Improving Chudnovsky-type algorithms over the projective line thanks to derivative evaluations

Bastien Pacifico[1]
Stéphane Ballet[1]

Institut de Mathématiques de Marseille
169 Avenue de Luminy, 13009 Marseille, France
bastien.pacifico@univ-amu.fr
stephane.ballet@univ-amu.fr

Abstract. Recently, the authors introduced a recursive construction of multiplication in finite fields algorithms. These algorithms are based on the method introduced by D. V. and G. V. Chudnovsky, that generalizes polynomial interpolation to the use of algebraic curves. Using evaluation at places of increasing degrees of the rational function field over $\mathbb{F}_q$, it has been proven that one can construct in polynomial time algorithms with a quasi-linear bilinear complexity. In this paper, we discuss how the use of evaluation with multiplicity, using generalized evaluation maps, can improve this construction.

1 Introduction

The seek for efficient algorithms for multiplication in finite fields is very active lately, especially due to its potential applications for cryptography and error correcting codes. Let q be a prime power, and n be a positive integer. In this paper, we consider the problem of the multiplication in a finite extension $\mathbb{F}_{q^n}$ of an arbitrary finite field $\mathbb{F}_q$. Such an algorithm involves different kind of operations in $\mathbb{F}_q$: additions, scalar multiplications (by a constant), and bilinear multiplications, that depend on the two elements being multiplied. Different models can be used to measure the performance of these algorithms. Among them, the model of the bilinear complexity [4, Chapter 14] focuses only on the number of bilinear multiplications in the base field used by the algorithm.

Definition 1.1. *Let $\mathcal{U}$ be an algorithm for the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Its number of bilinear multiplications is called its bilinear complexity, written $\mu(\mathcal{U})$. The bilinear complexity of the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, denoted by $\mu_q(n)$, is the quantity:*

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

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

While the degree of the extension is lower than $\frac{1}{2}q + 1$, polynomial interpolation gives algorithm reaching the optimal bilinear complexity $\mu_q(n) = 2n - 1$ [9, 6]. The case of $n = \frac{1}{2}q + 1$ can be solved using the evaluation of the leading coefficient of the polynomial, usually called evaluation at infinity. However, the polynomial interpolation cannot be used for larger extension, due to the lack of elements of $\mathbb{F}_q$ to be evaluated.

The method of Chudnovsky and Chudnovsky [5] is an answer to this problematic, allowing the evaluation at rational points of algebraic curves, or equivalently rational places of algebraic function fields. By the Hasse-Weil bound, the number of rational places is bounded relatively to the genus of the function field. The original strategy consists in the construction Chudnovsky-Chudnovsky multiplication algorithm using function fields of genus increasing relatively to the degree of the extension. This allowed Ballet to prove that the bilinear complexity of the multiplication in finite field extensions is linear with respect to the extension degree ([1], see [3]). The main problem of these algorithms is that there are not generically constructible, and thus there are very few results on their total complexity nor their implementation.

The method has since been extended, for instance to the evaluation at places of arbitrary degrees, or to the evaluation with multiplicity. Lately, the authors introduced a

recursive construction of Chudnovsky-type algorithms over the projective line. Using the rational function field only, and taking places by increasing degrees, we proved the existence of Chudnovsky-type algorithms with a quasi-linear bilinear complexity, that are constructible generically, deterministically and in polynomial time. What remains of this paper is dedicated to show that the use of evaluation with multiplicity can improve the algorithms given by this construction.

2 Chudnovsky-type multiplication algorithms

2.1 Background and notations

Let $F/\mathbb{F}_q$ be a function field of genus $g = g(F)$ over $\mathbb{F}_q$. For $\mathcal{O}$ a valuation ring, the place P is defined to be $P = \mathcal{O} \setminus \mathcal{O}^\times$. We denote by F_P the residue class field at the place P, that is isomorphic to $\mathbb{F}_{q^d}$, d being the degree of the place. A rational place is a place of degree 1. A divisor $\mathcal{D}$ is a formal sum $\mathcal{D} = \sum_i n_i P_i$, where P_i are places and n_i are relative integers. The support *supp* $\mathcal{D}$ of $\mathcal{D}$ is the set of the places P_j for which $n_j \neq 0$, and $\mathcal{D}$ is effective if all the n_i are positive. The degree of $\mathcal{D}$ is defined by $\deg \mathcal{D} = \sum_i n_i$. The Riemann-Roch space associated to the divisor $\mathcal{D}$ is denoted by $\mathcal{L}(\mathcal{D})$. A divisor $\mathcal{D}$ is said to be non-special if $\dim \mathcal{L}(\mathcal{D}) = \deg(\mathcal{D}) + 1 - g$. Details about algebraic function fields can be found in [8].

2.2 The algorithm

First, let us define generalized evaluation maps.

Definition 2.1. *For any divisor $\mathcal{D}$, P a place of degree d and the multiplicity $u \geq 1$ an integer, we define the generalized evaluation map*

$$\varphi_{\mathcal{D},P,u} : \left| \begin{array}{ccc} \mathcal{L}(\mathcal{D}) & \longrightarrow & (\mathbb{F}_{q^d})^u \\ f & \mapsto & (f(P), f'(P), \ldots, f^{(u-1)}(P)) \end{array} \right. \tag{1}$$

where the $f^{(k)}(P)$ are the coefficients of the local expansion

$$f = f(P) + f'(P)t_P + f''(P)t_P^2 + \cdots + f^{(k)}(P)t_P^k + \cdots \tag{2}$$

of f at P with respect to the local parameter t_P, i.e. in $\mathbb{F}_{q^d}[[t_P]]$.

The bilinear complexity of the multiplication in the truncated local expansion of order u at a place P of degree d, i.e. in $\mathbb{F}_{q^d}[[t_P]]/(t_P^u)$, is denoted by $\mu_q(d, u)$.

Using this definition, we can introduce a specialization of the latest version of the algorithm [3].

Theorem 2.1. *Let q be a prime power and n be a positive integer. Let $F/\mathbb{F}_q$ be an algebraic function field of genus g, Q be a degree n place, $\mathcal{D}$ be a divisor of $F/\mathbb{F}_q$, $\mathcal{P} = \{P_1, \ldots, P_N\}$ be a set of places of arbitrary degrees (lower than n) of $F/\mathbb{F}_q$, and $\underline{u} = (u_1, \ldots, u_N)$ be positive integers. We suppose that supp $\mathcal{D} \cap \{Q, P_1, ..., P_N\} = \emptyset$ and that*

(i) the evaluation map

$$\begin{array}{rcl} Ev_Q : \mathcal{L}(\mathcal{D}) & \to & F_Q \\ f & \mapsto & f(Q) \end{array}$$

is surjective,

(ii) the evaluation map

$$\begin{array}{rcl} Ev_{\mathcal{P}} : \mathcal{L}(2\mathcal{D}) & \to & (\mathbb{F}_{q^{\deg P_1}})^{u_1} \times \cdots \times (\mathbb{F}_{q^{\deg P_N}})^{u_N} \\ f & \mapsto & \left(\varphi_{2\mathcal{D},P_1,u_1}(f), \ldots, \varphi_{2\mathcal{D},P_N,u_N}(f)\right) \end{array}$$

is injective.

Then,

(1) we have a multiplication algorithm $\mathcal{U}_{q,n}^{F,\mathcal{P},\underline{u}}(\mathcal{D},Q)$ *such that for any two elements* x, y *in* $\mathbb{F}_{q^n}$*:*

$$xy = E_Q \circ {Ev_{\mathcal{P}}|_{ImEv_{\mathcal{P}}}}^{-1}\left(E_{\mathcal{P}} \circ Ev_Q^{-1}(x) \underline{\odot} E_{\mathcal{P}} \circ Ev_Q^{-1}(y)\right), \tag{3}$$

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*,* $E_{\mathcal{P}}$ *the extension of* $Ev_{\mathcal{P}}$ *on the valuation ring* $\mathcal{O}_Q$ *of the place* Q*,* ${Ev_{\mathcal{P}}|_{ImEv_{\mathcal{P}}}}^{-1}$ *the restriction of the inverse map of* $Ev_{\mathcal{P}}$ *on its image,* $\underline{\odot}$ *the generalized Hadamard product and* $\circ$ *the standard composition map;*

(2) the algorithm $\mathcal{U}_{q,n}^{F,\mathcal{P},\underline{u}}(\mathcal{D},Q)$ *defined by* (3) *has bilinear complexity*

$$\mu(\mathcal{U}_{q,n}^{F,\mathcal{P},\underline{u}}(\mathcal{D},Q)) = \sum_{i=1}^{N} \mu_q(\deg P_i, u_i).$$

2.3 Chudnovsky-type algorithms over the projective line

The following definition gives the specialization introduced in [2], that does not use evaluation with multiplicities.

Definition 2.2. *Let* q *be a prime power and* n *be a positive integer. A recursive Chudnovsky-type algorithm* $\mathcal{U}_{q,n}^{\mathcal{P}_n}(Q)$ *over the projective line is an algorithm* $\mathcal{U}_{q,n}^{F,\mathcal{P},\underline{u}}(\mathcal{D},Q)$ *satisfying the assumptions of Theorem 2.1 such that:*

- $F/\mathbb{F}_q$ *is the rational function field* $\mathbb{F}_q(x)$*,*
- Q *is a place of degree* n *of* $\mathbb{F}_q(x)$*,*
- $\mathcal{D} = (n-1)P_\infty$*, where* P_∞ *is the place at infinity of* $\mathbb{F}_q(x)$*,*
- $\mathcal{P}_n$ *is a set of places of degrees lower than* n *such that*

$$\sum_{P \in \mathcal{P}_n} \deg P = 2n-1,$$

- $\underline{u} = (1,\ldots,1)$
- *the multiplication in* $F_P \simeq \mathbb{F}_{q^d}$*, where* $d = \deg P$*, is computed by* $\mathcal{U}_{q,d}^{\mathcal{P}_d}(P)$*, where* $P \in \mathcal{P}_n$*.*

The bilinear complexity of these algorithms is given by

$$\mu_b(\mathcal{U}_{q,n}^{\mathcal{P}_n}(Q)) = \sum_{P \in \mathcal{P}_n} \mu_b(\mathcal{U}_{q,d}^{\mathcal{P}_d}(P)).$$

Note that the evaluation at P_∞ is defined specifically in this context, since P_∞ is in the support of $\mathcal{D}$.

Definition 2.3. *Let* k *be a positive integer and* P_∞ *be the place at infinity of* $\mathbb{F}_q(x)$*. Let* $\mathcal{D} = kP_\infty$*, and let* $f = \sum_{i=0}^{k} f_i x^i \in \mathcal{L}(\mathcal{D})$*. We define the evaluation at* P_∞ *to be for all* $f \in \mathcal{L}(\mathcal{D})$*,*

$$f(P_\infty) := f_k.$$

An example of such an algorithm is given by the Figure 1.

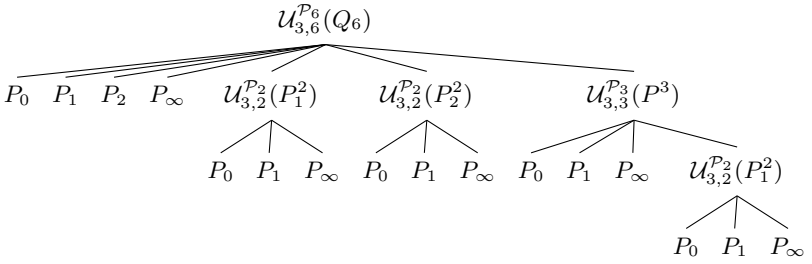

Fig. 1. Diagram of $\mathcal{U}_{3,6}^{\mathcal{P}_6}(Q_6)$

3 Chudnovsky-type algorithms over the projective line using generalized evaluation maps

Proposition 3.1. *Let q be a prime power and n be a positive integer. Let $F/\mathbb{F}_q$ be the rational function field $\mathbb{F}_q(x)$, Q be a place of degree n of $\mathbb{F}_q(x)$, and $\mathcal{D} = (n-1)P_\infty$. Let $\mathcal{P}_n$ be a set of places and $\underline{u} = (u_1, \ldots, u_N)$ be positive integers. If*

$$\sum_{i=0}^{N} u_i \deg P_i = 2n - 2, \tag{4}$$

then $\mathcal{U}_{q,n}^{\mathcal{P}_n,\underline{u}}(Q) := \mathcal{U}_{q,n}^{F,\mathcal{P},\underline{u}}(\mathcal{D}, Q)$ is a recursive Chudnovsky-type algorithm over the projective line is an algorithm satisfying

$$\mu_(\mathcal{U}_{q,n}^{\mathcal{P}_n,\underline{u}}(Q)) = \sum_{P \in \mathcal{P}_n} \mu_b(\mathcal{U}_{q,d}^{\mathcal{P}_d,\underline{u}}(P)).$$

Example 3.1. We define $\mathcal{U}_{3,6}^{\mathcal{P}',\underline{u}}$ with $\mathcal{P}' = \{P_\infty, P_0, P_1, P_2, P_1^2, P_2^2, P_3^2\}$, and $\underline{u} = (2, 1, \ldots, 1)$. This construction is illustrated in Figure 2, where $2P_0$ means that we evaluate at P_0 with multiplicity 2 and P_0' is the second coefficient of the local expansion at P_0. Its bilinear complexity reaches the best-known linear bound [3, Table 2].

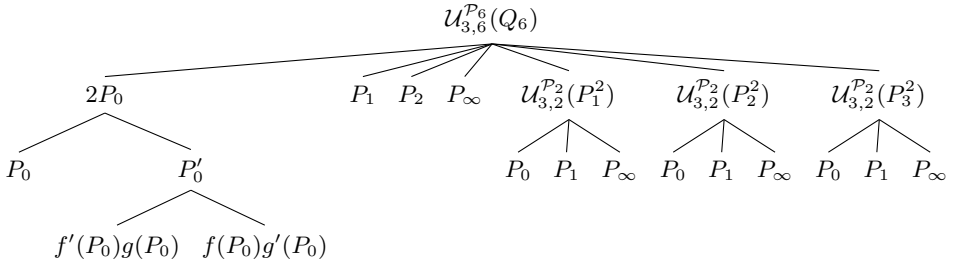

Fig. 2. Diagram of $\mathcal{U}_{3,6}^{\mathcal{P}',\underline{u}}(Q)$.

Remark 3.1. Contrary to the previous one, the algorithm given in Example 3.1 is asymmetric [7]. More precisely, the tree of Figure 2 shows that $f'(P_0)g(P_0)$ and $f(P_0)g'(P_0)$ have to be computed. These computations induce an asymmetry in the algorithm. However, one can obtain a symmetric algorithm with the same parameters, for instance by using Karatsuba algorithm to multiply the evaluations in the local expansion at P_0.

Table 1 shows some improvements of [2, Table 2], thanks to some derivative evaluations at rational places with multiplicity 2 only, as in Example 3.1. A result is underlined when it equalizes the best-known bilinear complexity.

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mu(\mathcal{U}_{2,n}^{\mathcal{P}',\underline{u}})$	-	-	10	14	-	$\underline{22}$	28	32	38	42	48	52	58	64	68	76	80
$\mu(\mathcal{U}_{3,n}^{\mathcal{P}',\underline{u}})$	-	-	-	-	$\underline{15}$	-	23	27	-	35	39	-	47	51	-	59	63

Table 1. Some improvements of [2] thanks to derivative evaluations.

References

1. Ballet, S.: Curves with Many Points and Multiplication Complexity in Any Extension of $\mathbb{F}_q$. Finite Fields and Their Applications **5**, 364–377 (1999)
2. Ballet, S., Bonnecaze, A., Pacifico, B.: Multiplication in finite fields with Chudnovsky-type algorithms on the projective line. arXiv (2020)
3. Ballet, S., Chaumine, J., Pieltant, J., Rambaud, M., Randriambololona, H., Rolland, R.: On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry. Uspekhi Mathematichskikh Nauk, 76:1(457), 31–94 (2021)
4. Bürgisser, P., Clausen, M., Shokrollahi, A.: Algebraic Complexity Theory. Springer (1997)
5. Chudnovsky, D., Chudnovsky, G.: Algebraic complexities and algebraic curves over finite fields. Journal of Complexity **4**, 285–316 (1988)
6. De Groote, H.: Characterization of division algebras of minimal rank and the structure of their algorithm varieties. SIAM Journal on Computing **12**(1), 101–117 (1983)
7. Seroussi, G., Lempel, A.: On symmetric algorithms for bilinear forms over finite fields. J. Algorithms **5**(3), 327–344 (1984)
8. Stichtenoth, H.: Algebraic Function Fields and Codes. No. 254 in Graduate Texts in Mathematics, Springer-Verlag, second edn. (2008)
9. Winograd, S.: On Multiplication in Algebraic Extension Fields. Theoretical Computer Science **8**, 359–377 (1979)