'un résultant de deux polynômes trivarié. Cette relation nous permet d'une part d'obtenir la borne ci-dessus sur la taille de la *RUR* et nous fourni d'autre part un algorithme simple pour la calculer. L'analyse de complexité montre qu'en utilisant cet algorithme, une Représentation Univariée Rationnelle peut se calculer pour le même prix qu'une représentation à la Gonzalez-Vega *c.a.d* $\tilde{O_B}(d^7 + d^6\tau)$ opérations binaires.

References

[1] L. González-Vega and M. El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic plane curve. *J. of Complexity*, 12(4):527–544, 1996.

[2] X. Dahan and E. Schost. Sharp estimates for triangular sets. *ISSAC 2004*.