Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 343 (2006) 265–266
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Géométrie algébrique

Complexité bilinéaire de la multiplication dans des petits corps finis

Jean Chaumine

Département de mathématiques, université de la Polynésie française, B.P. 6570, 98702 Faa'a, Tahiti, Polynésie française

Reçu le 5 octobre 2005 ; accepté après révision le 22 juin 2006

Disponible sur Internet le 21 juillet 2006

Présenté par Yves Meyer

Résumé

A partir de la structure de groupe abélien de l'ensemble des points rationnels d'une courbe elliptique, on améliore un théorème de Shokrollahi concernant l'application de l'algorithme de D.V. Chudnovsky et G.V. Chudnovsky sur des courbes algébriques de genre 1. Plus précisément, on montre que, si $\frac{1}{2}q+1<n\leqslant\frac{1}{2}(q+1+\epsilon(q))$, alors la complexité bilinéaire de la multiplication dans des extensions de degré n d'un corps fini $\mathbb{F}_q$ est égale à $2n$. ***Pour citer cet article : J. Chaumine, C. R. Acad. Sci. Paris, Ser. I 343 (2006).***

Abstract

On the bilinear complexity of the multiplication in small finite fields. In this Note, we improve a result of Shokrollahi who has applied the algorithm of D.V. Chudnovsky and G.V. Chudnovsky to algebraic curves of genus one. More precisely, from the Abelian group structure of the set of rational points on elliptic curves, we show that, if $\frac{1}{2}q+1<n\leqslant\frac{1}{2}(q+1+\epsilon(q))$, then the bilinear complexity of the multiplication in all extensions $\mathbb{F}_{q^n}$ is equal to $2n$. ***To cite this article: J. Chaumine, C. R. Acad. Sci. Paris, Ser. I 343 (2006).***

1. Complexité bilinéaire de la multiplication

Soient $\mathbb{F}_q$ un corps fini à q éléments où $q=p^r$ est une puissance d'un nombre premier p et $\mathbb{F}_{q^n}$ une extension de $\mathbb{F}_q$ de degré n. La complexité bilinéaire de la multiplication m dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, notée $\mu_q(n)$, est le rang du tenseur $t_m\in\mathbb{F}_{q^n}^*\otimes\mathbb{F}_{q^n}^*\otimes\mathbb{F}_{q^n}$ associé à m, où $\mathbb{F}_{q^n}^*$ désigne le dual de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ (voir [7,1]). Winograd [9] et De Groote [4] ont montré que $\mu_q(n)\geqslant 2n-1$, avec égalité si et seulement si $n\leqslant\frac{1}{2}q+1$. Par ailleurs, en appliquant l'algorithme de Chudnovsky [3] sur des courbes elliptiques, Shokrollahi [5] a montré le théorème suivant :

Théorème 1.1. *La complexité bilinéaire $\mu_q(n)$ de la multiplication dans $\mathbb{F}_{q^n}$ est égale à $2n$ si $\frac{1}{2}q+1<n<\frac{1}{2}(q+1+\epsilon(q))$ où ϵ est la fonction définie par* :

$$\epsilon(q)=\begin{cases}\text{le plus grand entier}\leqslant 2\sqrt{q}\text{ et premier avec } q, & \text{si } q \text{ n'est pas un carré parfait.}\\ 2\sqrt{q}, & \text{si } q \text{ est un carré parfait.}\end{cases}$$

Adresse e-mail : chaumine@upf.pf (J. Chaumine).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2006.06.030

2. Amélioration du résultat de Shokrollahi

Dans cette Note, on améliore, dans le cas des courbes elliptiques, le théorème de Shokrollahi, en élargissant la plage des degrés d'extension du corps fini $\mathbb{F}_q$ où l'on peut appliquer l'algorithme de Chudnovsky avec une complexité bilinéaire de la multiplication dans $\mathbb{F}_{q^n}$ égale à $2n$. Plus précisément, en utilisant la structure de groupe abélien de l'ensemble des points rationnels d'une courbe elliptique, on obtient le résultat suivant [2] :

Théorème 2.1. *Soient q une puissance d'un nombre premier et n un entier naturel tel que* :

$$\frac{1}{2}q + 1 < n \leqslant \frac{1}{2}\big(q + 1 + \epsilon(q)\big).$$

Alors la complexité bilinéaire de la multiplication dans $\mathbb{F}_{q^n}$ vérifie :

$$\mu_q(n) = 2n.$$

Ce théorème découle de l'existence d'un corps de fonctions elliptiques vérifiant les propriétés énoncées dans la proposition suivante :

Proposition 2.2. *Soit q une puissance d'un nombre premier. Soit n un entier naturel vérifiant l'inégalité $3 \leqslant n \leqslant \frac{1}{2}(q + 1 + \epsilon(q))$. Il existe un corps de fonctions elliptiques $E/\mathbb{F}_q$ contenant k places $P_0, \ldots, P_{k-1}$ de degré 1 avec $k \geqslant 2n$, une place Q de degré n et un diviseur $\mathcal{D}$ de degré n tels que* :

1. $[\mathcal{D}] \neq [Q]$,
2. $2\mathcal{D} - (P_{i_0} + \cdots + P_{i_{2n-1}})$ *n'est pas principal,*
3. $\operatorname{ord}_{P_i}(\mathcal{D}) = 0$ *pour* $i = 0, \ldots, k-1$.

Cette proposition se justifie à l'aide des deux lemmes suivants :

Lemme 2.3. *Soit $q \geqslant 4$ une puissance d'un nombre premier. Soit $n \geqslant 3$ un entier naturel. Alors tout corps de fonctions elliptiques $E/\mathbb{F}_q$ a au moins une place de degré n.*

Lemme 2.4. *Soit q une puissance d'un nombre premier. Soit E une courbe elliptique sur $\mathbb{F}_q$. Soient P_j un point rationnel de E et $\oplus$ la loi de groupe sur l'ensemble des points rationnels $E(\mathbb{F}_q)$ décrite dans* [8]. *Alors l'équation $P \oplus P = P_j$ a au plus quatre solutions.*

Remarque. Par exemple, si on veut multiplier dans $\mathbb{F}_{8^7}$, le résultat de Shokrollahi ne nous permet pas d'appliquer l'algorithme de Chudnovsky à une courbe elliptique. On peut au mieux utiliser une courbe hyperelliptique de genre 2 et on obtient une complexité bilinéaire $\mu_8(7) \leqslant 15$ d'après [1,6]. Le résultat obtenu dans cette Note montre l'existence d'un corps de fonctions elliptiques pour lequel la complexité bilinéaire de la multiplication dans $\mathbb{F}_{8^7}$ est égale à 14.

Références

[1] S. Ballet, Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$, Finite Fields and Their Applications 5 (1999) 364–377.
[2] J. Chaumine, Corps de Fonctions Algébriques et Algorithme de D.V. Chudnovsky et G.V. Chudnovsky pour la Multiplication dans les Corps Finis, Thèse, Université de la Polynésie française, 2005.
[3] D.V. Chudnovsky, G.V. Chudnovsky, Algebraic complexities and algebraic curves over finite fields, Journal of Complexity 4 (1988) 285–316.
[4] H.F. De Groote, Characterization of division algebras of minimal rank and the structure of their algorithm varieties, SIAM J. Comput. 12 (1) (1983) 101–117.
[5] M.A. Shokrollahi, Optimal algorithms for multiplication in certain finite fields using elliptic curves, SIAM J. Comput. 21 (6) (1992) 1193–1198.
[6] M.A. Shokrollahi, On the rank of certain finite fields, Comput. Complexity 1 (1991) 157–181.
[7] I.E. Shparlinski, M.A. Tsfasman, S.G. Vlăduţ, Curves with many points and multiplication in finite fields, in: Lecture Notes in Mathematics, vol. 1518, Springer-Verlag, Berlin, 1992, pp. 145–169.
[8] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
[9] S. Winograd, On multiplication in algebraic extension fields, Theoretical Computer Science 8 (1979) 359–377.