Sur la multiplication dans les corps finis avec des algorithmes de type Chudnovsky sur la droite projective

Bastien Pacifico
Travail joint avec Stéphane Ballet et Alexis Bonnecaze

Aix Marseille Université, I2M, Marseille, France.

Résumé

La multiplication dans une extension finie d'un corps fini $\mathbb{F}_{q^n}$ nécessite plusieurs types d'opérations dans le corps de base : des additions, des multiplications scalaires et des multiplications bilinéaires. Les multiplications scalaires sont celles par une constante de $\mathbb{F}_q$ fixée, alors que les multiplications bilinéaires dépendent des deux éléments que l'on multiplient. Il est connu que les multiplication bilinéaires sont plus coûteuses que les multiplications scalaires. Cela mène à l'étude de la complexité bilinéaire des algorithmes de multiplications.

La méthode de D.V. et G.V. Chudnovsky (1988) permet de construire des algorithmes ayant une bonne complexité bilinéaire. Ce sont des algorithmes d'interpolation sur les points rationnels de courbes algébriques, i.e. sur les places rationnelles d'un corps de fonctions. Cependant, lorsque l'on veut multiplier dans de grandes extensions, cela implique l'utilisation de courbes avec beaucoup de points rationnels, et donc de genres élevés. Il n'existe à l'heure actuelle pas de méthode pour construire ces algorithmes de manière efficace. Depuis, l'algorithme de multiplication de Chudnovsky-Chudnovsky a grandement été étudié et généralisé. Il a notamment été rendu possible l'uilisation de places de degrés quelconques d'un corps de fonctions.

Dans cet exposé, nous proposons une construction générique récursive d'algorithmes de type Chudnovsky pour la multiplication dans une extension de corps fini quelconque. Cette méthode est une spécialisation des algorithmes de type Chudnovsky à la droite projective sur $\mathbb{F}_q$, et qui utilise des places de degrés croissants. Notre construction permet d'obtenir des algorithmes d'interpolation polynômiale constructible en temps polynômial et ayant une complexité bilinéaire intéressante, pour un degré d'extension quelconque. Nous expliciterons cette construction, et indroduirons une stratégie permettant d'optimiser la complexité totale de ces algorithmes.

Preprint

https ://arxiv.org/abs/2007.16082