Bounds on the Bilinear Complexity of Multiplication in Any Extension of $\mathbb{F}_q$

S. Ballet, C.N.R.S. Institut de Mathématiques de Luminy
Luminy Case 907, F13288 Marseille CEDEX 9
e-mail: ballet@iml.univ-mrs.fr

1 Introduction - Notations

1.1 Bilinear complexity of multiplication

Let $\mathbb{F}_q$ be a finite field with q elements where q is a prime power and let $\mathbb{F}_{q^n}$ be a $\mathbb{F}_q$ extension of degree n. The multiplication M is a bilinear map from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ into $\mathbb{F}_{q^n}$, thus we can also represent M by a tensor $t_M = \sum_{l=1}^{\lambda} a_l \otimes b_l \otimes c_l \in \mathbb{F}^*_{q^n} \bigotimes \mathbb{F}^*_{q^n} \bigotimes \mathbb{F}_{q^n}$ where $\mathbb{F}^*_{q^n}$ denotes the dual of $\mathbb{F}_{q^n}$ as a $\mathbb{F}_q$-vector space. Hence the product of two elements x and y of $\mathbb{F}_{q^n}$ is :

$$x.y = t_M(x \otimes y) = \sum_{l=1}^{\lambda} a_l(x) b_l(y) c_l. \qquad (1)$$

Every expression (1) is called a bilinear multiplication algorithm $\mathcal{U}$. The number λ is called the multiplicative complexity $\mu(\mathcal{U})$ of $\mathcal{U}$. Let us set

$$\mu_q(n) = \min_{\mathcal{U}} \mu(\mathcal{U})$$

where $\mathcal{U}$ is running over all bilinear multiplication algorithms in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then $\mu_q(n)$ is called the bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and it corresponds to the minimum possible number of summands in any decomposition of tensor t_M.

1.2 Known results

For any integer n, the bilinear complexity $\mu_q(n)$ of multiplication in $\mathbb{F}_{q^n}$ is $\geq 2n-1$ by a result of Winograd [7]. Indeed, the multiplication in $\mathbb{F}_{q^n}$ consists on multiplying two polynomials of degree $\leq n-1$ modulo an irreducible polynomial of degree n. So, the result follows from the notion of interpolation. Then it is necessary to consider two cases:

a) If $\mathbb{F}_q$ is sufficiently large

De Groote [4] has shown that $\mu_q(n) = 2n - 1$ if $n \leq \frac{1}{2}q + 1$. Moreover, Winograd [7] has given a characterization of the class of algorithms realizing this complexity: these are interpolation algorithms of the projective line over $\mathbb{F}_q$ i.e polynomial interpolation algorithms.

b) If $\mathbb{F}_q$ is not sufficiently large

D.V. Chudnovsky and G.V. Chudnovsky in [2] have succeeded in obtaining a principle of construction of fast multiplication algorithms by using interpolation on algebraic curves. This principe generalizes the polynomial interpolation. Moreover, Shparlinsky, Tsfasman and Vladut in [6] have studied this principle, and found new asymptotic bounds. More precisely, they have proved that for any prime power $q \geq 3$, $M_{q^2} \leq 2(1 + \frac{1}{q-2})$, $M_q \leq 6(1 + \frac{1}{q-2})$ and $M_2 \leq 27$ where $M_q = lim\ sup_{n \to \infty} \mu_q(n)/n$. By using the D.V. and G.V. Chudnovsky algorithm applied to elliptic curves, M.A Shokrollahi has shown in [5] that the bilinear complexity of multiplication is equal to $2n$ for $\frac{1}{2}q + 1 < n < \frac{1}{2}(q + 1 + 2\epsilon(q))$ where ϵ is the function defined by:

$$\epsilon(q) = \begin{cases} \text{greatest integer} \leq 2\sqrt{q} \text{ prime to } q & \text{if } q \text{ is not a perfect square} \\ 2\sqrt{q} \quad \text{if } q \text{ is a perfect square.} \end{cases}$$

1.3 New results presented in this paper.

¿From the existence of algebraic function fields having some good properties, we obtain some new upper bounds on the bilinear complexity of multiplication in any extension of the finite field $\mathbb{F}_q$ where q is an arbitrary prime power q. More precisely, we prove the following result :

Theorem 1.1 *Let q be an arbitrary prime power and let n be a integer. Then the bilinear complexity of multiplication in any finite field $\mathbb{F}_{q^n}$ is such that $\mu_q(n) \leq B_q n$ where B_q is defined by:*

$$B_q = \begin{cases} 6(1 + \frac{q}{q-3}) \quad \textit{if } q > 3 \\ 2(1 + \frac{\sqrt{q}}{\sqrt{q}-3}) \quad \textit{if } q > 9 \textit{ and } q \textit{ is a perfect square} \\ 45 \quad \textit{if } q = 3 \\ 90 \quad \textit{if } q = 2. \end{cases}$$

So, we prove that the bilinear complexity of multiplication in the finite field $\mathbb{F}_{q^n}$ is linear uniformly in q with respect to the degree n. To this end, we use the following general theorem established in [1]:

Theorem 1.2 *Let q be a prime power and n be a natural number. If there exists an algebraic function field $F/\mathbb{F}_q$ of genus g, satisfying the following conditions:*
1) $F/\mathbb{F}_q$ contains a prime divisor Q of degree n.
2) $N(F/\mathbb{F}_q) > 2n + 2g - 2$.
Then

$$\mu_q(n) \leq 2n + g - 1.$$

A very important corollary of this theorem is the following theorem:

Theorem 1.3 *Let q be a prime power and n be a natural number. If there exits an algebraic function field $F/\mathbb{F}_q$ of genus g, satisfying the following conditions:*
1) $2g + 1 \leq q^{\frac{n-1}{2}}(q^{\frac{1}{2}} - 1)$ (in particular if $g \leq \frac{n-3}{4}$)
2) $N(F/\mathbb{F}_q) > 2n + 2g - 2$.
Then

$$\mu_q(n) \leq 2n + g - 1.$$

Then, we show that the tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, described by A. Garcia and H. Stichtenoth in [3], satisfies the properties of Theorem 1.3. From it, we deduce Theorem 1.1.

References

[1] **BALLET, S** *Curves with Many Points and Multiplication Complexity in Any Extension of $\mathbb{F}_q$.* Institut de Mathématiques de Luminy, Preprint 98-20, Juin 1998 (Submit for publication).

[2] **CHUDNOVSKY, D.V, CHUDNOVSKY, G.V.** *Algebraic Complexities and Algebraic Curves over Finite Fields.* J. Complexity, 4, 285-316, 1988.

[3] **GARCIA, A., STICHTENOTH, H.** *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound.* Inventiones Mathematicae, 121, 211-222, 1995.

[4] **GROOTE, H.F.** *Characterization of Division Algebras of Minimal Rank and the Structure of their algorithm Varieties.* Lectures Notes in Computer Science, 245, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1985.

[5] **SHOKROLLAHI, M.A.** *Optimal Algorithms for multiplication in certain finite fields using algebraic curves.* SIAM J. Comp. 21, No 6, 1193-1198, 1992.

[6] **SHPARLINSKY, I.E, TSFASMAN , M.A, VLADUT, S.G.** *Curves with Many Points and Multiplication in Finite Fields.* Lectures Notes in Mathematics, 1518, 145-169, Springer-Verlag, Berlin 1992.

[7] **WINOGRAD, S.** *On Multiplication in Algebraic Extension Fields.* Theorical Computer Science, 8, 359-377, 1979.