



**HAL**  
open science

# Optimization of the scalar complexity of Chudnovsky<sup>2</sup> multiplication algorithms in finite fields

Stéphane Ballet, Alexis Bonnetaze, Thanh-Hung Dang

► **To cite this version:**

Stéphane Ballet, Alexis Bonnetaze, Thanh-Hung Dang. Optimization of the scalar complexity of Chudnovsky<sup>2</sup> multiplication algorithms in finite fields. 2021. hal-02906403

**HAL Id: hal-02906403**

**<https://hal.science/hal-02906403>**

Preprint submitted on 27 May 2024

**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.

# Optimization of the scalar complexity of Chudnovsky<sup>2</sup> multiplication algorithms in finite fields

Stéphane Ballet<sup>1</sup>, Alexis Bonnetaze<sup>1</sup>, and Thanh-Hung Dang<sup>1</sup>

<sup>1</sup>*Aix-Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France*

July 17, 2020

## Abstract

We propose several constructions for the original multiplication algorithm of D.V. and G.V. Chudnovsky in order to improve its scalar complexity. We highlight the set of generic strategies who underlay the optimization of the scalar complexity, according to parameterizable criteria. As an example, we apply this analysis to the construction of type elliptic Chudnovsky<sup>2</sup> multiplication algorithms for small extensions. As a case study, we significantly improve the Baum-Shokrollahi construction for multiplication in  $\mathbb{F}_{256}/\mathbb{F}_4$ .

## 1 Introduction

### 1.1 Context

The construction of efficient arithmetic operation algorithms is still a problem of topicality. These algorithms are indeed heavily used in many domains of computer sciences or information theory. It is important to conceive and develop efficient arithmetic algorithms combined with an optimal implementation method. In this work, our interest lies in multiplication algorithms in any extension of finite field introduced in 1987 by D.V. and G.V Chudnovsky [8] and based upon interpolation on some algebraic curves defined over finite fields. Our goal is to improve this method so that its complexity in terms of number of operations is optimized.

More precisely, the complexity of a multiplication algorithm in  $\mathbb{F}_{q^n}$  depends on the number of multiplications and additions in  $\mathbb{F}_q$ . But here, we are particularly interested by the multiplicative complexity of multiplication in a finite field  $\mathbb{F}_{q^n}$ , i.e. by the number of multiplications in  $\mathbb{F}_q$  required to multiply in the  $\mathbb{F}_q$ -vector space  $\mathbb{F}_{q^n}$  of dimension  $n$ . There exist two types of multiplications

in  $\mathbb{F}_q$ : the scalar multiplication and the bilinear one. The scalar multiplication is the multiplication by a non-trivial constant (i.e. not equal to 0 or 1) in  $\mathbb{F}_q$ , which does not depend on the elements of  $\mathbb{F}_{q^n}$  that are multiplied. The bilinear multiplication is a multiplication that depends on the elements of  $\mathbb{F}_{q^n}$  that are multiplied. The bilinear complexity is independent of the chosen representation of the finite field.

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  $\mathbb{F}_q$ . If  $\mathcal{B} = \{e_1, \dots, e_n\}$  is a basis of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$  then for  $x = \sum_{i=1}^n x_i e_i$  and  $y = \sum_{j=1}^n y_j e_j$ , we have the product

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

where  $e_i e_j = \sum_{h=1}^n t_{ijh} e_h$ ,  $t_{ijh} \in \mathbb{F}_q$  being some constants.

Then, we see that the direct calculation of  $z = (z_1, \dots, z_n)$  using (1) *a priori* requires  $n^2$  non-scalar multiplications  $x_i y_j$ ,  $n^3$  scalar multiplications and  $n^3 - n$  additions.

**Definition 1.1.** *The total number of scalar multiplications in  $\mathbb{F}_q$  used in an algorithm  $\mathcal{U}_{q,n}$  of multiplication in  $\mathbb{F}_{q^n}$  is called scalar complexity of  $\mathcal{U}_{q,n}$  and denoted  $\mu_s(\mathcal{U}_{q,n})$ .*

Moreover, the multiplication of two elements of  $\mathbb{F}_{q^n}$  is an  $\mathbb{F}_q$ -bilinear map 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 map from the tensor product  $\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$  onto  $\mathbb{F}_{q^n}$ . Therefore, it can also be considered as an element  $T$  of  $(\mathbb{F}_{q^n})^* \otimes_{\mathbb{F}_q} (\mathbb{F}_{q^n})^* \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ , where  $\mathbb{F}_{q^n}^*$  denotes the dual of  $\mathbb{F}_{q^n}$ .

Set

$$T = \sum_{i=1}^r x_i^* \otimes y_i^* \otimes c_i,$$

where  $x_i^* \in \mathbb{F}_{q^n}^*$ ,  $y_i^* \in \mathbb{F}_{q^n}^*$  and  $c_i \in \mathbb{F}_{q^n}$ . The following holds for any  $x, y \in \mathbb{F}_{q^n}$ :

$$x \cdot y = T(x \otimes y) = \sum_{i=1}^r x_i^*(x) y_i^*(y) c_i.$$

**Definition 1.2.** *A multiplication algorithm  $\mathcal{U}_{q,n}$  in  $\mathbb{F}_{q^n}$  is an expression*

$$x \cdot y = \sum_{i=1}^r x_i^*(x) y_i^*(y) c_i,$$

where  $x_i^*, y_i^* \in (\mathbb{F}_{q^n})^*$ , and  $c_i \in \mathbb{F}_{q^n}$ .

*The number  $r$  of summands in this expression is called the bilinear complexity of the algorithm  $\mathcal{U}_{q,n}$  and is denoted by  $\mu_b(\mathcal{U}_{q,n})$ . The multiplicative complexity of  $\mathcal{U}_{q,n}$  is  $\mu_m(\mathcal{U}_{q,n}) = \mu_b(\mathcal{U}_{q,n}) + \mu_s(\mathcal{U}_{q,n})$ .*

**Definition 1.3.** *The minimal number of summands in a decomposition of the tensor  $T$  of the multiplication in  $\mathbb{F}_{q^n}$  is called the bilinear complexity of the multiplication in  $\mathbb{F}_{q^n}$  and is denoted by  $\mu_b(q, n)$ :*

$$\mu_b(q, n) = \min_{\mathcal{U}} \mu_b(\mathcal{U})$$

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

## 1.2 Some known results

Let us recall some known results useful for this study. In their seminal papers, Winograd [13] and De Groote [9] have shown that  $\mu_b(q, n) \geq 2n - 1$ , with equality holding if and only if  $n \leq \frac{1}{2}q + 1$ . Winograd has also proved [13] that optimal multiplication algorithms realizing the lower bound belong to the class of interpolation algorithms. Later, generalizing interpolation algorithms on the projective line over  $\mathbb{F}_q$  to algebraic curves of higher genus over  $\mathbb{F}_q$ , D.V. and G.V. Chudnovsky provided a method [8] which enabled to prove the *linearity* [2] of the bilinear complexity of multiplication in finite extensions of a finite field. This is the so-called Chudnovsky<sup>2</sup> multiplication algorithm (or CCMA). Applying CCMA with fitted elliptic curves, Shokrollahi in [11] (for the upper strict inequality) and Chaumine in [7] have shown that if

$$\frac{1}{2}q + 1 < n \leq \frac{1}{2}(q + 1 + \epsilon(q)) \quad (2)$$

where  $\epsilon$  is the function defined by:

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

then the bilinear complexity  $\mu_b(q, n)$  of the multiplication in the finite extension  $\mathbb{F}_{q^n}$  of the finite field  $\mathbb{F}_q$  is equal to  $2n$ .

Then, many studies focused on the qualitative improvement of CCMA with respect to the bilinear complexity (cf. [5]). But the problem of the optimization of its scalar complexity has never been studied, although it was first raised in 2015 by Atighehchi, Ballet, Bonnacaze and Rolland [1] and so far it remained an open problem (cf. [5, Open problem 10.2]). More explicitly, the structure of the involved matrices in CCMA should be examined more closely but unfortunately, there are no theoretical means or criteria today to build the best matrices because they depend on the geometry of the curves, the field of definition of these curves, as well as the involved Riemann-Roch spaces. The remaining open question is how to choose the geometrical objects, the associated Riemann-Roch vector-spaces as well as the suitable representation of those in order to minimise the number of zeros and 1 in the matrices of the evaluation maps involved in CCMA.

### 1.3 New results and organization

This article is the complete and generalized study of a preliminary introduction on the subject of scalar complexity, initiated in [4]. Its main goal is to identify the set of fundamental generic strategies underlying the scalar complexity optimization (known as scalar optimization) of CCMA and the relevant quantities related to it. To do so, after having recalled in detail the CCMA method (cf. Section 2.1) as well as the contextual framework (initial configuration) in which we are going to stand, we perform a detailed analysis (cf. Section 2.2) of the scalar complexity ( $\mu_s$ ) and the underlying relevant related quantities ( $\mu_{s,0}$  and  $\mu_{s,1}$ ).

Then, in Section 3.1.1, which is the core of the paper, we present the general results allowing to identify the main lever (degree of freedom) of CCMA scalar optimization for a given CCMA algorithm. Then, from these results, we give two main generic strategies (Propositions 3.2 and 3.3), whose optimization criteria can be parameterized (Remark 3.3), which are the cornerstone of the complete strategy (see Section 3.1.2). At this level (cf. Section 3.1.1), we give in particular the explicit presentation of the various corresponding optimization setup algorithms and lower bounds of the quantities  $\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^A)$  and  $\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n})$ . In the complete strategy, we then show that the scalar complexity of the CCMA algorithm is independent of the order of the rational places to be evaluated, for a given set of rational places. Finally, as an example, we specialize our study to elliptic CCMA algorithms, illustrated by two new designs of the Baum-Shokrollahi construction for multiplication in  $\mathbb{F}_{256}/\mathbb{F}_4$  based on the elliptic Fermat curve  $x^3 + y^3 = 1$ . These two new constructions, obtained by applying strategies guided by the optimization criterion of the number of zeros in the matrices involved, have scalar complexities significantly better than that of Baum-Shokrollahi.

## 2 The Chudnovsky<sup>2</sup> multiplication algorithm

### 2.1 Description and construction of CCMA

Let  $F/\mathbb{F}_q$  be an algebraic function field over the finite field  $\mathbb{F}_q$  of genus  $g(F)$ . We denote by  $N_k(F/\mathbb{F}_q)$  the number of places of degree  $k$  of  $F$  over  $\mathbb{F}_q$ . If  $D$  is a divisor,  $\mathcal{L}(D)$  denotes the Riemann-Roch space associated to  $D$ . 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  $Q$ . The order of a divisor  $D = \sum_P a_P P$  in the place  $P$  is the number  $a_P$ , denoted  $ord_P(D)$ . The support of a divisor  $D$  is the set  $supp D$  of the places  $P$  such that  $ord_P(D) \neq 0$ . The divisor  $D$  is called effective if  $ord_P(D) \geq 0$  for any  $P$ . Let us define the classical Hadamard product  $\odot$  in  $\mathbb{F}_q^N$ , where  $N$  is a positive integer, by  $(u_1, \dots, u_N) \odot (v_1, \dots, v_N) = (u_1 v_1, \dots, u_N v_N)$  for any  $u_i, v_i$  in  $\mathbb{F}_q$ . The following theorem describes the original multiplication algorithm of D.V. and G.V. Chudnovsky [8].

**Theorem 2.1.** *Let*

- $n$  be a positive integer,
- $F/\mathbb{F}_q$  be an algebraic function field,
- $Q$  be a degree  $n$  place of  $F/\mathbb{F}_q$ ,
- $D$  be a divisor of  $F/\mathbb{F}_q$ ,
- $\mathcal{P} = \{P_1, \dots, P_N\}$  be an ordered set of places of degree one of  $F/\mathbb{F}_q$ .

*We suppose that  $\text{supp } D \cap \{Q, P_1, \dots, P_N\} = \emptyset$  and that*

(i) *The evaluation map*

$$\begin{aligned} \text{Ev}_Q : \mathcal{L}(D) &\rightarrow F_Q \\ f &\mapsto f(Q) \end{aligned}$$

*is surjective*

(ii) *The evaluation map*

$$\begin{aligned} \text{Ev}_{\mathcal{P}} : \mathcal{L}(2D) &\rightarrow \mathbb{F}_q^N \\ f &\mapsto (f(P_1), \dots, f(P_N)) \end{aligned}$$

*is injective*

*Then*

(1) *For any two elements  $x, y$  in  $\mathbb{F}_{q^n}$ , we have a multiplication algorithm  $\mathcal{U}_{q,n}$ :*

$$xy = E_Q \circ \text{Ev}_{\mathcal{P}}|_{\text{Im Ev}_{\mathcal{P}}}^{-1} \left( E_{\mathcal{P}} \circ \text{Ev}_Q^{-1}(x) \odot E_{\mathcal{P}} \circ \text{Ev}_Q^{-1}(y) \right), \quad (3)$$

*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  $\text{Ev}_{\mathcal{P}}$  on the valuation ring  $\mathcal{O}_Q$  of the place  $Q$ ,  $\text{Ev}_{\mathcal{P}}|_{\text{Im Ev}_{\mathcal{P}}}^{-1}$  the restriction of the inverse map of  $\text{Ev}_{\mathcal{P}}$  on its image, and  $\odot$  the standard composition map.*

(2) *We have:*

$$\mu_b(\mathcal{U}_{q,n}) \leq N,$$

*with equality if  $N = \dim \mathcal{L}(2D)$ .*

Since  $Q$  is a place of degree  $n$ , the residue class field  $F_Q$  of place  $Q$  is an extension of degree  $n$  of  $\mathbb{F}_q$  and it therefore can be identified to  $\mathbb{F}_{q^n}$ . Moreover, the evaluation map  $\text{Ev}_Q$  being onto, one can associate the elements  $x, y \in \mathbb{F}_{q^n}$  with elements of  $\mathbb{F}_q$ -vector space  $\mathcal{L}(D)$ , denoted respectively  $f$  and  $g$ . We define  $h := fg$  by

$$(h(P_1), \dots, h(P_N)) = E_{\mathcal{P}}(f) \odot E_{\mathcal{P}}(g) = (f(P_1)g(P_1), \dots, f(P_N)g(P_N)). \quad (4)$$

We know that such an element  $h$  belongs to  $\mathcal{L}(2D)$  since the functions  $f, g$  lie in  $\mathcal{L}(D)$ . Moreover, thanks to injectivity of  $Ev_{\mathcal{P}}$ , the function  $h$  is in  $\mathcal{L}(2D)$  and is uniquely determined by (4). We have

$$xy = Ev_Q(f)Ev_Q(g) = E_Q(h)$$

where  $E_Q$  is the canonical projection from the valuation ring  $\mathcal{O}_Q$  of the place  $Q$  in its residue class field  $F_Q$ ,  $Ev_Q$  is the restriction of  $E_Q$  over the vector space  $\mathcal{L}(D)$ .

In order to make the study and the construction of this algorithm easier, we proceed in the following way. We choose a place  $Q$  of degree  $n$  and a divisor  $D$  of degree  $n + g - 1$ , such that  $Ev_Q$  and  $Ev_{\mathcal{P}}$  are isomorphisms. In this aim in [2], S. Ballet introduces simple numerical conditions on algebraic curves of an arbitrary genus  $g$  giving a sufficient condition for the application of CCMA (existence of places of certain degree, of non-special divisors of degree  $g - 1$ ) generalizing the result of A. Shokrollahi [11] for the elliptic curves. Let us recall this result:

**Theorem 2.2.** *Let  $q$  be a prime power and let  $n$  be an integer  $> 1$ . If there exists an algebraic function field  $F/\mathbb{F}_q$  of genus  $g$  satisfying the conditions*

1.  $N_n > 0$  (which is always the case if  $2g + 1 \leq q^{\frac{n-1}{2}}(q^{\frac{1}{2}} - 1)$ ),
2.  $N_1 > 2n + 2g - 2$ ,

*then there exists a divisor  $D$  of degree  $n + g - 1$  and a place  $Q$  such that:*

(i) *The evaluation map*

$$\begin{array}{ccc} Ev_Q : \mathcal{L}(D) & \rightarrow & \frac{\mathcal{O}_Q}{Q} \\ f & \mapsto & f(Q) \end{array}$$

*is an isomorphism of vector spaces over  $\mathbb{F}_q$ .*

(ii) *There exist places  $P_1, \dots, P_N$  such that the evaluation map*

$$\begin{array}{ccc} Ev_{\mathcal{P}} : \mathcal{L}(2D) & \rightarrow & \mathbb{F}_q^N \\ f & \mapsto & (f(P_1), \dots, f(P_N)) \end{array}$$

*is an isomorphism of vector spaces over  $\mathbb{F}_q$  with  $N = 2n + g - 1$ .*

**Remark 2.1.** *First, note that in the elliptic case, the condition (2) is a large inequality thanks to a result due to Chaumine [7]. Secondly, note also that the divisor  $D$  is not necessarily effective.*

By this last remark, it is important to add the property of effectivity for the divisor  $D$  in a perspective of implementation. Indeed, it is easier to construct the algorithm CCMA with this assumption because in this case  $\mathcal{L}(D) \subseteq \mathcal{L}(2D)$  and we can directly apply the evaluation map  $Ev_{\mathcal{P}}$  instead of  $E_{\mathcal{P}}$  in the algorithm

(3), by means of a suitable representation of  $\mathcal{L}(2D)$ . Moreover, in this case we need to consider simultaneously the assumption that the support of the divisor  $D$  does not contain the rational places and the place  $Q$  of degree  $n$  and the assumption of effectivity of the divisor  $D$ . Indeed, it is known that the support moving technic (cf. [10, Lemma 1.1.4.11]), which is a direct consequence of Strong Approximation Theorem (cf. [12, Proof of Theorem I.6.4]), applied on an effective divisor generates the loss of effectivity of the initial divisor (cf. also [1, Remark 2.2]). So, let us suppose these two last assumptions.

**Remark 2.2.** *As in [3], in practice, we take as a divisor  $D$  one place of degree  $n + g - 1$ . It has the advantage to solve the problem of the support of divisor  $D$  (cf. also [1, Remark 2.2]) as well as the problem of the effectivity of the divisor  $D$ . However, it is not required to be considered in the theoretical study, but, as we will see, it will have some importance in the strategy of optimization.*

We can therefore consider the basis  $\mathcal{B}_Q$  of the residue class field  $F_Q$  over  $\mathbb{F}_q$  as the image of a basis of  $\mathcal{L}(D)$  by  $Ev_Q$  or equivalently (which is sometimes useful following the considered situation) the basis of  $\mathcal{L}(D)$  as the reciprocal image of a basis of the residue class field  $F_Q$  over  $\mathbb{F}_q$  by  $Ev_Q^{-1}$ . Let

$$\mathcal{B}_D := \{f_1, \dots, f_n\} \quad (5)$$

be a basis of  $\mathcal{L}(D)$  and let us denote the basis of the supplementary space  $\mathcal{M}$  of  $\mathcal{L}(D)$  in  $\mathcal{L}(2D)$  by

$$\mathcal{B}_D^c := \{f_{n+1}, \dots, f_N\} \quad (6)$$

where  $N := \dim \mathcal{L}(2D) = 2n + g - 1$ . Then, we choose

$$\mathcal{B}_{2D} := \mathcal{B}_D \cup \mathcal{B}_D^c \quad (7)$$

as the basis of  $\mathcal{L}(2D)$ .

We denote by  $T_{2D}$  the matrix of the isomorphism  $Ev_{\mathcal{P}} : \mathcal{L}(2D) \rightarrow \mathbb{F}_q^N$  in the basis  $\mathcal{B}_{2D}$  of  $\mathcal{L}(2D)$  (the basis of  $\mathbb{F}_q^N$  will always be the canonical basis). Then, we denote by  $T_D$  the matrix of the first  $n$  columns of the matrix  $T_{2D}$ . Therefore,  $T_D$  is the matrix of the restriction of the evaluation map  $Ev_{\mathcal{P}}$  on the Riemann-Roch vector space  $\mathcal{L}(D)$ , which is an injective morphism.

Note that the canonical surjection  $E_Q$  is the extension of the isomorphism  $Ev_Q$  since, as  $Q \notin \text{supp}(D)$ , we have  $\mathcal{L}(D) \subseteq \mathcal{O}_Q$ . Moreover, as  $\text{supp}(2D) = \text{supp}(D)$ , we also have  $\mathcal{L}(2D) \subseteq \mathcal{O}_Q$ . We can therefore consider the images of elements of the basis  $\mathcal{B}_{2D}$  by  $E_Q$  and obtain a system of  $N$  linear equations as follows:

$$E_Q(f_r) = \sum_{m=1}^n c_r^m Ev_Q(f_m), \quad r = 1, \dots, N$$

where  $E_Q$  denotes the canonical projection from the valuation ring  $\mathcal{O}_Q$  of the place  $Q$  in its residue class field  $F_Q$ ,  $Ev_Q$  is the restriction of  $E_Q$  over the vector space  $\mathcal{L}(D)$  and  $c_r^m \in \mathbb{F}_q$  for  $r = 1, \dots, N$ . Let  $C$  be the matrix of the restriction



of the map  $E_Q$  on the Riemann-Roch vector space  $\mathcal{L}(2D)$ , from the basis  $\mathcal{B}_{2D}$  in the basis  $\mathcal{B}_Q$ . We obtain the product  $z := xy$  of two elements  $x, y \in \mathbb{F}_{q^n}$  by the algorithm (3) in Theorem 2.1, where  $M^t$  denotes the transposed matrix of the matrix  $M$ :

---

**Algorithm 1** Chudnovsky<sup>2</sup> Multiplication algorithm (CCMA) in  $\mathbb{F}_{q^n}$

---

**INPUT:**  $x = \sum_{i=1}^n x_i Ev_Q(f_i)$ , and  $y = \sum_{i=1}^n y_i Ev_Q(f_i)$ .

**OUTPUT:**  $z = xy = \sum_{i=1}^n z_i Ev_Q(f_i)$ .

1.  $X := (X_1, \dots, X_N) = (x_1, \dots, x_n) T_D^t = Ev_{\mathcal{P}}(x)$ .  
 $Y := (Y_1, \dots, Y_N) = (y_1, \dots, y_n) T_D^t = Ev_{\mathcal{P}}(y)$ .
  2.  $Z := X \odot Y = (Z_1, \dots, Z_N) = (X_1 Y_1, \dots, X_N Y_N)$ .
  3.  $(z_1, \dots, z_n) = (Z_1, \dots, Z_N) (T_{2D}^t)^{-1} C^t = E_Q \circ Ev_{\mathcal{P}}^{-1}(Z)$ .
- 

Now, we present an initial setup algorithm which is only done once.

---

**Algorithm 2** Setup algorithm of CCMA in  $\mathbb{F}_{q^n}$

---

**INPUT:**  $F/\mathbb{F}_q$ ,  $Q, D, \mathcal{P} = \{P_1, \dots, P_{2n+g-1}\}$ .

**OUTPUT:**  $\mathcal{B}_{2D}$ ,  $T_{2D}$  and  $CT_{2D}^{-1}$ .

1. Check the function field  $F/\mathbb{F}_q$ , the place  $Q$ , the divisors  $D$  are such that Conditions (i) and (ii) in Theorem 2.2 can be satisfied.
  2. Represent  $\mathbb{F}_{q^n}$  as the residue class field of the place  $Q$ .
  3. Construct a basis  $\mathcal{B}_{2D} := \{f_1, \dots, f_n, f_{n+1}, \dots, f_{2n+g-1}\}$  of  $\mathcal{L}(2D)$ , where  $\mathcal{B}_D := \{f_1, \dots, f_n\}$  is a basis of  $\mathcal{L}(D)$ , and  $\mathcal{B}_D^c := \{f_{n+1}, \dots, f_{2n+g-1}\}$  a basis of the supplementary space  $\mathcal{M}$  of  $\mathcal{L}(D)$  in  $\mathcal{L}(2D)$ .
  4. Compute the matrices  $T_{2D}$ ,  $C$  and  $CT_{2D}^{-1}$ .
- 

## 2.2 Complexity analysis

Recall that the bilinear complexity of Chudnovsky<sup>2</sup> algorithms of type (3) in Theorem 2.1 satisfying assumptions of Theorem 2.2 is optimized. Therefore, we only focus on optimizing the scalar complexity of the algorithm. From Algorithm 1 we observe that the number of scalar multiplications depends directly on the number of zeros and of coefficients equal to 1 in the matrices  $T_D$  and  $C.T_{2D}^{-1}$ . Indeed, all the involved matrices being constructed once, the multiplication by a coefficient zero or 1 in a matrix has not to be taken into account. Let us give an algorithm  $\mathcal{U}_{q,n}$  of type Algorithm 1 with a setup of type Algorithm 2. We can analyze the multiplicative complexity  $\mu_m(\mathcal{U}_{q,n})$  of the algorithm  $\mathcal{U}_{q,n}$ , i.e. in terms of the total number of multiplications in  $\mathbb{F}_q$ , in the following way. We

call  $\mu_{s,0}(\mathcal{U}_{q,n})$  (resp.  $\mu_{s,1}(\mathcal{U}_{q,n})$ ) the scalar complexity of the algorithm  $\mathcal{U}_{q,n}$ , taking into account uniquely the number of zeros  $N_z(T_D)$  (resp. the number of ones  $N_1(T_D)$ ) and  $N_z(CT_{2D}^{-1})$  (resp.  $N_1(CT_{2D}^{-1})$ ) respectively in the matrices  $T_D$  and  $CT_{2D}^{-1}$ . Consequently, we clearly have

$$\mu_s(\mathcal{U}_{q,n}) \leq \mu_{s,0}(\mathcal{U}_{q,n}) \quad (8)$$

$$\mu_s(\mathcal{U}_{q,n}) \leq \mu_{s,1}(\mathcal{U}_{q,n}) \quad (9)$$

and so

$$\mu_m(\mathcal{U}_{q,n}) \leq \mu_{s,0}(\mathcal{U}_{q,n}) + \mu_b(\mathcal{U}_{q,n}) \quad (10)$$

$$\mu_m(\mathcal{U}_{q,n}) \leq \mu_{s,1}(\mathcal{U}_{q,n}) + \mu_b(\mathcal{U}_{q,n}) \quad (11)$$

by Definition 1.2.

The multiplicative complexity of the algorithm  $\mathcal{U}_{q,n}$  is equal to

$$\mu_m(\mathcal{U}_{q,n}) = (3n + 1)(2n + g - 1),$$

including

$$\mu_s(\mathcal{U}_{q,n}) = 3n(2n + g - 1)$$

scalar multiplications in the least case. More precisely, we get the formula to compute the number of scalar multiplications of this algorithm with respect to the number of zeros and 1 of the involved matrices as follows:

$$\mu_s(\mathcal{U}_{q,n}) = 2 \left( n(2n + g - 1) - N_z(T_D) - N_1(T_D) \right) +$$

$$\left( n(2n + g - 1) - N_z(CT_{2D}^{-1}) - N_1(CT_{2D}^{-1}) \right) = 3n(2n + g - 1) - N_z - N_1, \quad (12)$$

where

$$N_z = 2N_z(T_D) + N_z(CT_{2D}^{-1}) \quad (13)$$

and

$$N_1 = 2N_1(T_D) + N_1(CT_{2D}^{-1}). \quad (14)$$

Moreover, we see in Algorithm 1 that all the scalar multiplications come from steps 1 and 3. Thus, for the analysis of the scalar complexity of any algorithm  $\mathcal{U}_{q,n}$ , we will distinguish the scalar complexities of steps 1 and 3 (resp. denoted  $\mathcal{U}_A$  and  $\mathcal{U}_R$ ) by respectively  $\mu_s(\mathcal{U}_A)$  and  $\mu_s(\mathcal{U}_R)$  which are by Formula (12):

$$\mu_s(\mathcal{U}_A) = 2 \left( n(2n + g - 1) - N_z(T_D) - N_1(T_D) \right) \quad (15)$$

and

$$\mu_s(\mathcal{U}_R) = \left( n(2n + g - 1) - N_z(C.T_{2D}^{-1}) - N_1(C.T_{2D}^{-1}) \right). \quad (16)$$

We also will distinguish the scalar complexity of these steps of the algorithm, taking only into account the number of zeros (resp. the number of 1). Note that if we take into account the number of zeros (resp. the number of 1) in the step  $\mathcal{U}_A$ , then we take into account the number of zeros (resp. the number of 1) in the step  $\mathcal{U}_R$ . Thus, we call  $\mu_{s,0}(\mathcal{U}_A)$  (resp.  $\mu_{s,1}(\mathcal{U}_A)$ ) and  $\mu_{s,0}(\mathcal{U}_R)$  (resp.  $\mu_{s,1}(\mathcal{U}_R)$ ) the quantities:

$$\mu_{s,0}(\mathcal{U}_A) = \mu_s(\mathcal{U}_A) \text{ with } N_1(T_D) = 0 \quad (17)$$

$$\mu_{s,1}(\mathcal{U}_A) = \mu_s(\mathcal{U}_A) \text{ with } N_z(T_D) = 0 \quad (18)$$

and

$$\mu_{s,0}(\mathcal{U}_R) = \mu_s(\mathcal{U}_R) \text{ with } N_1(C.T_{2D}^{-1}) = 0, \quad (19)$$

$$\mu_{s,1}(\mathcal{U}_R) = \mu_s(\mathcal{U}_R) \text{ with } N_z(C.T_{2D}^{-1}) = 0. \quad (20)$$

Thus, we have:

$$\mu_{s,0}(\mathcal{U}_{q,n}) = \mu_{s,0}(\mathcal{U}_A) + \mu_{s,0}(\mathcal{U}_R) = 3n(2n + g - 1) - N_z, \quad (21)$$

and

$$\mu_{s,1}(\mathcal{U}_{q,n}) = \mu_{s,1}(\mathcal{U}_A) + \mu_{s,1}(\mathcal{U}_R) = 3n(2n + g - 1) - N_1. \quad (22)$$

**Remark 2.3.** *For the scalar complexity (i.e. the number of scalar multiplications), the coefficients 1 and 0 play a symmetrical role. However, if we are looking at the additions, this role is no longer symmetrical because the coefficients 1 present in the matrices increase the number of additions in the multiplication algorithm. Thus, from this point of view, it is in every interest to favor the maximization of the number of zeros. It is for this reason in particular that this article will give priority to the study of  $\mu_{s,0}(\mathcal{U}_{q,n})$ .*

### 3 Optimization of the scalar complexity

In this paper, we mainly focus on the optimization of the quantity  $\mu_{s,0}(\mathcal{U}_{q,n})$  introduced in Section 2.2. In this sense, reducing the number of operations means finding an algebraic function field  $F/\mathbb{F}_q$  having a genus  $g$  as small as possible and a suitable set of divisor and places  $(D, Q, \mathcal{P})$  with a good representation of the associated Riemann-Roch spaces, namely such that the matrices  $T_D$  and  $C.T_{2D}^{-1}$  are as hollow as possible (i.e. with a maximal number of zeros). Therefore, for a place  $Q$  and a suitable divisor  $D$ , we seek the best possible representations of Riemann-Roch spaces  $\mathcal{L}(D)$  and  $\mathcal{L}(2D)$  to maximize mainly both parameters  $N_z(T_D)$  and  $N_z(C.T_{2D}^{-1})$ .

### 3.1 Different types of generic strategy

#### 3.1.1 With fixed divisor and places

In this section, we consider the optimization of any algorithm  $\mathcal{U}_{q,n}$  for a fixed suitable set of divisor and places  $(D, Q, \mathcal{P})$  for a given algebraic function field  $F/\mathbb{F}_q$  of genus  $g$ . Hence, according to Section 2.2, we will denote here more precisely the algorithm  $\mathcal{U}_{q,n}$  as well as the associated quantities  $\mathcal{U}_A$  and  $\mathcal{U}_R$  thanks to the following definition:

**Definition 3.1.** We call  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n} := (\mathcal{U}_{D,Q,\mathcal{P}}^A, \mathcal{U}_{D,Q,\mathcal{P}}^R)$  a Chudnovsky<sup>2</sup> multiplication algorithm of type (3) where  $\mathcal{U}_{D,Q,\mathcal{P}}^A := E_{\mathcal{P}} \circ Ev_Q^{-1}$  and  $\mathcal{U}_{D,Q,\mathcal{P}}^R := E_Q \circ Ev_{\mathcal{P}}|_{Im Ev_{\mathcal{P}}}^{-1}$ , satisfying the assumptions of Theorem 2.1. We will say that two algorithms are equal, and we will note:  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n} = \mathcal{U}_{D',Q',\mathcal{P}'}^{F,n}$ , if  $\mathcal{U}_{D,Q,\mathcal{P}}^A = \mathcal{U}_{D',Q',\mathcal{P}'}^A$  and  $\mathcal{U}_{D,Q,\mathcal{P}}^R = \mathcal{U}_{D',Q',\mathcal{P}'}^R$ .

Note that in this case, this definition makes sense only if the bases of implied vector-spaces are fixed. So, we denote respectively by  $\mathcal{B}_Q$ ,  $\mathcal{B}_D$ , and  $\mathcal{B}_{2D}$  the basis of the residue class field  $F_Q$ , and of Riemann-Roch vector-spaces  $\mathcal{L}(D)$ , and  $\mathcal{L}(2D)$  associated to  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$ . Note that the basis of the  $\mathbb{F}_q$ -vector space  $\mathbb{F}_q^N$  is the canonical basis, up to permutation. Then, we obtain the following result:

**Proposition 3.1.** Let us consider an algorithm  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  such that the divisor  $D$  is an effective divisor,  $D - Q$  a non-special divisor of degree  $g - 1$ , and such that the cardinal of the set  $\mathcal{P}$  is equal to the dimension of the Riemann-Roch space  $\mathcal{L}(2D)$ . Then we can choose the basis  $\mathcal{B}_{2D}$  as (7) and for any  $\sigma$  in  $GL_{\mathbb{F}_q}(2n + g - 1)$ , where  $GL_{\mathbb{F}_q}(2n + g - 1)$  denotes the linear group, we have

$$\mathcal{U}_{\sigma(D),Q,\mathcal{P}}^{F,n} = \mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$$

where  $\sigma(D)$  denotes the action of  $\sigma$  on the basis  $\mathcal{B}_{2D}$  of  $\mathcal{L}(2D)$  in  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$ , with a fixed basis  $\mathcal{B}_Q$  of the residue class field of the place  $Q$  and  $\mathcal{B}_c$  the canonical basis of  $\mathbb{F}_q^{2n+g-1}$ . In particular, the quantities  $N_z(C.T_{2D}^{-1})$  and  $N_1(C.T_{2D}^{-1})$  are constant under this action.

*Proof.* Let  $E$ ,  $F$  and  $H$  be three vector spaces of finite dimension on a field  $K$  respectively equipped with the basis  $\mathcal{B}_E$ ,  $\mathcal{B}_F$  and  $\mathcal{B}_H$ . Consider two morphisms  $f$  and  $h$  respectively defined from  $E$  into  $F$  and from  $F$  into  $H$  and consider respectively their associated matrix  $M_f(\mathcal{B}_E, \mathcal{B}_F)$  and  $M_h(\mathcal{B}_F, \mathcal{B}_H)$ . Then it is obvious that the matrix  $M_{h \circ f}(\mathcal{B}_E, \mathcal{B}_H)$  of the morphism  $h \circ f$  is independant from the choice of the basis  $\mathcal{B}_F$  of  $F$ . As the divisor  $D$  is effective, we have  $\mathcal{L}(D) \subset \mathcal{L}(2D)$  and then  $\mathcal{U}_{D,Q,\mathcal{P}}^A := E_{\mathcal{P}} \circ Ev_Q^{-1} = Ev_{\mathcal{P}} \circ Ev_Q^{-1}$  and as  $D - Q$  a non-special divisor of degree  $g - 1$ ,  $Ev_Q$  is an isomorphism from  $\mathcal{L}(D)$  into  $F_Q$  and we have  $\mathcal{U}_{D,Q,\mathcal{P}}^A = Ev_{\mathcal{P}}|_{\mathcal{L}(D)} \circ Ev_Q^{-1}$ . Moreover, as the cardinal of the set  $\mathcal{P}$  is equal to the dimension of the Riemann-Roch space  $\mathcal{L}(2D)$ ,  $Ev_{\mathcal{P}}$  is an isomorphism from  $\mathcal{L}(2D)$  into  $\mathbb{F}_q^{2n+g-1}$  equipped with the canonical basis  $\mathcal{B}_c$ . Thus,  $\mathcal{U}_{D,Q,\mathcal{P}}^R := E_Q \circ Ev_{\mathcal{P}}^{-1}|_{Im Ev_{\mathcal{P}}} = E_Q|_{\mathcal{L}(2D)} \circ Ev_{\mathcal{P}}^{-1}$ . Then, the matrix of

$\mathcal{U}_{D,Q,\mathcal{P}}^A$  (resp.  $\mathcal{U}_{D,Q,\mathcal{P}}^R$ ) is invariant under the action of  $\sigma$  in  $GL_{\mathbb{F}_q}(n)$  (resp. in  $GL_{\mathbb{F}_q}(2n+g-1)$ ) on the basis  $\mathcal{B}_D$  (resp.  $\mathcal{B}_{2D}$ ) since the set  $(E, F, H)$  is equal to  $(F_Q, \mathcal{L}(D), \mathbb{F}_q^{2n+g-1})$  (resp.  $(\mathbb{F}_q^{2n+g-1}, \mathcal{L}(2D), F_Q)$ ) for  $h \circ f := Ev_{\mathcal{P}}|_{\mathcal{L}(D)} \circ Ev_Q^{-1}$  (resp.  $E_Q|_{\mathcal{L}(2D)} \circ Ev_{\mathcal{P}}^{-1}$ ).  $\square$

Apart from the fact that this result provides a generic construction strategy of Chudnovsky's algorithm leading to significantly improve (and even optimize) the scalar complexity of this algorithm, this result also highlights a preferential configuration. Indeed, since the quantities  $N_z(C.T_{2D}^{-1})$  and  $N_1(C.T_{2D}^{-1})$  are constant under the action of the linear group, one has the choice, without consequence upon the scalar complexity, of the basis of the supplement  $\mathcal{L}(D)$  in  $\mathcal{L}(2D)$ . Also, we favor a kernel-type configuration which not only has the particularity of having no negative impact on the global scalar complexity of the algorithm  $\mathcal{U} = (\mathcal{U}_A, \mathcal{U}_R)$  but also to simplify the scalar optimization process of these algorithms as well as their use in the return phase  $\mathcal{U}_R$ , the latter item having already been noticed in the context of the exponentiation in [1]. Therefore, we need the following definition:

**Definition 3.2.** Let  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n} := (\mathcal{U}_{D,Q,\mathcal{P}}^A, \mathcal{U}_{D,Q,\mathcal{P}}^R)$  be a Chudnovsky<sup>2</sup> multiplication algorithm in a finite field  $\mathbb{F}_{q^n}$ , satisfying the assumptions of Proposition 3.1. Then the algorithm  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  is said kernel-type if the basis  $\mathcal{B}_{2D}$  of  $\mathcal{L}(2D)$  used in the evaluation map  $\mathcal{U}_{D,Q,\mathcal{P}}^R := E_Q \circ Ev_{\mathcal{P}}^{-1}$  is such that

$$\mathcal{B}_{2D} = \mathcal{B}_D \cup \mathcal{B}_D^c,$$

where  $\mathcal{B}_D$  is a basis of  $\mathcal{L}(D)$  used in the evaluation map  $\mathcal{U}_{D,Q,\mathcal{P}}^A := E_{\mathcal{P}}|_{\mathcal{L}(D)} \circ Ev_Q^{-1}$  and  $\mathcal{B}_D^c$  is a basis of the supplementary space  $\mathcal{M} := Ker E_Q|_{\mathcal{L}(2D)}$  of  $\mathcal{L}(D)$  in  $\mathcal{L}(2D)$ . Any construction of a kernel-type algorithm  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  will be called a kernel-type construction.

**Proposition 3.2.** Let  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n} = (\mathcal{U}_{D,Q,\mathcal{P}}^A, \mathcal{U}_{D,Q,\mathcal{P}}^R)$  be a kernel-type Chudnovsky<sup>2</sup> multiplication algorithm in a finite field  $\mathbb{F}_{q^n}$ . The optimal scalar complexity  $\mu_{s,0}^{opti}(\mathcal{U}_{D,Q,\mathcal{P}}^A)$  of  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  is reached for the set  $\{\mathcal{B}_{D,max}, \mathcal{B}_Q\}$  such that  $\mathcal{B}_{D,max}$  is a basis of  $\mathcal{L}(D)$  satisfying

$$N_z(T_{D,max}) = \max_{\sigma \in GL_{\mathbb{F}_q}(n)} \{N_z(T_{\sigma(D)})\},$$

where  $\sigma(D)$  denotes the action of  $\sigma$  on the basis  $\mathcal{B}_D$  of  $\mathcal{L}(D)$  in  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$ ,  $T_{D,max}$  the matrix of the restriction of the evaluation map  $Ev_{\mathcal{P}}$  on the Riemann-Roch vector space  $\mathcal{L}(D)$  equipped with the bases  $\mathcal{B}_{D,max}$  and  $\mathcal{B}_Q = Ev_Q(\mathcal{B}_{D,max})$ . More precisely, we have

$$\mu_{s,0}^{opti}(\mathcal{U}_{D,Q,\mathcal{P}}^A) = \min_{\sigma \in GL_{\mathbb{F}_q}(n)} \{\mu_{s,0}(\mathcal{U}_{\sigma(D),Q,\mathcal{P}}^A) \mid \sigma(\mathcal{B}_D) \text{ is the basis of } \mathcal{L}(D) \text{ and } \mathcal{B}_Q = Ev_Q(\mathcal{B}_D)\}$$

$$= 2 \left( n(2n + g - 1) - N_z(T_{D,max}) \right).$$

Then, the scalar complexity of the algorithm  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  relatively to the basis  $\mathcal{B}_{D,max}$  is:

$$\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}) = 3n(2n + g - 1) - \left( 2N_z(T_{D,max}) + N_z(T_{2D,n}^{-1}) \right),$$

where matrices  $C$  and  $T_{2D}$  are defined with respect to the basis  $\mathcal{B}_Q = Ev_Q(\mathcal{B}_{D,max})$ , and  $\mathcal{B}_{2D} = \mathcal{B}_{D,max} \cup \mathcal{B}_D^c$  and  $T_{2D,n}^{-1}$  denotes the matrix made up of the  $n$  first lines of the matrix  $T_{2D}^{-1}$ .

*Proof.* The value of  $\mu_{s,0}^{opti}(\mathcal{U}_{D,Q,\mathcal{P}}^A)$  follows directly from Proposition 3.1 and formulae (15) and (17). Then, the quantity  $\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}})$  obtained with the basis  $\mathcal{B}_{D,max}$  follows from formulae (12) and (13). Note that since the algorithm  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  is kernel-type then we have  $CT_{2D}^{-1} = T_{2D,n}^{-1}$  because  $\mathcal{B}_D^c$  is a basis of the kernel of  $E_Q|_{\mathcal{L}(2D)}$ . □

**Proposition 3.3.** Let  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  be a kernel-type Chudnovsky<sup>2</sup> multiplication algorithm in a finite field  $\mathbb{F}_q^n$  such that  $\mathcal{B}_{2D} = \mathcal{B}_D \cup \mathcal{B}_D^c$ . The optimal scalar complexity  $\mu_{s,0}^{opti}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n})$  of  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  is reached for the set  $\{\mathcal{B}_{D,max}, \mathcal{B}_Q\}$  such that  $\mathcal{B}_{D,max}$  is a basis of  $\mathcal{L}(D)$  for which  $2N_z(T_{\sigma(D)}) + N_z(T_{2\sigma(D),n}^{-1})$  is maximal under the action of  $\sigma \in GL_{\mathbb{F}_q}(n)$  on the basis  $\mathcal{B}_D$  of  $\mathcal{L}(D)$  of the matrix  $T_D$  where  $T_{\sigma(D)}$  (resp.  $T_{2\sigma(D),n}^{-1}$ ) denotes the matrix  $T_D$  (resp. the  $n$  first lines of the matrix  $T_{2D}^{-1}$ ) in the basis  $\sigma(\mathcal{B}_D)$  (resp.  $\sigma(\mathcal{B}_D) \cup \mathcal{B}_D^c$ ) of  $\mathcal{L}(D)$  (resp.  $\mathcal{L}(2D)$ ), and  $\mathcal{B}_Q = Ev_Q(\mathcal{B}_{D,max})$ . In particular,

$$\begin{aligned} \mu_{s,0}^{opti}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) &= \min_{\sigma \in GL_{\mathbb{F}_q}(n)} \{ \mu_{s,0}(\mathcal{U}_{\sigma(D),Q,\mathcal{P}}^{F,n}) \mid \sigma(\mathcal{B}_D) \text{ is the basis of } \mathcal{L}(D) \\ &\quad \text{and } \mathcal{B}_Q = Ev_Q(\mathcal{B}_D) \} \\ &= 3n(2n + g - 1) - N_{z,max}, \end{aligned}$$

where

$$N_{z,max} = \max_{\sigma \in GL_{\mathbb{F}_q}(n)} \{ 2N_z(T_{\sigma(D)}) + N_z(T_{2\sigma(D),n}^{-1}) \},$$

and matrices  $C$  and  $T_{2D}$  are defined with respect to the basis  $\mathcal{B}_Q = Ev_Q(\mathcal{B}_{D,max})$ , and  $\mathcal{B}_{2D} = \mathcal{B}_{D,max} \cup \mathcal{B}_D^c$ .

*Proof.* The value of  $\mu_{s,0}^{opti}(\mathcal{U}_{D,Q,\mathcal{P}})$  obtained with the basis  $\mathcal{B}_{D,max}$  follows directly from Proposition 3.1 and formulae (21). Note that since the algorithm  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  is kernel-type then we have  $CT_{2D}^{-1} = T_{2D,n}^{-1}$  because  $\mathcal{B}_D^c$  is a basis of the kernel of  $E_Q|_{\mathcal{L}(2D)}$ . □

**Remark 3.1.** Note that in Proposition 3.2, we can establish a similar result for  $\mu_{s,1}^{opti}(\mathcal{U}_{D,Q,\mathcal{P}}^A)$  (or even better resp.  $\mu_s^{opti}(\mathcal{U}_{D,Q,\mathcal{P}}^A)$ ) by optimizing the quantity

$N_1(T_D)$  (resp. the quantity  $N_z(T_D) + N_1(T_D)$ ) instead of  $N_z(T_D)$ . In the same way, in Proposition 3.3, we can establish a similar result for  $\mu_{s,1}^{opti}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n})$  (or even better resp.  $\mu_s^{opti}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n})$ ) by optimizing the quantity  $2N_1(T_D) + N_1(T_{2D,n}^{-1})$  (resp. the quantity  $2(N_z(T_D) + N_1(T_D)) + N_z(T_{2D,n}^{-1}) + N_1(T_{2D,n}^{-1})$ ) instead of  $2N_z(T_D) + N_z(T_{2D,n}^{-1})$ .

Now, from these two previous results, we can highlight several strategies to improve the scalar complexity. The complexities of these strategies are clearly different. Therefore, the use of this or that strategy may be useful depending on the constraints to which we are subject. New setup algorithms can be obtained directly from the analysis developed in Section 3.1.1. More precisely, the following setup corresponds to the optimization of  $\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^A)$  described by Proposition 3.2.

---

**Algorithm 3** New setup algorithm of CCMA in  $\mathbb{F}_{q^n}$  from Proposition 3.2

---

**INPUT:**  $F/\mathbb{F}_q$ ,  $Q, D, \mathcal{P} = \{P_1, \dots, P_{2n+g-1}\}$ .

**OUTPUT:**  $\mathcal{B}_{2D}, \mathcal{B}_Q, T_{2D}$  and  $T_{2D,n}^{-1}$ .

1. Check the function field  $F/\mathbb{F}_q$ , the place  $Q$ , the divisors  $D$  are such that Conditions (i) and (ii) in Theorem 2.2 can be satisfied.
  2. Take an initial basis  $\mathcal{B}_{D,0}$  for  $\mathcal{L}(D)$  and construct a basis  $\mathcal{B}_D^c := \{f_{n+1}, \dots, f_{2n+g-1}\}$  of the supplementary space  $\mathcal{M} := \text{Ker} E_Q|_{\mathcal{L}(2D)}$  of  $\mathcal{L}(D)$  in  $\mathcal{L}(2D)$ .
  3. Go through the set (or subset) of bases  $\mathcal{B}_D$  of  $\mathcal{L}(D)$  from  $\mathcal{B}_{D,0}$  and linear group  $GL_q(n)$  in order to compute  $T_D$  and  $N_z(T_D)$ .
  4. Choose a basis  $\mathcal{B}_D := \{f_1, \dots, f_n\}$  such that the matrix  $T_D$  owns the largest number of zeros (i.e. such that  $\mathcal{B}_D := \mathcal{B}_{D,max}$  and  $T_D := T_{D,max}$ ).
  5. Set  $\mathcal{B}_Q := \text{Ev}_Q(\mathcal{B}_{D,max})$  and  $\mathcal{B}_{2D} := \mathcal{B}_{D,max} \cup \mathcal{B}_D^c$ .
  6. Compute the matrices  $T_{2D}$  and  $T_{2D,n}^{-1}$  in the basis  $\mathcal{B}_{2D}$ .
- 

In the same way, from Proposition 3.3, we can obtain the following new setup corresponding to the optimization of  $\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n})$ .

---

**Algorithm 4** New setup algorithm of CCMA in  $\mathbb{F}_{q^n}$  from Proposition 3.3

---

**INPUT:**  $F/\mathbb{F}_q$ ,  $Q, D, \mathcal{P} = \{P_1, \dots, P_{2n+g-1}\}$ .

**OUTPUT:**  $\mathcal{B}_{2D}, \mathcal{B}_Q, T_{2D}$  and  $T_{2D,n}^{-1}$ .

1. Check the function field  $F/\mathbb{F}_q$ , the place  $Q$ , the divisors  $D$  are such that Conditions (i) and (ii) in Theorem 2.2 can be satisfied.
  2. Take an initial basis  $\mathcal{B}_{D,0}$  for  $\mathcal{L}(D)$  and construct a basis  $\mathcal{B}_D^c := \{f_{n+1}, \dots, f_{2n+g-1}\}$  of the supplementary space  $\mathcal{M} := \text{Ker} E_Q|_{\mathcal{L}(2D)}$  of  $\mathcal{L}(D)$  in  $\mathcal{L}(2D)$ .
  3. Go through the set (or subset) of bases  $\mathcal{B}_D$  of  $\mathcal{L}(D)$  from  $\mathcal{B}_{D,0}$  and linear group  $GL_q(n)$  in order to compute  $T_D$  (resp.  $T_{2D,n}^{-1}$  with  $\mathcal{B}_{2D} = \mathcal{B}_D \cup \mathcal{B}_D^c$ ) and  $N_z(T_D)$  (resp.  $N_z(T_{2D,n}^{-1})$ ).
  4. Choose a basis  $\mathcal{B}_D := \{f_1, \dots, f_n\}$  such that  $2N_z(T_D) + N_z(T_{2D,n}^{-1})$  is the largest possible (i.e. such that  $\mathcal{B}_D := \mathcal{B}_{D,max}$  and  $2N_z(T_D) + N_z(T_{2D,n}^{-1}) := N_{z,max}$ ).
  5. Set  $\mathcal{B}_Q := \text{Ev}_Q(\mathcal{B}_{D,max})$  and  $\mathcal{B}_{2D} := \mathcal{B}_{D,max} \cup \mathcal{B}_D^c$ .
- 

**Remark 3.2.** Note that in Algorithm 4, Step 6 of the Algorithm 3 was performed in steps 3 and 4 since in order to construct  $T_{2D,n}^{-1}$ , we required to construct before the matrix  $T_{2D}$ .

**Remark 3.3.** Note that in the setup algorithm 3, the steps 3 and 4 may be substituted by : choose a basis  $\mathcal{B}_D := (f_1, \dots, f_n)$  such that the matrix  $T_D$  owns the largest number of 1 or the largest number of 0 or 1 taken together, in the same spirit as Remark 3.1. So, in the setup algorithm 4, the number  $N_z$  in the steps 3 and 4 may be substituted by the number  $N_1$  resp.  $N_z + N_1$  for each matrix  $T_D$  and  $T_{2D,n}^{-1}$ . However, we have chosen in this paper to focus particularly on the number of zeros because it is possible to give an upper bound on this value, as we will see below.

Indeed, let  $F/\mathbb{F}_q$  be an algebraic function field of genus  $g$  and let  $\mathcal{P} = \{P_1, \dots, P_N\}$  be an ordered set of pairwise distinct places of degree one in  $F/\mathbb{F}_q$ . Let us adapt slightly the notation used in [12] to be homogeneous with the notation used in the description of CCMA. So, we consider that the divisors  $G = P_1 + \dots + P_N$  and  $D$  are divisors of  $F/\mathbb{F}_q$  such that  $\text{supp}G \cap \text{supp}D = \emptyset$ . The algebraic geometry code (or Goppa code)  $C_{\mathcal{L}}(G, D)$  associated with the divisors  $G$  and  $D$  is defined as

$$C_{\mathcal{L}}(G, D) := \{(f(P_1), \dots, f(P_N)) | f \in \mathcal{L}(D)\} \subseteq \mathbb{F}_q^N.$$

Then  $C_{\mathcal{L}}(G, D)$  is an  $[N, k, d]$  code with parameters  $k = \dim \mathcal{L}(D) - \dim \mathcal{L}(D - G)$  and minimum distance  $d \geq N - \deg D$  by [12, Theorem 2.2.2]. If  $\{f_1, \dots, f_k\}$  is a basis of  $\mathcal{L}(D)$ , then by [12, Corollary 2.2.3] we have the following generator



matrix for  $C_{\mathcal{L}}(G, D)$

$$M := \begin{pmatrix} f_1(P_1) & \cdots & f_1(P_N) \\ f_2(P_1) & \cdots & f_2(P_N) \\ \vdots & \vdots & \vdots \\ f_k(P_1) & \cdots & f_k(P_N) \end{pmatrix}.$$

In the Chudnovsky<sup>2</sup> multiplication algorithm (CCMA) defined in the context of Theorem 2.2, we consider the bijective evaluation map

$$\begin{aligned} \text{Ev}_{\mathcal{P}} : \mathcal{L}(2D) &\rightarrow \mathbb{F}_q^N. \\ f &\mapsto (f(P_1), \dots, f(P_N)) \end{aligned}$$

where  $\deg D = n + g - 1$  and  $N = 2n + g - 1$ . Moreover, we recall that our construction of CCMA is made with the assumptions of Proposition 3.1, hence  $\mathcal{L}(D) \subseteq \mathcal{L}(2D)$  since  $D$  is an effective divisor. Then, the image of the restriction  $\text{Ev}_{\mathcal{P}}|_{\mathcal{L}(D)}$  of  $\text{Ev}_{\mathcal{P}}$  on  $\mathcal{L}(D)$  is a  $\mathbb{F}_q$ -vector subspace of  $\mathbb{F}_q^N$  of dimension  $n$  which can be seen as an algebraic geometry code  $C_{\mathcal{L}}(G, D) = [N, n, d]$  where  $G = P_1 + \cdots + P_N$ . Therefore, we can prove the following results.

**Proposition 3.4.** *Let  $\mathcal{U}_{D, Q, \mathcal{P}}^{F, n}$  be a Chudnovsky<sup>2</sup> multiplication algorithm in a finite field  $\mathbb{F}_{q^n}$ , satisfying the assumptions of Proposition 3.2. Then we have:*

$$N_z(T_D) \leq n(n + g - 1).$$

*Proof.* The matrix  $T_D$  is such that

$$N_z(T_D) = n \cdot N - N_{nz}(T_D), \quad (23)$$

where  $N_{nz}(T_D)$  denotes the number of non-zero entries of  $T_D$  and  $N = 2n + g - 1$ . Moreover, as  $\text{Ev}_{\mathcal{P}}(\mathcal{L}(D))$  is an algebraic geometry code  $C_{\mathcal{L}}(G, D) = [N, n, d]$  where  $G = P_1 + \cdots + P_N$ , then  $T_D^t$  is a generator matrix of this code. So, we have

$$N_{nz}(T_D) \geq n \cdot d, \quad (24)$$

by the definition of the minimal distance of a code. Moreover, we have

$$d \geq N - \deg D \quad (25)$$

by [12, Theorem 2.2.2]. So, we obtain by (23), (24) and (25):

$$N_z(T_D) \leq n \cdot \deg D \quad (26)$$

As  $\deg D = n + g - 1$ , we obtain the result.  $\square$

**Theorem 3.1.** *Let  $\mathcal{U}_{D, Q, \mathcal{P}}^{F, n} = (\mathcal{U}_{D, Q, \mathcal{P}}^A, \mathcal{U}_{D, Q, \mathcal{P}}^R)$  be a Chudnovsky<sup>2</sup> multiplication algorithm in a finite field  $\mathbb{F}_{q^n}$ , satisfying the assumptions of Proposition 3.2. Then we have:*

$$\mu_{s,0}(\mathcal{U}_{D, Q, \mathcal{P}}^A) \geq 2n^2$$

and

$$\mu_{s,0}(\mathcal{U}_{D, Q, \mathcal{P}}^{F, n}) > 2n^2.$$

*Proof.* By Equalities (15) and (17), we have

$$\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^A) = 2(n(2n+g-1) - N_z(T_D)).$$

Then, since  $N_z(T_D) \leq n(n+g-1)$  by Proposition 3.4, we deduce the first inequality. Moreover, we have the trivial bound  $N_z(T_{2D,n}^{-1}) < n(2n+g-1)$ . Thus, as  $\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = 3n(2n+g-1) - N_z = 3n(2n+g-1) - 2N_z(T_D) - N_z(T_{2D,n}^{-1})$  by Equality (21), we obtain  $\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) > 2n^2$ .  $\square$

Now, we can give an optimization using a criterium obtained from Proposition 3.4.

---

**Algorithm 5** New setup algorithm of CCMA in  $\mathbb{F}_{q^n}$  from Proposition 3.4

---

**INPUT:**  $F/\mathbb{F}_q$ ,  $Q, D, \mathcal{P} = \{P_1, \dots, P_{2n+g-1}\}$ .

**OUTPUT:**  $\mathcal{B}_{2D}, \mathcal{B}_Q, T_{2D}$  and  $T_{2D,n}^{-1}$ .

1. Check the function field  $F/\mathbb{F}_q$ , the place  $Q$ , the divisors  $D$  are such that Conditions (i) and (ii) in Theorem 2.2 can be satisfied.
  2. Take an initial basis  $\mathcal{B}_{D,0}$  for  $\mathcal{L}(D)$  and construct a basis  $\mathcal{B}_D^c := \{f_{n+1}, \dots, f_{2n+g-1}\}$  of the supplementary space  $\mathcal{M} := \text{Ker} E_Q|_{\mathcal{L}(2D)}$  of  $\mathcal{L}(D)$  in  $\mathcal{L}(2D)$ .
  3. Go through the set (or subset) of bases  $\mathcal{B}_D$  of  $\mathcal{L}(D)$  from  $\mathcal{B}_{D,0}$  and linear group  $GL_q(n)$  in order to compute  $T_D$  and to construct the set  $mB_D = \{\mathcal{B}_D \mid N_z(T_D) = n(n+g-1)\}$ .
  4. Choose a basis  $\mathcal{B}_D := \{f_1, \dots, f_n\} \in mB_D$  such that  $N_z(T_{2D,n}^{-1})$  is the largest possible.
  5. Set  $\mathcal{B}_Q := \text{Ev}_Q(\mathcal{B}_{D,max})$  and  $\mathcal{B}_{2D} := \mathcal{B}_{D,max} \cup \mathcal{B}_D^c$ .
  6. Compute the matrices  $T_{2D}$  and  $T_{2D,n}^{-1}$  in the basis  $\mathcal{B}_{2D}$ .
- 

**Remark 3.4.** Note that in the setup algorithm 5, the step 4 may be substituted by the best following criterium: choose a basis  $\mathcal{B}_D \in mB_D$  such that  $2N_1(T_D) + N_z(T_{2D,n}^{-1}) + N_1(T_{2D,n}^{-1})$  is the largest possible.

**Remark 3.5.** As one can see, the algorithms proposed in this section are generic and in this sense they are well automatized for any set  $(q, n, F/\mathbb{F}_q, D, Q)$ . Indeed the complexity of the optimization increases with the cardinal of  $GL_q(n)$ . However, this complexity of optimization (although not having currently an accurate estimate) is much lower than that of a brute force optimization where all the bases of each of the vector spaces involved in the two linear applications must be tested. In fact, the strong point of the analysis conducted in this section is that it shows that the only relevant lever to optimize the CCMA algorithm concerns the representation of the  $\mathcal{L}(D)$  space and only this space. Therefore, most of the complexity of this optimization lies in running over the linear group (or a subset) underlying this space, as well as in related operations.

### 3.1.2 Strategy of complete optimization

In the view of a complete optimization (with respect to scalar complexity i.e. with fixed bilinear complexity) of the multiplication in a finite field  $\mathbb{F}_{q^n}$  by a Chudnovsky<sup>2</sup> multiplication algorithm, we have to vary the eligible sets  $(F, D, Q, \mathcal{P})$ . We can vary the couples  $(D, Q)$  satisfying the assumptions of Proposition 3.1 and apply complete optimization Algorithm 4 (or Algorithm 4 with optimization criterium  $N_1$  resp.  $N_z + N_1$  as mentioned in Remark 3.3): for instance, we can start by fixing the place  $Q$  and then vary the suitable divisors  $D$ . Concerning the set  $\mathcal{P}$  of rational places, we can show that two algorithms which differ only by the order of the places on which we evaluate have the same scalar complexity. That is to say, for any permutation  $\pi$  of the set  $\mathcal{P}$ , we wonder whether  $\mathcal{U}_{D,Q,\pi(\mathcal{P})}^{F,n}$  is different from  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  in order to answer to the open problem mentioned in [4, Remark 3]. The action of  $\pi$  corresponds to a permutation of the canonical basis  $\mathcal{B}_c$  of  $\mathbb{F}_q^{2n+g-1}$ . It corresponds to a permutation of the rows of the matrix  $T_{2D}$ . In this case,  $N_z(T_D)$  and  $N_1(T_D)$  are obviously constant under the action of  $\pi$ . The following proposition also enables us to claim that  $N_z(CT_{2D}^{-1})$  and  $N_1(CT_{2D}^{-1})$  are constant under the action of  $\pi$ .

**Proposition 3.5.** *Let us consider an algorithm  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$  such that  $D$  is an effective divisor,  $D - Q$  a non-special divisor of degree  $g - 1$ , and  $|\mathcal{P}| = \dim \mathcal{L}(2D) = N$ .*

*Then for any  $\pi$  in  $S_N$  where  $S_N$  is the symmetric group on the set  $\{1, 2, \dots, N\}$ , we have*

$$\mu_s(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = \mu_s(\mathcal{U}_{D,Q,\pi(\mathcal{P})}^{F,n})$$

and

$$\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = \mu_{s,0}(\mathcal{U}_{D,Q,\pi(\mathcal{P})}^{F,n}).$$

*In particular, the quantities  $N_z(T_D)$  (resp.  $N_1(T_D)$ ) and  $N_z(CT_{2D}^{-1})$  (resp.  $N_1(CT_{2D}^{-1})$ ) are constants under the action  $\pi$ .*

*Proof.* Let  $\mathcal{P} := \{P_1, P_2, \dots, P_N\}$  be the ordered set of  $N$  rational places used in the algorithm  $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$ . We consider the action of the permutation  $\pi \in S_N$  on the set  $\mathcal{P}$  by setting  $\mathcal{P}' = \pi \cdot \mathcal{P} = \{P_{\pi(1)}, P_{\pi(2)}, \dots, P_{\pi(N)}\}$ .

Given a basis  $\mathcal{B}_{2D}$  of Riemann-Roch space  $\mathcal{L}(2D)$ , we consider two evaluation maps:

$$\begin{aligned} Ev_{\mathcal{P}} : \mathcal{L}(2D) &\rightarrow \mathbb{F}_q^N \\ f &\mapsto (f(P_1), \dots, f(P_N)) \end{aligned} \quad (27)$$

and

$$\begin{aligned} Ev_{\mathcal{P}'} : \mathcal{L}(2D) &\rightarrow \mathbb{F}_q^N \\ f &\mapsto (f(P_{\pi(1)}), \dots, f(P_{\pi(N)})) \end{aligned} \quad (28)$$

We denote  $\mathcal{B}_{\mathbb{F}_q^N}^c = (e_1, \dots, e_N)$  the canonical basis of  $\mathbb{F}_q^N$  in (27) and  $\mathcal{B}_{\mathbb{F}_q^N}^\pi = (e_{\pi(1)}, \dots, e_{\pi(N)})$  the basis of  $\mathbb{F}_q^N$  in (28).

Let us define an isomorphism  $p : \mathbb{F}_q^N \rightarrow \mathbb{F}_q^N$  by  $p(e_i) = e_{\pi(i)}$  for  $i = 1..N$ . The matrix representation of this map is denoted by  $P$ . We see that  $P$  is a permutation matrix and note that  $P^{-1} = P^t$ . We have

$$Ev_{\mathcal{P}'} = p \circ Ev_{\mathcal{P}}.$$

Then

$$\mathcal{U}_{D,Q,\mathcal{P}'}^A = E_{\mathcal{P}'} \circ Ev_Q^{-1} = p \circ E_{\mathcal{P}} \circ Ev_Q^{-1} = p \circ \mathcal{U}_{D,Q,\mathcal{P}}^A \quad (29)$$

and

$$\mathcal{U}_{D,Q,\mathcal{P}'}^R = E_Q \circ Ev_{\mathcal{P}'}^{-1} |_{Im(Ev_{\mathcal{P}'})} = E_Q \circ (p \circ Ev_{\mathcal{P}} |_{Im(Ev_{\mathcal{P}})})^{-1} = \mathcal{U}_{D,Q,\mathcal{P}}^R \circ p^{-1}. \quad (30)$$

Observing the changement of the positions of rows of  $T_{2D}$  and columns of  $CT_{2D}^{-1}$  affected by (29) and (30) respectively, we have  $N_z(T_D)$  (resp.  $N_1(T_D)$ ) and  $N_z(CT_{2D}^{-1})$  (resp.  $N_1(CT_{2D}^{-1})$ ) are constants for any  $\pi \in S_N$ .

By (12) we obtain

$$\mu_s(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = \mu_s(\mathcal{U}_{D,Q,\pi(\mathcal{P})}^{F,n})$$

and

$$\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = \mu_{s,0}(\mathcal{U}_{D,Q,\pi(\mathcal{P})}^{F,n})$$

for any  $\pi \in S_N$ . □

Finally, we can then look for a fixed suitable algebraic function field of genus  $g$ , up to isomorphism, and repeat all the previous steps. Moreover, it is still possible to look at the trade-off between scalar complexity and bilinear complexity by increasing the genus and then re-conducting all the previous optimizations (i.e. we take algebraic function fields with a genus larger than required for multiplying in  $\mathbb{F}_{q^n}$ ).

## 3.2 Optimization of scalar complexity in the elliptic case

Now, we study a specialisation of the Chudnovsky<sup>2</sup> multiplication algorithm of type (3) in the case of the elliptic curves (cf. inequality (2)). In particular, we improve the effective algorithm constructed in the article of U. Baum and M.A. Shokrollahi [6] which presented an optimal algorithm from the point of view of the bilinear complexity in the case of the multiplication in  $\mathbb{F}_{256}/\mathbb{F}_4$  based on Chudnovsky<sup>2</sup> multiplication algorithm applied on the Fermat curve  $x^3 + y^3 = 1$  defined over  $\mathbb{F}_4$ . Our method of construction leads to a multiplication algorithm in  $\mathbb{F}_{256}/\mathbb{F}_4$  having a lower scalar complexity with an optimal bilinear complexity.

### 3.2.1 Experiment of Baum-Shokrollahi

The article [6] presents Chudnovsky<sup>2</sup> multiplication in  $\mathbb{F}_{4^4}$ , for the case  $q = 4$  and  $n = 4$ . The elements of  $\mathbb{F}_4$  are denoted by  $0, 1, \omega$  and  $\omega^2$ . The algorithm construction requires the use of an elliptic curve over  $\mathbb{F}_4$  with at least 9  $\mathbb{F}_4$ -rational points (which is the maximum possible number by Hasse-Weil Bound).

Note that in this case, Conditions 1) and 2) of Theorem 2.2 are well satisfied. It is well known that the Fermat curve  $u^3 + v^3 = 1$  satisfies this condition. By the substitutions  $x = 1/(u + v)$  and  $y = u/(u + v)$ , we get the isomorphic curve  $y^2 + y = x^3 + 1$ . From now on,  $F/\mathbb{F}_q$  denotes the algebraic function field associated to the elliptic curve  $\mathcal{C}$  with plane model  $y^2 + y = x^3 + 1$ , of genus one. The projective coordinates  $(x : y : z)$  of  $\mathbb{F}_4$ -rational points of this elliptic curve are:

$$P_\infty = (0 : 1 : 0), P_1 = (0 : \omega : 1), P_2 = (0 : \omega^2 : 1), P_3 = (1 : 0 : 1), \\ P_4 = (1 : 1 : 1), P_5 = (\omega : 0 : 1), P_6 = (\omega : 1 : 1), P_7 = (\omega^2 : 0 : 1), P_8 = (\omega^2 : 1 : 1).$$

Now, we represent  $\mathbb{F}_{256}$  as  $\mathbb{F}_4[x]/\mathcal{Q}(x)$  with primitive root  $\alpha$ , where  $\mathcal{Q}(x) = x^4 + x^3 + \omega x^2 + \omega x + \omega$ .

- For the place  $Q$  of degree 4, the authors considered  $Q = \sum_{i=1}^4 \mathfrak{p}_i$  where  $\mathfrak{p}_1$  corresponds to the  $\mathbb{F}_{4^4}$ -rational point with projective coordinates  $(\alpha^{16} : \alpha^{17^4} : 1)$  and  $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$  are its conjugates under the Frobenius map. We see that  $\alpha^{16}$  is a root of the irreducible polynomial  $\mathcal{Q}(x) = x^4 + x^3 + \omega x^2 + \omega x + \omega$ . Thus, the place  $Q$  is a place lying over the place  $(\mathcal{Q}(x))$  of  $\mathbb{F}_4(x)/\mathbb{F}_4$ . Note also that the place  $(\mathcal{Q}(x))$  of  $\mathbb{F}_4(x)/\mathbb{F}_4$  is totally splitted in the algebraic function field  $F/\mathbb{F}_4$ , which means that there exist two places of degree  $n$  in  $F/\mathbb{F}_4$  lying over the place  $(\mathcal{Q}(x))$  of  $\mathbb{F}_4(x)/\mathbb{F}_4$ , since the function field  $F/\mathbb{F}_q$  is an extension of degree 2 of the rational function field  $\mathbb{F}_4(x)/\mathbb{F}_q$ . The place  $Q$  is one of the two places in  $F/\mathbb{F}_4$  lying over the place  $(\mathcal{Q}(x))$ . Notice that the second place is given by the orbit of the conjugated point  $(\alpha^{16} : \alpha^{17^4} + 1 : 1)$ . Therefore, we can represent  $\mathbb{F}_{256} = \mathbb{F}_{4^4} = \mathbb{F}_4[x]/\mathcal{Q}(x)$  as the residue class field  $F_Q$  of the place  $Q$  in  $F/\mathbb{F}_4$ .
- For the divisor  $D$ , we choose the place described as  $\sum_{i=1}^4 \mathfrak{d}_i$  where  $\mathfrak{d}_1$  corresponds to the  $\mathbb{F}_{4^4}$ -rational point  $(\alpha^{17} : \alpha^{14} : 1)$  and  $\mathfrak{d}_2, \mathfrak{d}_3, \mathfrak{d}_4$  are its conjugates under the Frobenius map. By computation we see that  $\alpha^{17}$  is a root of irreducible polynomial  $\mathcal{D}(x) = x^2 + x + \omega$  and  $\deg D = 4$  because  $\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3, \mathfrak{d}_4$  are all distinct. Therefore,  $D$  is the only place in  $F/\mathbb{F}_4$  lying over the place  $(\mathcal{D}(x))$  of  $\mathbb{F}_4(x)$  since the residue class field  $F_D$  of the place  $D$  is a quadratic extension of the residue class field  $F_{\mathcal{D}}$  of the place  $\mathcal{D}$ , which is an inert place of  $\mathbb{F}_4(x)$  in  $F/\mathbb{F}_4$ .

The matrix  $T_{2D}$  obtained in the basis of Riemann-Roch space  $L(2D)$ :  
 $\mathcal{B}_{2D} = \{f_1 = 1/f, f_2 = x/f, f_3 = y/f, f_4 = x^2/f, f_5 = 1/f^2, f_6 = xy/f^2, f_7 =$

$y/f^2, f_8 = x/f^2\}$ , with  $f = x^2 + x + \omega$  is the following:

$$T_{2D} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \omega^2 & 0 & 1 & 0 & \omega & 0 & \omega^2 & 0 \\ \omega^2 & 0 & \omega & 0 & \omega & 0 & 1 & 0 \\ \omega^2 & \omega^2 & 0 & \omega^2 & \omega & 0 & 0 & \omega \\ \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega & \omega \\ \omega & \omega^2 & 0 & 1 & \omega^2 & 0 & 0 & 1 \\ \omega & \omega^2 & \omega & 1 & \omega^2 & 1 & \omega^2 & 1 \\ \omega & 1 & 0 & \omega^2 & \omega^2 & 0 & 0 & \omega \end{pmatrix}.$$

Then, computation gives:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & \omega & 0 & \omega^2 & \omega \\ 0 & 1 & 0 & 0 & 0 & \omega^2 & \omega & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & \omega & 0 & \omega \end{pmatrix}$$

and

$$CT_{2D}^{-1} = \begin{pmatrix} 1 & \omega & 1 & \omega & 1 & 1 & \omega & 0 \\ 1 & 0 & \omega^2 & \omega & 1 & \omega^2 & 1 & \omega \\ 1 & \omega & \omega & \omega^2 & 1 & \omega^2 & \omega & \omega \\ 0 & \omega & \omega^2 & \omega & 1 & \omega^2 & 0 & 0 \end{pmatrix}.$$

Consequently, we obtain:

$$N_z(T_D) = 10, \quad N_z(CT_{2D}^{-1}) = 5.$$

and

$$N_1(T_D) = 5, \quad N_1(CT_{2D}^{-1}) = 10.$$

Thus, we have the following quantities:  $\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = 71$  by Formula (21),  $\mu_{s,1}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = 76$  by Formula (22) and finally  $\mu_s(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = 51$  by Formula (12).

### 3.2.2 New designs of the Baum-Shokrollahi Construction (BSC)

In this section, we follow the approach described previously and we improve the Chudnovsky<sup>2</sup> multiplication algorithm in  $\mathbb{F}_{4^4}$  constructed by Baum and Shokrollahi in [6]. By using the same elliptic curve and the same set  $\{D, Q, \mathcal{P}\}$  (up to a permutation of the set  $\mathcal{P}$  since it has no influence on scalar resp. bilinear complexity by Section 3.1.2), we obtain an algorithm with the same bilinear complexity and lower scalar complexity. The new construction of CCMA for the multiplication in  $\mathbb{F}_{256}/\mathbb{F}_4$  is based upon complexity analysis in Section 2.2 and the strategies highlighted in Section 3.1.1.

#### a) Optimization with Algorithm 4

By using Algorithm 3 (taking into account uniquely the optimization of the number of zeros) applied on the same set  $\{F/\mathbb{F}_q, D, Q, \mathcal{P}\}$  used in Section 3.2.1 (up to a permutation of the set  $\mathcal{P}$ ), we obtain the following basis

$$\mathcal{B}_{2D}^{opt} = \mathcal{B}_{D,max} \cup \mathcal{B}_D^c$$

of  $\mathcal{L}(2D)$ , where  $\mathcal{B}_{D,max} = \{f_1, f_2, f_3, f_4\}$  and  $\mathcal{B}_D^c = \{f_5, f_6, f_7, f_8\}$  with:

$$\begin{aligned} f_1 &= (\omega x^2 + x)/(x^2 + x + \omega), \\ f_2 &= (\omega^2 x^2 + \omega^2 x + \omega^2)/(x^2 + x + \omega), \\ f_3 &= \omega^2 y/(x^2 + x + \omega) + (\omega^2 x + 1)/(x^2 + x + \omega), \\ f_4 &= \omega^2 y/(x^2 + x + \omega) + (\omega^2 x + \omega)/(x^2 + x + \omega), \\ f_5 &= (x^2 + x)y/(x^4 + x^2 + \omega^2) + (x^4 + \omega x^3 + \omega x^2 + \omega x)/(x^4 + x^2 + \omega^2), \\ f_6 &= \omega^2 xy/(x^4 + x^2 + \omega^2) + (\omega x^4 + x^2 + \omega x + 1)/(x^4 + x^2 + \omega^2), \\ f_7 &= (\omega^2 x + 1)y/(x^4 + x^2 + \omega^2) + (\omega^2 x^4 + \omega^2 x^3 + \omega x^2 + \omega)/(x^4 + x^2 + \omega^2), \\ f_8 &= (x^2 + \omega x + 1)y/(x^4 + x^2 + \omega^2) + (x^4 + \omega x^3 + x^2 + \omega^2 x + \omega^2)/(x^4 + x^2 + \omega^2). \end{aligned}$$

In this basis, we obtained the matrice  $T_{2D}$  of the second evaluation map  $Ev_{\mathcal{P}}$ , where  $\mathcal{P} := \{P_{\infty}, P_1, P_2, P_7, P_8, P_3, P_4, P_5\}$  is the ordered set of rational places used in CCMA:

$$T_{2D} = \begin{pmatrix} \omega & \omega^2 & 0 & 0 & 1 & \omega & \omega^2 & 1 \\ 0 & \omega & 0 & \omega & 0 & \omega & 0 & \omega \\ 0 & \omega & \omega & 0 & 0 & \omega & \omega & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & \omega^2 & \omega^2 \\ 1 & 0 & 1 & 0 & \omega & \omega & \omega^2 & 0 \\ 0 & 0 & 1 & 0 & \omega & \omega & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & \omega^2 & \omega & 0 \\ \omega & \omega & 1 & \omega^2 & 1 & 0 & 0 & \omega^2 \end{pmatrix}$$

and

$$T_{2D,4}^{-1} = \begin{pmatrix} 0 & \omega & 1 & 0 & 0 & 1 & 1 & \omega^2 \\ 0 & 0 & 0 & 0 & 1 & \omega & \omega & \omega^2 \\ \omega^2 & \omega & \omega^2 & \omega^2 & \omega & \omega & 0 & 0 \\ 1 & \omega^2 & \omega & \omega^2 & 0 & 0 & 1 & \omega^2 \end{pmatrix}.$$

Therefore,  $N_z(T_D) = 16$  and  $N_z(T_{2D,4}^{-1}) = 11$ . Note that without taking into account the optimization criterium mentioned in Remark 3.4, we have:  $N_1(T_D) = 7$  and  $N_1(T_{2D,4}^{-1}) = 6$ . So, we obtain  $\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = 53$  (a gain of 25% with respect to BSC). Finally, if we compute the other quantities, we obtain  $\mu_{s,1}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = 76$  (equality with BSC) and  $\mu_s(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = 33$  (a gain of 54,5% with respect to BSC).

## b) Optimization with Algorithm 5

By using Algorithm 5 (taking into account uniquely the optimization of the number of zeros) applied on the same set  $\{F/\mathbb{F}_q, D, Q, \mathcal{P}\}$  used in Section 3.2.1 (up to a permutation of the set  $\mathcal{P}$ ), we obtain the following basis

$$\mathcal{B}_{2D}^{opt} = \mathcal{B}_{D,max} \cup \mathcal{B}_D^c$$

of  $\mathcal{L}(2D)$ , where  $\mathcal{B}_{D,max} = \{f_1, f_2, f_3, f_4\}$  and  $\mathcal{B}_D^c = \{f_5, f_6, f_7, f_8\}$  with:

$$\begin{aligned} f_1 &= (y + \omega x + \omega^2)/(x^2 + x + \omega), \\ f_2 &= (y + \omega^2 x + \omega)/(x^2 + x + \omega), \\ f_3 &= (\omega x^2 + \omega^2 x)/(x^2 + x + \omega), \\ f_4 &= (\omega y)/(x^2 + x + \omega), \\ f_5 &= (\omega x^2 + \omega x)y + \omega^2 x^4 + \omega x^3 + x^2 + x + \omega)/(x^4 + x^2 + \omega^2), \\ f_6 &= (\omega^2 x^2 y + \omega x^4 + \omega x^3 + x^2 + \omega x)/(x^4 + x^2 + \omega^2), \\ f_7 &= (x^2 + \omega^2 x)y + \omega x^4 + \omega x^2)/(x^4 + x^2 + \omega^2), \\ f_8 &= (\omega x + \omega)y + \omega x^4)/(x^4 + x^2 + \omega^2). \end{aligned}$$

In this basis, we obtained the matrix  $T_{2D}$  of the second evaluation map  $Ev_{\mathcal{P}}$ , where  $\mathcal{P} := \{P_\infty, P_1, P_2, P_7, P_8, P_3, P_4, P_5\}$  is the ordered set of rational places used in CCMA:

$$T_{2D} = \begin{pmatrix} 0 & 0 & \omega & 0 & \omega^2 & \omega & \omega & \omega \\ \omega^2 & 0 & 0 & \omega & \omega^2 & 0 & 0 & 1 \\ 0 & \omega^2 & 0 & \omega^2 & \omega^2 & 0 & 0 & \omega \\ \omega^2 & \omega^2 & \omega^2 & 0 & 1 & 1 & 0 & \omega^2 \\ 0 & 0 & \omega^2 & 1 & 1 & 0 & \omega^2 & \omega^2 \\ 0 & 1 & 0 & 0 & 0 & \omega^2 & 1 & \omega \\ \omega & \omega^2 & 0 & \omega^2 & 1 & \omega & 0 & 1 \\ \omega^2 & 0 & \omega & 0 & \omega & 0 & 1 & \omega^2 \end{pmatrix}$$

and

$$T_{2D,4}^{-1} = \begin{pmatrix} 1 & 0 & 0 & \omega^2 & \omega & 0 & \omega^2 & \omega^2 \\ 1 & 1 & \omega^2 & 0 & 0 & \omega^2 & 0 & 1 \\ 0 & 1 & \omega & 1 & \omega^2 & \omega & 0 & 0 \\ \omega^2 & \omega & \omega^2 & 0 & \omega & 0 & \omega^2 & 0 \end{pmatrix}.$$

Therefore,  $N_z(T_D) = 16$  and  $N_z(T_{2D,4}^{-1}) = 12$ . Note that without taking into account the optimization criterium mentioned in Remark 3.4, we have:  $N_1(T_D) = 2$  and  $N_1(T_{2D,4}^{-1}) = 6$ . So, we obtain  $\mu_{s,0}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = 52$  (a gain of 27% over BSC). Note also that we improve the result obtained in [4] (+2%). Finally, if we compute the other quantities, we obtain  $\mu_{s,1}(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = 86$  (a loss of 13% with respect to BSC) and  $\mu_s(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}) = 42$  (a gain of 21,5% with respect to BSC).



**Remark 3.6.** *Regarding the total scalar complexity, we notice that a worse result is obtained using Algorithm 5 than using Algorithm 4. However, this is not significant because we did not take into account the optimization criterion for the number of 1, wishing to focus on the optimization of the number of zeros. It is therefore likely to obtain even better constructions, by using the criteria mentioned in Remark 3.3.*

## References

- [1] Kevin Atighehchi, Stéphane Ballet, Alexis Bonnetcaze, and Robert Rolland. Arithmetic in Finite Fields based on Chudnovsky’s multiplication algorithm. *Mathematics of Computation*, 86(308):2977–3000, 2017.
- [2] 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.
- [3] Stéphane Ballet. Quasi-optimal Algorithms for Multiplication in the Extensions of  $\mathbb{F}_{16}$  of degree 13, 14, and 15. *Journal of Pure and Applied Algebra*, 171:149–164, 2002.
- [4] Stéphane Ballet, Alexis Bonnetcaze, and Thanh-Hung Dang. On the scalar complexity of chudnovsky<sup>2</sup> multiplication algorithm in finite fields. In *CAI’19*, volume 11545 of *Lecture Notes in Computer Science*, pages 64–75. Springer, 2019.
- [5] Stéphane Ballet, Jean Chaumine, Julia Pieltant, Matthieu Rambaud, Hugues Randriambololona, and Robert Rolland. On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry. *Uspekhi Matematicheskikh Nauk (Russian Mathematical Surveys)*, to appear.
- [6] Ulrich Baum and Amin Shokrollahi. An optimal algorithm for multiplication in  $\mathbb{F}_{256}/\mathbb{F}_4$ . *Applicable Algebra in Engineering, Communication and Computing*, 2(1):15–20, 1991.
- [7] Jean Chaumine. On the bilinear complexity of multiplication in small finite fields. *Comptes Rendus de l’Académie des Sciences, Série I*, 343:265–266, 2006.
- [8] David Chudnovsky and Gregory Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4:285–316, 1988.
- [9] 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.

- [10] Julia Pielant. *Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis*. PhD thesis, Université d'Aix-Marseille, Institut de Mathématiques de Luminy, 2012.
- [11] Amin Shokhrollahi. Optimal algorithms for multiplication in certain finite fields using algebraic curves. *SIAM Journal on Computing*, 21(6):1193–1198, 1992.
- [12] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Number 254 in Graduate Texts in Mathematics. Springer-Verlag, second edition, 2008.
- [13] Shmuel Winograd. On Multiplication in Algebraic Extension Fields. *Theoretical Computer Science*, 8:359–377, 1979.