Améliorations des algorithmes de type Chudnovsky sur la droite projective

Bastien Pacifico
Travail joint avec Stéphane Ballet

Aix Marseille Université, I2M, Marseille, France.

Résumé

Il existe différentes manières de mesurer la complexité d'un algorithme de multiplication dans une extension de degré n d'un corps fini $\mathbb{F}_q$. La complexité bilinéaire d'un algorithme mesure son nombre de multiplications bilinéaires dans le corps de base, i.e. dépendant des deux éléments que l'on multiplie.

La méthode de D.V. et G.V. Chudnovsky (1988), qui généralise l'interpolation polynomiale à l'utilisation des courbes algébriques, permet de construire des algorithmes de bonne complexité bilinéaire. Précédemment, nous avions introduit une spécialisation de cette méthode à la droite projective, en utilisant des places de degrés croissants, et obtenu des algorithmes constructibles génériquement et efficacement tout en ayant une bonne complexité bilinéaire [1].

Dans cette présentation, nous verrons différents axes d'amélioration de ces algorithmes, notamment grâce à l'utilisation d'évaluations avec multiplicité.

1. Ballet, Bonnecaze and Pacifico, *Multiplication in finite fields with Chudnovsky-type algorithms over the projective line*, 2021.