Contemporary Mathematics

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

Stéphane Ballet, Julia Pieltant, Matthieu Rambaud, and Jeroen Sijsling

ABSTRACT. The aim of this paper is twofold. On the one hand, we establish new upper bounds for the symmetric multiplication tensor in any extension of finite fields. Note that these bounds are not asymptotic but uniform. On the other hand, we clarify the current state of the art by giving the detailed proof of some known unpublished uniform bounds, and we discuss the validity of some current asymptotic bounds and their relation with the fields of definition of certain Shimura curves.

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 $\mathbb{F}_{q^n}$. It can therefore 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 also considered as an element T of $(\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n})^\star \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} = \mathbb{F}_{q^n}^\star \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}^\star \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$. 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 $\mathbb{F}_{q^n}^\star$ 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 the decomposition (1). We therefore make the following definition:

DEFINITION 1.1. *The minimal number of summands in a decomposition of the multiplication tensor T is called the* bilinear complexity *of the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$*

2000 *Mathematics Subject Classification.* Primary .

The author wishes to thank the INFRES department for funding his visit to LTCI, where this work was partly done.

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

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 but the rank of the tensor T. Among others, a particular class of decompositions of 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 1.2. *The minimal number of summands in a symmetric decomposition of the multiplication tensor T 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 been exhibited so far. However, better upper bounds have been established in the asymmetric case [**31, 30**] 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 these two quantities separately.

Note 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, among others, arithmetic secret sharing and multiparty computation (see [**11, 14**])...

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 [**42**] and H. de Groote [**18**] 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 [**15**] applied to elliptic curves, M.A. Shokrollahi has shown in [**34**] 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 was generalized to algebraic function fields of genus g.

Let us recall that the original algorithm of D.V. and G.V. Chudnovsky introduced in [**15**] is symmetric by definition and leads to the following result from [**2**]:

THEOREM 1.3. *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 expressions for C_q have been obtained, such as the following best current published estimates:

$$C_q = \begin{cases} \text{if } q=2, & \text{then } \frac{4824}{247} \simeq 19,6 \quad [\mathbf{7}] \text{ and } [\mathbf{13}] \\ \text{else if } q=3, & \text{then } 27 \quad [\mathbf{3}] \\ \text{else if } q=p\geq 5, & \text{then } 3\left(1+\frac{4}{q-3}\right) \quad [\mathbf{4}] \\ \text{else if } q=p^2\geq 25, & \text{then } 2\left(1+\frac{2}{p-3}\right) \quad [\mathbf{4}] \\ \text{else if } q\geq 4, & \text{then } 6\left(1+\frac{p}{q-3}\right) \quad [\mathbf{3}] \end{cases}$$

Now we introduce the generalized Chudnovsky-Chudnovskytype algorithm described in [**13**]; the original algorithm given in [**15**] 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 1.4. *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

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

is injective, where the application φ_i is defined by

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

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 was introduced independently by N. Arnaud in [**1**], and can be seen as a corollary of Theorem 1.4 by gathering the places used with the same multiplicity. In fact $a_j := |\{i \mid \deg P_i = j \text{ and } u_i = 2\}|$ for $j = 1, 2$ in the statement of the Corollary.

COROLLARY 1.5. *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 $F/\mathbb{F}_q$,*
- *$\mathscr{P} = \{P_1, \ldots, P_{N_1}\}$ be a set of N_1 places of degree one and $\mathscr{P}' = \{R_1, \ldots, R_{N_2}\}$ be a set of N_2 places of degree two,*
- *$0 \leq a_1 \leq N_1$ and $0 \leq a_2 \leq N_2$ be two integers.*

Suppose that Q and all the places in $\mathscr{P}$ are not in the support of $\mathscr{D}$ and that furthermore

a) the map

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

is onto,

b) the map

$$Ev_{\mathscr{P},\mathscr{P}'} : \left| \begin{array}{ccl} \mathscr{L}(2\mathscr{D}) & \rightarrow & \mathbb{F}_q^{N_1} \times \mathbb{F}_q^{a_1} \times \mathbb{F}_{q^2}^{N_2} \times \mathbb{F}_{q^2}^{a_2} \\ f & \mapsto & \big(f(P_1), \ldots, f(P_{N_1}), f'(P_1), \ldots, f'(P_{a_1}), \\ & & f(R_1), \ldots, f(R_{N_2}), f'(R_1), \ldots, f'(R_{a_2})\big) \end{array} \right.$$

is injective.

Then

$$\mu_q^{\mathrm{sym}}(n) \leq N_1 + 2a_1 + 3N_2 + 6a_2.$$

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 $\mu_2^{\mathrm{sym}}(6) = 15$ [**15**].

1.3. New results and organization of the paper. The paper is organized as follows. First we establish new uniform upper bounds for the tensor rank of multiplication in any finite field, not necessarily of square cardinality. These bounds are stated in the following theorem:

THEOREM 1.6. *Let $q = p^r$ be a power of the prime p. Then:*

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

(ii) If $p \geq 5$, then $\mu_p^{\mathrm{sym}}(n) \leq 3\left(1 + \frac{8}{3p-5}\right)n.$

These bounds are based on heretofore unpublished work of Arnaud: in fact, we improve his bounds by using the same general principle, namely the algorithm that is introduced in Corollary 1.5 applied to two Garcia-Stichtenoth towers of function fields.

Nevertheless, thanks to a more accurate study of the number of multiplications in the ground field, we are able to obtain a better bound for $\mu_q^{\mathrm{sym}}(n)$ and $\mu_p^{\mathrm{sym}}(n)$.

Second, we give a detailed proof of two previously known, but also unpublished bounds that were obtained by Arnaud in his thesis [**1**]. These bounds hold for extensions of square finite fields and are the following:

THEOREM 1.7. *Let $q = p^r$ be a power of the prime p. Then:*

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

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

Note that even though bound (i) was established in 2006, it has never been published in any journal. The proof that is given in this paper is more complete than the one that can be found in [**1**]. Arnaud also gave bounds which are similar to bound (ii), but with $p-2$ as denominator. Unfortunately, this denominator is slightly overestimated under Arnaud's hypotheses and no calculation is given to prove it in [**1**]. Thus we give a corrected version with a detailed proof. These two bounds, together with those of Theorem 1.6, rely on a detailed study and careful calculations in the towers that are presented in §2.1.

The last section of this paper is devoted to a discussion of an unproven assumption on a family of Shimura curves that has been used by various authors to established some asymptotic bounds, admitted to be the current benchmarks. We first explained how critical the unproven assumption is and give counter-examples to emphasize its non-triviality. Moreover, we show which published bounds should no longer be considered as proven.

Our paper therefore consists of two main parts, Section 2 and Section 3, which are widely independent, but both devoted to a reappraisal of the state of the art of the bounds for the tensor rank in finite fields.

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. An improved version of Corollary 1.5 is applied to the algebraic function fields of these towers to obtain new bounds for the bilinear complexity. A given curve cannot be used for multiplication 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 suitable curve, it will be desirable to have a tower for which the quotients of two consecutive genera are as small as possible, or in other words 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 $N_k(F/\mathbb{F}_q)$ the number of places of degree k in $F/\mathbb{F}_q$.

2.1.1. *A Garcia-Stichtenoth tower of Artin-Schreier function field extensions.* We now present a modified Garcia-Stichtenoth tower (cf. [**23, 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 elementary abelian tower over $\mathbb{F}_{q^2}$ after Garcia-Stichtenoth [**23**]. This is 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. Then we have the following formulae:

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

As in [**3**], let us consider the completed Garcia-Stichtenoth tower

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

It has the property 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 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 $\mathbb{F}_q$. It is related to the tower T_2 by

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

In other words, $F_{k,s}$ can be obtained from $G_{k,s}$ by extending the constant field from $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$. 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) $\big(g_k - 1\big)p^s + 1 \leq g_{k,s} \leq \frac{g_{k+1}}{p^{r-s}} + 1$,

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

2.1.2. *A 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 [**24**]:

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

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

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

2.2. Some preliminary results. We now proceed to establish some technical results on the genus and number of places of the steps 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 the previous section. These results will allow us to determine a suitable step of the tower to which we can apply the algorithm.

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 2.2. *Let $q > 3$. We have the following bounds on the genus for the steps 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 is odd, 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 $g_k > q^k$.

On the other hand, if k is even, 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) This follows from Formula (3) since for all $k \geq 1$ we have $2q^{\frac{k-1}{2}} \geq 1$, which deals with the case of odd k, and $\frac{3}{2}q^{\frac{k}{2}} + q^{\frac{k}{2}-1} \geq 1$ which deal with the case of even k since $\frac{1}{2}q \geq \sqrt{q}$.

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

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

Otherwise we have that $s < r$. Then 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) This 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 $k \geq 2$. $\square$

LEMMA 2.3. *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 $N_{k,s} := N_1(F_{k,s}/\mathbb{F}_{q^2}) = N_1(G_{k,s}/\mathbb{F}_q) + 2N_2(G_{k,s}/\mathbb{F}_q)$. One has:*

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

Proof. *(i)* From the Riemann–Hurwitz 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 the Riemann–Hurwitz formula s more times, we get $g_{k,s+1} - g_{k,s} \geq (p-1)p^s\big(g(G_k) - 1\big)$. Thus Lemma 2.2(i) gives that $g_{k,s+1} - g_{k,s} \geq (p-1)p^s q^k$ since $q > 3$ and $k \geq 4$.

(ii) According to Proposition 2.1, one has

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

□

LEMMA 2.4. *Let $N_{k,s} := N_1(F_{k,s}/\mathbb{F}_{q^2}) = N_1(G_{k,s}/\mathbb{F}_q) + 2N_2(G_{k,s}/\mathbb{F}_q)$. For all $k \geq 1$ and $s = 0, \ldots, r$, we have*

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

Proof. From Proposition 2.1 and Lemma 2.2 iii), we get

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

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

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 $N_k := N_1(H_k/\mathbb{F}_{p^2}) = N_1(H_k/\mathbb{F}_p) + 2N_2(H_k/\mathbb{F}_p)$. The following lemma follows from Formulae (4) and (6):

LEMMA 2.5. *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 2.6. *For all $k \geq 0$, we set $\Delta g_k := g_{k+1} - g_k$. Then one has $\Delta g_k \geq 2^{k+1} - 2^{\frac{k+1}{2}}$ and $N_k \geq \frac{4}{3}\Delta g_k$ (so we also have that $N_k \geq \Delta g_k$).*

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 first equality holds trivially. Moreover, since $p \geq 3$, the first second follows from the bounds (5) and (6) which gives $N_k \geq 2^{k+2} > 2\Delta g_k$. □

LEMMA 2.7. *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 the bounds (5) and (6) for N_k and Lemma 2.5(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 2.8. *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 §2.1, that is to say a step that will be optimal for the bilinear complexity of multiplication:

LEMMA 2.9. *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 $s \in \{0, \dots, r\}$. First, we prove that condition (2) is verified. Lemma 2.2(iv) gives:

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

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 ensures that condition (2) is satisfied according to Corollary 5.2.10 in [**40**].

Now suppose in addition 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 by using Theorem 2.8, since $q \geq 4$ and $g_{k,s} \geq g_2 \geq 6$ according to Formula (3).

□

The similar result for the tower $T_3/\mathbb{F}_q$ is as follows:

LEMMA 2.10. *Let $n \geq \frac{1}{2}(q+1+\epsilon(q))$ 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 2.8 since $q \geq 4$ and $g_{k,s} \geq g_2 \geq 6$ according to Formula (3).

To complete the proof, we deal with 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 $n \geq \frac{1}{2}(q+1+\epsilon(q))$ 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 [**17**] 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
$\frac{1}{2}(q+1+\epsilon(q))$	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
$\frac{1}{2}(q+1+\epsilon(q))$	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
$q^{\frac{n-1}{2}}(\sqrt{q}-1) \geq \ldots$	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 2.8,
- $2g_{k,s}+1 \leq q^{\frac{n-1}{2}}(\sqrt{q}-1)$ 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.

□

The similar result for the tower $T/\mathbb{F}_{p^2}$ is as follows:

LEMMA 2.11. *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 [**41**]. 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 $k+2 \leq \log_2\big(4(p^{n-1}-1)\big) \leq \log_2(4p^{n-1}-1)$ 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 2.5(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 the bound (5) and Lemma 2.5(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 $\big[\log_2(2n-1)-2; n-2\big]$. Indeed, $\log_2(2 \cdot 18-1)-2 \approx 3.12 > 2$, the size of this interval increases with n, and it is larger than 1 for $n = 18$. To conclude, remark that for such an integer k, condition (1) is easily verified from Theorem 2.8 since $p^2 \geq 4$ and $g_k \geq g_2 = 3$ according to Formula (4).

□

The similar result for the tower $T/\mathbb{F}_p$ is as follows:

LEMMA 2.12. *Let $p \geq 5$ and $n \geq \frac{1}{2}(p+1+\epsilon(p))$. 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 that condition (2) is verified according to Corollary 5.2.10 in [**41**]. 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 2.5(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 $\big[\log_2(2n-1)-2; n-3\big]$ 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 2.8 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 at places of degree one (respectively places of degree one and two). The upcoming first theorem can be found in Arnaud's thesis [**1**], but since the proof is rather short, we give it in order for this article to be self-contained.

THEOREM 2.13. *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 $\mathcal{P}:=\{P_1,\ldots,P_N\}$ be a set of N places of degree 1 and $\mathcal{P}'$ be a subset of $\mathcal{P}$ of cardinality a. According to Lemma 2.7 in [**7**], we can choose an effective 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 1.4 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 $\dim(\mathcal{D}-Q)=\dim(\mathcal{R})=0$ and $\dim(\mathrm{Im}\,Ev_Q)=\dim\mathcal{D}=\deg\mathcal{D}-g+1+i(\mathcal{D})\geq n$ according to the Riemann-Roch Theorem. Thus $\dim(\mathrm{Im}\,Ev_Q)=n$. Moreover, $Ev_{\mathcal{P}}$ is injective. Indeed, $\ker Ev_{\mathcal{P}}=\mathcal{L}(2\mathcal{D}-\sum_{i=1}^N u_iP_i)$ with $\deg(2\mathcal{D}-\sum_{i=1}^N u_iP_i)=2(n+g-1)-N-a<0$. Furthermore, one has $\mathrm{rank}\,Ev_{\mathcal{P}}=\dim(2\mathcal{D})=\deg(2\mathcal{D})-g+1+i(2\mathcal{D})$, and $i(2\mathcal{D})=0$ since $2\mathcal{D}\geq\mathcal{D}\geq\mathcal{R}$ with $i(\mathcal{R})=0$. So $\mathrm{rank}\,Ev_{\mathcal{P}}=2n+g-1$, and we can extract a subset $\mathcal{P}_1$ of $\mathcal{P}$ and a subset $\mathcal{P}_1'$ of $\mathcal{P}'$ 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 1.4, this leads to $\mu_q(n)\leq N_1+2a_1\leq N_1+a_1+a$, which gives the result. □

This second theorem is a refinement of [**1**, Theorem 3.8], that will allow us to improve Arnaud's bound for $\mu_q^{\mathrm{sym}}(n)$ and $\mu_p^{\mathrm{sym}}(n)$ in the next paragraph.

THEOREM 2.14. *Let $q>2$ 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

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

Remark. Under the same hypotheses, the bounds obtained in [**1**, Theorem 3.8] are $\mu_q^{\mathrm{sym}}(n)\leq 2n+2g+N_2+a_1+4a_2$ and $\mu_q^{\mathrm{sym}}(n)\leq 3n+3g+\frac{a_1}{2}+3a_2$.

Proof. We use the same notation as in Corollary 1.5: $\mathcal{P}:=\{P_1,\ldots,P_{N_1}\}$ is a set of N_1 places of degree one and $\mathcal{P}':=\{R_1,\ldots,R_{N_2}\}$ is a set of N_2 places of degree two. According to hypothesis (iii), one can always reduce to the case where

$$2n+2g-1\leq N_1+a_1+2(N_2+a_2)\leq 2n+2g. \tag{8}$$

According to Lemma 2.7 in [**7**], we can choose an effective divisor $\mathscr{D}$ equivalent to $Q+\mathscr{R}$ such that $\operatorname{supp}(\mathscr{D})\cap(\mathscr{P}\cup\mathscr{P}')=\emptyset$. We then define the maps Ev_Q and $Ev_{\mathscr{P},\mathscr{P}'}$ as in Corollary 1.5 but for the second one, we fix $\mathbb{F}_q^{N_1+a_1+2(N_2+a_2)}$ as codomain instead of $\mathbb{F}_q^{N_1}\times\mathbb{F}_q^{a_1}\times\mathbb{F}_{q^2}^{N_2}\times\mathbb{F}_{q^2}^{a_2}$ (this means that we choose a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and take the components of each element of $\mathbb{F}_{q^2}$ with respect to this basis).

The same reasoning as in the previous proof shows that Ev_Q is bijective. Moreover, the map $Ev_{\mathscr{P},\mathscr{P}'}$ is injective since

$$\ker Ev_{\mathscr{P}}=\mathscr{L}\left(2\mathscr{D}-\left(\sum_{i=1}^{N_1}P_i+\sum_{i=1}^{a_1}P_i+\sum_{i=1}^{N_2}R_i+\sum_{i=1}^{a_2}R_i\right)\right)$$

with $\deg\left(2\mathscr{D}-\left(\sum_{i=1}^{N_1}P_i+\sum_{i=1}^{a_1}P_i+\sum_{i=1}^{N_2}R_i+\sum_{i=1}^{a_2}R_i\right)\right)<0$ from hypothesis (iii). Furthermore, one has $\operatorname{rank}Ev_{\mathscr{P},\mathscr{P}'}=\dim(2\mathscr{D})=\deg(2\mathscr{D})-g+1+i(2\mathscr{D})$, and $i(2\mathscr{D})=0$ since $2\mathscr{D}\geq\mathscr{D}\geq\mathscr{R}$ with $i(\mathscr{R})=0$. So $\operatorname{rank}Ev_{\mathscr{P},\mathscr{P}'}=2n+g-1$. Thus, $Ev_{\mathscr{P},\mathscr{P}'}$ being injective with rank $2n+g-1$, it follows that one can choose a suitable subset of coordinates of size $2n+g-1$ (among the $N_1+a_1+2(N_2+a_2)$ ones in $\mathbb{F}_q^{N_1+a_1+2(N_2+a_2)}$) of any element in the image to define its preimage.

Now we will focus on the number of multiplications in $\mathbb{F}_q$ needed to define the $2n+g-1$ coordinates of the image of a product fg for $f,g\in\mathscr{L}(2\mathscr{D})$, from the coordinates of the images of f and g. Note that we will need more than the two subsets of $2n+g-1$ coordinates from $Ev_{\mathscr{P},\mathscr{P}'}(f)$ and $Ev_{\mathscr{P},\mathscr{P}'}(g)$ to compute the coordinates of the image fg. But in the end, we need only $2n+g-1$ of these coordinates to define the preimage of fg in $\mathscr{L}(2\mathscr{D})$. There are 4 types of such “useful” coordinates:

(a) those which come from a classical evalution over a place of degree 1, such as $f(P_1)$; we denote the number of such coordinates by L_1.
(b) those which come from a derivated evalution over a place of degree 1, such as $f'(P_1)$; we denote the number of such coordinates by ℓ_1.
(c) those which come from a classical evalution over a place of degree 2, such as both coordinates in $\mathbb{F}_q$ of $f(R_1)$; we denote the number of such coordinates by L_2.
(d) those which come from a derivated evalution over a place of degree 2, such as both coordinates in $\mathbb{F}_q$ of $f'(R_1)$; we denote the number of such coordinates by ℓ_2.

With these notations, we have that:

$$L_1+\ell_1+L_2+\ell_2=2n+g-1 \tag{9}$$

with

$$L_1\leq N_1,\quad \ell_1\leq a_1,\quad L_2\leq 2N_2\quad\text{and}\quad \ell_2\leq 2a_2. \tag{10}$$

Now we will estimate how many multiplications in $\mathbb{F}_q$ are needed to compute each type of coordinate for the image of the product fg.

- to obtain a type (a) coordinate, we need 1 multiplication in $\mathbb{F}_q$ since
$$(fg)(P_i)=f(P_i)\cdot g(P_i)\quad\text{with } f(P_i),g(P_i)\in\mathbb{F}_q.$$
- to obtain a type (b) coordinate, we need 2 multiplications in $\mathbb{F}_q$ since
$$(fg)'(P_i)=f'(P_i)\cdot g(P_i)+f(P_i)\cdot g'(P_i)\quad\text{with } f(P_i),g(P_i),f'(P_i),g'(P_i)\in\mathbb{F}_q.$$
- to obtain a type (c) coordinate, we need 2 multiplications in $\mathbb{F}_q$. Indeed, this type of coordinate is only one of the two coordinates in $\mathbb{F}_q$ of an element in $\mathbb{F}_{q^2}$. For example, if we denote by $\left(f(R_i)_1,f(R_i)_2\right)$ the two coordinates in $\mathbb{F}_q$

of the vector which represents $f(R_i) \in \mathbb{F}_{q^2}$, in a $\mathbb{F}_q$-basis $(1, \alpha)$ of $\mathbb{F}_{q^2}$ where $\alpha^2 = -1$, we get

$$(fg)(R_i)_1 = f(R_i)_1 \cdot g(R_i)_1 - f(R_i)_2 \cdot g(R_i)_2$$

for the first coordinate, or

$$(fg)(R_i)_2 = f(R_i)_1 \cdot g(R_i)_2 + f(R_i)_2 \cdot g(R_i)_1$$

for the second one.

- to obtain a type (d) coordinate, we need 4 multiplications in $\mathbb{F}_q$ since we have to determine either $U \in \mathbb{F}_q$ or $V \in \mathbb{F}_q$ such that:

$$(fg)'(R_i) = f'(R_i) \cdot g(R_i) + f(R_i) \cdot g'(R_i) = U + \alpha V$$

so we need to compute

$$U = f(R_i)_1 \cdot g'(R_i)_1 - f(R_i)_2 \cdot g'(R_i)_2 + g(R_i)_1 \cdot f'(R_i)_1 - g(R_i)_2 \cdot f'(R_i)_2$$

or

$$V = f(R_i)_2 \cdot g'(R_i)_1 + f(R_i)_1 \cdot g'(R_i)_2 + g(R_i)_2 \cdot f'(R_i)_1 + g(R_i)_1 \cdot f'(R_i)_2.$$

So far, it seems that we need $L_1 + 2\ell_1 + 2L_2 + 4\ell_2$ multiplications in $\mathbb{F}_q$ to obtain the $L_1 + \ell_1 + L_2 + \ell_2 = 2n + g - 1$ coordinates of a product, which would be bounded by $N_1 + 2a_1 + 4N_2 + 8a_2$ according to (10). We have to be a bit more precise to obtain a better bound. Indeed, when we use more than half the coordinates in $\mathbb{F}_q$ coming from places of degree 2, we know that we can be more efficient since we will have to compute some coordinates which come from the same evaluation. Namely, if we know that we will have to compute both $(fg)(R_i)_1$ and $(fg)(R_i)_2$ for some i, then we would not need $2 \cdot 2 = 4$ multiplications in $\mathbb{F}_q$, but only 3, thanks to Karatsuba algorithm. The same reasonning holds for derivated evalutations at places of degree 2: if we need to compute both $(fg)'(R_i)_1$ and $(fg)'(R_i)_2$, then we would not need $2 \cdot 4 = 8$ multiplications in $\mathbb{F}_q$ but only 6.

We therefore have to distinguish cases were we know how many "paired" coordinates we have. Here is how we proceed:

	$L_2 \leq N_2$	$N_2 < L_2 \leq 2N_2$
$\ell_2 \leq a_2$	Case 1	Case 2
$a_2 < \ell_2 \leq 2a_2$	Case 3	Case 4

Thus, for the L_2 type (c) coordinates, we know that in cases 1 and 3, there are at least $2(L_2 - N_2)$ "paired" coordinates (since $L_2 \leq N_2$), and that each couple requires 3 multiplications in $\mathbb{F}_q$, so we perform $3(L_2 - N_2)$ such multiplications. The remaining $2N_2 - L_2$ coordinates have to be computed independently: it costs 2 multiplications in $\mathbb{F}_q$ for each.

The same reasoning applies to the type (d) coordinates in cases 2 and 4: since $N_2 < L_2 \leq 2N_2$, there are $2(L_2 - N_2)$ coordinates which can be computed "pairwise", each couple needing 3 multiplications in $\mathbb{F}_q$, so we perform $3(L_2 - N_2)$ multiplications in $\mathbb{F}_q$. The remaining $2N_2 - L_2$ coordinates have to be computed independently; it costs 4 multiplications in $\mathbb{F}_q$ for each.

From this reasoning and the inequalities (9) and (10), we get the following bounds for the obtention of the $2n + g - 1$ coordinates of a product:

Case 1:

$$\begin{aligned} L_1+2\ell_1+2L_2+4\ell_2 &= (L_1+\ell_1+L_2+\ell_2)+\ell_1+L_2+3\ell_2 \\ &\leq 2n+g-1+a_1+N_2+3a_2 \end{aligned}$$

Case 2:

$$\begin{aligned} L_1+2\ell_1+3(L_2-N_2)+2(2N_2-L_2)+4\ell_2 &= L_1+2\ell_1+N_2+L_2+4\ell_2 \\ &= (L_1+\ell_1+L_2+\ell_2)+\ell_1+N_2+3\ell_2 \\ &\leq 2n+g-1+a_1+N_2+3a_2 \end{aligned}$$

Case 3:

$$\begin{aligned} L_1+2\ell_1+2L_2+6(\ell_2-a_2)+4(2a_2-\ell_2) &= L_1+2\ell_1+2L_2+2(a_2+\ell_2) \\ &= (L_1+\ell_1+L_2+\ell_2)+\ell_1+L_2+\ell_2+2a_2 \\ &\leq 2n+g-1+a_1+N_2+4a_2 \end{aligned}$$

Case 4:

$$\begin{aligned} & L_1+2\ell_1+3(L_2-N_2)+2(2N_2-L_2)+6(\ell_2-a_2)+4(2a_2-\ell_2) \\ = \; & L_1+2\ell_1+L_2+N_2+2(a_2+\ell_2) \\ = \; & (L_1+\ell_1+L_2+\ell_2)+\ell_1+N_2+\ell_2+2a_2 \\ \leq \; & 2n+g-1+a_1+N_2+4a_2 \end{aligned}$$

Thus $2n+g-1+a_1+N_2+4a_2$ is a bound which holds in all the four cases, so it gives an upper bound for the minimal number of multiplications in $\mathbb{F}_q$ needed to obtain the $2n+g-1$ coordinates in $\mathbb{F}_q$ necessary to define a preimage by $Ev_{\mathscr{P},\mathscr{P}'}$ of an element $Ev_{\mathscr{P},\mathscr{P}'}(fg) \in \mathbb{F}_q^{N_1+a_1+2(N_2+a_2)}$. Thus we have that

$$\mu_q^{\mathrm{sym}}(n) \leq 2n+g-1+a_1+N_2+4a_2.$$

The second bound of the theorem comes from (8), which implies that $\frac{a_1}{2}+N_2+a_2 \leq n+g$, and therefore

$$2n+g-1+a_1+N_2+4a_2 \leq 3n+2g+\frac{a_1}{2}+3a_2.$$

□

2.4. Proof of the upper bounds stated in the introduction. Here we give the detailed proof of Theorems 1.6 and 1.7 by combining the results of the previous section. We use the same notations concerning the number of places and the genera of curves in the towers. Recall that depending on the tower under consideration the following holds:

- $N_{k,s} := N_1(F_{k,s}/\mathbb{F}_{q^2}) = N_{k,s} = N_1(G_{k,s}/\mathbb{F}_q) + 2N_2(G_{k,s}/\mathbb{F}_q)$
- $N_k := N_1(H_k/\mathbb{F}_{p^2}) = N_1(H_k/\mathbb{F}_p) + 2N_2(H_k/\mathbb{F}_p)$
- $\Delta g_{k,s} := g_{k,s+1} - g_{k,s}$ and $\Delta g_k := g_{k+1} - g_k$
- $D_{k,s} := (p-1)p^s q^k$.

Proof of Theorem 1.6.

(i) Let $n \geq \frac{1}{2}(q+1+\epsilon(q))$; in the complementary case, we already know from Section 1.2 that $\mu_q^{\mathrm{sym}}(n) \leq 2n$. According to Lemma 2.10, there exists a step of the tower $T_3/\mathbb{F}_q$ to which we can apply Theorem 2.14 with $a_1 = a_2 = 0$. We denote by $G_{k,s+1}/\mathbb{F}_q$ the first step of the tower that satisfies the hypotheses of Theorem 2.14 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 $N_{k,s} \geq 2n_0^{k,s} + 2g_{k,s} - 1$, so that we have the equality $n_0^{k,s} = \sup\left\{n \in \mathbb{N} \,|\, 2n \leq N_{k,s} - 2g_{k,s} + 1\right\}$. To perform multiplication in $\mathbb{F}_{q^n}$, we have the following alternative approaches:

(a) use the algorithm at step $G_{k,s+1}$. In this case, a bound for the bilinear complexity is given by Theorem 2.14 applied with $a_1 = a_2 = 0$:
$$\mu_q^{\mathrm{sym}}(n) \leq 3n + 2g_{k,s+1} = 3n_0^{k,s} + 2g_{k,s} + 3(n - n_0^{k,s}) + 2\Delta g_{k,s}.$$

(b) use the algorithm on the step $G_{k,s}$ with an appropriate number of derivative evaluations. Let $a_1 + 2a_2 := 2(n - n_0^{k,s})$ 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 , if $a_1 + 2a_2 \leq N_{k,s}$, we can perform $a_1 + a_2$ derivative evaluations in the algorithm using the step $G_{k,s}$ and we have:
$$\mu_q^{\mathrm{sym}}(n) \leq 3n + 2g_{k,s} + \frac{3}{2}(a_1 + 2a_2) = 3n_0^{k,s} + 2g_{k,s} + 6(n - n_0^{k,s}).$$

Thus if $a_1 + 2a_2 \leq N_{k,s}$, then case (b) gives a better bound as soon as $n - n_0^{k,s} < \frac{2}{3}\Delta g_{k,s}$. So we have from Lemma 2.3, with $\tilde{D}_{k,s} := \frac{3}{4}D_{k,s}$: $N_{k,s} \geq \frac{4}{3}\tilde{D}_{k,s}$ and $\Delta g_{k,s} \geq \tilde{D}_{k,s}$. Hence if $a_1 + 2a_2 < \frac{4}{3}\tilde{D}_{k,s}$ (i.e. $2(n - n_0^{k,s}) < \frac{4}{3}\tilde{D}_{k,s}$), then we both have that $2(n - n_0^{k,s}) < \frac{4}{3}\Delta g_{k,s}$ and $a_1 + 2a_2 \leq N_{k,s}$. We can therefore perform a_1 derivative evaluations at places of degree 1 and a_2 derivative evaluations at places of degree 2 in the step $G_{k,s}$ and case (b) gives a better bound than case (a). Moreover, $a_1 + 2a_2 < \frac{4}{3}\tilde{D}_{k,s}$ is equivalent to $n - n_0^{k,s} < D_{k,s}$.

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

We define the function Φ for $x \geq 0$ to be 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 pieces: 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 $\left(n_0^{k,s} + D_{k,s}, \Phi(n_0^{k,s} + D_{k,s})\right)$, since these are the vertices of the graph. If we let $X := n_0^{k,s} + D_{k,s}$, then
$$\begin{aligned} \Phi(X) &\leq 3X + 2g_{k,s+1} \\ &= 3\left(1 + \frac{2g_{k,s+1}}{3X}\right)X. \end{aligned}$$

We want to give a bound for $\Phi(X)$ that is independent of k and s. Recall that $D_{k,s} := (p-1)p^s q^k$, and
$$n_0^{k,s} \geq \frac{1}{2}q^{k-1}p^s(q+1)(q-3) \quad \text{by Lemma 2.4}$$

and

$$g_{k,s+1} \leq q^{k-1}(q+1)p^{s+1} \quad \text{by Lemma 2.2 (iii).}$$

So we have

$$\begin{aligned}
\frac{2g_{k,s+1}}{3X} &= \frac{2g_{k,s+1}}{3(n_0^{k,s}+D_{k,s})} \\
&\leq \frac{2q^{k-1}(q+1)p^{s+1}}{3(\frac{1}{2}q^{k-1}p^s(q+1)(q-3)+(p-1)p^sq^k)} \\
&= \frac{2q^{k-1}(q+1)p^sp}{q^{k-1}(q+1)p^s\left(\frac{3}{2}(q-3)+3(p-1)\frac{q}{q+1}\right)} \\
&= \frac{\frac{4}{3}p}{(q-3)+2(p-1)\frac{q}{q+1}}.
\end{aligned}$$

Thus the graph of the function Φ lies below the line $y = 3\left(1+\frac{\frac{4}{3}p}{(q-3)+2(p-1)\frac{q}{q+1}}\right)x$. In particular, we obtain

$$\Phi(n) \leq 3\left(1+\frac{\frac{4}{3}p}{(q-3)+2(p-1)\frac{q}{q+1}}\right)n.$$

(ii) Let $n \geq \frac{1}{2}(p+1+\epsilon(p))$; in the complementary case, we already know from Section 1.2 that $\mu_p^{\mathrm{sym}}(n) \leq 2n$. According to Lemma 2.12, there exists a step of the tower $T/\mathbb{F}_p$ on which we can apply Theorem 2.14 with $a_1 = a_2 = 0$. We denote by $H_{k+1}/\mathbb{F}_p$ the first step of the tower that satisfies the hypotheses of Theorem 2.14 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 we have $N_k \geq 2n_0^k+2g_k-1$, 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 approaches:

(a) use the algorithm at the step H_{k+1}. In this case, a bound for the bilinear complexity is given by Theorem 2.14 applied with $a_1 = a_2 = 0$:

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

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

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

Thus, if $a_1 + 2a_2 \leq N_{k,s}$, then case (b) gives a better bound as soon as $n - n_0^{k,s} < \frac{2}{3}\Delta g_{k,s}$.

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 follows:

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

Note that when case (b) gives a better bound, that is to say when $\frac{3}{2}(x-n_0^k) < \Delta g_k$, then according to Lemma 2.6 we also have that

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

since $\frac{4}{3}\Delta g_k \leq N_k$. We can therefore proceed as in case (b), since there are enough places of degree 1 and 2 at which we can perform $a_1+a_2 = 2(x-n_0^k)$ derivative evaluations on.

We define the function Φ for $x \geq 0$ to be 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 pieces: 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 $\left(n_0^k+\frac{2}{3}\Delta g_k, \Phi(n_0^k+\frac{2}{3}\Delta g_k)\right)$, since these are the vertices of the graph. If we let $X := n_0^k+\frac{2}{3}\Delta g_k$, then

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

We want to give a bound for $\Phi(X)$ that is independent of k. Lemmas 2.5(ii), 2.6 and 2.7 give:

$$\begin{aligned} \frac{2g_{k+1}}{3X} &\leq \frac{2^{k+3}}{3\left(2^k(p-3)+2+\frac{2}{3}(2^{k+1}-2^{\frac{k+1}{2}})\right)} \\ &= \frac{8\cdot 2^k}{2^k\left(3(p-3)+3\cdot 2^{-k+1}+4(1-2^{-\frac{k+1}{2}})\right)} \\ &= \frac{8/3}{p-3+\frac{4}{3}+2^{-k+1}-\frac{1}{3}2^{-\frac{k-3}{2}}} \\ &\leq \frac{8/3}{p-\frac{5}{3}} \end{aligned}$$

since $2^{-k+1}-\frac{1}{3}2^{-\frac{k-3}{2}} \geq 0$. Thus the graph of the function Φ lies below the line $y = 3\left(1+\frac{8}{3p-5}\right)x$. In particular, we obtain

$$\Phi(n) \leq 3\left(1+\frac{8}{3p-5}\right)n.$$

□

Proof of Theorem 1.7.

(i) Let $n \geq \frac{1}{2}(q^2+1+\epsilon(q^2))$; in the complementary case, we already know from the pioneering works recalled in Section 1.2 that $\mu_{q^2}^{\text{sym}}(n) \leq 2n$. According to Lemma 2.9, there exists a step of the tower $T_2/\mathbb{F}_{q^2}$ at which we can apply Theorem 2.13 with $a = 0$. We denote by $F_{k,s+1}/\mathbb{F}_{q^2}$ the first step of the tower that satisfies the hypotheses of Theorem 2.13 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. $n_0^{k,s} = \sup\left\{n \in \mathbb{N} \mid 2n \leq N_{k,s} - 2g_{k,s} + 1\right\}$. To perform multiplication in $\mathbb{F}_{q^{2n}}$, we have the following alternative approaches:

(a) use the algorithm at the step $F_{k,s+1}$. In this case, a bound for the bilinear complexity is given by Theorem 2.13 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 at 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 2.13 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 $a \leq N_{k,s}$, then case (b) gives a better bound as soon as $a < \Delta g_{k,s}$. Since Lemma 2.3 gives the inequalities $N_{k,s} \geq D_{k,s}$ and $\Delta g_{k,s} \geq D_{k,s}$, we know that if $a \leq D_{k,s}$, then we can perform a derivative evaluations on places of degree 1 in the step $F_{k,s}$. This implies that case (b) gives a better bound than 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 follows:

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

We define the function Φ for $x \geq 0$ to be 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 pieces: 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. If we let $X := n_0^{k,s} + \frac{D_{k,s}}{2}$, then we have

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

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

$$2n_0^{k,s} \geq q^{k-1}p^s(q+1)(q-3) \quad \text{by Lemma 2.4}$$

and

$$g_{k,s+1} \leq q^{k-1}(q+1)p^{s+1} \quad \text{by Lemma 2.2 (iii).}$$

So we have

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

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 obtain

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

(ii) Let $n \geq \frac{1}{2}(p^2+1+\epsilon(p^2))$; in the complementary case, we already know from Section 1.2 that $\mu_{p^2}^{\mathrm{sym}}(n) \leq 2n$. According to Lemma 2.11, there exists a step of the tower $T/\mathbb{F}_{p^2}$ at which we can apply Theorem 2.13 with $a=0$. We denote by $H_{k+1}/\mathbb{F}_{p^2}$ the first step of the tower that satisfies the hypotheses of Theorem 2.13 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 $N_k\geq 2n_0^k+2g_k-1$, so that we have the equality $n_0^k=\sup\left\{n\in\mathbb{N}\,|\,2n\leq N_k-2g_k+1\right\}$. To perform multiplication in $\mathbb{F}_{p^{2n}}$, we have the following alternative approaches:

(a) use the algorithm at the step H_{k+1}. In this case, a bound for the bilinear complexity is given by Theorem 2.13 applied with $a=0$:

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

(b) use the algorithm at 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 2.13 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 $a\leq N_k$, then 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 follows:

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

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 2.6 we also have that

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

so that we can proceed as in case (b) since there are enough rational places at which we can take $a = 2(x - n_0^k)$ derivative evaluations on.

We define the function Φ for $x \geq 0$ to be 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 pieces: 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. If we 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 2.5 ii), 2.6 and 2.7 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 obtain

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

□

3. Note on some unproven bounds

In this section, we discuss a result in the paper [**12**] that to us seems to be still unproven, and the consequences of this gap for some asymptotic bounds that were based on this assertion.

3.1. The result in question. The following assertion is a folklore conjecture. It states that there exist curves which, seen over an extension of the base field, have many points. In the form [**12**, Lemma IV.4], it is given as follows:

ASSERTION 3.1. *Let p be a prime number. For each even positive integer $2t$, there exists a family X_s of curves:*

(i) defined over $\mathbb{F}_p$;
(ii) whose genera tend to infinity and grow slowly: $g_{s+1}/g_s \longrightarrow 1$;
(iii) whose number of $\mathbb{F}_{p^{2t}}$-points is asymptotically optimal (i.e. the ratio of this number to the genus tends to $p^t - 1$).

Thus, by Lemma IV.3 of the same paper [**12**], the family X_s attains the generalized Drinfeld-Vladut bound for the number of points of degree $2t$. The paper [**12**] claims to give a proof for this assertion.

3.2. Our criticism in a nutshell. The main problem in reading of [**12**, Lemma IV.4] is that the claims in the proof of said Lemma are not only highly ambiguous, but also incorrect in general. The Shimura curves considered in *loc. cit.* have Atkin-Lehner automorphisms, which in general leads to descent obstructions and the existence of twists. These issues are not dealt with or even mentioned by the authors, who state without proof that their Shimura curves are defined over $\mathbb{Q}$. This forms a sufficiently serious problem to invalidate their proof, at least in our analysis so far.

In what follows, we will discuss how we have tried to read the claims by the authors in the most canonical way possible, which leads to the following claim:

Claim A. The canonical model of a Shimura curve descends to $\mathbb{Q}$.

In general, Claim A is incorrect; we give a counterexample below in Section 3.6. Note that the results [**12**, Theorem IV.6, Theorem IV.7, Corollary IV.8], [**11**, Theorem 5.18, Corollary 5.19] and [**30**, Theorem 5.3, Corollary 5.4, Corollary 5.5] depend on the aforementioned Lemma IV.3 of [**12**].

3.3. Hypotheses of the Lemma and some further restrictions. Here we describe the complex analytic quotients of [**12**]. We will narrow our hypotheses as we go, even beyond those in *loc. cit.* This is both in order to simplify the presentation and to exclude some cases in which the statement of the Lemma is clearly false (such as those in which the quaternion algebra is ramified at primes over p).

- Again, p is any prime number (the one by which the curve is to be reduced), and t any integer ($2t$ being the degree for which one wants the reduction to have an optimal number of $\mathbb{F}_{p^{2t}}$-rational points).
- We fix any totally real field F of degree t, in which p is inert. Choose an embedding $\iota_\infty : F \hookrightarrow \mathbb{R}$, under which F will be seen as a subfield of $\mathbb{R}$.
- Finally, fix any given set of finite places $\mathfrak{p}_i$ of F not above p,[1] provided that their number plus $t-1$ is even. Call $\mathfrak{D}^f$ their product.
- Now, consider B the quaternion algebra over F which is ramified at exactly every real place other than ι_∞ and all the finite places in $\mathfrak{D}^f$.
- We impose the following further requirements, the first of which is demanded in [**12**] as well:
  - $\mathfrak{D}^f$ is Galois-invariant.
  - B has one single conjugacy class of maximal orders (a sufficient condition for this being that F has narrow class number 1).

  The corollary of [**20**] then implies that the Shimura curves considered here will have field of moduli equal to $\mathbb{Q}$ (if it were not the case, then the curves would certainly not descend to $\mathbb{Q}$).

[1]Notice that the authors do not exclude discriminants $\mathfrak{D}^f$ with support meeting p. Furthermore, in the cases the parity condition allows this, the authors even suggest to choose the discriminant equal to the set of primes above p. (Note that p being inert, this set has one element). Thus, everything is made for the Shimura curves to have bad reduction at p (see for example [**38**, Theorem 3.1.6]). But this contradicts what is stated later in the paper. So we will not consider this case. What the authors might actually have meant here is: $\mathfrak{D}^f$ equal to a prime *not* above p (this is exactly the requirement asked by [**35**], to which the authors refer for this suggestion).

- Choose a maximal order $\mathcal{O}$ in B. Finally, consider the action of the subgroup of norm one units $\mathcal{O}^1$ on the upper half-plane[2], induced by

$$\mathcal{O}^1 \xrightarrow{\iota_\infty} SL_2(\mathbb{R}) \xrightarrow{\text{mod}\pm} PSL_2(\mathbb{R})$$

and call Y_0^1 the corresponding compact complex analytic quotient.
- Finally, counterexamples are even simpler if one restricts to fields F with narrow class number 1. Indeed, under this additional condition, the curves Y_0^1 then coincide with Y_0^+ (see [**36**, Proposition 3.2.1] and the survey below). Thus, they have canonical models available in the literature, and moreover defined over $F^\infty = F$.

3.4. Classical results on Shimura curves. A first line of ideas originates from the main theorem of Shimura [**32**, Theorem I §3.2], that gives canonical models for certain quotients of the upper half plane, $Y^+(l)$, which have good reduction above p (by the main result of [**29**]). These models are defined over the ray class $\mathrm{Cl}((l).\infty)$-extension of F. With the help of canonical models of Shimura for more general quotients of the upper half plane [**33**], Ihara builds a family of curves with arbitrary large genus, smooth over the ring of (p)-adic integers of $F_{(p)}$ [**25**, §6]; their reduction have an asymptotically optimal number of $\mathbb{F}_{p^{2f}}$-points (see [**25**, (1.4.3)] and also the later note [**26**]).

The second line of ideas uses the construction of Deligne. It can be illustrated following [**21**] and [**38**]. Fix the following notations:

- $\mathcal{O}(l) \subset \mathcal{O}$ the Eichler suborders of level l of the paper (maximal at every finite place, except at the inert prime (l), where they are upper-triangular modulo (l));
- B^+ (resp. $\mathcal{O}(l)^+$) the quaternions (resp. the elements of the order) with totally positive norm;
- $\mathbf{A}^f$ the finite adeles and $\mathcal{H}^\pm$ the union of the upper and lower half-planes.

Consider the double coset space:

$$Y(\mathcal{O}(l)^\bullet_{\mathbf{A}^f}) = B^\bullet \backslash \mathcal{H}^\pm \times B^\bullet_{\mathbf{A}^f} / \mathcal{O}(l)^\bullet_{\mathbf{A}^f}$$

on which $B^\bullet$ acts on $\mathcal{H}^\pm$ and $B^\bullet_{\mathbf{A}^f}$ on the left, and $\mathcal{O}(l)^\bullet_{\mathbf{A}^f}$ acts on $B^\bullet_{\mathbf{A}^f}$ on the right. This space is compact (see [**28**, Example 3.4]) and has a familiar decomposition in connected components. Indeed, consider representatives b_i for the quotient $B^+ \backslash B^\bullet_{\mathbf{A}^f} / \mathcal{O}(l)^\bullet_{\mathbf{A}^f}$ Then, we have (see [**28**, Lemma 5.13]):

$$Y(\mathcal{O}(l)^\bullet_{\mathbf{A}^f}) \cong \bigcup_i Y(b_i \mathcal{O}(l)^+ b_i^{-1}),$$

where $Y(b_i \mathcal{O}(l)^+ b_i^{-1})$ stands for $(b_i \mathcal{O}(l)^+ b_i^{-1}) \backslash \mathcal{H}$. One has a canonical model over F for the total (non connected) curve $Y(\mathcal{O}(l)^\bullet_{\mathbf{A}^f})$ (see [**10**, §1.2]); over the narrow class field, this canonical model becomes a product of conjugates of the component $Y(\mathcal{O}(l)^+)$ containing $[i, 1]$, as in [**38**, (2.9)]. (Note that because we are dealing with an Eichler order we indeed have that $F = F^\infty$, in light of [**38**, Theorem 1.2.1].) One concludes by using the fact that $Y(\mathcal{O}(l)^\bullet_{\mathbf{A}^f})$ has good reduction mod p with many $\mathbb{F}_{p^{2f}}$-points, by [**10**, §11.2 Remarque (3)].

This is the approach of Zink (who studies the reduction of more general canonical models by hand). On the contrary, the present paper uses the more computable-friendly curves $Y(\mathcal{O}(l)^1)$ (popularized by [**22**]). They occur as coverings of the $Y(\mathcal{O}(l)^+)$ but

[2] To make things simple, we do not consider level l suborders of $\mathcal{O}$ here (which means we consider only the case $l = 1$).

they are actually also encompassed by the same theory (in a non-canonical manner, see the tweak described in [**36**, §3.2]).

3.5. The main issue: field of definition versus field of moduli. The paper [**12**] states without further ado that the Shimura curves $Y(\mathcal{O}(l)^+)$ of the previous section are defined over $\mathbb{Q}$. While we do not have a counterexample to this statement, it seems unlikely to hold true in general. It may be true that their field of moduli is $\mathbb{Q}$, but since the curves $Y(\mathcal{O}(l)^+)$ typically have non-trivial automorphisms (namely Atkin-Lehner involutions), there is always a risk that a descent obstruction occurs, and we expect that in general this will happen.

Even if the curve did descend, the resulting models would admit twists, which is to say that there would exists curves over $\mathbb{Q}$ isomorphic with the chosen model over $\mathbb{C}$ but not over $\mathbb{Q}$. In particular, the statement in *loc. cit.* that the model over $\mathbb{Q}$ has good reduction modulo p is meaningless, since it depends on the choice of model.

Moreover, in order to obtain many points over quadratic extensions, we need the model over $\mathbb{Q}$ to be related with the canonical model in the sense of Shimura. Read in this way, *loc. cit.* seems to suggest that the canonical model admits a descent to $\mathbb{Q}$. Thus we end up with Claim A above. While it would solve the problem, the statement of that claim is false in general, as we now proceed to show.

3.6. Counterexamples to descent of the canonical model. The following table summarizes the properties of three such counterexamples. The left-hand column is a reference for the data for each of the three curves, as given in the tables of [**38**]. The second and last columns give the number field F and the discriminant $\mathfrak{D}^f$ defining the quaternion algebra as above (where, for example, $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ stand for the two primes over the split prime 3). The two columns in the middle describe whether the primes 2 and 3 are inert in F.[3]

TABLE 1. Counterexamples

curve	F	2 inert	3 inert	$\mathfrak{D}^f$
e2d13D4	$\mathbb{Q}(\sqrt{13})$	yes	no	$\mathfrak{p}_2$
e2d13D36				$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'$
e3d8D9	$\mathbb{Q}(\sqrt{2})$	no	yes	$\mathfrak{p}_3$

For these three curves of genus 1, the canonical models, defined over F, do not descend to $\mathbb{Q}$.

3.7. Proof for one counterexample. Let X be the curve e2d13D36. X is defined over F, of genus 1, but doesn't necessarily have a rational point. However, we were able to derive properties of its jacobian J, which is an elliptic curve over F:

- Its conductor equals 6, by [**38**, Proposition 2.1.6].
- The valuation of its j-invariant at $\mathfrak{p}_2$ is equal to -10 (resp. -2 at $\mathfrak{p}_3$ and $\mathfrak{p}_3'$). Let us detail this result for the valuation at $\mathfrak{p}_2$. First, define the quaternion algebra H ramified exactly at both infinite places of F and at $\mathfrak{p}_3\mathfrak{p}_3'$. Call $\mathcal{O}_H$ the maximal order of H. As in [**38**, Proposition 3.1.9 (ii)] , consider $\mathcal{O}_H(\mathfrak{p}_2)$, a level $\mathfrak{p}_2$ suborder of $\mathcal{O}_H$. Consider the set of classes of right ideals of $\mathcal{O}_H(\mathfrak{p}_2)$, noted $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}_2))$. To each ideal class $[\mathrm{I}(\mathfrak{p}_2)]$ in this set, associate the weight

[3]Thus, one can see that we are unlucky because these counterexamples would not have been, anyway, good candidates for reduction modulo or 3 (these primes either meet the discriminant, or they are not inert).

$|\mathscr{O}_l(\mathrm{I}(\mathfrak{p}_2))^\bullet/\mathbb{Z}_F^\bullet|$ (equal to the cardinality of the projectivized group of units of the left-order of $\mathrm{I}(\mathfrak{p}_2)$). These weights can be computed by running the Magma ([**9**]) file PadInit in [**37**]. The sum of these weights is then equal to the opposite of the valuation of j at $\mathfrak{p}_2$, by [**38**, Proposition 3.1.14 (iii)].

Now if the curve X were defined over $\mathbb{Q}$, then the jacobian J would descend to an *elliptic curve* $J_\mathbb{Q}$ over $\mathbb{Q}$, by the argument of [**27**, Proposition 1.9]. So, let us suppose that such a rational model $J_\mathbb{Q}$ does exist, then

- the conductor of $J_\mathbb{Q}$ is either equal to 6, or to $6 \cdot 13^2$. Indeed:
  - at every place p but 13, the extension $F_\mathfrak{P}\mathbb{Q}_p$ does not ramify, so the conductor of $J_\mathbb{Q}$ has the same valuation than that of J, by Proposition 5.4 (a) of [**39**]. (As regards the particular cases of 2 and 3, note that J has multiplicative reduction at these places, so the valuation of the conductor of $J_\mathbb{Q}$ is necessarily equal to 1 at these places.)
  - at the place 13 where the extension $F_\mathfrak{P}/\mathbb{Q}_{13}$ ramifies, $J_\mathbb{Q}$ cannot have multiplicative reduction. For that if it were the case, then J would also have multiplicative reduction at 13 (by [**39**, Proposition 5.4 (b)]). This contradicts the above result on the conductor of J.
- the j-invariant of $J_\mathbb{Q}$ should be equal to the one of J. So, in particular, it should have the valuations at 2 and 3 predicted above.

Then, by a lookup in the tables of Cremona (proved to be exhaustive, see the introduction of [**16**]), only two elliptic curves E_1 and E_2 over $\mathbb{Q}$ fulfill the conditions above:

$$y^2 + xy + y = x^3 - 70997x + 7275296$$
$$y^2 + xy = x^3 - 11998412x + 15995824272$$

But considered over F, neither of their conductors is equal to 6 (one obtains isomorphic curves over F of conductor 6.13). So neither of them can be $J_\mathbb{Q}$, which therefore does not exist.

3.8. Alternative verifications. In [**36**, Chapter 7], the fourth author showed that the canonical model of J over F is given by

$$y^2 + (r+1)xy + (r+1)y = x^3 + (16383r - 38230)x + (1551027r - 3576436), \tag{11}$$

where r is a root of $t^2 - t - 3$. Explicit methods to verify this equation were also furnished in [**36**]. While these already show the correctness of the equation (11), we performed some additional sanity checks:

- First, we checked that every quadratic twist of this model involving $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_3'$, leads to a strict increase of the actual conductor 6, so cannot be a candidate for J.
- In addition, we compared the traces of Frobenius on J at several primes, to those predicted by the isomorphism (5.16) of [**38**]. This isomorphism asserts that the representation of the Hecke algebra on the (one-dimensional) space of differentials on E, is isomorphic to the representation of the Hecke algebra on the space of $\mathfrak{D}^f$-new Hilbert cusp forms on F. The comparison was made possible, since the traces for this last representation are also computable in Magma (by the work of Dembélé and Donnelly [**19**]).

Now, as remarked above, to show that the curve e2d13D36 is not defined over $\mathbb{Q}$, it suffices to show that the jacobian J does not descend to an *elliptic* curve over $\mathbb{Q}$. The equation for J given above (11) enables one to check this fact directly. For example, here are two ways to see it :

- The trace of the Frobenius of J at the inert prime (11), is equal to 22, which is not of the form $n^2 - 2 \cdot 11$.
- Alternatively, one can check that the Weil cocycle criterion is not satisfied for the curve J. Namely, denoting the conjugation of the quadratic field F by σ, this boils down to verifying that, for any F-isomorphism $f_\sigma : J \to J^\sigma$ from J to the conjugate curve, then f_σ does not satisfy $f_\sigma \circ \sigma(f_\sigma) = \mathrm{id}$. The automorphism group of the elliptic curve J being of order 2, this is quickly done.

Finally, there exists a last – and more straightforward – way to prove that e2d13D36 is a counterexample. It does not use the actual equation for the canonical model J, nor appeals to the various sophisticated theories used above (that predict the traces, conductor and j-invariant). This approach consists in computing the traces of the Hecke operators on J in the direct manner. Namely, [**36**, Algorithm 4.2.1] (available in [**37**], TakData) enables one to compute the action of the Hecke operators on the homology of the complex curve Y_0^1. Then, the computation of the trace at the inert prime (11) leads to the same result, and thus conclusion, as above.

3.9. Further exegesis. This concludes our discussion of the claims made in [**12**, Lemma IV.4]. We consider the proof of that Lemma as essentially flawed. That said, it seems likely that there are yet ways in which the result can be salvaged, which requires a finer analysis of the automorphism groups and the cohomological descent problems encountered. We hope to deal with these issues in the future.

Acknowledgment

The authors wish to thank the anonymous referee for his constructive and valuable comments which helped a lot to improve the manuscript.

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. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

10. Henri Carayol. Sur la mauvaise réduction des courbes de Shimura. *Compositio Mathematica*, 59(2):151–230, 1986.
11. 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.
12. 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.
13. Murat Cenk and Ferruh Özbudak. On multiplication in finite fields. *Journal of Complexity*, 26(2):172–186, 2010.
14. 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.
15. David V. Chudnovsky and Gregory V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4:285–316, 1988.
16. John E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.
17. Mario Daberkow, Claus Fieker, Jürgen Klüners, Michael E. Pohst, Roegner Katherine, and Klaus Wildanger. KANT V4. *Journal of Symbolic Computation*, 24:267–283, 1997.
18. 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.
19. Lassina Dembélé and Steve Donnelly. Computing Hilbert modular forms over fields with nontrivial class group. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 371–386. Springer, Berlin, 2008.
20. Koji Doi and Hidehisa Naganuma. On the algebraic curves uniformized by arithmetical automorphic functions. *Annals of Mathematics*, 86(3):449–460, 1967.
21. Virgile Ducet. *Construction of algebraic curves with many rational points over finite fields*. PhD thesis, Université d'Aix-Marseille, Institut de Mathématiques de Luminy, 2013.
22. Noam D. Elkies. Explicit modular towers. In Tamer Basar and Alexander Vardy, editors, *Proceedings of the Thirty-fifth annual Allerton conference on communication, control and computing*, pages 23–32, 1997.
23. 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.
24. 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.
25. Yasutaka Ihara. Congruence relations and Shimūra curves. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 291–311. Amer. Math. Soc., Providence, R.I., 1979.
26. Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *Journal of the Faculty of Science. University of Tokyo. Section IA. Mathematics*, 28(3):721–724, 1981.
27. James S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.
28. James S. Milne. Introduction to Shimura varieties. *Online notes*, 2004.
29. Yasuo Morita. Reduction modulo $\mathfrak{P}$ of Shimura curves. *Hokkaido Mathematical Journal*, 10(2):209–238, 1981.
30. 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.
31. Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *Journal of Complexity*, 28:489–517, 2012.
32. Goro Shimura. Construction of class fields and zeta functions of algebraic curves. *Annals of Mathematics. Second Series*, 85:58–159, 1967.
33. Goro Shimura. On canonical models of arithmetic quotients of bounded symmetric domains. *Annals of Mathematics. Second Series*, 91:144–222, 1970.
34. Amin Shokhrollahi. Optimal algorithms for multiplication in certain finite fields using algebraic curves. *SIAM Journal on Computing*, 21(6):1193–1198, 1992.
35. 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.
36. Jeroen Sijsling. *Equations for arithmetic pointed tori*. PhD thesis, Utrecht University, 2010.

37. Jeroen Sijsling. Magma programs for arithmetic pointed tori. Available at: https://sites.google.com/site/sijsling/programs, 2010.
38. Jeroen Sijsling. Canonical models of arithmetic $(1;e)$-curves. *Mathematische Zeitschrift*, 273(1-2):173–210, 2013.
39. Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
40. Henning Stichtenoth. *Algebraic Function Fields and Codes*. Number 314 in Lectures Notes in Mathematics. Springer-Verlag, 1993.
41. Henning Stichtenoth. *Algebraic Function Fields and Codes*. Number 254 in Graduate Texts in Mathematics. Springer, second edition, 2008.
42. Shmuel Winograd. On multiplication in algebraic extension fields. *Theoretical Computer Science*, 8:359–377, 1979.

AIX-MARSEILLE UNIVERSITÉ, CNRS, CENTRALE MARSEILLE, INSTITUT DE MATHÉMATIQUES DE MARSEILLE, CASE 907, 163 AVENUE DE LUMINY, F-13288 MARSEILLE CEDEX 9, FRANCE.
E-mail address: stephane.ballet@univ-amu.fr

CNRS LTCI, TÉLÉCOM PARISTECH, 46 RUE BARRAULT, F-75634 PARIS CEDEX 13, FRANCE.
E-mail address: pieltant@enst.fr

CNRS LTCI, TÉLÉCOM PARISTECH, 46 RUE BARRAULT, F-75634 PARIS CEDEX 13, FRANCE.
E-mail address: rambaud@enst.fr

UNIVERSITÄT ULM, INSTITUT FÜR REINE MATHEMATIK, HELMHOLTZSTRASSE 18, D-89069 ULM, GERMANY.
E-mail address: sijsling@gmail.com