Calculer les équations de courbes avec beaucoup de points

Virgile Ducet

Soit C une courbe définie sur un corps fini $\mathbb{F}_q$ et $N(C)$ le nombre de ses points $\mathbb{F}_q$-rationnels. Il est naturel de se demander quelle est la valeur maximale que peut atteindre $N(C)$. Les bornes de Hasse-Weil-Serre ou de Oestérlé par exemple en donnent une majoration, et les travaux récents de Howe et Lauter permettent dans certains cas d'améliorer encore l'estimation des valeurs possibles pour $N(C)$ en prouvant qu'il ne peut exister de courbes avec un nombre précis de points. Afin de vérifier si ces bornes supérieures sont optimales, il est nécessaire de construire des courbes avec le plus grand nombre de points possible. D'un autre côté, construire des courbes avec beaucoup de points est utile pour les applications aux codes de Goppa. Notons que ces courbes étant construites grâce à diverses propriétés théoriques, il est généralement difficile d'obtenir leurs équations.

Le but du travail effectué en collaboration avec Claus Fieker ("Computing Equations of Curves with Many Points", à paraître dans les proceedings de la conférence "ANTS X"), est d'une part d'expliquer comment calculer explicitement les équations des revêtement abéliens de n'importe quelle courbe définie sur un corps fini, et d'autre part de décrire un algorithme permettant de trouver des courbes munies de beaucoup de points rationnels sur des petits corps finis. L'implémentation de cet algorithme a produit 7 nouveaux records sur $\mathbb{F}_2$.

L'article s'articule autour de la théorie du corps de classe sur les corps de fonctions, dont le théorème principal explicite une correspondance bijective entre les revêtements abéliens d'une courbe C et des données de nature arithmétique propres à C (groupes de classes dit "de rayon", diviseurs effectifs,...). Cette correspondance est l'outil principal de l'algorithme permettant de trouver de bonnes courbes. C'est également un outil important pour le calcul des équations des revêtements abéliens de C, où l'on fait en plus intervenir les descriptions explicites fournies par les théories de Kummer et d'Artin-Schreier-Witt.