HAL open science

On the construction of the asymmetric Chudnovsky multiplication algorithm in finite fields without derivated evaluation

Alexis Bonnecaze, Stéphane Ballet, Nicolas Baudru, Mila Tukumuli

▶ **To cite this version:**

Alexis Bonnecaze, Stéphane Ballet, Nicolas Baudru, Mila Tukumuli. On the construction of the asymmetric Chudnovsky multiplication algorithm in finite fields without derivated evaluation. Comptes Rendus. Mathématique, 2017, 355 (7), pp.729 - 733. 10.1016/j.crma.2017.06.002 . hal-01705865

HAL Id: hal-01705865

https://hal.science/hal-01705865

Submitted on 13 Jun 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

C. R. Acad. Sci. Paris, Ser. I 355 (2017) 729–733

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number theory/Computer science

On the construction of the asymmetric Chudnovsky multiplication algorithm in finite fields without derivated evaluation

Construction effective de l'algorithme asymétrique de multiplication de Chudnovsky dans les corps finis

Stéphane Ballet [a], Nicolas Baudru [b], Alexis Bonnecaze [a], Mila Tukumuli [a]

[a] *Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France*
[b] *Aix Marseille Univ, CNRS, Centrale Marseille, LIF, Marseille, France*

ARTICLE INFO

Article history:
Received 21 November 2016
Accepted after revision 2 June 2017
Available online 16 June 2017

Presented by the Editorial Board

ABSTRACT

The Chudnovsky algorithm for the multiplication in extensions of finite fields provides a bilinear complexity uniformly linear with respect to the degree of the extension. Recently, Randriambololona has generalized the method, allowing asymmetry in the interpolation procedure and leading to new upper bounds on the bilinear complexity. In this note, we describe the construction of this asymmetric method without derived evaluation. To do this, we translate this generalization into the language of algebraic function fields and we give a strategy of construction and implementation.
© 2017 Académie des sciences. Published by Elsevier Masson SAS. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

RÉSUMÉ

L'algorithme de multiplication dans les corps finis de Chudnovsky a une complexité bilinéaire uniformément linéaire en le degré de l'extension. Randriambololona a récemment généralisé cette méthode en introduisant l'asymétrie dans la procédure d'interpolation et en obtenant ainsi de nouvelles bornes sur la complexité bilinéaire. Dans cette note, nous décrivons la construction de cette méthode asymétrique sans évaluation dérivée. Pour ce faire, nous traduisons cette généralisation dans le langage des corps de fonctions algébriques, et nous donnons une stratégie de construction et d'implantation.
© 2017 Académie des sciences. Published by Elsevier Masson SAS. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

E-mail addresses: stephane.BALLET@univ-amu.fr (S. Ballet), nicolas.BAUDRU@univ-amu.fr (N. Baudru), alexis.BONNECAZE@univ-amu.fr (A. Bonnecaze), tukumulimila@gmail.com (M. Tukumuli).

http://dx.doi.org/10.1016/j.crma.2017.06.002
1631-073X/© 2017 Académie des sciences. Published by Elsevier Masson SAS. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

Let q be a prime power, $\mathbb{F}_q$ the finite field with q elements and $\mathbb{F}_{q^n}$ the degree n extension of $\mathbb{F}_q$. Among all algorithms of multiplications in $\mathbb{F}_{q^n}$, those based on the Chudnovsky–Chudnovsky [6] method are known to provide the lowest bilinear complexity. This method is based on interpolation on algebraic curves defined over a finite field and provides a bilinear complexity, which is linear in n. The original algorithm uses only points of degree 1, with multiplicity 1. Ballet and Rolland [4,5] and Arnaud [1] improved the algorithm, introducing interpolation at points of higher degree or higher multiplicity. The symmetry of the original construction involves 2-torsion points that represent an obstacle to the improvement of upper bilinear complexity bounds. To eliminate this difficulty, Randriambololona [8] allowed asymmetry in the interpolation procedure, and then Pieltant and Randriambololona [7] derived new bounds, uniform in q, of the bilinear complexity. Unlike symmetric constructions, no effective implementation of this asymmetric construction has been done yet. When $g = 1$, it is known [3] that an asymmetric algorithm can always be symmetrized. However, for greater values of g, it may not be the case. Thus, it is of interest to know an effective construction of this asymmetric algorithm. So far, no effective implementation has been proposed for such an algorithm.

1.1. Multiplication algorithm and tensor rank

The multiplication of two elements of $\mathbb{F}_{q^n}$ is an $\mathbb{F}_q$-bilinear application from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ onto $\mathbb{F}_{q^n}$. Then it can be considered as an $\mathbb{F}_q$-linear application from the tensor product $\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ onto $\mathbb{F}_{q^n}$. Consequently, it can also be considered as an element T_m of $\mathbb{F}_{q^n}{}^\star \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}{}^\star \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ where $\star$ denotes the dual. When T_m is written

$$T_m = \sum_{i=1}^{r} x_i^\star \otimes y_i^\star \otimes c_i, \tag{1}$$

where the r elements $x_i^\star$ as well as the r elements $y_i^\star$ are in the dual $\mathbb{F}_{q^n}{}^\star$ of $\mathbb{F}_{q^n}$ while the r elements c_i are in $\mathbb{F}_{q^n}$, the following holds for any $x, y \in \mathbb{F}_{q^n}$: $x \cdot y = \sum_{i=1}^{r} x_i^\star(x) y_i^\star(y) c_i$. The decomposition (1) is not unique.

Definition 1.1. Every expression $x \cdot y = \sum_{i=1}^{r} x_i^\star(x) y_i^\star(y) c_i$ defines a bilinear multiplication algorithm $\mathcal{U}$ of bilinear complexity $\mu(\mathcal{U}) = r$. Such an algorithm is said symmetric if $x_i = y_i$ for all i.

Definition 1.2. The minimal number of summands in a decomposition of the tensor T_m of the multiplication is called the bilinear complexity (resp. symmetric bilinear complexity) of the multiplication and is denoted by $\mu_q(n)$ (resp. $\mu_q^{sym}(n)$):

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

where $\mathcal{U}$ is running over all bilinear multiplication algorithms (resp. all bilinear symmetric multiplication algorithms) in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

1.2. Organisation of the note

In Section 2, we give an explicit translation of the generalization of the Chudnovsky algorithm given by Randriambololona [8, Theorem 3.5]. Then in Section 3, by defining a new design of this algorithm, we give a strategy of construction and implementation. In particular, thanks to a suitable representation of the Riemann–Roch spaces, we present the first construction of asymmetric effective algorithms of multiplication in finite fields. These algorithms are tailored to hardware implementation and they allow computations to be parallelized while maintaining a low number of bilinear multiplications. In Section 4, we give an analysis of the not asymptotical complexity of this algorithm.

2. Multiplication algorithms of type Chudnovsky: generalization of Randriambololona

In this section, we present a generalization of Chudnovsky-type algorithms, introduced in [8, Theorem 3.5] by Randriambololona, which is possibly asymmetric. Since our aim is to describe explicitly the effective construction of this asymmetric algorithm, we transform the representation of this algorithm, initially made in the abstract geometrical language, in the more explicit language of algebraic function fields.

Let $F/\mathbb{F}_q$ be an algebraic function field over the finite field $\mathbb{F}_q$ of genus $g(F)$. We denote by $N_1(F/\mathbb{F}_q)$ the number of places of degree one of F over $\mathbb{F}_q$. If D is a divisor, $\mathcal{L}(D)$ denotes the Riemann–Roch space associated with D. We denote by $\mathcal{O}_Q$ the valuation ring of the place Q and by F_Q its residue class field $\mathcal{O}_Q/Q$, which is isomorphic to $\mathbb{F}_{q^{\deg Q}}$, where $\deg Q$ is the degree of the place Q.

In the framework of algebraic function fields, the result [8, Theorem 3.5] of Randriambololona can be stated as in Theorem 2.1. Note that we do not take into account derived evaluations, since we are not interested in asymptotic results. It means that we describe this asymmetric algorithm with the divisor $G = P_1 + \cdots + P_N$ where the P_i are pairwise distinct closed points of degree $\deg P_i = d_i$.

Let us define the following Hadamard product in $\mathbb{F}_{q^{l_1}} \times \mathbb{F}_{q^{l_2}} \times \cdots \times \mathbb{F}_{q^{l_N}}$, where the l_i's denote positive integers, by $(u_1, \ldots, u_N) \odot (v_1, \ldots, v_N) = (u_1 v_1, \ldots, u_N v_N)$.

Theorem 2.1. *Let $F/\mathbb{F}_q$ be an algebraic function field of genus g over $\mathbb{F}_q$. Suppose that there exists a place Q of degree n. Let $\mathcal{P} = \{P_1, \ldots, P_N\}$ be a set of N places of arbitrary degree not containing the place Q. Suppose that there exist two effective divisors D_1, D_2 of $F/\mathbb{F}_q$ such that:*

(i) the place Q and the places of $\mathcal{P}$ are not in the support of the divisors D_1 and D_2;
(ii) the natural evaluation maps E_i for $i = 1, 2$ defined as follows are surjective

$$E_i \ : \ \begin{cases} \mathcal{L}(D_i) & \longrightarrow \ \mathbb{F}_{q^n} \simeq F_Q \\ f & \longmapsto \ f(Q) \end{cases}$$

(iii) the natural evaluation map defined as follows is injective

$$T \ : \ \begin{cases} \mathcal{L}(D_1 + D_2) & \longrightarrow \ \mathbb{F}_{q^{\deg P_1}} \times \mathbb{F}_{q^{\deg P_2}} \times \cdots \times \mathbb{F}_{q^{\deg P_N}} \\ f & \longmapsto \ (f(P_1), f(P_2), \ldots, f(P_N)) \end{cases}$$

Then for any two elements x, y in $\mathbb{F}_{q^n}$, we have:

$$xy = E_Q \circ T^{-1}_{|\mathrm{Im}\, T} \left(T \circ E_1^{-1}(x) \odot T \circ E_2^{-1}(y) \right),$$

where E_Q denotes the canonical projection from the valuation ring $\mathcal{O}_Q$ of the place Q in its residue class field F_Q, $\circ$ the standard composition map, $T^{-1}_{|\mathrm{Im}\, T}$ the restriction of the inverse map of T on the image of T, E_i^{-1} the inverse map of the restriction of the map E_i on the quotient group $\mathcal{L}(D_i)/\ker E_i$ and $\odot$ the Hadamard product in $\mathbb{F}_{q^{\deg P_1}} \times \mathbb{F}_{q^{\deg P_2}} \times \cdots \times \mathbb{F}_{q^{\deg P_N}}$; and $\mu_q(n) \leq \sum_{i=1}^{N} \mu_q(\deg P_i)$.

3. Effective algorithm

3.1. Method and strategy of implementation

The construction of the algorithm is based on the choice of the place Q, the effective divisors D_1 and D_2, the bases of spaces $\mathcal{L}(D_1)$, $\mathcal{L}(D_2)$ and $\mathcal{L}(D_1 + D_2)$ and the basis of the residue class field F_Q.

In practice, following the ideas of [2], divisors D_1 and D_2 are chosen as places of degree $n + g - 1$. Furthermore, we require some additional properties, which are described below.

3.2. Finding good places D_1, D_2, and Q

In order to obtain the good places, we proceed as follows:

- we draw at random an irreducible polynomial $\mathcal{Q}(x)$ of degree n in $\mathbb{F}_q[X]$ and check that this polynomial is primitive and totally decomposed in the algebraic function field $F/\mathbb{F}_q$;
- we choose a place Q of degree n above the polynomial $\mathcal{Q}(x)$;
- we choose a place Q of degree n among the places of $F/\mathbb{F}_q$ lying above the polynomial $\mathcal{Q}(x)$;
- we draw at random a place D_1 of degree $n + g - 1$ and check that $D_1 - Q$ is a non-special divisor of degree $g - 1$, i.e. $\dim \mathcal{L}(D_1 - Q) = 0$;
- we draw at random a place D_2 of degree $n + g - 1$ and check that $D_2 - Q$ is a non-special divisor of degree $g - 1$, i.e. $\dim(D_2 - Q) = 0$.

3.3. Choosing good bases of the spaces

The residue field F_Q.

We choose the canonical basis $\mathcal{B}_Q$ generated by a root α of the polynomial $\mathcal{Q}(x)$, namely $\mathcal{B}_Q = (1, \alpha, \alpha^2, ..., \alpha^{n-1})$. From now on, we identify $\mathbb{F}_{q^n}$ to F_Q, as the residue class field F_Q of the place Q is isomorphic to the finite field $\mathbb{F}_{q^n}$.

The Riemann–Roch spaces $\mathcal{L}(D_1)$ and $\mathcal{L}(D_2)$.

We choose as basis of $\mathcal{L}(D_i)$ the reciprocal image $\mathcal{B}_{D_i}$ of the basis $\mathcal{B}_Q = (\phi_1, \ldots, \phi_n)$ of F_Q by the evaluation map E_i, namely $\mathcal{B}_{D_i} = (E_i^{-1}(\phi_i), \ldots, E_i^{-1}(\phi_n))$.

Let us denote $\mathcal{B}_{D_i} = (f_{i,1}, ..., f_{i,n})$ with $f_{i,1} = 1$ for $i = 1, 2$.

The Riemann–Roch space $\mathcal{L}(D_1 + D_2)$.

Note that since D_1 and D_2 are effective divisors, we have $\mathcal{L}(D_1) \subset \mathcal{L}(D_1 + D_2)$ and $\mathcal{L}(D_2) \subset \mathcal{L}(D_1 + D_2)$.

Lemma 3.1. *Let D_1 and D_2 be two effective divisors with disjoint supports. Then $\mathcal{L}(D_1) \cap \mathcal{L}(D_2) = \mathbb{F}_q$.*

Proposition 3.1. *Let D_1, D_2 and Q be places having the properties described in (3.2). Consider the map $\Lambda : \mathcal{L}(D_1 + D_2) \to F_Q$ such that $\Lambda(f) = f(Q)$ for $f \in \mathcal{L}(D_1 + D_2)$. There exists a vector space $\mathcal{M} \subseteq \ker \Lambda$ of dimension g such that*

$$\mathcal{L}(D_1 + D_2) = \mathcal{L}(D_1) \oplus \mathcal{L}_r(D_2) \oplus \mathcal{M},$$

where $\mathcal{L}_r(D_2)$ is such that $\mathcal{L}(D_2) = \mathbb{F}_q \oplus \mathcal{L}_r(D_2)$ and $\oplus$ denotes the direct sum. In particular, if $g = 0$, then $\mathcal{M} = Ker\Lambda$ is equal to $\{0\}$.

We choose as basis of $\mathcal{L}(D_1 + D_2)$ the basis $\mathcal{B}_{D_1+D_2}$ defined by $\mathcal{B}_{D_1+D_2} = (f_1, \ldots, f_n, f_{n+1}, \ldots, f_{2n+g-1})$ where $\mathcal{B}_{D_1} = (f_1, \ldots, f_n)$ is the basis of $\mathcal{L}(D_1)$, $(f_{n+1}, \ldots, f_{2n-1})$ is a basis of $\mathcal{L}_r(D_2)$ such that $f_{n+j} = f_{2,j+1} \in \mathcal{B}_{D_2}$ with $\mathcal{B}_{D_1}$ and $\mathcal{B}_{D_2}$ defined in Section 3.3 and $\mathcal{B}_{\mathcal{M}} = (f_{2n}, \ldots, f_{2n+g-1})$ is a basis of $\mathcal{M}$.

3.4. Product of two elements in $\mathbb{F}_{q^n}$

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be two elements of $\mathbb{F}_{q^n}$ given by their components over $\mathbb{F}_q$ relative to the chosen basis $\mathcal{B}_Q$. According to the previous notation, we can consider that x and y are identified as respectively $f_x = \sum_{i=1}^n x_i f_{1,i} \in \mathcal{L}(D_1)$ and $f_y = \sum_{i=1}^n y_i f_{2,i} \in \mathcal{L}(D_2)$.

The product $f_x f_y$ of the two elements f_x and f_y is their product in the valuation ring $\mathcal{O}_Q$. This product lies in $\mathcal{L}(D_1 + D_2)$, since D_1 and D_2 are effective divisors. We consider that x and y are respectively the elements f_x and f_y embedded in the Rieman–Roch space $\mathcal{L}(D_1 + D_2)$, via respectively the embeddings $I_i : \mathcal{L}(D_i) \longrightarrow \mathcal{L}(D_1 + D_2)$, defined by $I_1(f_x)$ and $I_2(f_y)$ as follows. If, f_x and f_y have respectively coordinates f_{x_i} and f_{y_i} in $\mathcal{B}_{D_1+D_2}$, where $i \in \{1, \ldots, 2n + g - 1\}$, we have: $I_1(f_x) = (f_{x_1} := x_1, \ldots, f_{x_n} := x_n, 0, \ldots, 0)$ and $I_2(f_y) = (f_{x_1} := y_1, 0, \ldots, 0, f_{y_{n+1}} := y_2, \ldots, f_{y_{2n-1}} := y_n, 0, \ldots 0)$. Now it is clear that knowing x (resp. y) or f_x (resp. f_y) by their coordinates is the same thing.

Theorem 3.2. *Let $P_{\mathcal{M}^s}$ be the projection of $\mathcal{L}(D_1 + D_2)$ onto $\mathcal{M}^s = \mathcal{L}(D_1) \oplus \mathcal{L}_r(D_2)$, and let Λ be the map defined as in Proposition 3.1. Then, for any elements $x, y \in \mathbb{F}_{q^n}$, the product of x by y is such that*

$$xy = \Lambda \circ P_{\mathcal{M}^s}\left(T^{-1}_{|\mathrm{Im}\, T}\left(T \circ I_1 \circ E_1^{-1}(x) \odot T \circ I_2 \circ E_2^{-1}(y)\right)\right),$$

where $\circ$ denotes the standard composition map, $T^{-1}_{|\mathrm{Im}\, T}$ the restriction of the inverse map of T on the image of T, and $\odot$ the Hadamard product as in Theorem 2.1.

We can now present the setup algorithm (Algorithm 1), which is done only once.

Algorithm 1 Setup algorithm.

INPUT: $F/\mathbb{F}_q$, $Q, D_1, D_2, P_1, \ldots, P_N$.
OUTPUT: T and T^{-1}.

(i) The representation of the finite field $\mathbb{F}_q =< a >$, where a is a fixed primitive element.
(ii) The function field $F/\mathbb{F}_q$, the place Q, the divisors D_1 and D_2 and the points $P_1, \ldots, P_N$ are such that Conditions (ii) and (iii) in Theorem 2.1 are satisfied. In addition, we require that $\sum_{1 \le i \le N} \deg P_i = 2n + g - 1$.
(iii) Represent $\mathbb{F}_{q^n}$ in the canonical basis $\mathcal{B}_Q = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, where $\mathbb{F}_{q^n} =< \alpha >$ with α a primitive element as in Section 3.3.
(iv) Construct a basis $(f_1, \ldots, f_n, f_{n+1}, \ldots, f_{2n+g-1})$ of $\mathcal{L}(D_1 + D_2)$, where $(f_1, \ldots, f_n)$ is the basis of $\mathcal{L}(D_1)$, $(f_1, f_{n+1}, \ldots, f_{2n-1})$ the basis of $\mathcal{L}(D_2)$ and $(f_{2n}, \ldots, f_{2n+g-1})$ the basis of $\mathcal{M}$, defined in Section 3.3.
(v) Compute the matrices T and T^{-1}.
(vi) Compute the matrix Λ.

The multiplication algorithm (Algorithm 2) is presented hereafter.

4. Complexity analysis

In terms of number of multiplications in $\mathbb{F}_q$, the complexity of this multiplication algorithm is as follows: calculation of z and t needs $2(2n^2 + ng - n)$ multiplications, calculation of u needs $(2n + 2g - 2 + r) \sup_{1 \le i \le r} \frac{\mu_q(i)}{i}$ bilinear multiplications and calculation of $2n - 1$ first components of w needs $(2n + g - 1)(2n - 1)$ multiplications (remark that, in Algorithm 2, we just have to compute the $2n - 1$ first components of w). The calculation of xy needs $n + g$ multiplications. The total complexity in terms of multiplications is bounded by $8n^2 + n(4g - 5) + (2n + 2g - 2 + r) \sup_{1 \le i \le r} \frac{\mu_q(i)}{i}$.

The general construction of the set-up algorithm involves some random choice of divisors having prescribed properties over an exponentially large set of divisors. To get a polynomially constructible algorithm with linear complexity, one needs to construct explicitly (i.e. polynomially) points of corresponding degrees n on curves of arbitrary genus with many rational points. Unfortunately, so far it is unknown how to produce such points (cf. [9, Section 4, Remark 5] and [8, Remark 6.6]). Hence, the asymptotic complexity of such a construction is an open problem.

Algorithm 2 Multiplication algorithm.

INPUT: $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$.
OUTPUT: xy.

(i) Compute

$$\begin{pmatrix} z_{1,d_1} \\ \vdots \\ z_{n,d_n} \\ z_{n+1,d_{n+1}} \\ \vdots \\ z_{N,d_N} \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \\ z_{n+1} \\ \vdots \\ z_{2n+g-1} \end{pmatrix} = T \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} t_{1,d_1} \\ \vdots \\ t_{n,d_n} \\ t_{n+1,d_{n+1}} \\ \vdots \\ t_{N,d_N} \end{pmatrix} = \begin{pmatrix} t_1 \\ \vdots \\ t_n \\ t_{n+1} \\ \vdots \\ t_{2n+g-1} \end{pmatrix} = T \begin{pmatrix} y_1 \\ \underline{0} \\ y_2 \\ \vdots \\ y_n \\ \underline{0} \end{pmatrix},$$

where $\sum_{i=1}^{N} d_i = 2n + g - 1$, $(z_{i,j}, t_{i,j}) \in (\mathbb{F}_{q^{d_j}})^2$, $(z_i, t_i) \in (\mathbb{F}_q)^2$ and $\underline{0}$ stands for the null vector.

(ii) Compute the Hadamard product $u = (u_{1,d_1}, \dots, u_{N,d_N}) = (u_1, \dots, u_{2n+g-1})$, where $u_{i,d_i} = z_{i,d_i} t_{i,d_i}$, in $\mathbb{F}_{q^{d_1}} \times \mathbb{F}_{q^{d_2}} \times \cdots \times \mathbb{F}_{q^{d_N}}$ as in Theorem 2.1.

(iii) Compute $w = (w_1, \dots, w_{2n+g-1}) = T^{-1}(u)$.

(iv) Extract $w' = (w_1, \dots, w_{2n-1})$ (in step (iii), just the $2n - 1$ first components have to be computed).

(v) Return $xy = \Lambda(w')$.

References

[1] N. Arnaud, Évaluation dérivées, multiplication dans les corps finis et codes correcteurs, PhD Thesis, Université de la Méditerranée, Institut de mathématiques de Luminy, France, 2006.

[2] S. Ballet, Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$, Finite Fields Appl. 5 (4) (1999) 364–377.

[3] S. Ballet, A. Bonnecaze, M. Tukumuli, On the construction of elliptic Chudnovsky-type algorithms for multiplication in large extensions of finite fields, J. Algebra Appl. 15 (1) (2016) 1650005.

[4] S. Ballet, R. Rolland, Multiplication algorithm in a finite field and tensor rank of the multiplication, J. Algebra 272 (1) (2004) 173–185.

[5] S. Ballet, R. Rolland, On the bilinear complexity of the multiplication in finite fields, in: Proceedings of the Conference Arithmetic, Geometry and Coding Theory (AGCT 2003), in: Semin. Congr., vol. 11, Société mathématique de France, 2005, pp. 179–188.

[6] D.V. Chudnovsky, G.V. Chudnovsky, Algebraic complexities and algebraic curves over finite fields, J. Complex. 4 (1988) 285–316.

[7] J. Pieltant, H. Randriambololona, New uniform and asymptotic upper bounds on the tensor rank of multiplication in extensions of finite fields, Math. Comput. 84 (2015) 2023–2045.

[8] H. Randriambololona, Bilinear complexity of algebras and the Chudnovsky–Chudnovsky interpolation method, J. Complex. 28 (2012) 489–517.

[9] I. Shparlinski, M. Tsfasman, S. Vladut, Curves with many points and multiplication in finite fields, in: H. Stichtenoth, M.A. Tsfasman (Eds.), Coding Theory and Algebraic Geometry, Proceedings of AGCT-3 Conference, Luminy, France, 17–21 June 1991, in: Lect. Notes Math., vol. 1518, Springer-Verlag, Berlin, 1992, pp. 145–169.