Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 339 (2004) 383–385
COMPTES RENDUS MATHEMATIQUE

Théorie des nombres

Amélioration des bornes de la complexité bilinéaire de la multiplication dans certains corps finis

Stéphane Ballet, Jean Chaumine

Laboratoire de géométrie algébrique et applications à la théorie de l'information, université de la Polynésie française, BP 6570, 98702 Faa'a, Tahiti, Polynésie française

Reçu le 27 avril 2004 ; accepté après révision le 8 juin 2004

Disponible sur Internet le 21 août 2004

Présenté par Yves Meyer

Résumé

À partir de l'existence d'une tour de corps de fonctions algébriques, on améliore les bornes de la complexité bilinéaire de la multiplication dans toutes les extensions des corps finis $\mathbb{F}_p$ et $\mathbb{F}_{p^2}$ où p est un nombre premier $\geqslant 5$. En particulier, on améliore les bornes supérieures asymptotiques de cette complexité pour les corps finis premiers en caractéristique $p > 5$. ***Pour citer cet article : S. Ballet, J. Chaumine, C. R. Acad. Sci. Paris, Ser. I 339 (2004).***

Abstract

An improvement of bilinear complexity bounds in some finite fields. From the existence of a tower of algebraic function fields, we improve upper bounds on the bilinear complexity of multiplication in all extensions of the finite fields $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ where p is a prime $\geqslant 5$. In particular, we improve asymptotic upper bounds on this complexity for prime finite fields. ***To cite this article: S. Ballet, J. Chaumine, C. R. Acad. Sci. Paris, Ser. I 339 (2004).***

1. Complexité bilinéaire de la multiplication

Soit $\mathbb{F}_q$ un corps fini à q éléments où q est une puissance d'un nombre premier p et soit $\mathbb{F}_{q^n}$ une extension de degré n de $\mathbb{F}_q$. La multiplication m dans le corps fini $\mathbb{F}_{q^n}$ est une application bilinéaire de $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ dans $\mathbb{F}_{q^n}$, par conséquent il lui correspond une application linéaire M définie du produit tensoriel $\mathbb{F}_{q^n} \bigotimes \mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ dans $\mathbb{F}_{q^n}$. On peut aussi représenter M par un tenseur $t_M \in \mathbb{F}_{q^n}^* \bigotimes \mathbb{F}_{q^n}^* \bigotimes \mathbb{F}_{q^n}$ où $\mathbb{F}_{q^n}^*$ désigne le dual de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. La complexité bilinéaire de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, notée $\mu_q(n)$, est le rang du tenseur t_M (cf. [5,1]). On sait d'après [1,2] et [3] que, dans tout corps fini $\mathbb{F}_{q^n}$, cette complexité vérifie $\mu_q(n) \leqslant C_q n$ où C_q est la constante définie par :

Adresses e-mail : ballet@upf.pf (S. Ballet), chaumine@upf.pf (J. Chaumine).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2004.06.011

$$C_q = \begin{cases} 54 & \text{si } q = 2, \\ 27 & \text{si } q = 3, \\ 2\left(1 + \dfrac{p}{\sqrt{q}-3}\right) & \text{si } q > 16 \text{ et si } q \text{ est un carré parfait}, \\ 6\left(1 + \dfrac{p}{q-3}\right) & \text{si } q > 3, \\ 3\left(1 + \dfrac{8}{q-5}\right) & \text{si } q = 2^r \geqslant 16. \end{cases}$$

Ces bornes sont obtenues par l'existence de tours de corps de fonctions algébriques vérifiant les conditions du théorème suivant [1,3] :

Théorème 1.1. *Soit q une puissance d'un nombre premier et n un entier naturel > 1. Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre g et N_k le nombre de places de degré k de $F/\mathbb{F}_q$. Si $F/\mathbb{F}_q$ est tel que $2g + 1 \leqslant q^{(n-1)/2}(q^{1/2} - 1)$ et :*

(1) *si $N_1 > 2n + 2g - 2$, alors*

$$\mu_q(n) \leqslant 2n + g - 1,$$

(2) *s'il existe un diviseur non-spécial de degré $g - 1$ et si $N_1 + 2N_2 > 2n + 2g - 2$, alors*

$$\mu_q(n) \leqslant 3n + 3g,$$

(3) *si $N_1 + 2N_2 > 2n + 4g - 2$, alors*

$$\mu_q(n) \leqslant 3n + 6g.$$

Dans cette Note, en utilisant une tour de corps de fonctions algébriques introduite par Garcia et Stichtenoth dans [4] vérifiant les conditions du Théorème 1.1, nous obtenons de nouvelles bornes de la complexité bilinéaire de la multiplication dans toutes les extensions de $\mathbb{F}_{p^2}$ et $\mathbb{F}_p$ de caractéristique $p \geqslant 5$.

2. Nouvelles bornes de la complexité bilinéaire

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. Pour tout corps de fonctions algébriques $F/\mathbb{F}_q$, on notera $g(F/\mathbb{F}_q)$ le genre de $F/\mathbb{F}_q$ et $N_k(F/\mathbb{F}_q)$ le nombre de places de degré k de $F/\mathbb{F}_q$. Considérons la tour T sur $\mathbb{F}_q$ définie par récurrence par l'équation suivante étudiée dans [4] :

$$y^2 = \frac{x^2 + 1}{2x}.$$

La tour $T/\mathbb{F}_q$ est représentée par une suite de corps de fonctions $(T_0, T_1, T_2, \ldots)$ où $T_n = \mathbb{F}_q(x_0, x_1, \ldots, x_n)$ et $x_{i+1}^2 = (x_i^2 + 1)/2x_i$ pour tout $i \geqslant 0$. Notons que T_0 est le corps des fractions rationnelles. Pour tout nombre premier $p \geqslant 3$, la tour $T/\mathbb{F}_{p^2}$ est asymptotiquement optimale sur le corps $\mathbb{F}_{p^2}$, c'est-à-dire $T/\mathbb{F}_{p^2}$ atteint la borne de Drinfeld–Vladut [6]. De plus, pour tout entier k, $T_k/\mathbb{F}_{p^2}$ est l'extension du corps des constantes de $T_k/\mathbb{F}_p$. Plus précisément, on a :

Théorème 2.1. *Soit p un nombre premier $\geqslant 3$. Alors pour tout entier k, on a* :

(1) $N_1(T_k/\mathbb{F}_{p^2}) \geqslant 2^{k+1}(p-1)$ *et* $g(T_k/\mathbb{F}_{p^2}) \leqslant 2^{k+1}$,
(2) $N_1(T_k/\mathbb{F}_p) + 2N_2(T_k/\mathbb{F}_p) \geqslant 2^{k+1}(p-1)$ *et* $g(T_k/\mathbb{F}_p) \leqslant 2^{k+1}$.

On déduit de l'existence de cette tour la proposition suivante :

Proposition 2.2. *Soit p un nombre premier $\geqslant 5$. Alors pour tout entier $n \geqslant \frac{1}{2}(p+1+\epsilon(p))$ où $\epsilon(p)$ est le plus grand entier $< 2\sqrt{p}$,*

(1) *il existe un corps de fonctions algébriques $T_k/\mathbb{F}_{p^2}$ de genre $g(T_k/\mathbb{F}_{p^2})$ tel que $2g(T_k/\mathbb{F}_{p^2})+1 \leqslant p^{n-1}(p-1)$ et $N_1(T_k/\mathbb{F}_{p^2}) > 2n+2g(T_k/\mathbb{F}_{p^2})-2$,*
(2) *il existe un corps de fonctions algébriques $T_k/\mathbb{F}_p$ de genre $g(T_k/\mathbb{F}_p)$ tel que $2g(T_k/\mathbb{F}_p)+1 \leqslant p^{(n-1)/2}(p^{1/2}-1)$ et $N_1(T_k/\mathbb{F}_p)+2N_2(T_k/\mathbb{F}_p) > 2n+2g(T_k/\mathbb{F}_p)-2$ et un diviseur non-spécial de degré $g(T_k/\mathbb{F}_p)-1$.*

On en déduit alors le théorème suivant améliorant les bornes de la complexité bilinéaire de la multiplication dans toutes les extensions des corps finis $\mathbb{F}_{p^2}$ et $\mathbb{F}_p$ où p est un nombre premier $\geqslant 5$:

Théorème 2.3. *Soit p un nombre premier $\geqslant 5$. Alors pour tout entier $n \geqslant 1$,*

$$\mu_{p^2}(n) \leqslant 2n\left(1+\frac{2}{p-3}\right)$$

et

$$\mu_p(n) \leqslant 3n\left(1+\frac{4}{p-3}\right).$$

Ce résultat améliore, en particulier, les bornes supérieures asymptotiques de cette complexité pour les corps finis premiers en caractéristique $p > 5$, obtenues par Shparlinski, Tsfasman et Vladut dans [5], à savoir pour tout nombre premier $p \geqslant 3$:

$$\mathcal{M}_p = \limsup_{n\to\infty} \frac{\mu_p(n)}{n} \leqslant 6\left(1+\frac{1}{p-2}\right).$$

Plus précisément :

Corollaire 2.4. *Si p est un nombre premier > 5, alors*

$$\mathcal{M}_p = \limsup_{n\to\infty} \frac{\mu_p(n)}{n} \leqslant 3\left(1+\frac{4}{p-3}\right).$$

Références

[1] S. Ballet, Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$, Finite Fields Appl. 5 (1999) 364–377.
[2] S. Ballet, Low increasing tower of algebraic function fields and bilinear complexity of multiplication in any extension of $\mathbb{F}_q$, Finite Fields Appl. 9 (2003) 472–478.
[3] S. Ballet, R. Rolland, Multiplication algorithm in a finite field and tensor rank of the multiplication, J. Algebra 272 (1) (2004) 173–185.
[4] A. Garcia, H. Stichtenoth, H.-G. Ruck, On tame towers over finite fields, J. Reine Angew. Math. 557 (2003) 53–80.
[5] I.E. Shparlinski, M.A. Tsfasman, S.G. Vladut, Curves with many points and multiplication in finite fields, in: Coding Theory and Algebraic Geometry, in: Lectures Notes in Math., vol. 1518, Springer-Verlag, Berlin, 1992, pp. 145–169.
[6] H. Stichtenoth, Algebraic Function Fields and Codes, Lectures Notes in Math., vol. 314, Springer-Verlag, Berlin, 1993.