
Une stratégie d'optimisation des algorithmes de type Chudnovsky sur la droite projective

Bastien Pacifico^{*1}, Stéphane Ballet¹, and Alexis Bonnetaze¹

¹Institut de Mathématiques de Marseille – Centre National de la Recherche Scientifique : UMR7373,
Ecole Centrale de Marseille : UMR7373, Aix Marseille Université : UMR7373 – France

Résumé

L'algorithme de multiplication de Chudnovsky et Chudnovsky permet de multiplier dans une extension $\mathbb{F}_{q^n}$ d'un corps fini $\mathbb{F}_q$. Il s'agit d'un algorithme d'interpolation utilisant l'évaluation sur les points rationnels d'une courbe algébrique. L'intérêt principal de cette construction est qu'elle fournit des algorithmes ayant une bonne complexité bilinéaire relativement au degré de l'extension. Néanmoins, la complexité totale de ces algorithmes reste élevée, ce qui les rend principalement utiles pour des considérations théoriques.

Récemment, des premiers travaux considèrent l'optimisation de la complexité totale de ces algorithmes. La méthode utilisée donne de premiers résultats intéressants, mais est très coûteuse puisqu'elle consiste à chercher exhaustivement la meilleure base parmi l'ensemble des bases possibles de $\mathbb{F}_{q^n}$.

D'autre part, il a également été étudié une stratégie de construction de tels algorithmes sur la droite projective, utilisant des places non seulement rationnelles mais de degrés croissants. Cette stratégie permet de voir l'algorithme de Chudnovsky dans le cadre de l'interpolation polynomiale. Cela a permis de déceler une stratégie constructive permettant d'améliorer la complexité totale des algorithmes de type Chudnovsky dans ce cadre.

^{*}Intervenant