Séminaires & Congrès
11, 2005, p. 179–188

ON THE BILINEAR COMPLEXITY OF THE MULTIPLICATION IN FINITE FIELDS

by

Stéphane Ballet & Robert Rolland

Abstract. — The aim of this paper is to introduce the bilinear complexity of the multiplication in finite fields and to give a brief exposition of the recent results obtained in this part of algebraic complexity theory. In particular we present the new results obtained using the Chudnovsky-Chudnovsky algorithm and its generalizations.

Résumé **(Sur la complexité bilinéaire de la multiplication dans les corps finis)**
L'objectif de cet article est de présenter la complexité bilinéaire de la multiplication dans les corps finis et de faire un bref tour d'horizon des résultats récents obtenus dans cette partie de la théorie de la complexité algébrique. En particulier, nous présentons les résultats nouveaux qui découlent de l'utilisation de l'algorithme de Chudnovsky-Chudnovsky et de ses généralisations.

1. Introduction

The aim of this paper is to introduce the bilinear complexity of the multiplication in finite fields and to give a brief exposition of the recent results obtained in this part of algebraic complexity theory. The best general reference here is [**8**].

In this section we introduce the problem, we set up notation and terminology and we review some of the standard results on the multiplication of two polynomials modulo a given polynomial.

In section 2, we summarize without proof the algorithm of D.V. Chudnovski and G.V. Chudnovski (*cf.* [**9**]). This algorithm results in the *linearity of the bilinear complexity of the multiplication.* We explain that, in some sense, the algorithm of D.V. Chudnovski and G.V. Chudnovski is not so far from a Fourier Transform. We give also lower and upper asymptotic estimates of the bilinear complexity, due to Shparlinski, Tsfasman, Vladut (*cf.* [**15**]). We present the results obtained by the use of the D.V. Chudnovski and G.V. Chudnovski algorithm with elliptic curves (*cf.* [**14**]).

2000 ***Mathematics Subject Classification.*** — 11YXX, 12E20, 14H05.
Key words and phrases. — Bilinear complexity, finite field, algebraic function field.

In section 3, we introduce a generalization of the D.V. Chudnovski and G.V. Chudnovski algorithm (*cf.* [**6**]), and the recent results we have obtained on the upper bounds for the bilinear complexity of the multiplication. We also describe some towers of algebraic function fields used to obtain the different estimates.

1.1. The bilinear complexity of the multiplication. — Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements where p is a prime number. Let $\mathbb{F}_{q^n}$ be a degree n extension of $\mathbb{F}_q$. The multiplication m in the finite field $\mathbb{F}_{q^n}$ is a bilinear map from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ into $\mathbb{F}_{q^n}$, thus it corresponds to a linear map M from the tensor product $\mathbb{F}_{q^n} \otimes \mathbb{F}_{q^n}$ into $\mathbb{F}_{q^n}$. One can also represent M by a tensor $t_M \in \mathbb{F}^*_{q^n} \otimes \mathbb{F}^*_{q^n} \otimes \mathbb{F}_{q^n}$ where $\mathbb{F}^*_{q^n}$ denotes the algebraic dual of $\mathbb{F}_{q^n}$. Each decomposition

$$t_M = \sum_{i=1}^{k} a_i^* \otimes b_i^* \otimes c_i \tag{1}$$

of the tensor t_M, where $a_i^*, b_i^* \in \mathbb{F}^*_{q^n}$ and $c_i \in \mathbb{F}_{q^n}$, brings forth a multiplication algorithm

$$x \cdot y = t_M(x \otimes y) = \sum_{i=1}^{k} a_i^*(x) \otimes b_i^*(x) \otimes c_i.$$

The bilinear complexity of the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, denoted by $\mu_q(n)$, is the minimum number of summands in the decomposition (1). Alternatively, we can say that the bilinear complexity of the multiplication is the rank of the tensor t_M (*cf.* [**15**], [**2**]).

1.2. Complexity and bilinear complexity of the multiplication. — Let us remark that the bilinear complexity of the multiplication is far from being the global complexity of the multiplication. If we use the decomposition (1), all the operations involved in the linear part of the computation, namely the computations of $x_i^*(x)$ and $y_i^*(y)$, are not taken in account for the bilinear complexity. But in fact these operations can have a heavy cost. If we take for example the multiplication of polynomials with complex coefficients, and if we use a well fitted Fourier transform, the bilinear complexity is linear, but the complexity of the fast Fourier transforms which constitute the linear part of the algorithm is $O(n \ln(n))$. However, it is suitable to count separately the linear complexity and the bilinear complexity. Indeed, if we want to multiply two variables x and y we have to design a general algorithm of multiplication, but if we want to multiply a given constant a by a variable x, the algorithm can be simpler, because we can adapt the algorithm to the particular value a (think for example to the particular case $a = 1$). In the paper, our purpose is to study the bilinear complexity. No attempt has been made here to develop a study of the linear complexity.

1.3. Old classical results. — Let

$$P(u) = \sum_{i=0}^{n} a_i u^i$$

be a monic irreducible polynomial of degree n with coefficients in a field F. Let

$$R(u) = \sum_{i=0}^{n-1} x_i u^i \quad \text{and} \quad S(u) = \sum_{i=0}^{n-1} y_i u^i$$

be polynomial of degree $\leqslant n-1$ where the coefficients x_i and y_i are indeterminates. As a consequence of a result of Fiduccia and Zalestein (*cf.* [**10**], [**8**] p. 367 prop. 14.47) the bilinear complexity of the multiplication $R(u)\times S(u)$ is $\geqslant 2n-1$. When the field F is infinite, an algorithm reaching exactly this bound was previously given by Toom in [**16**]. Winograd described in [**17**] all the algorithms reaching the bound $2n-1$. Moreover, Winograd proved in [**18**] that up to some transformation every algorithm for computing the coefficients of $R(u)\times S(u) \mod P(u)$ which is of bilinear complexity $2n-1$, necessarily computes the coefficients of $R(u)\times S(u)$, and consequently uses one of the algorithms described in [**17**]. These algorithms use interpolation technics and cannot be performed if the cardinality of the field F is $< 2n-2$. In conclusion we have the following result:

Theorem 1.1. — *If the cardinality of F is $< 2n-2$, every algorithm computing the coefficients of $R(u)\times S(u) \mod P(u)$ has a bilinear complexity $> 2n-1$.*

Applying the results of Winograd and Theorem 1.1 to the multiplication in a finite extension $\mathbb{F}_{q^n}$ of a finite field $\mathbb{F}_q$ we obtain:

Theorem 1.2. — *The bilinear complexity $\mu_q(n)$ of the multiplication in the finite field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ verifies*

$$\mu_q(n) \geqslant 2n-1,$$

with equality holding if and only if

$$n \leqslant \frac{q}{2}+1.$$

This result does not give any estimate of an upper bound for $\mu_q(n)$, when n is large. In [**13**], Lempel, Seroussi and Winograd proved that $\mu_q(n)$ has a quasi-linear upper bound. More precisely:

Theorem 1.3. — *The bilinear complexity of the multiplication in the finite field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ verifies:*

$$\mu_q(n) \leqslant f_q(n)n,$$

where $f_q(n)$ is a very slowly growing function, namely

$$f_q(n) = O(\underbrace{\log_q \log_q \cdots \log_q}_{k \ times}(n))$$

for any $k \geqslant 1$.

2. Interpolation on algebraic curves

We have seen in the previous section that if the number of points of the ground field is too low, we cannot perform the multiplication by the Winograd interpolation method. D.V. and G.V. Chudnowski have designed in [**9**] an algorithm where the interpolation is done on points of an algebraic curve over the groundfield with a sufficient number of rational points. Using this algorithm, D.V. and G.V. Chudnowski proved that *the bilinear complexity of the multiplication in finite extensions of a finite field is linear.*

2.1. Linearity of the bilinear complexity of the multiplication

2.1.1. The D.V Chudnovski and G.V. Chudnovski algorithm. — Let us introduce first the D.V Chudnovski and G.V. Chudnovski theorems proved in [**9**].

Theorem 2.1. — *Let*

- *$F/\mathbb{F}_q$ be an algebraic function field,*
- *Q be a degree n place of $F/\mathbb{F}_q$,*
- *$\mathcal{D}$ be a divisor of $F/\mathbb{F}_q$,*
- *$\mathcal{P} = \{P_1, \ldots, P_N\}$ be a set of places of degree 1.*

We suppose that Q, $P_1, \ldots, P_N$ are not in the support of $\mathcal{D}$ and that:

(a) *The evaluation map*

$$\mathrm{Ev}_Q : \mathcal{L}(\mathcal{D}) \longrightarrow \mathbb{F}_{q^n} \simeq F_Q$$

is onto (where F_Q is the residue class field of Q),

(b) *the application*

$$\mathrm{Ev}_{\mathcal{P}} : \begin{cases} \mathcal{L}(2\mathcal{D}) \longrightarrow \mathbb{F}_q^N \\ \qquad f \longmapsto (f(P_1), \ldots, f(P_N)) \end{cases}$$

is injective.

Then

$$\mu_q(n) \leqslant N.$$

Sketch of proof. — Let x an y be two elements of $\mathbb{F}_{q^n}$. We know that the residue class field F_Q is isomorphic to $\mathbb{F}_{q^n}$, hence x and y can be considered as element of F_Q. From the condition a), there exist two algebraic functions f and g in $\mathcal{L}(\mathcal{D})$ such that $f(Q) = x$ and $g(Q) = y$. Now we can evaluate f and g on the points $P_1, \ldots, P_N$. In this way we can compute with N bilinear multiplications the evaluation of $h = f \cdot g$ on these points:

$$(h(P_1) \cdots h(P_N)) = (f(P_1)g(P_1), \ldots, f(P_N)g(P_N)).$$

We know that $h \in \mathcal{L}(2\mathcal{D})$, hence, using the condition b) we can find h. Now we can conclude by computing $h(Q)$ which is in fact $f(Q)g(Q) = xy$. The only bilinear computation is the computation of the N products $f(P_i)g(P_i)$. □

Using this algorithm with a good sequence of algebraic function fields, D.V. Chudnovski and G.V. Chudnovski proved the linearity of the bilinear complexity of the multiplication:

Theorem 2.2. — *For any prime power q, there exists a constant C_q such that*

$$\mu_q(n) \leqslant C_q n.$$

2.1.2. Asymptotic bounds. — Shparlinski, Tsfasman, Vladut have given in [**15**] many interesting remarks on the algorithm of D.V. and G.V. Chudnovski. They have linked the algorithm with coding theory, and more precisely with the notion of supercode. They have also obtained in the same paper asymptotic bounds for the bilinear complexity. Following the authors, let us define

$$M_q = \limsup_{k\to\infty} \frac{\mu_q(k)}{k} \quad \text{and} \quad m_q = \liminf_{k\to\infty} \frac{\mu_q(k)}{k}.$$

Let us summarize the estimates given in [**15**]:

(1) $q = 2$

$$3.52 \leqslant m_2 \leqslant 35/6.$$
$$M_2 \leqslant 27.$$

(2) $q \geqslant 9$ is a square

$$2 + \frac{1}{q-1} \leqslant m_q \leqslant 2\left(1 + \frac{1}{\sqrt{q}-2}\right).$$
$$M_q \leqslant 2\left(1 + \frac{1}{\sqrt{q}-2}\right).$$

(3) $q > 2$

$$2 + \frac{1}{q-1} \leqslant m_q \leqslant 3\left(1 + \frac{1}{q-2}\right).$$
$$M_q \leqslant 6\left(1 + \frac{1}{q-2}\right).$$

2.1.3. The use of elliptic curves. — Applying the D.V. and G.V. Chudnovski algorithm with well fitted elliptic curves, Shokrollahi has shown (*cf.* [**14**]) that:

Theorem 2.3. — *The bilinear complexity $\mu_q(n)$ of the multiplication in the finite extension $\mathbb{F}_{q^n}$ of the finite field $\mathbb{F}_q$ is equal to $2n$ for*

$$\frac{1}{2}q + 1 < n < \frac{1}{2}(q + 1 + \varepsilon(q)) \tag{2}$$

where ε is the function defined by:

$$\varepsilon(q) = \begin{cases} \textit{greatest integer} \leqslant 2\sqrt{q} \textit{ prime to } q, & \textit{if } q \textit{ is not a perfect square} \\ 2\sqrt{q}, & \textit{if } q \textit{ is a perfect square.} \end{cases}$$

We do not know if the converse is true. More precisely the question is: suppose that $\mu_q(n) = 2n$, are the inequalities (2) true?

2.2. Link to Fourier and Laplace transforms. — Let us examine the proof of Theorem 2.1. This proof consists in an algorithm, the so-called Chudnovski-Chudnovski algorithm. Let us follow, the different transforms applied to the element x (or y). First, we associate to x a function f in $\mathcal{L}(\mathcal{D})$. This is very similar to a discrete Laplace transform (sometimes called Z-transform). Then we evaluate the function f on the points $P_1, \ldots, P_N$. This is very similar to a discrete Fourier transform, where we evaluate the Laplace transform on the unit roots.

3. Upper bounds for the bilinear complexity

3.1. Extensions of the algorithm. — In order to obtain good estimates for the constant C_q, Ballet has given in [**1**] some easy to verify conditions allowing the use of the D.V and G.V algorithm, then Ballet and Rolland [**6**] have improved the algorithm using places of degree 1 and 2. Let us set the last version of the theorem:

Theorem 3.1. — *Let*

- $F/\mathbb{F}_q$ *be an algebraic function field,*
- Q *be a degree* n *place of* $F/\mathbb{F}_q$*,*
- $\mathcal{D}$ *be a divisor of* $F/\mathbb{F}_q$*,*
- $\mathcal{P} = \{P_1, \ldots, P_{N_1}, Q_1, \ldots, Q_{N_2}\}$ *be a set of places of degree* 1 *and* 2*.*

We suppose that Q*,* $P_1, \ldots, P_N, Q_1, \ldots, Q_{N_2}$ *are not in the support of* $\mathcal{D}$ *and that:*

(a) *The application*

$$\mathrm{Ev}_Q : \mathcal{L}(\mathcal{D}) \longrightarrow \mathbb{F}_{q^n} \simeq F_Q$$

is onto,

(b) *the application*

$$\mathrm{Ev}_{\mathcal{P}} : \begin{cases} \mathcal{L}(2\mathcal{D}) \longrightarrow \mathbb{F}_q^{N_1} \times \mathbb{F}_{q^2}^{N_2} \\ \qquad f \longmapsto (f(P_1), \ldots, f(P_{N_1}, f(Q_1), \ldots, f(Q_{N_2})) \end{cases}$$

is injective.

Then

$$\mu_q(n) \leqslant N_1 + 3N_2.$$

Let us remark that the algorithm given in [**9**] by D.V. and G.V. Chudnovski is the case $N_2 = 0$. The generalization introduced here is useful. Indeed, we know good towers of function fields, with many rational points, over $\mathbb{F}_{q^2}$ and not over $\mathbb{F}_q$. So, if we want to obtain good results for the multiplication over $\mathbb{F}_q$ we need to interpolate not only on places of degree 1 but also on places of degree 2. At a first glance it seems that places of degree greater than two cannot give us better results.

3.2. The main theorem. — From the results of [**1**] and the previous algorithm, we obtain (*cf.* [**1**], [**6**]):

Theorem 3.2. — *Let q be a prime power and let n be an integer > 1. Let $F/\mathbb{F}_q$ be an algebraic function field of genus g and N_k the number of places of degree k in $F/\mathbb{F}_q$. If $F/\mathbb{F}_q$ is such that $2g+1 \leqslant q^{(n-1)/2}(q^{1/2}-1)$ then:*

(1) *if $N_1 > 2n+2g-2$, then*

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

(2) *if there exists a non-special divisor of degree $g-1$ and $N_1+2N_2 > 2n+2g-2$, then*

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

(3) *if $N_1+2N_2 > 2n+4g-2$, then*

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

3.3. Towers of algebraic function fields. — In this section, we introduce some towers of algebraic function fields. Theorem 3.2 applied to the algebraic functions fields of these towers gives us bounds for the bilinear complexity. A given curve cannot permit to multiply in every extension of $\mathbb{F}_q$, just for n lower than some value. With a tower of function fields we can adapt the curve to the degree of the extension. The important point to note here is that in order to obtain a well adapted curve it will be desirable to have a tower for which the quotients of two consecutive genus are as small as possible, namely a "dense" tower.

For any algebraic function field $F/\mathbb{F}_q$ defined over the finite field $\mathbb{F}_q$, we denote by $g(F/\mathbb{F}_q)$ the genus of $F/\mathbb{F}_q$ and by $N_k(F/\mathbb{F}_q)$ the number of places of degree k in $F/\mathbb{F}_q$.

3.3.1. Garcia-Stichtenoth tower of Artin-Schreier algebraic function field extensions

We present now a modified Garcia-Stichtenoth's tower (*cf.* [**11**], [**3**], [**6**]) having good properties. Let us consider a finite field $\mathbb{F}_{q^2}$ with $q = p^r > 3$ and r an odd integer. Let us consider the Garcia-Stichtenoth's elementary abelian tower T_1 over $\mathbb{F}_{q^2}$ constructed in [**11**] and defined by the sequence $(F_0, F_1, F_2, \dots)$ where

$$F_{k+1} := F_k(z_{k+1})$$

and z_{k+1} satisfies the equation :

$$z_{k+1}^q + z_{k+1} = x_k^{q+1}$$

with

$$x_k := z_k/x_{k-1} \ in\ F_k(for\ k \geqslant 1).$$

Moreover $F_0 := \mathbb{F}_{q^2}(x_0)$ is the rational function field over $\mathbb{F}_{q^2}$ and F_1 the Hermitian function field over $\mathbb{F}_{q^2}$. Let us consider the completed Garcia-Stichtenoth tower

$$T_2 = F_{0,0} \subseteq F_{0,1} \subseteq \cdots \subseteq F_{0,r} \subseteq F_{1,0} \subseteq F_{1,1} \subseteq \cdots \subseteq F_{1,r} \cdots$$

considered in [**3**] such that $F_k \subseteq F_{k,s} \subseteq F_{k+1}$ for any integer s such that $s = 0, \dots, r$, with $F_{k,0} = F_k$ and $F_{k,r} = F_{k+1}$. Recall that each extension $F_{k,s}/F_k$ is Galois of degree p^s with full constant field $\mathbb{F}_{q^2}$. Now, we consider the tower studied in [**6**]

$$T_3 = G_{0,0} \subseteq G_{0,1} \subseteq \cdots \subseteq G_{0,r} \subseteq G_{1,0} \subseteq G_{1,1} \subseteq \cdots \subseteq G_{1,r}, \dots$$

defined over the constant field $\mathbb{F}_q$ and related to the tower T_2 by

$$F_{k,s} = \mathbb{F}_{q^2} G_{k,s} \quad \text{for all } k \text{ and } s,$$

namely $\mathbb{F}_{k,s}/\mathbb{F}_{q^2}$ is the constant field extension of $G_{k,s}/\mathbb{F}_q$. Note that the tower T_3 is well defined by [**6**] and [**7**]. From the existence of these towers, we have the following result by [**6**], [**7**] and [**5**]:

Proposition 3.3. — *Let q be a prime power $\geqslant 5$. Then for any integer $n \geqslant \frac{1}{2}(q+1+\varepsilon(q))$ where $\varepsilon(q)$ is the greatest integer $< 2\sqrt{q}$,*

(1) *there exists an algebraic function field $F_{k,s}/\mathbb{F}_{q^2}$ of genus $g(F_{k,s}/\mathbb{F}_{q^2})$ such that $2g(F_{k,s}/\mathbb{F}_{q^2}) + 1 \leqslant q^{n-1}(q-1)$ and $N_1(F_{k,s}/\mathbb{F}_{q^2}) > 2n + 2g(F_{k,s}/\mathbb{F}_{q^2}) - 2$,*

(2) *there exists an algebraic function field $G_{k,s}/\mathbb{F}_q$ of genus $g(G_{k,s}/\mathbb{F}_q)$ such that $2g(G_{k,s}/\mathbb{F}_p) + 1 \leqslant q^{(n-1)/2}(q^1/2 - 1)$ and $N_1(G_{k,s}/\mathbb{F}_q) + 2N_2(G_{k,s}/\mathbb{F}_q) > 2n + 2g(G_{k,s}/\mathbb{F}_q) - 2$ and containing a non-special divisor of degree $g(G_{k,s}/\mathbb{F}_q) - 1$.*

3.3.2. Garcia-Stichtenoth tower of Kummer function field extensions. — In this section we present a Garcia-Stichtenoth's tower (*cf.* [**4**]) having good properties. Let $\mathbb{F}_q$ be a finite field of characteristic $p \geqslant 3$. Let us consider the tower T over $\mathbb{F}_q$ that is defined recursively by the following equation, studied in [**12**]:

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

The tower $T/\mathbb{F}_q$ is represented by the sequence of function fields $(T_0, T_1, T_2, \dots)$ where $T_n = \mathbb{F}_q(x_0, x_1, \dots, x_n)$ and $x_{i+1}^2 = (x_i^2+1)/2x_i$ holds for each $i \geqslant 0$. Note that T_0 is the rational function field. For any prime number $p \geqslant 3$, the tower $T/\mathbb{F}_{p^2}$ is asymptotically optimal over the field $\mathbb{F}_{p^2}$, *i.e.* $T/\mathbb{F}_{p^2}$ reaches the Drinfeld-Vladut bound. Moreover, for any integer k, $T_k/\mathbb{F}_{p^2}$ is the constant field extension of $T_k/\mathbb{F}_p$.

From the existence of this tower, we can obtain the following proposition [**4**]:

Proposition 3.4. — *Let p be a prime number $\geqslant 5$. Then for any integer $n \geqslant \frac{1}{2}(p+1+\varepsilon(p))$ where $\varepsilon(p)$ is the greatest integer $< 2\sqrt{p}$,*

(1) *there exists an algebraic function field $T_k/\mathbb{F}_{p^2}$ of genus $g(T_k/\mathbb{F}_{p^2})$ such that $2g(T_k/\mathbb{F}_{p^2}) + 1 \leqslant p^{n-1}(p-1)$ and $N_1(T_k/\mathbb{F}_{p^2}) > 2n + 2g(T_k/\mathbb{F}_{p^2}) - 2$,*

(2) *there exists an algebraic function field $T_k/\mathbb{F}_p$ of genus $g(T_k/\mathbb{F}_p)$ such that $2g(T_k/\mathbb{F}_p)+1 \leqslant p^{(n-1)/2}(p^{1/2}-1)$ and $N_1(T_k/\mathbb{F}_p)+2N_2(T_k/\mathbb{F}_p) > 2n+2g(T_k/\mathbb{F}_p)-2$ and containing a non-special divisor of degree $g(T_k/\mathbb{F}_p) - 1$.*

3.4. Results. — From these towers of algebraic functions fields satisfying Theorem 3.2, it was proved in [**1**], [**3**], [**6**], [**7**], [**5**] and [**4**]:

Theorem 3.5. — *Let $q = p^r$ a power of the prime p. The bilinear complexity $\mu_q(n)$ of multiplication in any finite field $\mathbb{F}_{q^n}$ is linear with respect to the extension degree, more precisely:*

$$\mu_q(n) \leqslant C_q n$$

where C_q is the constant defined by:

$$C_q = \begin{cases} \textit{if } q = 2 & \textit{then} \quad 54. & [\mathbf{1}] \\ \textit{else if } q = 3 & \textit{then} \quad 27. & [\mathbf{1}] \\ \textit{else if } q = p \geqslant 5 & \textit{then} \quad 3(1 + \frac{4}{q-3}) & [\mathbf{4}] \\ \textit{else if } q = p^2 \geqslant 25 & \textit{then} \quad 2(1 + \frac{2}{\sqrt{q}-3}) & [\mathbf{4}] \\ \textit{else if } q = p^{2k} \geqslant 16 & \textit{then} \quad 2(1 + \frac{p}{\sqrt{q}-3}) & [\mathbf{3}] \\ \textit{else if } q \geqslant 16 & \textit{then} \quad 3(1 + \frac{2p}{q-3}) & [\mathbf{6}],[\mathbf{7}], \textit{ and } [\mathbf{5}] \\ \textit{else if } q > 3 & \textit{then} \quad 6(1 + \frac{p}{q-3}) & [\mathbf{3}]. \end{cases}$$

References

[1] S. Ballet – Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$, *Finite Fields and Their Applications* **5** (1999), p. 364–377.

[2] ———, Quasi-optimal algorithms for multiplication in the extensions of $\mathbb{F}_{16}$ of degree 13, 14, and 15, *J. Pure Appl. Algebra* **171** (2002), p. 149–164.

[3] ———, Low increasing tower of algebraic function fields and bilinear complexity of multiplication in any extension of $\mathbb{F}_q$, *Finite Fields and Their Applications* **9** (2003), p. 472–478.

[4] S. Ballet & J. Chaumine – On the bounds of the bilinear complexity of multiplication in some finite fields, *Appl. Algebra Engrg. Comm. Comput.* **15** (2004), p. 205–211.

[5] S. Ballet & D. Le Brigand – On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$, submitted preprint, 2005.

[6] S. Ballet & R. Rolland – Multiplication algorithm in a finite field and tensor rank of the multiplication, *J. Algebra* **272** (2004), no. 1, p. 173–185.

[7] ———, The definition field of a tower of function fields and applications, submitted preprint, 2005.

[8] P. Burgisser, M. Clausen & A. Shokrollahi – *Algebraic complexity theory*, Springer, 1997.

[9] D. Chudnovsky & G. Chudnovsky – Algebraic complexities and algebraic curves over finite fields, *J. Complexity* **4** (1988), p. 285–316.

[10] C. Fiduccia & Y. Zalcstein – Algebras having linear multiplicative complexities, *J. ACM* **24** (1977), p. 311–331.

[11] A. Garcia & H. Stitchtenoth – A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, *Invent. Math.* **121** (1995), p. 211–222.

[12] A. Garcia, H. Stitchtenoth & H.-G. Ruck – On tame towers over finite fields, *J. reine angew. Math.* **557** (2003), p. 53–80.

[13] A. Lempel, G. Seroussi & S. Winograd – On the complexity of multiplication in finite fields, *Theoret. Comput. Sci.* **22** (1983), p. 285–296.

[14] A. Shokhrollahi – Optimal algorithms for multiplication in certain finite fields using algebraic curves, *SIAM J. Comput.* **21** (1992), no. 6, p. 1193–1198.

[15] I. Shparlinski, M. Tsfasman & S. Vladut – Curves with many points and multiplication in finite fields, in *Coding theory and algebraic geometry* (H. Stichtenoth & M. Tsfasman, eds.), Lect. Notes in Math., vol. 1518, Springer-Verlag, 1992, p. 145–169.

[16] A. Toom – The complexity of schemes of functional elements realizing the multiplication of integers, *Soviet Math. Dokl.* **4** (1963), p. 714–716.

[17] S. Winograd – Some bilinear forms whose multiplicative complexity depends on the field of constants, *Math. Systems Theory* **10** (1977), p. 169–180.

[18] ———, On multiplication in algebraic extension fields, *Theoret. Comput. Sci.* **8** (1979), p. 359–377.

S. Ballet, Laboratoire de Géométrie Algébrique et Applications à la Théorie de l'Information, Université de la Polynésie Française, B.P. 6570, 98702 Faa'a, Tahiti, Polynésie Française.
E-mail : `ballet@upf.pf`

R. Rolland, Institut de Mathématiques de Luminy, Case 907, 13288 Marseille cedex 9.
E-mail : `rolland@iml.univ-mrs.fr`