Un algorithme géométrique efficace pour le calcul d'espaces de Riemann-Roch

Aude Le Gluher et Pierre-Jean Spaenlehauer
Université de Lorraine, INRIA Nancy - Grand Est, CNRS

Les espaces de Riemann-Roch sont des espaces vectoriels de fonctions sur une courbe algébrique auxquelles on demande de satisfaire un certain nombre de conditions quant à la localisation et l'ordre de leurs zéros et de leurs pôles. Le théorème de Riemann-Roch assure que ces espaces sont de dimension finie ; néanmoins, il ne donne pas de méthode explicite permettant d'en construire une base. Or, le calcul effectif de bases d'espaces de Riemann-Roch intervient dans de nombreux domaines pratiques, notamment pour l'arithmétique dans les jacobiennes de courbes ou dans des codes correcteurs d'erreurs algébraico-géométriques.

Donnons nous une courbe projective plane et irréductible C de degré d, non nécessairement lisse, sur un corps parfait $\mathbf{K}$. Choisissons sur cette courbe un diviseur D ne faisant pas intervenir de point singulier de C — c'est-à-dire une somme formelle finie à coefficients dans $\mathbf{Z}$ de points de la courbe — dont le degré, noté $\deg(D)$, correspond à la somme des multiplicités des points intervenant dans D.

On propose une variante probabiliste de type Las Vegas de l'algorithme de Brill et Noether décrit par Goppa [1] pour le calcul de l'espace de Riemann-Roch $L(D)$ associé à D. On prouve que sa complexité (estimée par le nombre d'opérations arithmétiques dans le corps $\mathbf{K}$) est en

$$O(\max(d^{2\omega}, \deg(D_+)^\omega)),$$

où $\omega \leq 2.38$ est la constante de l'algèbre linéaire et D_+ est le plus petit diviseur effectif vérifiant $D_+ \geq D$.

Cet algorithme probabiliste peut éventuellement échouer mais sous quelques conditions, on prouve que sa probabilité d'échec est bornée par

$$O(\max(d^4, \deg(D_+)^2)/|E|),$$

où E est un sous ensemble fini de $\mathbf{K}$ dans lequel peut choisir des éléments de $\mathbf{K}$ uniformément aléatoirement.

A notre connaissance, cette borne sur la complexité de notre algorithme est la meilleure obtenue jusqu'alors pour le calcul d'espaces de Riemann-Roch dans un cadre général. Elle améliore par exemple la borne en $O(d^6\deg(D_+)^6)$ obtenue par Huang et Ierardi [2]. Dans le contexte du calcul de la loi de groupe dans la jacobienne d'une courbe lisse, cas où $\deg(D_+) = O(d^2)$, notre borne améliore légèrement la meilleure borne connue à ce jour en $O(d^{2\omega+\varepsilon})$ (avec $\varepsilon > 0$) obtenue par Khuri-Makdisi [3].

Outre cette amélioration de complexité, notre algorithme jouit également du fait que son efficacité repose sur deux blocs pour lesquels des algorithmes efficaces existent : l'arithmétique des polynômes univariés et l'algèbre linéaire. Il peut donc être implémenté dans tout système de calcul formel disposant de ces briques de base. Nous avons implémenté cet algorithme en C++/NTL. Les résultats expérimentaux obtenus via cette implémentation semblent indiquer une amélioration des temps de calculs par rapport à l'implémentation dans le logiciel de calcul formel Magma. Ils confirment aussi la prédominance du coût de l'algèbre linéaire établie lors de l'analyse théorique.

Références

[1] V. D. Goppa. Algebraico-geometric codes *Izvestiya : Mathematics*, 21(1) :75–91, 1983.

[2] Ming-Deh Huang and Doug Ierardi. Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve. *Journal of Symbolic Computation*, 18(6) :519–539, 1994.

[3] Kamal Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Mathematics of Computation*, 76(260) :2213–2239, 2007.