Multiplication in finite fields with Chudnovsky-type algorithms over the projective line

Stéphane Ballet, Alexis Bonnecaze, and Bastien Pacifico

Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France
Stephane.Ballet@univ-amu.fr
Alexis.Bonnecaze@univ-amu.fr
Bastien.Pacifico@univ-amu.fr

Abstract. We propose a Recursive Polynomial Generic Construction (RPGC) of multiplication algorithms in any finite field $\mathbb{F}_{q^n}$ based on the method of D.V. and G.V. Chudnovsky specialized on the projective line. These algorithms are of type polynomial interpolation and the Karatsuba algorithm is seen as a particular case of this construction. We show that the bilinear complexity of algorithms provided by our method is quasi-linear with respect to the extension degree n, and we give a uniform bound for this complexity. We also prove that the construction of these algorithms is deterministic and can be done in polynomial time. We give an asymptotic bound for the complexity of their construction.

Keywords: Finite fields, Bilinear complexity, Polynomial interpolation, Algebraic function fields.

1 Introduction

Multiplication in finite fields has been at the heart of many works since the end of the twentieth century [20,8]. In addition to being interesting for the theoretical side, this subject is of interest to many applications that need fast arithmetic, such as cryptography. Different strategies have been studied to build a multiplication algorithm. Among them, interpolation algorithms on algebraic curves, due to D.V. and G.V. Chudnovsky [10], have been widely studied for their qualities in terms of bilinear complexity [2]. Nevertheless, they present a certain number of weaknesses, including their difficulty of construction and use. In this paper, we propose a construction method that allows us to bypass these difficulties, by doing polynomial interpolation, while preserving the benefit of Chudnovsky-type algorithms.

Multiplications in a degree n extension of $\mathbb{F}_q$ require different kind of operations in $\mathbb{F}_q$. Let $x = \sum_{i=1}^{n} x_i e_i$ and $y = \sum_{i=1}^{n} y_i e_i$ be two elements of $\mathbb{F}_{q^n}$, in a basis $\{e_1, \ldots, e_n\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. By the usual method, the product of x and y

is given by the formula

$$z = xy = \sum_{h=1}^{n} z_h e_h = \sum_{h=1}^{n} \Big(\sum_{i,j=1}^{n} t_{ijh} x_i y_j \Big) e_h, \tag{1}$$

with

$$e_i e_j = \sum_{h=1}^{n} t_{ijh} e_h,$$

where $t_{ijh} \in \mathbb{F}_q$ are constants in $\mathbb{F}_q$. Two different types of multiplications are involved in this product. The scalar ones are multiplications by a constant in $\mathbb{F}_q$, and the bilinear ones depend on the two elements being multiplied (i.e. the $x_i y_j$). Of the two, bilinear multiplications are known to be computationally heavier ([18], see Survey [2]). This explains the motivation to reduce the number of bilinear multiplications in multiplication algorithms and led to the study of the bilinear complexity, that can be defined as follows.

Definition 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 $\mathbb{F}_q$.

1.1 Some known-results

From the works of Winograd and De Groote [11] applied to the multiplication in any finite field $\mathbb{F}_{q^n}$, it is proven that for all n we have $\mu_q(n) \geq 2n - 1$, equality being ensured if and only if $n \leq \frac{1}{2}q + 1$ ([2], Theorem 2.2). Winograd also proved that this lower bound is obtained with interpolation algorithms [21]. In 1987, D.V. and G.V. Chudnovsky proposed an interpolation method on algebraic curves [10], generalizing polynomial interpolation. This method makes it possible to multiply in any extension of degree n of $\mathbb{F}_q$, with a good bilinear complexity, provided that one has an algebraic curve with a sufficient number of rational points. This original algorithm is called the Chudnovsky–Chudnovsky Multiplication Algorithm (CCMA). More generally, a multiplication algorithm using interpolation over algebraic curves is said to be of type Chudnovsky.

For an increasing degree of the extension, the interpolation requires more and more rational points (i.e. rational places). From the Serre–Weil bound, the number of rational places is bounded for a fixed genus. Hence, the classical strategy is to build these algorithms over function fields of growing genus. Ballet proved that the bilinear complexity is linear in the degree of the extension ([3], see [2]) using the original algorithm over an explicit tower of function fields defined by Garcia and Stichtenoth [12]. However, it is not clear that these algorithms can be constructed in a reasonable time since we have no method to find the

place of degree n required to represent $\mathbb{F}_{q^n}$ ([18], Remark 5). Moreover, there is no generic and deterministic construction for both the divisors and the bases of the Riemann–Roch spaces involved in the algorithms.

The strategy of growing genus was natural since the original algorithm evaluates only on rational places of a function field. But several years later, thanks to the works of Ballet and Rolland [6], Arnaud [1], Cenk and Özbudak [9], and Randriambololona [17], the method has been extended to the evaluations at places of higher degrees, and to the use of derivative evaluations. These generalizations led to the introduction of another strategy for constructing the algorithm for asymptotically large extensions. The evaluation at places of higher degrees allows one to fix a function field and to evaluate at places of growing degrees. In [5], Ballet, Bonnecaze and Tukumuli built Chudnovsky-type algorithms with interpolation only over elliptic curves, i.e. fixing the genus g of the function field to be equal to 1, and using places of increasing degrees. This work gave a quasi-linear asymptotic bound for the bilinear complexity of these algorithms with respect to the degree of the extension. Moreover, they can be constructed in polynomial time. This latest result is not yet established for the growing genus strategy.

1.2 New results and organization

This extended abstract is based on the preprint [4]. In this paper, we build Chudnovsky-type algorithms for the multiplication in any finite field $\mathbb{F}_{q^n}$, with interpolation only over the projective line, i.e. fixing the genus g to be equal to 0, and using places of increasing degrees. In small extensions, the bilinear complexity of the obtained algorithms can equalize the best known bound and sometimes even improve it. Compared with the construction over elliptic curves, our work has the advantages of giving an uniform bound for the bilinear complexity of our algorithms and of giving a generic construction of algorithms for the multiplication in any finite field. Namely, the implied Riemann–Roch spaces and their associated representations are generic. More precisely, the divisors defining the Riemann–Roch spaces as well as the associated bases are of the same form for all q and n. These are explicitly given and do not have to be computed. Moreover, our set up enables us to interpolate with polynomials. This makes our algorithms closer to well-known algorithms based on polynomial interpolation such as Karatsuba [16] or Cook [7].

This paper begins with an overview of the current generalizations of CCMA. Section 3 focuses on the multiplication in small extensions. We explain how to reach the equality in the Winograd–De Groote bound with our construction. Moreover, this construction naturally integrates the trick of Karatsuba algorithm. In Section 4, we give a Recursive Polynomial Generic Construction (RPGC) of algorithms for the multiplication in any extension of $\mathbb{F}_q$, and give a natural strategy to build algorithms with a good bilinear complexity. In Section 5, we prove the existence of such algorithms having a quasi-linear uniform bound for their bilinear complexities, with respect to the extension degrees. Then, we show that their construction is deterministic, and give a polynomial asymptotic bound for this construction.

2 Chudnovsky and Chudnovsky Multiplication Algorithm

A large description of CCMA and its generalizations is given in [2]. We first recall some basics of function field theory and introduce the notions required for our study. Then, we recall a specialized version of the generalized theorem/algorithm over a function field of arbitrary genus g, which will be useful for the proposed construction.

Let $F/\mathbb{F}_q$ be a function field of genus g 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. We also denote by $B_d(F/\mathbb{F}_q)$ the number of places of degree d of F over $\mathbb{F}_q$. 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 [19].

Since Ballet and Rolland [6], Arnaud [1], then Cenk and Özbudak [9] and finally the best current generalization due to Randriambololona [17], the algorithm has been extended to the evaluation at places of arbitrary degrees and with multiplicity greater than 1. In the following, we only consider the generalization to the evaluation at places of arbitrary degrees. The statement of the algorithm requires the following definition of the generalized Hadamard product.

Definition 2. *Let q be a prime power. The generalized Hadamard product in $\mathbb{F}_{q^{d_1}} \times \cdots \times \mathbb{F}_{q^{d_N}}$, denoted by $\underline{\odot}$, is given for all $(a_1, \ldots, a_N), (b_1, \ldots, b_N) \in \mathbb{F}_{q^{d_1}} \times \cdots \times \mathbb{F}_{q^{d_N}}$ by*

$$(a_1, \ldots, a_N) \underline{\odot} (b_1, \ldots, b_N) = (a_1 b_1, \ldots, a_N b_N).$$

Now, let us introduce a specialized version of the current generalization of CCMA.

Theorem 1 (CCMA at places of arbitrary degrees without derivative evaluations).

Let

- *n be a positive integer,*
- *$F/\mathbb{F}_q$ be an algebraic function field of genus g,*
- *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 arbitrary degrees of $F/\mathbb{F}_q$,*

We suppose that supp $\mathcal{D} \cap \{Q, P_1, ..., P_N\} = \emptyset$ and that

(i) the evaluation map

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

is surjective,

(ii) the evaluation map

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

is injective.

Then,

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

$$xy = E_Q \circ {Ev_{\mathcal{P}}|_{ImEv_{\mathcal{P}}}}^{-1} \left(E_{\mathcal{P}} \circ Ev_Q^{-1}(x) \underline{\odot} E_{\mathcal{P}} \circ Ev_Q^{-1}(y) \right), \qquad (2)$$

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 $\mathcal{U}_{q,n}^{F,\mathcal{P}}(\mathcal{D}, Q)$ defined by (2) has bilinear complexity

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

Remark 1. The condition that the supports of the divisor D and $Q, P_1, ..., P_n$ are disjoint is not necessary because it is always possible to move the support (see [18, Remark 2.3]). However, this is a simplifying assumption almost always made in the literature.

Moreover, recall that sufficient application conditions are given in [2]:

Theorem 2. *Existence of the objects satisfying the conditions of Theorem 1 above is ensured by the following numerical criteria:*

(a) a sufficient condition for the existence of a place Q in $F/\mathbb{F}_q$ of degree n is that $2g + 1 \leq q^{(n-1)/2}(q^{1/2} - 1)$, where g is the genus of F,

(b) a sufficient condition for (i) is that the divisor $D - Q$ is non-special,

(c) a necessary and sufficient condition for (ii) is that the divisor $2\mathcal{D} - \mathcal{G}$ is zero-dimensional:

$$\dim \mathcal{L}(2\mathcal{D} - \mathcal{G}) = 0$$

where $\mathcal{G} = P_1 + \cdots + P_N$.

In the following, we specialize these results to the rational function field $\mathbb{F}_q(x)$.

3 CCMA and the multiplication in small extensions of $\mathbb{F}_q$

3.1 Polynomial interpolation over rational points

As seen in the introduction, the multiplication in any extension of $\mathbb{F}_q$ of degree $n \leq \frac{1}{2}q + 1$ requires exactly $2n - 1$ bilinear multiplications [11], and every algorithm reaching this optimal bilinear complexity is of type interpolation [21]. In this section, we construct Chudnovsky-type algorithms over the projective line using polynomial interpolation, and which have optimal bilinear complexity for q a prime power and $n \leq \frac{1}{2}q + 1$. We begin with the following set up.

PGC : Polynomial Generic Construction
For q a prime power and $n < \frac{1}{2}q + 1$ a positive integer. We set

- Q is a place of degree n of $\mathbb{F}_q(x)$,
- $\mathcal{D} = (n-1)P_\infty$,
- $\mathcal{P}$ is a set of rational places distinct from P_∞ of cardinal $|\mathcal{P}| = 2n - 1$,
- the basis of $\mathcal{L}(\mathcal{D})$ is $\{1, x, \ldots, x^{n-1}\}$, and
- the basis of $\mathcal{L}(2\mathcal{D})$ is $\{1, x, \ldots, x^{2n-1}\}$.

In our construction, we set the function field to be $\mathbb{F}_q(x)$, and the divisor to be $\mathcal{D} = (n-1)P_\infty$. In order to define an algorithm for the multiplication in $\mathbb{F}_{q^n}$ with Theorem 1, the only variables left are the place Q, and the set $\mathcal{P}$. Hence, we denote the algorithm using these parameters by $\mathcal{U}^{\mathcal{P}}_{q,n}(Q)$ to lighten the notations.

Proposition 1. *Let q be a prime power, $n < \frac{1}{2}q+1$ be an integer and $\mathcal{P}$ be a set of rational places distinct from P_∞ of cardinal $|\mathcal{P}| = 2n-1$. Then, PGC is a set-up for a CCMA from Theorem 1, denoted by $\mathcal{U}^{\mathcal{P}}_{q,n}(Q)$, for the multiplication in $\mathbb{F}_{q^n}$. This algorithm interpolates over polynomials and computes $2n-1$ bilinear multiplications in $\mathbb{F}_q$.*

Remark 2. CCMA cannot be constructed with PGC when $n = \frac{1}{2}q + 1$.

When q is odd, the equality of Remark 2 never happens, because $\frac{1}{2}q + 1$ is not an integer. For an even $q \geq 4$, we can use a place $\mathcal{R}$ of degree $n-1$ to define the divisor, i.e. set $\mathcal{D} = \mathcal{R}$. With this setting, we obtain an algorithm of bilinear complexity $2n - 1$, but that interpolates no longer with polynomials but with rational functions. When $q = 2$ and $n = 2$, the rational function field over $\mathbb{F}_2$ has only 3 rational places, while 4 are required by our construction (3 for the evaluations, and 1 to define $\mathcal{D}$), and we cannot use the previous argument to obtain an algorithm of optimal bilinear complexity. In the next section, we see how to obtain a polynomial interpolation algorithm in these cases.

3.2 The case of $n = \frac{1}{2}q + 1$ and polynomial interpolation

We consider the case of Remark 2: the extension of $\mathbb{F}_q$ of degree $n = \frac{1}{2}q + 1$. We want to build a Chudnovsky-type algorithm over the rational function field $\mathbb{F}_q(x)$, demanding $\mathcal{D} = (n-1)P_\infty$ to interpolate with polynomials. From the results of Winograd and De Groote, it must be possible to construct such an algorithm with optimal bilinear complexity. We use that the evaluation at a place in the support of the divisor can be defined [18, Remark 2.3]. In our context, it yields to the following definition of evaluation at P_∞.

Definition 3. *Let k be a positive integer and P_∞ be the place at infinity of $\mathbb{F}_q(x)$. Set $\mathcal{L}(\mathcal{D}) = \mathcal{L}(kP_\infty)$, we define the evaluation at P_∞ to be for all $f = \sum_{i=0}^{k-1} f_i x^i \in \mathcal{L}(\mathcal{D})$,*

$$f_{\mathcal{D}}(P_\infty) := f_{k-1},$$

that is the leading coefficient of f. We specify the divisor $\mathcal{D}$ in the notation as the evaluation depends on the Riemann–Roch space from which it is defined.

This definition makes sense since

$$f_{\mathcal{D}}(P_\infty) g_{\mathcal{D}}(P_\infty) = (fg)_{2\mathcal{D}}(P_\infty), \tag{3}$$

and using this, we obtain the following result.

Proposition 2. *Let $q \geq 2$ be an even prime power and $n = \frac{1}{2}q + 1$. Let $\mathcal{P}$ be the set of all rational places of $\mathbb{F}_q(x)$. Given Q a place of degree n, there exists a Chudnovsky-type algorithm over the projective line $\mathcal{U}^{\mathcal{P}}_{q,n}(Q)$ for the multiplication in $\mathbb{F}_{q^n}$. This algorithm interpolates over polynomials and computes $2n-1$ bilinear multiplications in $\mathbb{F}_q$.*

3.3 A particular case: the quadratic extension of $\mathbb{F}_2$

The case of $q = 2$ and $n = 2$ is problematic and interesting. CCMA cannot be constructed with PGC for the multiplication in $\mathbb{F}_{2^2}$ over $\mathbb{F}_2$. In fact, the rational function field $\mathbb{F}_2(x)$ has only three rational places: P_0, the place associated to the polynomial x, P_1, associated to $x-1$, and P_∞, the place at infinity. The proposed construction requires P_∞ to define the Riemann–Roch space and three other places to evaluate. Proposition 2 gives a Chudnovsky-type algorithm reaching this optimal bilinear complexity, that is exactly the Karatsuba's algorithm.

Corollary 1. *Let Q be the degree 2 place of $\mathbb{F}_2(x)$ and $\mathcal{P} = \{P_0, P_1, P_\infty\}$, where P_0 and P_1 are the places associated to x and $x-1$ respectively, and P_∞ is the place at infinity. Then, $\mathcal{U}^{\mathcal{P}}_{2,2}(Q)$ is a Chudnovsky-type algorithm for the multiplication in the quadratic extension of $\mathbb{F}_2$ with bilinear complexity $\mu(\mathcal{U}_{2,2}) = 3$. Moreover, its bilinear multiplications are corresponding to those of the Karatsuba Algorithm.*

Remark 3. Corollary 1 becomes generalized to any prime power q. Let P_0, P_1 and P_∞ be the places of $\mathbb{F}_q(x)$ associated to x, $x-1$ and at infinity. Let $\mathcal{P}_2 = \{P_0, P_1, P_\infty\}$, and Q be a degree 2 place of $\mathbb{F}_q(x)$. Then, $\mathcal{U}_{q,2}^{\mathcal{P}_2}(Q)$ is a Chudnovsky-type algorithm for the multiplication in the quadratic extension of $\mathbb{F}_q$, such that $\mu(\mathcal{U}_{2,2}^{\mathcal{P}_2}) = 3$. The bilinear multiplications of this algorithm are again exactly those of Karatsuba Algorithm i.e. let $f = f_0 + f_1 x$ and $g = g_0 + g_1 x$ be two elements of $\mathcal{L}(P_\infty)$, then

$$fg = f(P_0)g(P_0) + \big(f(P_1)g(P_1) - f(P_0)g(P_0) - f_{\mathcal{D}}(P_\infty)g_{\mathcal{D}}(P_\infty)\big)x \\ + f_{\mathcal{D}}(P_\infty)g_{\mathcal{D}}(P_\infty)x^2$$

4 Recursive Chudnovsky-type algorithm on $\mathbb{F}_q(x)$

4.1 Recursive Polynomial Generic Construction

In this section, we propose a recursive generic construction of Chudnovsky-type algorithms specialized to the projective line for the multiplication in all extensions $\mathbb{F}_{q^n}$, using places of increasing degrees. But at this step, we still do not have any information about how to compute the multiplications of the evaluations at places of an arbitrary degree. Concretely, let $P_i \in \mathcal{P}$ be a place of degree d_i. Then, for $f, g \in \mathcal{L}((n-1)P_\infty)$, the evaluations $f(P_i)$ and $g(P_i)$ are some elements in $\mathbb{F}_{q^{d_i}}$. To compute $(fg)(P_i) = f(P_i)g(P_i)$, we use the algorithm $\mathcal{U}_{q,d_i}^{\mathcal{P}_i}(P_i)$. Such an algorithm is called a recursive Chudnovsky-type algorithm over the projective line.

Definition 4. *Let q be a prime power and $n > \frac{1}{2}q + 1$ be a positive integer. We call a recursive Chudnovsky-type algorithm over the projective line an algorithm, that computes the multiplications in intermediate extensions with recursively-defined algorithms.*

Example 1. Set $\mathcal{P}_3 = \{P_0, P_1, P_\infty, P_1^2\}$. The sum of the degrees of the places in $\mathcal{P}_3$ is equal to $3\times 1 + 1\times 2 = 5 = 2\times 3 - 1$, and this set is suitable. The algorithm $\mathcal{U}_{3,3}^{\mathcal{P}_3}$ computes 3 bilinear multiplications in $\mathbb{F}_q$, and $\mathcal{U}_{3,2}^{\mathcal{P}_2}(P_1^2)$ computing itself 3 more bilinear multiplications. Finally, its bilinear complexity is $\mu(\mathcal{U}_{3,3}^{\mathcal{P}_3}) = 3 \times 1 + 1 \times 3 = 6$. That is the best-known (and optimal) bound for the multiplication in the extensions of degree 3 of $\mathbb{F}_3$. Table 1 illustrates the structure of $\mathcal{U}_{3,3}^{\mathcal{P}_3}$.

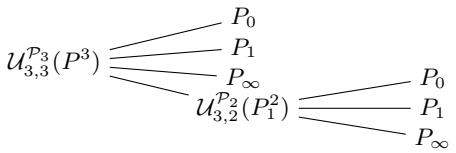

Table 1: Diagram of the construction of $\mathcal{U}_{3,3}^{\mathcal{P}_3}(Q)$.

Our strategy can be summarized as follows:

RPGC: Recursive Polynomial Generic Construction
For q a prime power and $n \geq 2$ a positive integer, let Q be a place of degree n of $\mathbb{F}_q(x)$. Then, $\mathcal{U}^{\mathcal{P}}_{q,n}(Q)$ is an algorithm for the multiplication in $\mathbb{F}_{q^n}$, with the following settings:

- $\mathcal{D} = (n-1)P_\infty$,
- $\mathcal{P} = \{P_1, \ldots, P_N\}$ is a set of places such that $\sum_{i=1}^{N} \deg P_i = 2n-1$,
- the basis of $\mathcal{L}(\mathcal{D})$ is $\{1, x, \ldots, x^{n-1}\}$,
- the basis of $\mathcal{L}(2\mathcal{D})$ is $\{1, x, \ldots, x^{2n-1}\}$, and
- apply recursively RPGC to every non-rational places in $\mathcal{P}$.

Table 2 shows this bilinear complexity for the extensions of degree lower than 18 of $\mathbb{F}_q$, with $q = 2, 3, 4$. We underline the bilinear complexity when it equals the one given by Table 2 of [2], and we denote by $^+$ when we beat this complexity.

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mu(\mathcal{U}^{\mathcal{P}^{\deg}}_{2,n})$	$\underline{3}$	$\underline{6}$	11	15	18	26	29	37	40	48	51	60	65	70	78	81	90
$\mu(\mathcal{U}^{\mathcal{P}^{\deg}}_{3,n})$	$\underline{3}$	$\underline{6}$	$\underline{9}$	12	16	$\underline{19}$	24	28	31	36	40	43	48	52	55	60	64
$\mu(\mathcal{U}^{\mathcal{P}^{\deg}}_{4,n})$	$\underline{3}$	$\underline{5}$	$\underline{8}$	$\underline{11}$	$\underline{14}$	$\underline{17}$	$\underline{20}$	$\underline{23}$	$\underline{27}$	$\underline{30}$	$\underline{33}$	$\underline{37}$	40	43^+	47	50^+	53

Table 2: Bilinear complexity of $\mathcal{U}^{\mathcal{P}}_{q,n}$ in small extensions of $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$.

5 Asymptotical study for RPGC

5.1 Bound for the bilinear complexity of RPGC

Our bound for the bilinear complexity requires to introduce the iterated logarithm.

Definition 5. *Let q be a prime power. For all integer n, the iterated logarithm of n in the basis $\sqrt{q}$, denoted by $\log^*_{\sqrt{q}}(n)$, is defined by the following recursive function:*

$$\log^*_{\sqrt{q}}(n) = \begin{cases} 0 & \text{if } n \leq 1 \text{ and } q > 2 \\ 0 & \text{if } n \leq 5 \text{ and } q = 2 \\ 1 + \log^*(\log(n)) & \text{elsewhere.} \end{cases}$$

Theorem 3. *Let q be a prime power and $n \geq 2$ a positive integer. Then, there exists a recursive Chudnovsky-type algorithm $\mathcal{U}^{\mathcal{P}}_{q,n}$ over the projective line for the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that its bilinear complexity verifies*

$$\mu(\mathcal{U}^{\mathcal{P}}_{q,n}) \leq Cn \left(\frac{4q^2}{(q-1)} \right)^{\log^*_{\sqrt{q}}(2n)},$$

where $C = 1$ for $q \geq 3$ and $C = \frac{14}{5}$ for $q = 2$.

Asymptotically, this bound is the same as for the construction of [5], i.e. with algorithms constructed over elliptic curves. On the other hand, the generalized Karatsuba algorithm, which is a Divide and Conquer construction based on the multiplication of two polynomials of degree 1 (i.e. $\mathcal{U}^{\mathcal{P}_2}_{2,2}$ here), requires $\mathcal{O}(n^{\log_2 3})$ multiplications, all of them bilinear. This is much more than the bilinear complexity obtained with our construction.

Remark 4. Note that [13, Section 9.5] gives a similar bound on the bilinear complexity, but this bound is a lower bound while our is an upper bound. However, it would possibly be relevant to compare our algorithms more thoroughly with the recent results by Harvey, van der Hoeven and Lecerf [13,15,14]. But this work of comparison is sufficiently important to require a further work of its own.

5.2 Complexity of the construction of $\mathcal{U}^{\mathcal{P}}_{q,n}$

Our construction has the advantage of using generic parameters. In particular, the divisor and the bases of the Riemann Roch spaces are explicitly given. The construction of our algorithms consists mainly in the construction of an irreductible polynomial of degree n on $\mathbb{F}_q$ as well as the matrices corresponding to the evaluation maps. This gives the following complexity, given by the number of elementary operations in $\mathbb{F}_q$. We use the standard Landau notation $\mathcal{O}$.

Theorem 4. *For all prime power q and all positive integer n, the recursive Chudnovsky-type algorithms over the projective line $\mathcal{U}^{\mathcal{P}}_{q,n}$ of Theorem 3 are constructible deterministically and in time $\mathcal{O}(n^4)$.*

References

1. Nicolas Arnaud. *Évaluations dérivées, multiplication dans les corps finis et codes correcteurs*. PhD thesis, Université de la Méditerranée, Institut de Mathématiques de Luminy, 2006.
2. S. Ballet, J. Pieltant, M. Rambaud, H. Randriambololona, R. Rolland, and J. Chaumine. On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry. *Russian Mathematical Surveys*, 76(1):29–89, feb 2021.
3. Stéphane Ballet. Curves with Many Points and Multiplication Complexity in Any Extension of $\mathbb{F}_q$. *Finite Fields and Their Applications*, 5:364–377, 1999.

4. Stéphane Ballet, Alexis Bonnecaze, and Bastien Pacifico. Multiplication in finite fields with Chudnovsky-type algorithms on the projective line. https://hal.archives-ouvertes.fr/hal-02911546.
5. Stéphane Ballet, Alexis Bonnecaze, and Mila Tukumuli. On the construction of elliptic Chudnovsky-type algorithms for multiplication in large extensions of finite fields. *Journal of Algebra and Its Applications*, 15(1):26 pages, 2016.
6. Stéphane Ballet and Robert Rolland. Multiplication algorithm in a finite field and tensor rank of the multiplication. *Journal of Algebra*, 272(1):173–185, 2004.
7. Marco Bodrato. Towards optimal Toom-Cook multiplication for univariate and multivariate polynomials in characteristic 2 and 0. In Claude Carlet and Berk Sunar, editors, *Arithmetic of Finite Fields*, pages 116–133, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.
8. A. Bostan, G. Lecerf, and É. Schost. Tellegen's principle into practice. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, ISSAC '03, page 37–44, New York, NY, USA, 2003. Association for Computing Machinery.
9. Murat Cenk and Ferruh Özbudak. On multiplication in finite fields. *Journal of Complexity*, pages 172–186, 2010.
10. David Chudnovsky and Gregory Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4:285–316, 1988.
11. Hans De Groote. Characterization of division algebras of minimal rank and the structure of their algorithm varieties. *SIAM Journal on Computing*, 12(1):101–117, 1983.
12. Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. *Inventiones Mathematicae*, 121:211–222, 1995.
13. David Harvey, Joris Van Der Hoeven, and Grégoire Lecerf. Faster polynomial multiplication over finite fields. *J. ACM*, 63(6), jan 2017.
14. David Harvey and Joris Van Der Hoeven. Faster polynomial multiplication over finite fields using cyclotomic coefficient rings. *Journal of Complexity*, 54:101404, October 2019.
15. David Harvey and Joris Van Der Hoeven. Polynomial multiplication over finite fields in time O(n log n). working paper or preprint, March 2019.
16. Anatolii Karatsuba. Multiplication of multidigit number on automata. *Soviet Physics Doklady*, 7:595–596, 1963.
17. Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *Journal of Complexity*, 28(4):489–517, 2012.
18. Igor Shparlinski, Michael Tsfasman, and Serguei Vlăduţ. Curves with many points and multiplication in finite fields. In H. Stichtenoth and M.A. Tsfasman, editors, *Coding Theory and Algebraic Geometry*, number 1518 in Lectures Notes in Mathematics, pages 145–169, Berlin, 1992. Springer-Verlag. Proceedings of AGCT-3 conference, June 17-21, 1991, Luminy.
19. Henning Stichtenoth. *Algebraic Function Fields and Codes*. Number 254 in Graduate Texts in Mathematics. Springer-Verlag, second edition, 2008.
20. Joachim von zur Gathen and Jugen Gerhard. *Modern Computer Algebra*. Cambridge University Press, 2003.
21. Shmuel Winograd. On Multiplication in Algebraic Extension Fields. *Theoretical Computer Science*, 8:359–377, 1979.