arXiv:1601.00126v1 [cs.IT] 2 Jan 2016

On some bounds for symmetric tensor rank of multiplication in finite fields

Stéphane Ballet[2]

Aix-Marseille Université, CNRS, Centrale Marseille, Institut de Mathématiques de Marseille
Case 907, 163 Avenue de Luminy, F-13288 Marseille Cedex 9, France.

Julia Pieltant[1,3]

CNRS LTCI, Télécom ParisTech
46 rue Barrault, F-75634 Paris Cedex 13, France.

Matthieu Rambaud

CNRS LTCI, Télécom ParisTech
46 rue Barrault, F-75634 Paris Cedex 13, France.

Abstract

We establish new upper bounds about symmetric bilinear complexity in any extension of finite fields. Note that these bounds are not asymptotical but uniform. Moreover, we discuss the validity of certain published bounds.

Keywords: Finite field, tensor rank of the multiplication, algebraic function field.

1. Introduction

1.1. Tensor rank and symmetric tensor rank

Let q be a prime power, $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_{q^n}$ be the degree n extension of $\mathbb{F}_q$. The multiplication of two elements of $\mathbb{F}_{q^n}$ is a $\mathbb{F}_q$-bilinear application from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ onto $\mathbb{F}_{q^n}$. Then it can be considered as an $\mathbb{F}_q$-linear application from the tensor product $\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ onto $\mathbb{F}_{q^n}$. Consequently it can be

Email addresses: `stephane.ballet@univ-amu.fr` (Stéphane Ballet), `pieltant@enst.fr` (Julia Pieltant), `rambaud@enst.fr` (Matthieu Rambaud)

URL: `http://iml.univ-mrs.fr/~ballet` (Stéphane Ballet), `http://www.lix.polytechnique.fr/~pieltant` (Julia Pieltant)

[1] Corresponding author

[2] The author wishes to thank the INFRES departement for funding his venue at LTCI where this work was partly done.

[3] This work was supported by a public grant as part of the *Investissement d'avenir* project, reference ANR-11-LABX-0056-LMH, LabEx LMH.

January 5, 2016

also considered as an element T of $(\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n})^\star \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$, namely an element of $\mathbb{F}^\star_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}^\star_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$. More precisely, when T is written

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

where the r elements $x_i^\star$ and the r elements $y_i^\star$ are in the dual $\mathbb{F}^\star_{q^n}$ of $\mathbb{F}_{q^n}$ and the r elements c_i are in $\mathbb{F}_{q^n}$, the following holds for any $x, y \in \mathbb{F}_{q^n}$:

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

The decomposition (1) is not unique and neither is the length of these decompositions, thus we set:

Definition 1. *The minimal number of summands in a decomposition of the tensor T of the multiplication is called the bilinear complexity of the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and is denoted by $\mu_q(n)$:*

$$\mu_q(n) = \min \left\{ r \;\middle|\; T = \sum_{i=1}^{r} x_i^\star \otimes y_i^\star \otimes c_i \right\}.$$

Hence the bilinear complexity of the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is nothing else than the rank of the tensor T. Among others, a special case of decompositions for T is of particular interest, namely the symmetric decompositions:

$$T = \sum_{i=1}^{r} x_i^\star \otimes x_i^\star \otimes c_i. \tag{2}$$

Definition 2. *The minimal number of summands in a symmetric decomposition of the tensor T of the multiplication is called the symmetric bilinear complexity of the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and is denoted by $\mu_q^{\mathrm{sym}}(n)$:*

$$\mu_q^{\mathrm{sym}}(n) = \min \left\{ r \;\middle|\; T = \sum_{i=1}^{r} x_i^\star \otimes x_i^\star \otimes c_i \right\}.$$

One easily gets that $\mu_q(n) \leq \mu_q^{\mathrm{sym}}(n)$. Some cases where $\mu_q(n) = \mu_q^{\mathrm{sym}}(n)$ are known but to the best of our knowledge, no example where $\mu_q(n) < \mu_q^{\mathrm{sym}}(n)$ has already been exhibited. However, better upper bounds have been established in the asymmetric case [20, 19] and this may suggest that in general the asymmetric bilinear complexity of the multiplication and the symmetric one are distinct. In any case, at the moment, we must consider separately these two quantities.

Remark that from an algorithmic point on view as well as for some specific applications, a symmetric bilinear algorithm can be more interesting than an asymmetric one, unless if *a priori*, the constant factor in the bilinear complexity estimation is a little worse. Moreover, many other research domains are closely related to the determination of symmetric bilinear multiplication algorithms such as, amoung others, arithmetic secret sharing and multiparty computation (see [9, 12])...

1.2. Known results

The bilinear complexity $\mu_q(n)$ of the multiplication in the n-degree extension of a finite field $\mathbb{F}_q$ is known for certain values of n. In particular, S. Winograd [25] and H. de Groote [15] have shown that this complexity is $\geq 2n-1$, with equality holding if and only if $n \leq \frac{1}{2}q+1$. Using the principle of the D.V. and G.V. Chudnovsky algorithm [13] applied to elliptic curves, M.A. Shokrollahi has shown in [21] that the symmetric bilinear complexity of multiplication is equal to $2n$ for $\frac{1}{2}q+1 < n < \frac{1}{2}(q+1+\epsilon(q))$ where ϵ is the function defined by:

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

Later in [2, 3, 6, 8, 5, 4], the study made by M.A. Shokrollahi has been generalized to algebraic function fields of genus g.

Let us recall that the original algorithm of D.V. and G.V. Chudnovsky introduced in [13] is symmetric by definition and leads to the following theorem obtained in [2]:

Theorem 3. *Let q be a power of a prime p. The symmetric tensor rank $\mu_q^{\mathrm{sym}}(n)$ of multiplication in any finite field $\mathbb{F}_{q^n}$ is linear with respect to the extension degree; more precisely, there exists a constant C_q such that:*

$$\mu_q^{\mathrm{sym}}(n) \leq C_q n.$$

General forms for C_q have been established such as the following best current known estimates:

$$C_q = \begin{cases} \text{if } q=2, & \text{then} \quad \frac{4824}{247} \simeq 19,6 & \text{[7] and [11]} \\ \text{else if } q=3, & \text{then} \quad 27 & \text{[2]} \\ \text{else if } q=p \geq 5, & \text{then} \quad 3\left(1+\frac{4}{q-3}\right) & \text{[4]} \\ \text{else if } q=p^2 \geq 25, & \text{then} \quad 2\left(1+\frac{2}{p-3}\right) & \text{[4]} \\ \text{else if } q \geq 4, & \text{then} \quad 6\left(1+\frac{p}{q-3}\right) & \text{[3]} \end{cases}$$

Now we introduce the generalized Chudnovsky-Chudnovsky type algorithm described in [11]; the original algorithm given in [13] by D.V. and G.V. Chudnovsky being the case where $\deg P_i = 1$ and $u_i = 1$ for $i = 1, \ldots, N$. Here a wider notion of complexity is involved: the quantity $\mu_q^{\mathrm{sym}}(m, \ell)$, which corresponds to the symmetric bilinear complexity of the multiplication over $\mathbb{F}_q$ in $\mathbb{F}_{q^m}[X]/(X^\ell)$, the $\mathbb{F}_q$-algebra of polynomials in one indeterminate with coefficients in $\mathbb{F}_{q^m}$ truncated at order ℓ.

Theorem 1.1. *Let*

- *q be a prime power,*
- *$\mathbf{F}/\mathbb{F}_q$ be an algebraic function field,*
- *Q be a degree n place of $F/\mathbb{F}_q$,*
- *$\mathcal{D}$ be a divisor of $F/\mathbb{F}_q$,*
- *$\mathcal{P} = \{P_1, \ldots, P_N\}$ be a set of N places of arbitrary degree,*
- *$u_1, \ldots, u_N$ be positive integers.*

We suppose that Q and all the places in $\mathcal{P}$ are not in the support of $\mathcal{D}$ and that:

a) the map

$$Ev_Q : \left| \begin{array}{ccc} \mathcal{L}(\mathcal{D}) & \rightarrow & \mathbb{F}_{q^n} \simeq F_Q \\ f & \longmapsto & f(Q) \end{array} \right.$$

is onto,

b) the map

$$Ev_{\mathcal{P}} : \left| \begin{array}{ccc} \mathcal{L}(2\mathcal{D}) & \longrightarrow & \left(\mathbb{F}_{q^{\deg P_1}}\right)^{u_1} \times \left(\mathbb{F}_{q^{\deg P_2}}\right)^{u_2} \times \cdots \times \left(\mathbb{F}_{q^{\deg P_N}}\right)^{u_N} \\ f & \longmapsto & (\varphi_1(f), \varphi_2(f), \ldots, \varphi_N(f)) \end{array} \right.$$

is injective, where the application φ_i is defined by

$$\varphi_i : \left| \begin{array}{ccc} \mathcal{L}(2\mathcal{D}) & \longrightarrow & \left(\mathbb{F}_{q^{\deg P_i}}\right)^{u_i} \\ f & \longmapsto & \left(f(P_i), f'(P_i), \ldots, f^{(u_i-1)}(P_i)\right) \end{array} \right.$$

with $f = f(P_i) + f'(P_i)t_i + f''(P_i)t_i^2 + \ldots + f^{(k)}(P_i)t_i^k + \ldots$, the local expansion at P_i of f in $\mathcal{L}(2\mathcal{D})$, with respect to the local parameter t_i. Note that we set $f^{(0)} = f$.

Then

$$\mu_q^{\mathrm{sym}}(n) \leq \sum_{i=1}^{N} \mu_q^{\mathrm{sym}}(\deg P_i)\mu_{q^{\deg P_i}}^{\mathrm{sym}}(\deg P_i, u_i).$$

The following special case of this result has been introduced independently by N. Arnaud in [1], and can be seen as a corollary of Theorem 1.1 by gathering the places used with the same multiplicity; namely one has to set for $j = 1$ and 2, $\ell_j := |\{i \mid \deg P_i = j \text{ and } u_i = 2\}|$.

Corollary 1.2. *Let*

- *q be a prime power,*
- *$F/\mathbb{F}_q$ be an algebraic function field,*
- *Q be a degree n place of $F/\mathbb{F}_q$,*

- *$\mathscr{D}$ be a divisor of $F/\mathbb{F}_q$,*
- *$\mathscr{P} = \{P_1, \ldots, P_{N_1}, P_{N_1+1}, \ldots, P_{N_1+N_2}\}$ be a set of N_1 places of degree one and N_2 places of degree two,*
- *$0 \leq \ell_1 \leq N_1$ and $0 \leq \ell_2 \leq N_2$ be two integers.*

We suppose that Q and all the places in $\mathscr{P}$ are not in the support of $\mathscr{D}$ and that:

a) the map

$$Ev_Q : \mathscr{L}(\mathscr{D}) \rightarrow \mathbb{F}_{q^n} \simeq F_Q$$

is onto,

b) the map

$$Ev_{\mathscr{P}} : \left| \begin{array}{ccl} \mathscr{L}(2\mathscr{D}) & \rightarrow & \mathbb{F}_q^{N_1} \times \mathbb{F}_q^{\ell_1} \times \mathbb{F}_{q^2}^{N_2} \times \mathbb{F}_{q^2}^{\ell_2} \\ f & \mapsto & \big(f(P_1), \ldots, f(P_{N_1}), f'(P_1), \ldots, f'(P_{\ell_1}), \\ & & f(P_{N_1+1}), \ldots, f(P_{N_1+N_2}), f'(P_{N_1+1}), \ldots, f'(P_{N_1+\ell_2})\big) \end{array} \right.$$

is injective.

Then

$$\mu_q^{\mathrm{sym}}(n) \leq N_1 + 2\ell_1 + 3N_2 + 6\ell_2.$$

From the results of [2, Corollary 2.1] and [8, Theorems 2.3 and 2.3] and the algorithm of Corollary 1.2 with $\ell_1 = \ell_2 = 0$, we obtain:

Theorem 1.3. *Let q be a prime power and let n be an integer > 1. Let $F/\mathbb{F}_q$ be an algebraic function field of genus g and N_k the number of places of degree k in $F/\mathbb{F}_q$. If $F/\mathbb{F}_q$ is such that $2g + 1 \leq q^{\frac{n-1}{2}}(q^{\frac{1}{2}} - 1)$ then:*

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

$$\mu_q^{\mathrm{sym}}(n) \leq 2n + g - 1,$$

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

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + 3g,$$

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

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + 6g.$$

To conclude, we recall some particular exact values for $\mu_q^{\mathrm{sym}}(n)$ wich will be useful for computational use: $\mu_q(2) = \mu_q^{\mathrm{sym}}(2) = 3$ for any prime power q, $\mu_2^{\mathrm{sym}}(4) = 9$, $\mu_4^{\mathrm{sym}}(4) = \mu_5^{\mathrm{sym}}(4) = 8$ and $\mu_2^{\mathrm{sym}}(6) = 15$ [13].

1.3. New results

In this paper, we prove new uniform bounds for the symmetric bilinear complexity, namely the following ones:

Theorem 1.4. *Let $q = p^r$ be a power of the prime p. Then:*

(i) If $q \geq 4$, then $\mu^{\mathrm{sym}}_{q^2}(n) \leq 2\left(1+\frac{p}{q-3+(p-1)\left(1-\frac{1}{q+1}\right)}\right)n.$

(ii) If $q \geq 4$, then $\mu^{\mathrm{sym}}_{q}(n) \leq 3\left(1+\frac{p}{q-3+(p-1)\left(1-\frac{1}{q+1}\right)}\right)n.$

(iii) If $p \geq 5$, then $\mu^{\mathrm{sym}}_{p^2}(n) \leq 2\left(1+\frac{2}{p-\frac{33}{16}}\right)n.$

(iv) If $p \geq 5$, then $\mu^{\mathrm{sym}}_{p}(n) \leq 3\left(1+\frac{2}{p-\frac{33}{16}}\right)n.$

Remark. Even if Bound (i) was established by Arnaud in [1] it has never been published in any journal, and the proof that is given in this paper is more complete than the one that can be found in [1]. Moreover, Bound (ii) is an amelioration of [1, Theorem 5.9] since it holds for $q \geq 4$ whereas Arnaud's bound in [1, Theorem 5.9] holds for $q \geq 16$. Furthermore, Arnaud also gave bounds which are similar to Bounds (iii) and (iv) in [1, Theorems 5.13 and 5.12] with respectively $p-2$ and $p-1$ as denominators. Unfortunatly, these denominators are slightly overestimated under Arnaud's hypotheses and no calculation is given to prove these bounds. Thus we will give a corrected version of these bounds with detailed proofs.

In the last part of this paper, we discuss the validity of certain published bounds and explain why some of them should not be considered as proven.

2. New upper bounds for the symmetric bilinear complexity

2.1. Towers of algebraic function fields

In this section, we introduce some towers of algebraic function fields. Theorem 1.3 applied on the algebraic function fields of these towers gives us bounds for the bilinear complexity. A given curve cannot permit to multiply in every extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, but only for n lower than some value. With a tower of function fields, we can adapt the curve to the degree of the extension. The important point to note here is that in order to obtain a well adapted curve it will be desirable to have a tower for which the quotients of two consecutive genus are as small as possible, namely a dense tower.

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

2.1.1. Garcia-Stichtenoth tower of Artin-Schreier function field extensions

We present now a modified Garcia-Stichtenoth tower (cf. [17, 3, 8]) having good properties. Let us consider a finite field $\mathbb{F}_{q^2}$ with $q = p^r > 3$ and let T_1 be the Garcia-Stichtenoth elementary abelian tower over $\mathbb{F}_{q^2}$ constructed in [17] and defined by the sequence $(F_1, F_2, \ldots)$ where

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

and z_{k+1} satisfies the equation:

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

with

$$x_k := z_k/x_{k-1} \text{ in } F_k \text{ (for } k \geq 2).$$

Moreover $F_1 := \mathbb{F}_{q^2}(x_1)$ is the rational function field over $\mathbb{F}_{q^2}$ and F_2 the Hermitian function field over $\mathbb{F}_{q^2}$. Let us denote by g_k the genus of F_k, we recall the following *formulae*:

$$g_k = \begin{cases} q^k + q^{k-1} - q^{\frac{k+1}{2}} - 2q^{\frac{k-1}{2}} + 1 & \text{if } k \equiv 1 \mod 2, \\ q^k + q^{k-1} - \frac{1}{2}q^{\frac{k}{2}+1} - \frac{3}{2}q^{\frac{k}{2}} - q^{\frac{k}{2}-1} + 1 & \text{if } k \equiv 0 \mod 2. \end{cases} \tag{3}$$

Let us consider the completed Garcia-Stichtenoth tower

$$T_2 = F_{1,0} \subseteq F_{1,1} \subseteq \cdots \subseteq F_{1,r} = F_{2,0} \subseteq F_{2,1} \subseteq \cdots \subseteq F_{2,r} \subseteq \cdots$$

considered in [3] such that $F_k \subseteq F_{k,s} \subseteq F_{k+1}$ for any integer $s \in \{0, \ldots, r\}$, where $F_{k,0} = F_k$ and $F_{k,r} = F_{k+1}$. Recall that each extension $F_{k,s}/F_k$ is Galois of degree p^s with full constant field $\mathbb{F}_{q^2}$. Now, we consider the tower studied in [8]:

$$T_3 = G_{1,0} \subseteq G_{1,1} \subseteq \cdots \subseteq G_{1,r} = G_{2,0} \subseteq G_{2,1} \subseteq \cdots \subseteq G_{2,r} \subseteq \cdots$$

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

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

namely $\mathbf{F}_{k,s}/\mathbb{F}_{q^2}$ is the constant field extension of $G_{k,s}/\mathbb{F}_q$. Note that the tower T_3 is well defined by [8] and [6]. Moreover, we have the following result:

Proposition 2.1. *Let $q = p^r \geq 4$ be a prime power. For all integers $k \geq 1$ and $s \in \{0, \ldots, r\}$, there exists a step $F_{k,s}/\mathbb{F}_{q^2}$ (respectively $G_{k,s}/\mathbb{F}_q$) with genus $g_{k,s}$ and $N_{k,s}$ rational places in $F_{k,s}/\mathbb{F}_{q^2}$ (respectively $N_{k,s} = N_1(G_{k,s}/\mathbb{F}_q) + 2N_2(G_{k,s}/\mathbb{F}_q)$) such that:*

(1) $F_k \subseteq F_{k,s} \subseteq F_{k+1}$*, where we set* $F_{k,0} = F_k$ *and* $F_{k,r} = F_{k+1}$*,*
(respectively $G_k \subseteq G_{k,s} \subseteq G_{k+1}$*, where we set* $G_{k,0} = G_k$ *and* $G_{k,r} = G_{k+1}$*),*

(2) $\left(g_k - 1\right)p^s + 1 \leq g_{k,s} \leq \frac{g_{k+1}}{p^{r-s}} + 1$*,*

(3) $N_{k,s} \geq (q^2 - 1)q^{k-1}p^s$*.*

2.1.2. Garcia-Stichtenoth tower of Kummer function field extensions

In this section, we present a Garcia-Stichtenoth tower (cf. [4]) having good properties. Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$. Let us consider the tower T over $\mathbb{F}_q$ which is defined recursively by the following equation, studied in [18]:

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

The tower $T/\mathbb{F}_q$ is represented by the sequence of function fields $(H_0, H_1, H_2, \ldots)$ where $H_n = \mathbb{F}_q(x_0, x_1, \ldots, x_n)$ and $x_{i+1}^2 = (x_i^2 + 1)/2x_i$ holds for each $i \geq 0$. Note that H_0 is the rational function field. For any prime number $p \geq 3$, the tower $T/\mathbb{F}_{p^2}$ is asymptotically optimal over the field $\mathbb{F}_{p^2}$, i.e. $T/\mathbb{F}_{p^2}$ reaches the Drinfeld-Vladut bound. Moreover, for any integer k, $H_k/\mathbb{F}_{p^2}$ is the constant field extension of $H_k/\mathbb{F}_p$.

From [4], we know that the genus $g(H_k)$ of the step H_k is given by:

$$g(H_k) = \begin{cases} 2^{k+1} - 3 \cdot 2^{\frac{k}{2}} + 1 & \text{if } k \equiv 0 \mod 2, \\ 2^{k+1} - 2 \cdot 2^{\frac{k+1}{2}} + 1 & \text{if } k \equiv 1 \mod 2. \end{cases} \tag{4}$$

and that the following bounds hold for the number of rational places in H_k over $\mathbb{F}_{p^2}$ and for the number of places of degree 1 and 2 over $\mathbb{F}_p$:

$$N_1(H_k/\mathbb{F}_{p^2}) \geq 2^{k+1}(p-1) \tag{5}$$

and

$$N_1(H_k/\mathbb{F}_p) + 2N_2(H_k/\mathbb{F}_p) \geq 2^{k+1}(p-1). \tag{6}$$

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

Proposition 2.2. *Let* $p \geq 5$ *be a prime number. Then for any integer* $n \geq \frac{1}{2}(p + 1 + \epsilon(p))$ *where* $\epsilon(p)$ *is defined as in Theorem* **??***:*

1) there exists an algebraic function field $H_k/\mathbb{F}_{p^2}$ *of genus* $g(H_k/\mathbb{F}_{p^2})$ *such that*

$$2g(H_k/\mathbb{F}_{p^2}) + 1 \leq p^{n-1}(p-1)$$

and

$$\mathrm{B}_1(H_k/\mathbb{F}_{p^2}) > 2n + 2g(H_k/\mathbb{F}_{p^2}) - 2,$$

2) there exists an algebraic function field $H_k/\mathbb{F}_p$ *of genus* $g(H_k/\mathbb{F}_p)$ *containing a non-special divisor of degree* $g(H_k/\mathbb{F}_p) - 1$ *and such that*

$$2g(H_k/\mathbb{F}_p) + 1 \leq p^{\frac{n-1}{2}}(p^{\frac{1}{2}} - 1)$$

and

$$\mathrm{B}_1(H_k/\mathbb{F}_p) + 2\mathrm{B}_2(H_k/\mathbb{F}_p) > 2n + 2g(H_k/\mathbb{F}_p) - 2.$$

2.2. Some preliminary results

Here we establish some technical results about the genus and number of places of each step of the towers $T_2/\mathbb{F}_{q^2}$, $T_3/\mathbb{F}_q$, $T/\mathbb{F}_{p^2}$ and $T/\mathbb{F}_p$ defined in Section 2.1. These results will allow us to determine a suitable step of the tower to apply the algorithm on.

2.2.1. About the Garcia-Stichtenoth tower of Artin-Schreier extensions

In this section, $q := p^r$ is a power of the prime p.

Lemma 2.3. *Let $q > 3$. We have the following bounds for the genus of each step of the towers $T_2/\mathbb{F}_{q^2}$ and $T_3/\mathbb{F}_q$:*

i) $g_k > q^k$ *for all* $k \geq 4$*,*

ii) $g_k \leq q^{k-1}(q+1) - \sqrt{q}q^{\frac{k}{2}}$*,*

iii) $g_{k,s} \leq q^{k-1}(q+1)p^s$ *for all* $k \geq 0$ *and* $s = 0, \dots, r$*,*

iv) $g_{k,s} \leq \frac{q^k(q+1) - q^{\frac{k}{2}}(q-1)}{p^{r-s}}$ *for all* $k \geq 2$ *and* $s = 0, \dots, r$*.*

Proof. *i)* According to Formula (3), we know that if $k \equiv 1 \mod 2$, then

$$g_k = q^k + q^{k-1} - q^{\frac{k+1}{2}} - 2q^{\frac{k-1}{2}} + 1 = q^k + q^{\frac{k-1}{2}}(q^{\frac{k-1}{2}} - q - 2) + 1.$$

Since $q > 3$ and $k \geq 4$, we have $q^{\frac{k-1}{2}} - q - 2 > 0$, thus $g_k > q^k$.
Else if $k \equiv 0 \mod 2$, then

$$g_k = q^k + q^{k-1} - \frac{1}{2}q^{\frac{k}{2}+1} - \frac{3}{2}q^{\frac{k}{2}} - q^{\frac{k}{2}-1} + 1 = q^k + q^{\frac{k}{2}-1}(q^{\frac{k}{2}} - \frac{1}{2}q^2 - \frac{3}{2}q - 1) + 1.$$

Since $q > 3$ and $k \geq 4$, we have $q^{\frac{k}{2}} - \frac{1}{2}q^2 - \frac{3}{2}q - 1 > 0$, thus $g_k > q^k$.

ii) It follows from Formula (3) since for all $k \geq 1$ we have $2q^{\frac{k-1}{2}} \geq 1$ which works out for odd k cases and $\frac{3}{2}q^{\frac{k}{2}} + q^{\frac{k}{2}-1} \geq 1$ which works out for even k cases, since $\frac{1}{2}q \geq \sqrt{q}$.

iii) If $s = r$, then according to Formula (3), we have

$$g_{k,s} = g_{k+1} \leq q^{k+1} + q^k = q^{k-1}(q+1)p^s.$$

Else, $s < r$ and Proposition 2.1 says that $g_{k,s} \leq \frac{g_{k+1}}{p^{r-s}} + 1$. Moreover, since $q^{\frac{k+2}{2}} \geq q$ and $\frac{1}{2}q^{\frac{k+1}{2}+1} \geq q$, we obtain $g_{k+1} \leq q^{k+1} + q^k - q + 1$ from Formula (3). Thus, we get

$$\begin{aligned} g_{k,s} &\leq \frac{q^{k+1} + q^k - q + 1}{p^{r-s}} + 1 \\ &= q^{k-1}(q+1)p^s - p^s + p^{s-r} + 1 \\ &\leq q^{k-1}(q+1)p^s + p^{s-r} \\ &\leq q^{k-1}(q+1)p^s \text{ since } 0 \leq p^{s-r} < 1 \text{ and } g_{k,s} \in \mathbb{N}. \end{aligned}$$

iv) It follows from ii) since Proposition 2.1 gives $g_{k,s} \leq \frac{g_{k+1}}{p^{r-s}} + 1$, so $g_{k,s} \leq \frac{q^k(q+1)-\sqrt{q}q^{\frac{k+1}{2}}}{p^{r-s}} + 1$ which gives the result since $p^{r-s} \leq q^{\frac{k}{2}}$ for all $k \geq 2$. □

Lemma 2.4. *Let $q > 3$ and $k \geq 4$. We set $\Delta g_{k,s} := g_{k,s+1} - g_{k,s}, D_{k,s} := (p-1)p^s q^k$ and $M_{k,s} := N_1(F_{k,s}/\mathbb{F}_{q^2}) = N_1(G_{k,s}/\mathbb{F}_q) + 2N_2(G_{k,s}/\mathbb{F}_q)$. One has:*

(i) $\Delta g_{k,s} \geq D_{k,s}$,

(ii) $M_{k,s} \geq D_{k,s}$.

Proof. (i) From Hurwitz Genus Formula, one has $g_{k,s+1} - 1 \geq p(g_{k,s} - 1)$, so $g_{k,s+1} - g_{k,s} \geq (p-1)(g_{k,s} - 1)$. Applying s more times Hurwitz Genus Formula, we get $g_{k,s+1} - g_{k,s} \geq (p-1)p^s\big(g(G_k) - 1\big)$. Thus $g_{k,s+1} - g_{k,s} \geq (p-1)p^s q^k$, from Lemma 2.3 i) since $q > 3$ and $k \geq 4$.
(ii) According to Proposition 2.1, one has

$$\begin{aligned} M_{k,s} &\geq (q^2-1)q^{k-1}p^s \\ &= (q+1)(q-1)q^{k-1}p^s \\ &\geq (q-1)q^k p^s \\ &\geq (p-1)q^k p^s. \end{aligned}$$

□

Lemma 2.5. *Let $M_{k,s} := N_1(F_{k,s}/\mathbb{F}_{q^2}) = N_1(G_{k,s}/\mathbb{F}_q) + 2N_2(G_{k,s}/\mathbb{F}_q)$. For all $k \geq 1$ and $s = 0, \ldots, r$, we have*

$$\sup\left\{n \in \mathbb{N} \mid 2n \leq M_{k,s} - 2g_{k,s} + 1\right\} \geq \frac{1}{2}(q+1)q^{k-1}p^s(q-3).$$

Proof. From Proposition 2.1 and Lemma 2.3 iii), we get

$$\begin{aligned} M_{k,s} - 2g_{k,s} + 1 &\geq (q^2-1)q^{k-1}p^s - 2q^{k-1}(q+1)p^s + 1 \\ &= (q+1)q^{k-1}p^s\big((q-1)-2\big) + 1 \\ &\geq (q+1)q^{k-1}p^s(q-3) \end{aligned}$$

thus we have $\sup\left\{n \in \mathbb{N} \mid 2n \leq M_{k,s} - 2g_{k,s} + 1\right\} \geq \frac{1}{2}q^{k-1}p^s(q+1)(q-3)$. □

2.2.2. About the Garcia-Stichtenoth tower of Kummer extensions

In this section, p is an odd prime. We denote by g_k the genus of the step H_k and we fix $N_k := \mathrm{B}_1(H_k/\mathbb{F}_{p^2}) = \mathrm{B}_1(H_k/\mathbb{F}_p) + 2\mathrm{B}_2(H_k/\mathbb{F}_p)$. The following lemma is straightforward according to Formulae (4) and (6):

Lemma 2.6. *These two bounds hold for the genus of each step of the towers $T/\mathbb{F}_{p^2}$ and $T/\mathbb{F}_p$:*

i) $g_k \leq 2^{k+1} - 2 \cdot 2^{\frac{k+1}{2}} + 1$, *ii)* $g_k \leq 2^{k+1}$.

Lemma 2.7. *For all* $k \geq 0$*, we set* $\Delta g_k := g_{k+1} - g_k$*. Then one has* $N_k \geq \Delta g_k \geq 2^{k+1} - 2^{\frac{k+1}{2}}$*.*

Proof. If k is even then $\Delta g_k = 2^{k+1} - 2^{\frac{k}{2}}$, else $\Delta g_k = 2^{k+1} - 2^{\frac{k+1}{2}}$ so the second equality holds trivially. Moreover, since $p \geq 3$, the first one follows from Bounds (5) and (6) which gives $N_k \geq 2^{k+2}$. □

Lemma 2.8. *Let* H_k *be a step of one of the towers* $T/\mathbb{F}_{p^2}$ *or* $T/\mathbb{F}_p$*. One has:*

$$\sup\left\{n \in \mathbb{N} \mid N_k \geq 2n + 2g_k - 1\right\} \geq 2^k(p-3) + 2.$$

Proof. From Bounds (5) and (6) for N_k and Lemma 2.6 i), we get

$$\begin{aligned}
N_k - 2g_k + 1 &\geq 2^{k+1}(p-1) - 2(2^{k+1} - 2 \cdot 2^{\frac{k+1}{2}} + 1) + 1 \\
&= 2^{k+1}(p-3) + 4 \cdot 2^{\frac{k+1}{2}} - 1 \\
&\geq 2^{k+1}(p-3) + 4 \text{ since } k \geq 0.
\end{aligned}$$

□

2.3. General results for $\mu_q^{\mathrm{sym}}(n)$

In [5], Ballet and Le Brigand proved the following useful result:

Theorem 2.9. *Let* $F/\mathbb{F}_q$ *be an algebraic function field of genus* $g \geq 2$*. If* $q \geq 4$*, then there exists a non-special divisor of degree* $g-1$*.*

The four following lemmas prove the existence of a "good" step of the towers defined in Section 2.1, that is to say a step that will be optimal for the bilinear complexity of multiplication:

Lemma 2.10. *Let* $n \geq \frac{1}{2}\left(q^2 + 1 + \epsilon(q^2)\right)$ *be an integer. If* $q = p^r \geq 4$*, then there exists a step* $F_{k,s}/\mathbb{F}_{q^2}$ *of the tower* $T_2/\mathbb{F}_{q^2}$ *such that all the three following conditions are verified:*

(1) there exists a non-special divisor of degree $g_{k,s} - 1$ *in* $F_{k,s}/\mathbb{F}_{q^2}$*,*

(2) there exists a place of $F_{k,s}/\mathbb{F}_{q^2}$ *of degree* n*,*

(3) $N_1(F_{k,s}/\mathbb{F}_{q^2}) \geq 2n + 2g_{k,s} - 1$*.*

Moreover, the first step for which both Conditions (2) and (3) are verified is the first step for which (3) is verified.

Proof. Note that $n \geq 9$ since $q \geq 4$ and $n \geq \frac{1}{2}(q^2+1) \geq 8.5$. Fix $1 \leq k \leq n-4$ and $s \in \{0, \ldots, r\}$. First, we prove that Condition (2) is verified. Lemma 2.3 iv) gives:

$$\begin{aligned}
2g_{k,s}+1 &\leq 2\frac{q^k(q+1)-q^{\frac{k}{2}}(q-1)}{p^{r-s}}+1 \\
&= 2p^s\left(q^{k-1}(q+1)-q^{\frac{k}{2}}\frac{q-1}{q}\right)+1 \\
&\leq 2q^{k-1}p^s(q+1) \quad \text{since } 2p^sq^{\frac{k}{2}}\frac{q-1}{q} \geq 1 \qquad (7)\\
&\leq 2q^k(q^2-1).
\end{aligned}$$

On the other hand, one has $n-1 \geq k+3 > k+\frac{1}{2}+2$ so $n-1 \geq \log_q(q^k)+\log_q(2)+\log_q(q+1)$. This gives $q^{n-1} \geq 2q^k(q+1)$, hence $q^{n-1}(q-1) \geq 2q^k(q^2-1)$. Therefore, one has $2g_{k,s}+1 \leq q^{n-1}(q-1)$ which ensure us that Condition (2) is satisfied according to Corollary 5.2.10 in [23].
Now suppose also that $k \geq \log_q\left(\frac{2n}{5}\right)+1$. Note that for all $n \geq 9$ there exists such an integer k since the size of the interval $[\log_q\left(\frac{2n}{5}\right)+1, n-4]$ is bigger than $9-4-\log_4\left(\frac{2\cdot 9}{5}\right)-1 \geq 3 > 1$. Moreover such an integer k verifies $q^{k-1} \geq \frac{2}{5}n$, so $n \leq \frac{1}{2}q^{k-1}(q+1)(q-3)$ since $q \geq 4$. Then one has

$$\begin{aligned}
2n+2g_{k,s}-1 &\leq 2n+2g_{k,s}+1 \\
&\leq 2n+2q^{k-1}p^s(q+1) \quad \text{according to (7)} \\
&\leq q^{k-1}(q+1)(q-3)+2q^{k-1}p^s(q+1) \\
&\leq q^{k-1}p^s(q+1)(q-1) \\
&= (q^2-1)q^{k-1}p^s
\end{aligned}$$

which gives $N_1(F_{k,s}/\mathbb{F}_{q^2}) \geq 2n+2g_{k,s}-1$ according to Proposition 2.1 (3). Hence, for any integer $k \in [\log_q\left(\frac{2n}{5}\right)+1, n-4]$, Conditions (2) and (3) are satisfied and the smallest integer k for which they are both satisfied is the smallest integer k for which Condition (3) is satisfied.
To conclude, remark that for such an integer k, Condition (1) is easily verified from Theorem 2.9 since $q \geq 4$ and $g_{k,s} \geq g_2 \geq 6$ according to Formula (3).

□

This is a similar result for the tower $T_3/\mathbb{F}_q$:

Lemma 2.11. *Let $n \geq \frac{1}{2}\left(q+1+\epsilon(q)\right)$ be an integer. If $q = p^r \geq 4$, then there exists a step $G_{k,s}/\mathbb{F}_q$ of the tower $T_3/\mathbb{F}_q$ such that all the three following conditions are verified:*

(1) there exists a non-special divisor of degree $g_{k,s}-1$ in $G_{k,s}/\mathbb{F}_q$,

(2) there exists a place of $G_{k,s}/\mathbb{F}_q$ of degree n,

(3) $N_1(G_{k,s}/\mathbb{F}_q)+2N_2(G_{k,s}/\mathbb{F}_q) \geq 2n+2g_{k,s}-1$.

Moreover, the first step for which both Conditions (2) and (3) are verified is the first step for which (3) is verified.

Proof. Note that $n \geq 5$ since $q \geq 4$, $\epsilon(q) \geq \epsilon(4) = 4$ and $n \geq \frac{1}{2}(q+1+\epsilon(q)) \geq 4.5$. First, we focus on the case $n \geq 12$. Fix $1 \leq k \leq \frac{n-5}{2}$ and $s \in \{0, \ldots, r\}$. One has $2p^s q^k \frac{q+1}{\frac{\sqrt{q}}{2}} \leq q^{\frac{n-1}{2}}$ since

$$\frac{n-1}{2} \geq k+2 = k - \frac{1}{3} + 1 + 1 + \frac{3}{2} \geq \log_q(q^{k-\frac{3}{2}}) + \log_q(4) + \log_q(p^s) + \log_q(q+1).$$

Hence $2p^s q^{k-1}(q+1) \leq q^{\frac{n-1}{2}}(\sqrt{q}-1)$ since $\frac{\sqrt{q}}{2} \leq \sqrt{q}-1$ for $q \geq 4$. According to (7) in the previous proof, this proves that Condition (2) is satisfied.
The same reasoning as in the previous proof shows that Condition (3) is also satisfied as soon as $k \geq \log_q\left(\frac{2n}{5}\right) + 1$. Moreover, for $n \geq 12$, the interval $[\log_q\left(\frac{2n}{5}\right) + 1, \frac{n-7}{2}]$ contains at least one integer and the smallest integer k in this interval is the smallest integer k for which Condition (3) is verified. Furthermore, for such an integer k, Condition (1) is easily verified from Theorem 2.9 since $q \geq 4$ and $g_{k,s} \geq g_2 \geq 6$ according to Formula (3).

To complete the proof, we want to focus on the case $5 \leq n \leq 11$. For this case, we have to look at the values of $q = p^r$ and n for which we have both $n \geq \frac{1}{2}\left(q+1+\epsilon(q)\right)$ and $5 \leq n \leq 11$. For each value of n such that these two inequalities are satisfied, we have to check that Conditions (1), (2) and (3) are verified. In this aim, we use the KASH packages [14] to compute the genus and number of places of degree 1 and 2 of the first steps of the tower $T_3/\mathbb{F}_q$. Thus we determine the first step $G_{k,s}/\mathbb{F}_q$ that satisfied all the three Conditions (1), (2) and (3). We resume our results in the following table:

$q = p^r$	2^2	2^3	3^2
$\epsilon(q)$	4	5	6
$\frac{1}{2}\left(q+1+\epsilon(q)\right)$	4.5	7	8
n to be considered	$5 \leq n \leq 11$	$7 \leq n \leq 11$	$8 \leq n \leq 11$
(k,s)	$(1,1)$	$(1,1)$	$(1,1)$
$N_1(G_{k,s}/\mathbb{F}_q)$	5	9	10
$N_2(G_{k,s}/\mathbb{F}_q)$	14	124	117
$\Gamma(G_{k,s}/\mathbb{F}_q)$	15	117	113
$g_{k,s}$	2	12	9
$2g_{k,s}+1$	5	25	19
$q^{\frac{n-1}{2}}(\sqrt{q}-1) \geq \ldots$	16	936	4374

$q = p^r$	5	7	11	13
$\epsilon(q)$	4	5	6	7
$\frac{1}{2}\left(q+1+\epsilon(q)\right)$	5	6.5	9	10.5
n to be considered	$5 \leq n \leq 11$	$7 \leq n \leq 11$	$9 \leq n \leq 12$	$n = 11$
(k,s)	$(2,0)$	$(2,0)$	$(2,0)$	$(2,0)$
$N_1(G_{k,s}/\mathbb{F}_q)$	6	8	12	14
$N_2(G_{k,s}/\mathbb{F}_q)$	60	168	660	1092
$\Gamma(G_{k,s}/\mathbb{F}_q)$	53	151.5	611.5	1021.5
$g_{k,s}$	10	21	55	78
$2g_{k,s}+1$	21	43	11	157
$q^{\frac{n-1}{2}}(\sqrt{q}-1) \geq \dots$	30	564	33917	967422

In this table, one can check that for each value of q and n to be considered and every corresponding step $G_{k,s}/\mathbb{F}_q$ one has simultaneously:

- $g_{k,s} \geq 2$ so Condition (1) is verified according to Theorem 2.9,
- $2g_{k,s}+1 \leq q^{\frac{n-1}{2}}(\sqrt{q}-1)$ so Condition (2) is verified.
- $\Gamma(G_{k,s}/\mathbb{F}_q) := \frac{1}{2}\left(N_1(G_{k,s}/\mathbb{F}_q)+2N_2(G_{k,s}/\mathbb{F}_q)-2g_{k,s}+1\right) \geq n$ so Condition (3) is verified.

□

This is a similar result for the tower $T/\mathbb{F}_{p^2}$:

Lemma 2.12. *Let $p \geq 5$ and $n \geq \frac{1}{2}\left(p^2+1+\epsilon(p^2)\right)$. There exists a step $H_k/\mathbb{F}_{p^2}$ of the tower $T/\mathbb{F}_{p^2}$ such that the three following conditions are verified:*

(1) there exists a non-special divisor of degree g_k-1 in $H_k/\mathbb{F}_{p^2}$,

(2) there exists a place of $H_k/\mathbb{F}_{p^2}$ of degree n,

(3) $N_1(H_k/\mathbb{F}_{p^2}) \geq 2n+2g_k-1$.

Moreover the first step for which all the three conditions are verified is the first step for which (3) is verified.

Proof. Note that $n \geq \frac{1}{2}(5^2+1+\epsilon(5^2)) = 18$. We first prove that for all integers k such that $2 \leq k \leq n-2$, we have $2g_k+1 \leq p^{n-1}(p-1)$, so Condition (2) is verified according to Corollary 5.2.10 in [24]. Indeed, for such an integer k, since $p \geq 5$ one has $k \leq \log_2(p^{n-2}) \leq \log_2(p^{n-1}-1)$, thus it holds that $k+2 \leq \log_2\left(4(p^{n-1}-1)\right) \leq \log_2(4p^{n-1}-1)$ and then $2^{k+2}+1 \leq 4p^{n-1}$. Hence $2 \cdot 2^{k+1}+1 \leq p^{n-1}(p-1)$ since $p \geq 5$, which gives the result according to Lemma 2.6 ii).
We prove now that for $k \geq \log_2(2n-1)-2$, Condition (3) is verified. Indeed,

for such an integer k, we have $k+2 \geq \log_2(2n-1)$, so $2^{k+2} \geq 2n-1$. Hence we get $2^{k+3} \geq 2n+2^{k+2}-1$ and so $2^{k+1}(p-1) \geq 2^{k+1} \cdot 4 \geq 2n+2^{k+2}-1$ since $p \geq 5$. Thus we have $N_1(H_k/\mathbb{F}_{p^2}) \geq 2n+2g_k-1$ according to Bound (5) and Lemma 2.6 ii).

Hence, we have proved that for any integers $n \geq 18$ and $k \geq 2$ such that $\log_2(2n-1)-2 \leq k \leq n-2$, both Conditions (2) and (3) are verified. Moreover, note that for any $n \geq 18$, there exists an integer $k \geq 2$ in the interval $\left[\log_2(2n-1)-2; n-2\right]$. Indeed, $\log_2(2 \cdot 18-1)-2 \approx 3.12 > 2$ and the size of this interval increases with n and is greater than 1 for $n = 18$. To conclude, remark that for such an integer k, Condition (1) is easily verified from Theorem 2.9 since $p^2 \geq 4$ and $g_k \geq g_2 = 3$ according to Formula (4).

□

This is a similar result for the tower $T/\mathbb{F}_p$:

Lemma 2.13. *Let $p \geq 5$ and $n \geq \frac{1}{2}\left(p+1+\epsilon(p)\right)$. There exists a step $H_k/\mathbb{F}_p$ of the tower $T/\mathbb{F}_p$ such that the three following conditions are verified:*

(1) there exists a non-special divisor of degree $g_k - 1$ in $H_k/\mathbb{F}_p$,

(2) there exists a place of $H_k/\mathbb{F}_p$ of degree n,

(3) $N_1(H_k/\mathbb{F}_p) + 2N_1(H_k/\mathbb{F}_p) \geq 2n + 2g_k - 1$.

Moreover the first step for which all the three conditions are verified is the first step for which (3) is verified.

Proof. Note that $n \geq \frac{1}{2}(5+1+\epsilon(5)) = 5$. We first prove that for all integers k such that $2 \leq k \leq n-3$, we have $2g_k + 1 \leq p^{\frac{n-1}{2}}(\sqrt{p}-1)$, so Condition (2) is verified according to Corollary 5.2.10 in [24]. Indeed, for such an integer k, since $p \geq 5$ and $n \geq 5$ one has $\log_2(p^{\frac{n-1}{2}}-1) \geq \log_2(5^{\frac{n-1}{2}}-1) \geq \log_2(2^{n-1}) = n-1$. Thus $k+2 \leq n-1 \leq \log_2(p^{\frac{n-1}{2}}-1)$ and it follows from Lemma 2.6 ii) that $2g_k + 1 \leq 2^{k+2}+1 \leq p^{\frac{n-1}{2}} \leq p^{\frac{n-1}{2}}(\sqrt{p}-1)$, which gives the result.

The same reasoning as in the previous proof shows that Condition (3) is also satisfied as soon as $k \geq \log_2(2n-1)-2$. Hence, we have proved that for any integers $n \geq 5$ and $k \geq 2$ such that $\log_2(2n-1)-2 \leq k \leq n-3$, both Conditions (2) and (3) are verified. Moreover, note that the size of the interval $\left[\log_2(2n-1)-2; n-3\right]$ increases with n and that for any $n \geq 5$, this interval contains at least one integer $k \geq 2$. To conclude, remark that for such an integer k, Condition (1) is easily verified from Theorem 2.9 since $p \geq 4$ and $g_k \geq g_2 = 3$ according to Formula (4).

□

Now we establish general bounds for the bilinear complexity of multiplication by using derivative evaluations on places of degree one (respectively places of degree one and two).

Theorem 2.14. *Let q be a prime power and $n > 1$ be an integer. If there exists an algebraic function field $F/\mathbb{F}_q$ of genus g with N places of degree 1 and an integer $0 < a \leq N$ such that* *(i) there exists $\mathcal{R}$, a non-special divisor of degree $g-1$,*

(ii) there exists Q, a place of degree n,

(iii) $N+a \geq 2n+2g-1$,

then

$$\mu_q^{\mathrm{sym}}(n) \leq 2n+g-1+a.$$

Proof. Let $\mathcal{P} := \{P_1, \dots, P_N\}$ be a set of N places of degree 1 and $\mathcal{P}'$ be a subset of $\mathcal{P}$ with cardinality a. According to Lemma 2.7 in [7], we can choose an effectif divisor $\mathcal{D}$ equivalent to $Q+\mathcal{R}$ such that $\mathrm{supp}(\mathcal{D}) \cap \mathcal{P} = \emptyset$. We define the maps Ev_Q and $Ev_{\mathcal{P}}$ as in Theorem 1.1 with $u_i = 2$ if $P_i \in \mathcal{P}'$ and $u_i = 1$ if $P_i \in \mathcal{P} \backslash \mathcal{P}'$. Then Ev_Q is bijective, since $\ker Ev_Q = \mathcal{L}(\mathcal{D}-Q)$ with $\dim(\mathcal{D}-Q) = \dim(R) = 0$ and $\dim(\mathrm{Im}\, Ev_Q) = \dim \mathcal{D} = \deg \mathcal{D} - g + 1 + i(\mathcal{D}) \geq n$ according to Riemann-Roch Theorem. Thus $\dim(\mathrm{Im}\, Ev_Q) = n$. Moreover, $Ev_{\mathcal{P}}$ is injective. Indeed, $\ker Ev_{\mathcal{P}} = \mathcal{L}(2\mathcal{D} - \sum_{i=1}^{N} u_i P_i)$ with $\deg(2\mathcal{D} - \sum_{i=1}^{N} u_i P_i) = 2(n+g-1) - N - a < 0$. Furthermore, one has $\mathrm{rk}\, Ev_{\mathcal{P}} = \dim(2\mathcal{D}) = \deg(2\mathcal{D}) - g + 1 + i(2\mathcal{D})$, and $i(2\mathcal{D}) = 0$ since $2\mathcal{D} \geq \mathcal{D} \geq \mathcal{R}$ with $i(\mathcal{R}) = 0$. So $\mathrm{rk}\, Ev_{\mathcal{P}} = 2n+g-1$, and we can extract a subset $\mathcal{P}_1$ from $\mathcal{P}$ and a subset $\mathcal{P}_1'$ from $\mathcal{P}'$ with cardinality $N_1 \leq N$ and $a_1 \leq a$, such that:

- $N_1 + a_1 = 2n+g-1$,
- the map $Ev_{\mathcal{P}_1}$ defined as $Ev_{\mathcal{P}}$ with $u_i = 2$ if $P_i \in \mathcal{P}_1'$ and $u_i = 1$ if $P_i \in \mathcal{P}_1 \backslash \mathcal{P}_1'$, is injective.

According to Theorem 1.1, this leads to $\mu_q(n) \leq N_1 + 2a_1 \leq N_1 + a_1 + a$ which gives the result. □

Theorem 2.15. *Let q be a prime power and $n > 1$ be an integer. If there exists an algebraic function field $F/\mathbb{F}_q$ of genus g with N_1 places of degree 1, N_2 places of degree 2 and two integers $0 < a_1 \leq N_1$, $0 < a_2 \leq N_2$ such that*

(i) there exists $\mathcal{R}$, a non-special divisor of degree $g-1$,

(ii) there exists Q, a place of degree n,

(iii) $N_1 + a_1 + 2(N_2 + a_2) \geq 2n+2g-1$,

then

$$\mu_q^{\mathrm{sym}}(n) \leq 2n + g + N_2 + a_1 + 4a_2$$

and

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + \frac{3}{2}g + \frac{a_1}{2} + 3a_2.$$

Proof. Let $\mathcal{P}_1 := \{P_1, \dots, P_{N_1}\}$ be a set of N_1 places of degree 1 and $\mathcal{P}_1'$ be a subset of $\mathcal{P}_1$ with cardinality a_1. Let $\mathcal{P}_2 := \{Q_1, \dots, Q_{N_2}\}$ be a set of N_2 places of degree 2 and $\mathcal{P}_2'$ be a subset of $\mathcal{P}_2$ with cardinality a_2. According to Lemma 2.7 in [7], we can choose an effectif divisor $\mathcal{D}$ equivalent to $Q+\mathcal{R}$ such that $\mathrm{supp}(\mathscr{D}) \cap (\mathscr{P}_1 \cup \mathscr{P}_2) = \emptyset$. We define the maps Ev_Q and $Ev_{\mathscr{P}}$ as in Theorem 1.1 with $u_i = 2$ if $P_i \in \mathscr{P}'_1 \cup \mathscr{P}'_2$ and $u_i = 1$ if $P_i \in (\mathscr{P}_1 \backslash \mathscr{P}'_1) \cup (\mathscr{P}_2 \backslash \mathscr{P}'_2)$. Then the same raisoning as in the previous proof shows that Ev_Q is bijective. Moreover, $Ev_{\mathscr{P}}$ is injective. Indeed, $\ker Ev_{\mathscr{P}} = \mathscr{L}(2\mathscr{D} - \sum_{i=1}^{N} u_i P_i)$ with $\deg(2\mathscr{D} - \sum_{i=1}^{N} u_i P_i) = 2(n+g-1)-(N_1+a_1+2(N_2+a_2)) < 0$. Furthermore, one has $\mathrm{rk}\, Ev_{\mathscr{P}} = \dim(2\mathscr{D}) = \deg(2\mathscr{D}) - g + 1 + i(2\mathscr{D})$, and $i(2\mathscr{D}) = 0$ since $2\mathscr{D} \geq \mathscr{D} \geq \mathscr{R}$ with $i(\mathscr{R}) = 0$. So $\mathrm{rk}\, Ev_{\mathscr{P}} = 2n + g - 1$, and we can extract a subset $\tilde{\mathscr{P}}_1$ from $\mathscr{P}_1$, a subset $\tilde{\mathscr{P}}'_1$ from $\mathscr{P}'_1$, a subset $\tilde{\mathscr{P}}_2$ from $\mathscr{P}_2$ and a subset $\tilde{\mathscr{P}}'_2$ from $\mathscr{P}'_2$ with respective cardinality $\tilde{N}_1 \leq N_1$, $\tilde{a}_1 \leq a_1$, $\tilde{N}_2 \leq N_2$ and $\tilde{a}_2 \leq a_2$, such that:

- $2n + g \geq \tilde{N}_1 + \tilde{a}_1 + 2(\tilde{N}_2 + \tilde{a}_2) \geq 2n + g - 1$,
- the map $Ev_{\tilde{\mathscr{P}}}$ defined as $Ev_{\mathscr{P}}$ with $u_i = 2$ if $P_i \in \tilde{\mathscr{P}}'_1 \cup \tilde{\mathscr{P}}'_2$ and $u_i = 1$ if $(\tilde{\mathscr{P}}_1 \backslash \tilde{\mathscr{P}}'_1) \cup (\tilde{\mathscr{P}}_2 \backslash \tilde{\mathscr{P}}'_2)$, is injective.

According to Theorem 1.1, this leads to $\mu_q(n) \leq \tilde{N}_1 + 2\tilde{a}_1 + 3(\tilde{N}_2 + 2\tilde{a}_2)$ since $M_k(2) \leq 3$ for all prime power k. Hence, one has the first result since $\tilde{N}_1 + \tilde{a}_1 + 2(\tilde{N}_2 + \tilde{a}_2) \leq 2n + g$ and the second one since $\frac{\tilde{a}_1}{2} + \tilde{N}_2 + \tilde{a}_2 \leq \frac{g}{2} + n$. □

2.4. New upper bounds for $\mu_q^{\mathrm{sym}}(n)$

Here, we give a detailed proof of Bound (i) of Theorem 1.4 and of an improvement of [1, Theorem 5.9]. Moreover, we established the new bounds for $\mu_{p^2}^{\mathrm{sym}}(n)$ and $\mu_p^{\mathrm{sym}}(n)$ announced in Section 1.3.

Proof of Theorem 1.4.

(i) Let $n \geq \frac{1}{2}(q^2 + 1 + \epsilon(q^2))$. Otherwise, we already know from the pionner works recalled in Section 1.2 that $\mu_{q^2}^{\mathrm{sym}}(n) \leq 2n$. According to Lemma 2.10, there exists a step of the tower $T_2/\mathbb{F}_{q^2}$ on which we can apply Theorem 2.14 with $a = 0$. We denote by $F_{k,s+1}/\mathbb{F}_{q^2}$ the first step of the tower that suits the hypothesis of Theorem 2.14 with $a = 0$, i.e. k and s are integers such that $N_{k,s+1} \geq 2n + 2g_{k,s+1} - 1$ and $N_{k,s} < 2n + 2g_{k,s} - 1$, where $N_{k,s} := N_1(F_{k,s}/\mathbb{F}_{q^2})$ and $g_k := g(F_{k,s})$. We denote by $n_0^{k,s}$ the biggest integer such that $N_{k,s} \geq 2n_0^{k,s} + 2g_{k,s} - 1$, i.e. $n_0^{k,s} = \sup\left\{n \in \mathbb{N} \,|\, 2n \leq N_{k,s} - 2g_{k,s} + 1\right\}$. To perform multiplication in $\mathbb{F}_{q^{2n}}$, we have the following alternative:

(a) use the algorithm on the step $F_{k,s+1}$. In this case, a bound for the bilinear complexity is given by Theorem 2.14 applied with $a = 0$:

$$\mu_{q^2}^{\mathrm{sym}}(n) \leq 2n + g_{k,s+1} - 1 = 2n + g_{k,s} - 1 + \Delta g_{k,s}.$$

(Recall that $\Delta g_{k,s} := g_{k,s+1} - g_{k,s}$)

(b) use the algorithm on the step $F_{k,s}$ with an appropriate number of derivative evaluations. Let $a := 2(n - n_0^{k,s})$ and suppose that $a \leq N_{k,s}$. Then $N_{k,s} \geq 2n_0^{k,s} + 2g_{k,s} - 1$ implies that $N_{k,s} + a \geq 2n + 2g_{k,s} - 1$ so Condition

(iii) of Theorem 2.14 is satisfied. Thus, we can perform a derivative evaluations in the algorithm using the step $F_{k,s}$ and we have:

$$\mu_{q^2}^{\mathrm{sym}}(n) \leq 2n + g_{k,s} - 1 + a.$$

Thus, if $a \leq N_{k,s}$ Case (b) gives a better bound as soon as $a < \Delta g_{k,s}$. Since we have from Lemma 2.4 both $N_{k,s} \geq D_{k,s}$ and $\Delta g_{k,s} \geq D_{k,s}$, if $a \leq D_{k,s}$ then we can perform a derivative evaluations on places of degree 1 in the step $F_{k,s}$ and Case (b) gives a better bound then Case (a).
For $x \in \mathbb{R}^+$ such that $N_{k,s+1} \geq 2[x] + 2g_{k,s+1} - 1$ and $N_{k,s} < 2[x] + 2g_{k,s} - 1$, we define the function $\Phi_{k,s}(x)$ as follow:

$$\Phi_{k,s}(x) = \begin{cases} 2x + g_{k,s} - 1 + 2(x - n_0^{k,s}) & \text{if } 2(x - n_0^{k,s}) < D_{k,s} \\ 2x + g_{k,s+1} - 1 & \text{else.} \end{cases}$$

We define the function Φ for all $x \geq 0$ as the minimum of the functions $\Phi_{k,s}$ for which x is in the domain of $\Phi_{k,s}$. This function is piecewise linear with two kinds of piece: those which have slope 2 and those which have slope 4. Moreover, since the y-intercept of each piece grows with k and s, the graph of the function Φ lies below any straight line that lies above all the points $\left(n_0^{k,s} + \frac{D_{k,s}}{2}, \Phi(n_0^{k,s} + \frac{D_{k,s}}{2})\right)$, since these are the *vertices* of the graph.
Let $X := n_0^{k,s} + \frac{D_{k,s}}{2}$, then

$$\begin{aligned} \Phi(X) &\leq 2X + g_{k,s+1} - 1 \\ &\leq 2X + g_{k,s+1} \\ &= 2\left(1 + \frac{g_{k,s+1}}{2X}\right)X. \end{aligned}$$

We want to give a bound for $\Phi(X)$ which is independent of k and s.
Recall that $D_{k,s} := (p-1)p^s q^k$, and

$$2n_0^{k,s} \geq q^{k-1}p^s(q+1)(q-3) \quad \text{by Lemma 2.5}$$

and

$$g_{k,s+1} \leq q^{k-1}(q+1)p^{s+1} \quad \text{by Lemma 2.3 (iii).}$$

So we have

$$\begin{aligned} \frac{g_{k,s+1}}{2X} &= \frac{g_{k,s+1}}{2n_0^{k,s} + D_{k,s}} \\ &\leq \frac{q^{k-1}(q+1)p^{s+1}}{q^{k-1}p^s(q+1)(q-3) + (p-1)p^s q^k} \\ &= \frac{q^{k-1}(q+1)p^s p}{q^{k-1}(q+1)p^s\left(q - 3 + (p-1)\frac{q}{q+1}\right)} \\ &= \frac{p}{(q-3) + (p-1)\frac{q}{q+1}}. \end{aligned}$$

Thus, the graph of the function Φ lies below the line $y = 2\left(1 + \frac{p}{(q-3)+(p-1)\frac{q}{q+1}}\right)x$.
In particular, we get

$$\Phi(n) \leq 2\left(1 + \frac{p}{(q-3)+(p-1)\frac{q}{q+1}}\right)n.$$

(ii) Let $n \geq \frac{1}{2}(q+1+\epsilon(q))$. Otherwise, we already know from Section 1.2 that $\mu_q^{\mathrm{sym}}(n) \leq 2n$. According to Lemma 2.11, there exists a step of the tower $T_3/\mathbb{F}_q$ on which we can apply Theorem 2.15 with $a_1 = a_2 = 0$. We denote by $G_{k,s+1}/\mathbb{F}_q$ the first step of the tower that suits the hypothesis of Theorem 2.15 with $a_1 = a_2 = 0$, i.e. k and s are integers such that $N_{k,s+1} \geq 2n + 2g_{k,s+1} - 1$ and $N_{k,s} < 2n + 2g_{k,s} - 1$, where $N_{k,s} := N_1(G_{k,s}/\mathbb{F}_q) + 2N_2(G_{k,s}/\mathbb{F}_q)$ and $g_{k,s} := g(G_{k,s})$. We denote by $n_0^{k,s}$ the biggest integer such that $N_{k,s} \geq 2n_0^{k,s} + 2g_{k,s} - 1$, i.e. $n_0^{k,s} = \sup\left\{n \in \mathbb{N} \,|\, 2n \leq N_{k,s} - 2g_{k,s} + 1\right\}$. To perform multiplication in $\mathbb{F}_{q^n}$, we have the following alternative:

(a) use the algorithm on the step $G_{k,s+1}$. In this case, a bound for the bilinear complexity is given by Theorem 2.15 applied with $a_1 = a_2 = 0$:

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + \frac{3}{2}g_{k,s+1} = 3n_0^{k,s} + \frac{3}{2}g_{k,s} + 3(n - n_0^{k,s}) + \frac{3}{2}\Delta g_{k,s}.$$

(b) use the algorithm on the step $G_{k,s}$ with an appropriate number of derivative evaluations. Let $a_1 + 2a_2 := 2(n - n_0^{k,s})$ and suppose that $a_1 + 2a_2 \leq N_{k,s}$. Then $N_{k,s} \geq 2n_0^{k,s} + 2g_{k,s} - 1$ implies that $N_{k,s} + a_1 + 2a_2 \geq 2n + 2g_{k,s} - 1$. Thus we can perform $a_1 + a_2$ derivative evaluations in the algorithm using the step $G_{k,s}$ and we have:

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + \frac{3}{2}g_{k,s} + \frac{3}{2}(a_1 + 2a_2) = 3n_0^{k,s} + \frac{3}{2}g_{k,s} + 6(n - n_0^{k,s}).$$

Thus, if $a_1 + 2a_2 \leq N_{k,s}$ Case (b) gives a better bound as soon as $n - n_0^{k,s} < \frac{1}{2}\Delta g_{k,s}$. Since we have from Lemma 2.4 both $N_{k,s} \geq D_{k,s}$ and $\frac{1}{2}\Delta g_{k,s} \geq \frac{1}{2}D_{k,s}$, if $a_1 + 2a_2 \leq D_{k,s}$, i.e. $n - n_0^{k,s} \leq \frac{1}{2}D_{k,s}$, then we can perform a_1 derivative evaluations on places of degree 1 and a_2 derivative evaluations on places of degree 2 in the step $G_{k,s}$ and Case (b) gives a better bound then Case (a).
For $x \in \mathbb{R}^+$ such that $N_{k,s+1} \geq 2[x] + 2g_{k,s+1} - 1$ and $N_{k,s} < 2[x] + 2g_{k,s} - 1$, we define the function $\Phi_{k,s}(x)$ as follow:

$$\Phi_{k,s}(x) = \begin{cases} 3x + \frac{3}{2}g_{k,s} + 3(x - n_0^{k,s}) & \text{if } x - n_0^{k,s} < \frac{D_{k,s}}{2} \\ 3x + \frac{3}{2}g_{k,s+1} & \text{else.} \end{cases}$$

We define the function Φ for all $x \geq 0$ as the minimum of the functions $\Phi_{k,s}$ for which x is in the domain of $\Phi_{k,s}$. This function is piecewise linear with two kinds of piece: those which have slope 3 and those which have slope 6. Moreover, since the y-intercept of each piece grows with k and s, the graph of the function Φ lies below any straight line that lies above all the points $\left(n_0^{k,s} + \frac{D_{k,s}}{2}, \Phi(n_0^{k,s} + \frac{D_{k,s}}{2})\right)$, since these are the *vertices* of the graph.
Let $X := n_0^{k,s} + \frac{D_{k,s}}{2}$, then

$$\begin{aligned} \Phi(X) &\leq 3X + \frac{3}{2} g_{k,s+1} \\ &= 3\left(1 + \frac{g_{k,s+1}}{2X}\right) X. \end{aligned}$$

We want to give a bound for $\Phi(X)$ which is independent of k and s.
Recall that $D_{k,s} := (p-1)p^s q^k$, and

$$n_0^{k,s} \geq \frac{1}{2} q^{k-1} p^s (q+1)(q-3) \quad \text{by Lemma 2.5}$$

and

$$g_{k,s+1} \leq q^{k-1}(q+1)p^{s+1} \quad \text{by Lemma 2.3 (iii).}$$

So we have

$$\begin{aligned} \frac{g_{k,s+1}}{2X} &= \frac{g_{k,s+1}}{2(n_0^{k,s} + \frac{D_{k,s}}{2})} \\ &\leq \frac{q^{k-1}(q+1)p^{s+1}}{2(\frac{1}{2}q^{k-1}p^s(q+1)(q-3) + \frac{1}{2}(p-1)p^s q^k)} \\ &= \frac{q^{k-1}(q+1)p^s p}{q^{k-1}(q+1)p^s \left(q-3+(p-1)\frac{q}{q+1}\right)} \\ &= \frac{p}{(q-3)+(p-1)\frac{q}{q+1}}. \end{aligned}$$

Thus, the graph of the function Φ lies below the line $y = 3\left(1 + \frac{p}{(q-3)+(p-1)\frac{q}{q+1}}\right)x$.
In particular, we get

$$\Phi(n) \leq 3\left(1 + \frac{p}{(q-3)+(p-1)\frac{q}{q+1}}\right) n.$$

(iii) Let $n \geq \frac{1}{2}(p^2+1+\epsilon(p^2))$. Otherwise, we already know from Section 1.2 that $\mu_{p^2}^{\mathrm{sym}}(n) \leq 2n$. According to Lemma 2.12, there exists a step of the tower $T/\mathbb{F}_{p^2}$ on which we can apply Theorem 2.14 with $a = 0$. We denote by $H_{k+1}/\mathbb{F}_{p^2}$ the first step of the tower that suits the hypothesis of Theorem 2.14 with $a=0$, i.e. k is an integer such that $N_{k+1} \geq 2n+2g_{k+1}-1$ and $N_k < 2n+2g_k-1$, where $N_k := N_1(H_k/\mathbb{F}_{p^2})$ and $g_k := g(H_k)$. We denote by n_0^k the biggest integer such that $N_k \geq 2n_0^k + 2g_k - 1$, i.e. $n_0^k = \sup\{n \in \mathbb{N} \,|\, 2n \leq N_k - 2g_k + 1\}$. To perform multiplication in $\mathbb{F}_{p^{2n}}$, we have the following alternative:

(a) use the algorithm on the step H_{k+1}. In this case, a bound for the bilinear complexity is given by Theorem 2.14 applied with $a=0$:

$$\mu_{p^2}^{\mathrm{sym}}(n) \leq 2n + g_{k+1} - 1 = 2n + g_k - 1 + \Delta g_{k,s}.$$

(Recall that $\Delta g_k := g_{k+1} - g_k$)

(b) use the algorithm on the step H_k with an appropriate number of derivative evaluations. Let $a := 2(n - n_0^k)$ and suppose that $a \leq N_k$. Then $N_k \geq 2n_0^k + 2g_k - 1$ implies that $N_k + a \geq 2n + 2g_k - 1$ so Condition (3) of Theorem 2.14 is satisfied. Thus, we can perform a derivative evaluations in the algorithm using the step H_k and we have:

$$\mu_{p^2}^{\mathrm{sym}}(n) \leq 2n + g_k - 1 + a.$$

Thus, if $a \leq N_k$ Case (b) gives a better bound as soon as $a < \Delta g_k$. For $x \in \mathbb{R}^+$ such that $N_{k+1} \geq 2[x] + 2g_{k+1} - 1$ and $N_k < 2[x] + 2g_k - 1$, we define the function $\Phi_k(x)$ as follow:

$$\Phi_k(x) = \begin{cases} 2x + g_k - 1 + 2(x - n_0^k) & \text{if } 2(x - n_0^k) < \Delta g_k \\ 2x + g_{k+1} - 1 & \text{else.} \end{cases}$$

Note that when Case (b) gives a better bound, that is to say when $2(x - n_0^k) < \Delta g_k$, then according to Lemma 2.7 we have also

$$2(x - n_0^k) < N_k$$

so we can proceed as in Case (b) since there are enough rational places to use $a = 2(x - n_0^k)$ derivative evaluations on.

We define the function Φ for all $x \geq 0$ as the minimum of the functions Φ_k for which x is in the domain of Φ_k. This function is piecewise linear with two kinds of piece: those which have slope 2 and those which have slope 4. Moreover, since the y-intercept of each piece grows with k, the graph of the function Φ lies below any straight line that lies above all the points $\left(n_0^k + \frac{\Delta g_k}{2}, \Phi(n_0^k + \frac{\Delta g_k}{2})\right)$, since these are the *vertices* of the graph.
Let $X := n_0^k + \frac{\Delta g_k}{2}$, then

$$\Phi(X) \quad \leq \quad 2X + g_{k+1} - 1 \leq 2\left(1 + \frac{g_{k+1}}{2X}\right)X.$$

We want to give a bound for $\Phi(X)$ which is independent of k.

Lemmas 2.6 ii), 2.7 and 2.8 give

$$\begin{aligned}
\frac{g_{k+1}}{2X} &\leq \frac{2^{k+2}}{2^{k+1}(p-3)+4+2^{k+1}-2^{\frac{k+1}{2}}} \\
&= \frac{2^{k+2}}{2^{k+1}\left((p-3)+1+2^{-k+1}-2^{-\frac{k+1}{2}}\right)} \\
&= \frac{2}{p-2+2^{-k+1}-2^{-\frac{k+1}{2}}} \\
&\leq \frac{2}{p-\frac{33}{16}}
\end{aligned}$$

since $-\frac{1}{16}$ is the minimum of the function $k \mapsto 2^{-k+1}-2^{-\frac{k+1}{2}}$.

Thus, the graph of the function Φ lies below the line $y = 2\left(1+\frac{2}{p-\frac{33}{16}}\right)x$. In particular, we get

$$\Phi(n) \leq 2\left(1+\frac{2}{p-\frac{33}{16}}\right)n.$$

(iv) Let $n \geq \frac{1}{2}(p+1+\epsilon(p))$. Otherwise, we already know from Section 1.2 that $\mu_p^{\mathrm{sym}}(n) \leq 2n$. According to Lemma 2.13, there exists a step of the tower $T/\mathbb{F}_p$ on which we can apply Theorem 2.15 with $a_1 = a_2 = 0$. We denote by $H_{k+1}/\mathbb{F}_p$ the first step of the tower that suits the hypothesis of Theorem 2.15 with $a_1 = a_2 = 0$, i.e. k is an integer such that $N_{k+1} \geq 2n+2g_{k+1}-1$ and $N_k < 2n+2g_k-1$, where $N_k := N_1(H_k/\mathbb{F}_p)+2N_2(H_k/\mathbb{F}_p)$ and $g_k := g(H_k)$. We denote by n_0^k the biggest integer such that $N_k \geq 2n_0^k+2g_k-1$, i.e. $n_0^k = \sup\left\{n \in \mathbb{N} \,|\, 2n \leq N_k - 2g_k + 1\right\}$. To perform multiplication in $\mathbb{F}_{p^n}$, we have the following alternative:

(a) use the algorithm on the step H_{k+1}. In this case, a bound for the bilinear complexity is given by Theorem 2.15 applied with $a_1 = a_2 = 0$:

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + \frac{3}{2}g_{k+1} = 3n_0^k + \frac{3}{2}g_k + 3(n-n_0^k) + \frac{3}{2}\Delta g_k.$$

(b) use the algorithm on the step H_k with an appropriate number of derivative evaluations. Let $a_1 + 2a_2 := 2(n-n_0^k)$ and suppose that $a_1+2a_2 \leq N_k$. Then $N_k \geq 2n_0^k+2g_k-1$ implies that $N_k + a_1 + 2a_2 \geq 2n+2g_k-1$. Thus we can perform a_1+a_2 derivative evaluations in the algorithm using the step H_k and we have:

$$\mu_p^{\mathrm{sym}}(n) \leq 3n + \frac{3}{2}g_k + \frac{3}{2}(a_1+2a_2) = 3n_0^k + \frac{3}{2}g_k + 6(n-n_0^k).$$

Thus, if $a_1+2a_2 \leq N_{k,s}$ Case (b) gives a better bound as soon as $n - n_0^{k,s} < \frac{1}{2}\Delta g_{k,s}$. For $x \in \mathbb{R}^+$ such that $N_{k+1} \geq 2[x] + 2g_{k+1} - 1$ and $N_k < 2[x] + 2g_k - 1$, we define the function $\Phi_k(x)$ as follow:

$$\Phi_k(x) = \begin{cases} 3x + \frac{3}{2}g_k + 3(x - n_0^k) & \text{if } x - n_0^k < \frac{\Delta g_k}{2} \\ 3x + \frac{3}{2}g_{k+1} & \text{else.} \end{cases}$$

Note that when Case (b) gives a better bound, that is to say when $2(x - n_0^k) < \Delta g_k$, then according to Lemma 2.7 we have also

$$2(x - n_0^k) < N_k$$

so we can proceed as in Case (b) since there are enough places of degree 1 and 2 to use $a_1 + a_2 = 2(x - n_0^k)$ derivative evaluations on.

We define the function Φ for all $x \geq 0$ as the minimum of the functions Φ_k for which x is in the domain of Φ_k. This function is piecewise linear with two kinds of piece: those which have slope 3 and those which have slope 6. Moreover, since the y-intercept of each piece grows with k, the graph of the function Φ lies below any straight line that lies above all the points $\left(n_0^k + \frac{\Delta g_k}{2}, \Phi(n_0^k + \frac{\Delta g_k}{2})\right)$, since these are the *vertices* of the graph.
Let $X := n_0^k + \frac{\Delta g_k}{2}$, then

$$\Phi(X) \quad \leq \quad 3X + \frac{3}{2}g_{k+1} = 3\left(1 + \frac{g_{k+1}}{2X}\right)X.$$

We want to give a bound for $\Phi(X)$ which is independent of k.

The same reasoning as in (iii) gives

$$\frac{g_{k+1}}{2X} \leq \frac{2}{p - \frac{33}{16}}.$$

Thus, the graph of the function Φ lies below the line $y = 3\left(1 + \frac{2}{p - \frac{33}{16}}\right)x$. In particular, we get

$$\Phi(n) \leq 3\left(1 + \frac{2}{p - \frac{33}{16}}\right)n.$$

□

3. Note on some unproven bounds

The two papers [10, 19] predict new upper bounds for the limsup of the complexity of the multiplication in extensions of small prime finite fields. Unfortunatly these predictions are based on an asumption which is unproven (and might be false in general). This asumption is stated as Lemma IV.4 in the paper [10]. The claim is the following:

Let p a prime integer. For each even integer t, there exists a family $(X_s)_{s=1}^{\infty}$ of curves:

- defined over $\mathbb{F}_p$;
- whose genuses tend to infinity, and grow slowly, i.e. $g_{s+1}/g_s \underset{s\to\infty}{\longrightarrow} 1$;
- whose number of $\mathbb{F}_{p^t}$-points is asymptotically optimal (i.e. the ratio of this number with respect to the genus tends to $\sqrt{p^t}-1$).

And thus, by [10, Lemma IV.3], the family $(X_s)_{s=1}^{\infty}$ would attain the generalized Drinfeld-Vlăduţ bound for the number of points of degree t.

The new result claimed in [10] is that the curves are defined over $\mathbb{F}_p$. If one removes this property, the computations made in this paper would lead to results already known[4] since [22]. But to justify the fact that their curves are defined over $\mathbb{F}_p$, p being a prime, the authors need that these curves come from the reduction modulo p of Shimura curves that would be defined over $\mathbb{Q}$.

This latter claim is not proved, so this invalidates the result. We can further notice that it appears that, up to some details (e.g. add the sufficient hypothesis that K has narrow class number 1), some of these curves should indeed admit $\mathbb{Q}$ as field of moduli (by the first corollary of [16] the levels ℓ being assumed Galois invariant). But this potentially restrains the list of possible choices for p and t and even in those cases, it does not suffice to prove the assumption, since the field of moduli need not be the field of definition.

We give here a list of the bounds that, to the best of our knowledge, rely on this unproven assumption:

- the symmetric bounds in Theorem IV.6, Theorem IV.7 and the list of specific bounds in Corollary IV.8 of [10]; namely the followings:

$$\mathrm{M}_q^{\mathrm{sym}} \leq \mu_q^{\mathrm{sym}}(2t)\frac{q^t-1}{t(q^t-5)}$$

for any $t \geq 1$ as long as $q^t-5>0$ for q a prime power;

$$\mathrm{M}_q^{\mathrm{sym}} \leq \mu_q^{\mathrm{sym}}(t)\frac{q^{t/2}-1}{t(q^{t/2}-5)}$$

for any $t \geq 1$ as long as $q^{t/2}-5>0$ for q a prime power which is a square;

$$\mu_2^{\mathrm{sym}}(12) \leq 42 \quad \mu_3^{\mathrm{sym}}(10) \leq 27 \quad \mu_4^{\mathrm{sym}}(6) \leq 14 \quad \mu_5^{\mathrm{sym}}(4) = 8$$

[4] Modulo an error spotted by Cascudo, and then corrected by Ballet and Pieltant in [7, §4.5], and Randriam in [20, §5].

and

$$\mu_q^{\mathrm{sym}}(4) = 7 \text{ for } q = 7, 8, 9, 11, 13.$$

- the asymmetric bounds in Theorem 5.3, Corollary 5.4, Corollary 5.5 of [19], namely the followings:

$$M_q \leq \frac{2\mu_q(t)}{t}\left(1 + \frac{1}{q^{t/2} - 2}\right)$$

for q be a prime power and $t \geq 1$ an integer such that $q^t \geq 9$ is a square; and

$$M_2 \leq \frac{35}{6} \qquad M_3 \leq \frac{36}{7} \qquad M_4 \leq \frac{30}{7} \qquad M_5 \leq 4 \qquad M_7 \leq 3.6 \qquad M_8 \leq 3.5.$$

References

[1] Nicolas Arnaud. *Évaluation dérivée, multiplication dans les corps finis et codes correcteurs*. PhD thesis, Université de la Méditerranée, Institut de Mathématiques de Luminy, 2006.

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

[4] Stéphane Ballet and Jean Chaumine. On the bounds of the bilinear complexity of multiplication in some finite fields. *Applicable Algebra in Engineering Communication and Computing*, 15:205–211, 2004.

[5] Stéphane Ballet and Dominique Le Brigand. On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$. *Journal on Number Theory*, 116:293–310, 2006.

[6] Stéphane Ballet, Dominique Le Brigand, and Robert Rolland. On an application of the definition field descent of a tower of function fields. In *Proceedings of the Conference Arithmetic, Geometry and Coding Theory (AGCT 2005)*, volume 21, pages 187–203. Société Mathématique de France, sér. Séminaires et Congrès, 2009.

[7] Stéphane Ballet and Julia Pieltant. On the tensor rank of multiplication in any extension of $\mathbb{F}_2$. *Journal of Complexity*, 27:230–245, 2011.

[8] 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.

[9] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. Torsion limits and Riemann-Roch systems for function fields and applications. *IEEE, Transactions on Information Theory*, 60(7):3871–3888, 2014.

[10] Ignacio Cascudo, Ronald Cramer, Chaoping Xing, and An Yang. Asymptotic bound for multiplication complexity in the extensions of small finite fields. *IEEE Transactions on Information Theory*, 58(7):4930–4935, 2012.

[11] Murat Cenk and Ferruh Özbudak. On multiplication in finite fields. *Journal of Complexity*, 26(2):172–186, 2010.

[12] Hao Chen and Ronald Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 521–536. Springer Berlin Heidelberg, 2006.

[13] David V. Chudnovsky and Gregory V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4:285–316, 1988.

[14] Mario Daberkow, Claus Fieker, Jürgen Klüners, Michael E. Pohst, Roegner Katherine, and Klaus Wildanger. KANT V4. *Journal of Symbolic Computation*, 24:267–283, 1997.

[15] 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.

[16] Koji Doi and Hidehisa Naganuma. On the algebraic curves uniformized by arithmetical automorphic functions. *Annals of Mathematics*, 86(3):pp. 449–460, 1967.

[17] Arnaldo Garcia and Henning Stitchtenoth. A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound. *Inventiones Mathematicae*, 121:211–222, 1995.

[18] Arnaldo Garcia, Henning Stitchtenoth, and Hans-Georg Ruck. On tame towers over finite fields. *Journal fur die reine und angewandte Mathematik*, 557:53–80, 2003.

[19] Julia Pieltant and Hugues Randriam. New uniform and asymptotic upper bounds on the tensor rank of multiplication in extensions of finite fields. *Mathematics of Computation*, 84:2023–2045, 2015.

[20] Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *Journal of Complexity*, 28:489–517, 2012.

[21] Amin Shokhrollahi. Optimal algorithms for multiplication in certain finite fields using algebraic curves. *SIAM Journal on Computing*, 21(6):1193–1198, 1992.

[22] Igor Shparlinski, Michael Tsfasman, and Serguei Vladut. 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.

[23] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Number 314 in Lectures Notes in Mathematics. Springer-Verlag, 1993.

[24] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Number 254 in Graduate Texts in Mathematics. Springer, second edition, 2008.

[25] Shmuel Winograd. On multiplication in algebraic extension fields. *Theoretical Computer Science*, 8:359–377, 1979.