Courbes de Shimura et algorithmes bilinéaires de multiplication dans les corps finis

Matthieu Rambaud

RÉSUMÉ : Grâce à l'algorithme d'interpolation de Chudnovsky et Chudnovsky (1988), la complexité bilinéaire de la multiplication dans les extensions de corps finis est proportionnelle à la taille de l'extension.

$\rightarrow$ Notre première contribution, le Théorème A, généralise et améliore l'état de l'art des majorations asymptotiques de la complexité. Il corrige par ailleurs les lacunes de nombreux résultats dans la littérature.

Nous ciblons ensuite le paramètre le plus important, qui est le choix de la courbe d'interpolation. En effet la conjecture de folklore suivante permet de diminuer d'environ de moitié la complexité bilinéaire : soit p premier et $t' = 2t$ pair, existe-t-il une famille de courbes $(X_i)_i$ sur l'extension de degré $2t$ de $\mathbf{F}_p$ telles que :

(i) les genres g_i tendent vers l'infini, avec des rapports consécutifs tendant vers un (densité) ;
(ii) la famille a un ratio optimal de points de degré un (borne de Drinfeld-Vladuts) ;
(iii) et les courbes descendent sur $\mathbf{F}_p$?

Nous donnons des contre-exemples qui invalident une preuve de la conjecture publiée récemment.

$\rightarrow$ Notre deuxième contribution, le Théorème B, apporte ensuite une solution explicite à la conjecture dans le cas particulier ($p = 3$ et $2t = 6$). Elle consiste à entrelacer des tours de courbes de Shimura (qui sont des espaces de modules de variétés abéliennes), puis à descendre leur corps de définition. Ces mêmes techniques produisent également une nouvelle courbe avec un nombre record de points.

Les Théorèmes A et B permettent de réduire de presque de moitié les meilleures bornes asymptotiques connues en petite caractéristique.

Nous optimisons enfin la construction effective d'algorithmes sur une courbe donnée. D'abord dans les petites algèbres, puis dans les extensions de taille cryptographique.

MOTS-CLEFS : Courbes de Shimura, multiplication dans les corps finis, descente de revêtements.

ABSTRACT : Thanks to the interpolation algorithm of Chudnovsky and Chudnovsky (1988), the bilinear complexity of multiplication in extensions of finite fields is proportional to the size of the extension.

$\rightarrow$ Our first contribution, Theorem A, generalizes and improves the state of the art asymptotic upper-bounds. It also corrects gaps in several results in the litterature.

With then target the most important parameter, i.e. the choice of the curve. Indeed the following folklore conjecture enables to cut by half the bilinear complexity of multiplication : for p prime and $t' = 2t$ even, does there exist a family of curves $(X_i)_i$ over the extension of degree $2t$ of $\mathbf{F}_p$, such that :

(i) the genera g_i tend to infinity, with consecutive ratios tending to one (density condition)
(ii) the family $(X_i)_i$ has an optimal ratio of points of degree one (bound of Drinfeld-Vladuts)
(iii) the curves descend over $\mathbf{F}_p$?

We firstly give counterexamples that invalidate a recently published proof of the conjecture.

$\rightarrow$ Our second contribution, Theorem B, provides an explicit solution to the conjecture in the particular case ($p = 3$ and $2t = 6$). The construction consists in intertwinning towers of Shimura curves (which are moduli spaces of abelian varieties), then to descend their field of definition. The same techniques also provide a new curve with a record number of points.

Theorems A and B enable to cut nearly by half the asymptotic bounds in small characteristic.

We finally optimize the effective construction of algorithms on a given curve : firstly in small algebras, then in extensions of cryptographic size.

KEY-WORDS : Shimura curves, multiplication in finite fields, descent of covers.

TELECOM ParisTech

EDITE

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY