# New uniform and asymptotic upper bounds on the tensor rank of multiplication in extensions of finite fields

Julia Pieltant, Hugues Randriambololona

# NEW UNIFORM AND ASYMPTOTIC UPPER BOUNDS ON THE TENSOR RANK OF MULTIPLICATION IN EXTENSIONS OF FINITE FIELDS

JULIA PIELTANT AND HUGUES RANDRIAM

Abstract. We obtain new uniform upper bounds for the (non necessarily symmetric) tensor rank of the multiplication in the extensions of the finite fields $\mathbb{F}_q$ for any prime or prime power $q \geq 2$; moreover these uniform bounds lead to new asymptotic bounds as well. In addition, we also give purely asymptotic bounds which are substantially better by using a family of Shimura curves defined over $\mathbb{F}_q$, with an optimal ratio of $\mathbb{F}_{q^t}$-rational places to their genus where $q^t$ is a square.

## 1. Introduction

1.1. **Tensor rank of multiplication.** Let $K$ be a field and let $\mathcal{A}$ be a finite-dimensional $K$-algebra. We denote by $m_{\mathcal{A}}$ the multiplication map of $\mathcal{A}$. It can be seen as a $K$-bilinear map from $\mathcal{A} \times \mathcal{A}$ into $\mathcal{A}$, or equivalently, as a linear map from the tensor product $\mathcal{A} \bigotimes \mathcal{A}$ over $K$ into $\mathcal{A}$. One can also represent it by a tensor $t_{\mathcal{A}} \in \mathcal{A}^\star \bigotimes \mathcal{A}^\star \bigotimes \mathcal{A}$ where $\mathcal{A}^\star$ denotes the dual of $\mathcal{A}$ over $K$. Hence the product of two elements $x$ and $y$ of $\mathcal{A}$ is the convolution of this tensor with $x \otimes y \in \mathcal{A} \bigotimes \mathcal{A}$. If

$$t_{\mathcal{A}} = \sum_{l=1}^{\lambda} a_l \otimes b_l \otimes c_l \tag{1}$$

where $a_l \in \mathcal{A}^\star$, $b_l \in \mathcal{A}^\star$, $c_l \in \mathcal{A}$, then

$$x \cdot y = \sum_{l=1}^{\lambda} a_l(x) b_l(y) c_l. \tag{2}$$

Every expression (2) is called a bilinear multiplication algorithm $\mathcal{U}$ for $\mathcal{A}$ over $K$. The integer $\lambda$ is called the bilinear complexity $\mu(\mathcal{U})$ of $\mathcal{U}$.
Let us set

$$\mu_K(\mathcal{A}) = \min_{\mathcal{U}} \mu(\mathcal{U}),$$

where $\mathcal{U}$ is running over all bilinear multiplication algorithms for $\mathcal{A}$ over $K$. Then $\mu_K(\mathcal{A})$ corresponds to the minimum possible number of summands

*Date*: May 22, 2013.

2000 *Mathematics Subject Classification.* Primary 14H05; Secondaries 11Y16, 12E20.

*Key words and phrases.* Algebraic function field, tower of function fields, tensor rank, algorithm, finite field.

in any tensor decomposition of type (1), which is the rank of the tensor of multiplication in $\mathcal{A}$ over $K$. The tensor rank $\mu_K(\mathcal{A})$ is also called the bilinear complexity of multiplication in $\mathcal{A}$ over $K$.

When the decomposition (1) is symmetric, i.e. $a_l = b_l$ for all $l = 1, \dots, \lambda$, we say that the corresponding algorithm $\mathcal{U}$ is a symmetric bilinear multiplication algorithm. If we focus on such algorithms, then the corresponding complexity is called the symmetric bilinear complexity of multiplication in $\mathcal{A}$ over $K$ and we set:

$$\mu_K^{\mathrm{sym}}(\mathcal{A}) = \min_{\mathcal{U}^{\mathrm{sym}}} \mu(\mathcal{U}^{\mathrm{sym}}),$$

with $\mathcal{U}^{\mathrm{sym}}$ running over all symmetric bilinear multiplication algorithms for $\mathcal{A}$ over $K$. Note that one has

$$\mu_K(\mathcal{A}) \leq \mu_K^{\mathrm{sym}}(\mathcal{A}).$$

In this work we will be mainly interested in the case where $K = \mathbb{F}_q$ is the finite field with $q$ elements (where $q$ is a prime power) and $\mathcal{A} = \mathbb{F}_{q^n}$ is the extension field of degree $n$ of $\mathbb{F}_q$. We then set

$$\mu_q(n) = \mu_{\mathbb{F}_q}(\mathbb{F}_{q^n}).$$

However for technical reasons we will also need the quantities

$$\mu_q(m, l) = \mu_{\mathbb{F}_q}(\mathbb{F}_{q^m}[t]/(t^l))$$

so that $\mu_q(n) = \mu_q(n, 1)$.
Similarly, we set $\mu_q^{\mathrm{sym}}(n) = \mu_{\mathbb{F}_q}^{\mathrm{sym}}(\mathbb{F}_{q^n})$ and $\mu_q^{\mathrm{sym}}(m, l) = \mu_{\mathbb{F}_q}^{\mathrm{sym}}(\mathbb{F}_{q^m}[t]/(t^l))$.

1.2. **Notations.** Let $F/\mathbb{F}_q$ be an algebraic function field of one variable of genus $g$, with constant field $\mathbb{F}_q$, associated to a curve $X$ defined over $\mathbb{F}_q$. For any place $P$ we define $F_P$ to be the residue class field of $P$ and $\mathcal{O}_P$ its valuation ring. Every element $t \in P$ such that $P = t\mathcal{O}_P$ is called a local parameter for $P$ and we denote by $v_P$ a discrete valuation associated to the place $P$ of $F/\mathbb{F}_q$. Recall that this valuation does not depend on the choice of the local parameter. Let $f \in F\backslash\{0\}$, we denote by $(f) := \sum_P v_P(f)P$ where $P$ is running over all places in $F/\mathbb{F}_q$, the principal divisor of $f$. If $\mathcal{D}$ is a divisor then $\mathcal{L}(\mathcal{D}) = \{f \in F/\mathbb{F}_q; \mathcal{D} + (f) \geq 0\} \cup \{0\}$ is a vector space over $\mathbb{F}_q$ whose dimension $\dim \mathcal{D}$ is given by the Riemann-Roch Theorem. The degree of a divisor $\mathcal{D} = \sum_P a_P P$ is defined by $\deg \mathcal{D} = \sum_P a_P \deg P$ where $\deg P$ is the dimension of $F_P$ over $\mathbb{F}_q$. The order of a divisor $\mathcal{D} = \sum_P a_P P$ at $P$ is the integer $a_P$ denoted by $\mathrm{ord}_P \mathcal{D}$. The support of a divisor $\mathcal{D}$ is the set $\mathrm{supp}\, \mathcal{D}$ of the places $P$ such that $\mathrm{ord}_P \mathcal{D} \neq 0$. Two divisors $\mathcal{D}$ and $\mathcal{D}'$ are said to be equivalent if $\mathcal{D} = \mathcal{D}' + (x)$ for an element $x \in F\backslash\{0\}$.

We denote by $B_k(F/\mathbb{F}_q)$ the number of places of degree $k$ of $F$ and by $g(F/\mathbb{F}_q)$ the genus of $F/\mathbb{F}_q$.

1.3. **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 [20] and H. de Groote [14] have shown that this complexity is $\geq 2n-1$, with equality holding if and only if $n \leq \frac{1}{2}q+1$. Moreover, in this case one has $\mu_q^{\mathrm{sym}}(n) = \mu_q(n)$. Using the principle of the D.V. and G.V. Chudnovsky algorithm [13] applied to elliptic curves, M.A. Shokrollahi has shown in [18] 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 $\epsilon$ is the function defined by:

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

Moreover, U. Baum and M.A. Shokrollahi have succeeded in [10] to construct effective optimal algorithms of type Chudnovsky in the elliptic case.

Recently in [1], [2], [8], [6], [5], [4] and [3] 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] leads to the following theorem:

**Theorem 1.1.** *Let $q = p^r$ be a power of the 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:*

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

Moreover, one can give explicit values for $C_q$:

**Proposition 1.2.** *The best known values for the constant $C_q$ defined in the previous theorem are:*

$$C_q = \begin{cases} \textit{if } q = 2 & \textit{then } 22 & [12] \textit{ and } [7] \\ \textit{else if } q = 3 & \textit{then } 27 & [1] \\ \textit{else if } q = p \geq 5 & \textit{then } 3(1+\frac{4}{q-3}) & [4] \\ \textit{else if } q = p^2 \geq 25 & \textit{then } 2(1+\frac{2}{\sqrt{q}-3}) & [4] \\ \textit{else if } q = p^{2k} \geq 16 & \textit{then } 2(1+\frac{p}{\sqrt{q}-3}) & [2] \\ \textit{else if } q \geq 16 & \textit{then } 3(1+\frac{2p}{q-3}) & [8], [6] \textit{ and } [5] \\ \textit{else if } q > 3 & \textit{then } 6(1+\frac{p}{q-3}) & [2]. \end{cases}$$

In order to obtain these good estimates for the constant $C_q$, S. Ballet has given in [1] some easy to verify conditions allowing the use of the D.V. and G.V. Chudnovsky algorithm. Then S. Ballet and R. Rolland have generalized in [8] the algorithm using places of degree one and two.

Recently, various generalizations of this algorithm were introduced in [17]. We will use the version that can be found in [17, Proposition 5.7] and which, expressed in the language of function fields, reads as follows:

**Theorem 1.3.** *Let $F/\mathbb{F}_q$ be an algebraic function field of genus $g \geq 2$, and let $m, l \geq 1$ be two integers.*

*Suppose that $F$ admits a place of degree $m$ (a sufficient condition for this is $2g+1 \leq q^{(m-1)/2}(q^{1/2}-1)$).*

*Consider now a collection of integers $n_{d,u} \geq 0$ (for $d, u \geq 1$), such that almost all of them are zero, and that for any $d$,*

$$\sum_u n_{d,u} \leq B_d(F/\mathbb{F}_q).$$

*Suppose the following assumption is satisfied:*

$$\sum_{d,u} n_{d,u} du \geq 2ml + 3e + g - 1,$$

*where the constant $e$ is defined as $e = 2$ if $q = 2$; $e = 1$ if $q = 3, 4, 5$; and $e = 0$ if $q \geq 7$. Then we have*

$$\mu_q(m, l) \leq \sum_{d,u} n_{d,u} \mu_q(d, u).$$

Intuitively, the algorithm works as follows: if $x, y$ are two elements in $\mathbb{F}_{q^m}[t]/(t^l)$ to be multiplied, we lift them to functions $f_x, f_y$ in some well-chosen Riemann-Roch spaces of $F$, we evaluate these functions at various places of $F$ with multiplicities (more precisely, $n_{d,u}$ is the number of places of degree $d$ used with multiplicity $u$), we multiply these values locally, and then we interpolate to find the product function $f_x f_y$, from which the product $xy$ is deduced.

Note that this algorithm is a non necessarily symmetric algorithm since $f_x$ and $f_y$ can be lifted in two different Riemann-Roch spaces; so we obtain bounds for $\mu_q(m, l)$, and not for $\mu_q^{\mathrm{sym}}(m, l)$.

1.4. **New results established in this paper.** In Section 2, we describe a general method to obtain new uniform bounds for the bilinear complexity of multiplication, by applying the algorithm recalled in Theorem 1.3 on towers of function fields which satisfy some properties.

In Section 3, we recall some results about a completed Garcia-Stichtenoth tower [15] studied in [2] and about the Garcia-Stichtenoth tower introduced in [16]. For both towers, we study some of their properties which will be useful in Section 4, to apply the general method on these towers. By doing so, we obtain in Section 4, new uniform bounds on the (asymmetric) bilinear complexity of multiplication in extensions of $\mathbb{F}_2$, of $\mathbb{F}_{q^2}$ and $\mathbb{F}_q$ for any prime power $q \geq 4$ and of $\mathbb{F}_{p^2}$ and $\mathbb{F}_p$ for any prime $p \geq 3$, which are the currently known best ones.

Last, in Section 5, we turn to the asymptotics of the bilinear complexity as the degree of the extension goes to infinity. In some cases, the asymptotics of our uniform bounds already improve on previously known results. But then we also present some (non-uniform) bounds with even better asymptotics, which appear to establish a new present state of the art.

## 2. General algorithm used in this paper

**Lemma 2.1.** *Let $d$ be a positive integer. For any integer $0 < j \leq d$ such that $j < \frac{1}{2}(q+1+\epsilon(q))$ if $q \geq 4$, or $j \leq \frac{1}{2}q+1$ if $q \in \{2,3\}$, one has*

$$\frac{\mu_q^{\mathrm{sym}}(j)}{j} \leq \frac{\mu_q^{\mathrm{sym}}(d)}{d}.$$

**Proof.** Suppose that the lemma is false. Then there exists an integer $0 < j < d$ such that $j < \frac{1}{2}(q+1+\epsilon(q))$ if $q \geq 4$ (resp. $j \leq \frac{1}{2}q+1$ if $q \in \{2,3\}$) and $\mu_q^{\mathrm{sym}}(j) > \frac{j}{d}\mu_q^{\mathrm{sym}}(d)$. Two cases can occur:

- either $j \leq \frac{q}{2}+1$ (in particular, this is the case if $q \in \{2,3\}$), and then we have $\mu_q^{\mathrm{sym}}(j) > \frac{j}{d}\mu_q^{\mathrm{sym}}(d) \geq \frac{j}{d}(2d-1) > 2j-1$,
- or $\frac{q}{2}+1 < j < \frac{1}{2}(q+1+\epsilon(q))$, so $\mu_q^{\mathrm{sym}}(d) \geq 2d$ leads to $\mu_q^{\mathrm{sym}}(j) > \frac{j}{d}\mu_q^{\mathrm{sym}}(d) \geq 2j$,

so both cases contradict the results recalled in Section 1.3. □

**Proposition 2.2.** *Let $q$ be a prime power and $d$ be a positive integer such that any proper divisor $j$ of $d$ satisfies $j < \frac{1}{2}(q+1+\epsilon(q))$ if $q \geq 4$, or $j \leq \frac{1}{2}q+1$ if $q \in \{2,3\}$. Let $F/\mathbb{F}_q$ be an algebraic function field of genus $g \geq 2$ with $N_i$ places of degree $i$ and let $l_i$ be integers such that $0 \leq l_i \leq N_i$, for all $i|d$. Suppose that:*

*(i) there exists a place of degree $n$ of $F/\mathbb{F}_q$,*
*(ii) $\sum_{i|d} i(N_i+l_i) \geq 2n+g+\alpha_q$, where $\alpha_2 = 5$, $\alpha_3 = \alpha_4 = \alpha_5 = 2$ and $\alpha_q = -1$ for $q > 5$.*

*Then*

$$\mu_q(n) \leq \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(n+\frac{g}{2}\right) + \gamma_{q,d}\sum_{i|d} i l_i + \kappa_{q,d}, \tag{3}$$

*where $\gamma_{q,d} := \max_{i|d}\left(\frac{\mu_q(i,2)}{i}\right) - \frac{2\mu_q^{\mathrm{sym}}(d)}{d}$ and $\kappa_{q,d} \leq \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q+d-1)$.*

**Proof.** We apply Theorem 1.3 with $n_{i,1} = N_i - l_i$ and $n_{i,2} = l_i$ for any $i|d$, and the others $n_{j,u} = 0$. We choose $l = 1$ and $m = n$ and we get

$$\begin{aligned}
\mu_q(n) &\leq \sum_{i|d} \Big( n_{i,1}\mu_q(i) + n_{i,2}\mu_q(i,2) \Big) \\
&= \sum_{i|d} \Big( (N_i - l_i)\mu_q(i) + l_i\mu_q(i,2) \Big) \\
&\leq \sum_{i|d} \Big( (N_i - l_i)\mu_q^{\mathrm{sym}}(i) + l_i\mu_q(i,2) \Big) \\
&= \sum_{i|d} \Big( \big(N_i + l_i\big)\mu_q^{\mathrm{sym}}(i) + l_i\big(\mu_q(i,2) - 2\mu_q^{\mathrm{sym}}(i)\big) \Big) \\
&= \sum_{i|d} \left( i\big(N_i + l_i\big)\frac{\mu_q^{\mathrm{sym}}(i)}{i} + il_i \left( \frac{\mu_q(i,2) - 2\mu_q^{\mathrm{sym}}(i)}{i} \right) \right)
\end{aligned}$$

so

$$\begin{aligned}
\mu_q(n) &\leq \frac{\mu_q^{\mathrm{sym}}(d)}{d} \sum_{i|d} i\big(N_i + l_i\big) + \sum_{i|d} \left( i\big(N_i + l_i\big) \left( \frac{\mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d} \right) \right. \\
&\quad \left. + il_i \left( \frac{\mu_q(i,2) - 2\mu_q^{\mathrm{sym}}(i)}{i} \right) \right) \\
&\leq \frac{\mu_q^{\mathrm{sym}}(d)}{d} \sum_{i|d} i\big(N_i + l_i\big) + \sum_{i|d} il_i \left( \frac{\mu_q(i,2) - \mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d} \right) \\
&\quad + \sum_{i|d} iN_i \left( \frac{\mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d} \right)
\end{aligned}$$

According to Lemma 2.1, we have $\frac{\mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d} \leq 0$, so

$$\sum_{i|d} iN_i \left( \frac{\mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d} \right) \leq \sum_{i|d} il_i \left( \frac{\mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d} \right)$$

since $0 \leq l_i \leq N_i$ for any $i|d$. Moreover, w.l.o.g we can suppose from (ii) that $\sum_{i|d} i(N_i + l_i) = 2n + g + \alpha_q + k_d$, with $k_d \in \{0, \ldots, d-1\}$. We obtain:

$$\mu_q(n) \leq \frac{\mu_q^{\mathrm{sym}}(d)}{d}(2n + g + \alpha_q + k_d) + \sum_{i|d} il_i \left( \frac{\mu_q(i,2)}{i} - \frac{2\mu_q^{\mathrm{sym}}(d)}{d} \right)$$

which gives the result. □

The two following corollaries are straightforward and give explicit values for Bound (3) obtained from the preceding proposition applied for the special cases where $d = 1, 2$ or $4$.

**Corollary 2.3.** *Let $q \geq 3$ be a prime power and $F/\mathbb{F}_q$ be an algebraic function field of genus $g \geq 2$ with $N_i$ places of degree $i$ and let $l_i$ be integers such that $0 \leq l_i \leq N_i$. If*

*(i) there exists a place of degree $n$ of $F/\mathbb{F}_q$,*
*(ii) $N_1 + l_1 + 2(N_2 + l_2) \geq 2n + g + \alpha_q$, where $\alpha_3 = \alpha_4 = \alpha_5 = 2$ and $\alpha_q = -1$ for $q > 5$,*

*then*

$$\mu_3(n) \leq 3n + \frac{3}{2}g + \frac{3}{2}(l_1 + 2l_2) + \frac{9}{2},$$

$$\text{for } q = 4 \text{ or } 5,\ \mu_q(n) \leq 3n + \frac{3}{2}g + l_1 + 2l_2 + \frac{9}{2},$$

*and for $q > 5$*

$$\mu_q(n) \leq 3n + \frac{3}{2}g + \frac{1}{2}(l_1 + 2l_2),\ \text{if } q > 5$$

*or in the special case where $N_2 = l_2 = 0$ (corresponding to $d = 1$ in Prop. 2.2)*

$$\mu_q(n) \leq 2n + g + l_1 - 1.$$

**Proof.** To apply Proposition 2.2, let us recall that $\mu_q^{\mathrm{sym}}(2) = 3$ and $\mu_q(1, 2) \leq 3$ for any prime power $q$. Moreover according to [17, Example 4.4], one knows that $\mu_3(2, 2) \leq 9$, $\mu_q(2, 2) \leq 8$ for $q = 4$ or 5 and $\mu_q(2, 2) \leq 7$ for $q > 5$. Hence, we can deduce that $\gamma_{3,2} \leq \frac{9}{2} - 3 = \frac{3}{2}$, $\gamma_{q,2} \leq \frac{8}{2} - 3 = 1$ for $q = 4$ or 5, and $\gamma_{q,2} \leq \frac{7}{2} - 3 = \frac{1}{2}$ and $\gamma_{q,1} \leq 1$ for $q > 5$. □

**Corollary 2.4.** *Let $F/\mathbb{F}_2$ be an algebraic function field of genus $g \geq 2$ with $N_i$ places of degree $i$ and let $l_i$ be integers such that $0 \leq l_i \leq N_i$. If*

*(i) there exists a place of degree $n$ of $F/\mathbb{F}_2$,*
*(ii) $\sum_{i|4} i(N_i + l_i) \geq 2n + g + 5$,*

*then*

$$\mu_2(n) \leq \frac{9}{2}\left(n + \frac{g}{2}\right) + \frac{3}{2}\sum_{i|4} i l_i + 18.$$

**Proof.** We recall from [13, Example 6.1] that $\mu_2^{\mathrm{sym}}(4) = 9$ and from [17, Example 4.4, Lemma 4.6] that $\mu_2(2, 2) \leq 9$ and $\mu_2(4, 2) \leq 24$, which gives $\gamma_{2,4} \leq \frac{24}{4} - \frac{2 \cdot 9}{4} = \frac{3}{2}$. □

2.1. **General method to obtain uniform bounds for $\mu_q(n)$.** We consider a tower $\mathcal{F}$ of function fields $F_i/\mathbb{F}_q$ of genus $g(F_i)$ with $B_\ell(F_i)$ places of degree $\ell$. Let $d$ be an integer such that any proper divisor $j$ of $d$ satisfies $j < \frac{1}{2}(q + 1 + \epsilon(q))$ if $q \geq 4$, or $j \leq \frac{1}{2}q + 1$ if $q \in \{2, 3\}$.
Suppose there exists an integer $N$ such that, for all $n \geq N$, there is an integer $k(n)$ for which:
(A) $\sum_{j|d} j B_j(F_{k(n)+1}) \geq 2n + g(F_{k(n)+1}) + \alpha_q$ and $B_n(F_{k(n)+1}) > 0$,

(B) $\sum_{j|d} jB_j(F_{k(n)}) < 2n + g(F_{k(n)}) + \alpha_q$ but $B_n(F_{k(n)}) > 0$,
(C) $g(F_{k(n)}) \geq 2$ (so $g(F_{k(n)+1}) \geq 2$),
(D) $\Delta g_{k(n)} := g(F_{k(n)+1}) - g(F_{k(n)}) \geq \lambda D_{k(n)}$ with $\lambda := \frac{d\gamma_{q,d}}{\mu_q^{\mathrm{sym}}(d)}$,
(E) $\sum_{j|d} jB_j(F_{k(n)}) \geq D_{k(n)}$,
where $\alpha_q$ is as in Proposition 2.2 and $D_{k(n)}$ is chosen to satisfy (D) and (E), and is fixed for the tower $\mathcal{F}$.
We also set

$$n_0^l := \sup\left\{m \in \mathbb{N} \;\middle|\; \sum_{j|d} jB_j(F_l) \geq 2m + g(F_l) + \alpha_q\right\}.$$

Note that for the integer $n_0^{k(n)}$, the following holds:

$$\sum_{j|d} jB_j(F_{k(n)}) + 2\left(n - n_0^{k(n)}\right) \geq 2n + g(F_{k(n)}) + \alpha_q. \tag{4}$$

Now, fix an integer $n \geq N$ and let $k := k(n)$ satisfying Hypotheses (A) to (E).
To multiply in $\mathbb{F}_{q^n}$, one has the following alternative:

(a) apply the algorithm on the step $F_{k+1}$, with $B_j(F_{k+1})$ places of degree $j$ for any $j|d$, all of them used with multiplicity 1; this is possible according to (A) and (C). In this case, Proposition 2.2 gives the following bound for $\mu_q(n)$:

$$\mu_q(n) \leq \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(n + \frac{g(F_{k+1})}{2}\right) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1), \tag{5}$$

(b) apply the algorithm on the step $F_k$, with $B_j(F_k)$ places of degree $j$ of which $l_j$ used with multiplicity 2 and the remaining with multiplicity 1, for any $j|d$, where the integers $l_j \leq B_j(F_k)$ satisfy $\sum_{j|d} l_j \geq 2(n - n_0^k)$; for such integers $l_j$, we can apply Proposition 2.2 according to (B) and (4). In particular, if $2(n - n_0^k) + d - 1 \leq \sum_{j|d} jB_j(F_k)$, then we can choose the integers $l_j$ such that $\sum_{j|d} jl_j = 2(n - n_0^k) + \epsilon$ for some $\epsilon \in \{0, \ldots, d-1\}$, and this is a suitable choice. In this case, Proposition 2.2 gives:

$$\mu_q(n) \leq \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(n + \frac{g(F_k)}{2}\right) + \gamma_{q,d}\sum_{i|d} il_i + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1). \tag{6}$$

Note that we can rewrite (5) as follow:

$$\mu_q(n) \leq \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(n + \frac{g(F_k)}{2}\right) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}\Delta g_k + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1)$$

which makes clear that if $\gamma_{q,d}\sum_{i|d} il_i < \frac{\mu_q^{\mathrm{sym}}(d)}{d}\Delta g_k$, then Case (b) gives a better bound then Case (a).
So if $2(n - n_0^k) + d - 1 < D_k$ , then we can proceed as in Case (b) since

according to Hypothesis (E) we can choose $\epsilon \in \{0, \ldots, d-1\}$ and $l_j$ for $j|d$ such that $\sum_{j|d} j l_j = 2(n - n_0^k) + \epsilon$. Moreover, we have

$$\frac{d\gamma_{q,d}}{\mu_q^{\mathrm{sym}}(d)}(2(n - n_0^k) + d - 1) < \Delta g_k$$

from Hypothesis (D), so $\gamma_{q,d}\left(2(n - n_0^k) + \epsilon\right) < \frac{\mu_q^{\mathrm{sym}}(d)}{d}\Delta g_k$ which means that the bound obtained from Case (b) is sharper.
For $x \in \mathbb{R}^+$, $x \geq N$, such that $\sum_{j|d} jB_j(F_{k+1}) \geq 2\,[x] + g(F_{k+1}) + \alpha_q$ and $\sum_{j|d} jB_j(F_{k+1}) < 2\,[x] + g(F_k) + \alpha_q$, we define the function $\Phi_k(x)$ as follows:

$$\Phi_k(x) = \begin{cases} \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(x + \frac{g(F_k)}{2}\right) + \gamma_{q,d}\big(2(x - n_0^k) + d - 1\big) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1), \\ \qquad\qquad \text{if } 2(x - n_0^k) + d - 1 < D_k. \\ \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(x + \frac{g(F_{k+1})}{2}\right) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1), \text{ else.} \end{cases}$$

that is to say:

$$\Phi_k(x) = \begin{cases} \left(\frac{2\mu_q^{\mathrm{sym}}(d)}{d} + 2\gamma_{q,d}\right)(x - n_0^k) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}\left(2n_0^k + g(F_k) + \alpha_q + d - 1\right), \\ \qquad\qquad \text{if } 2(x - n_0^k) + d - 1 < D_k. \\ \frac{2\mu_q^{\mathrm{sym}}(d)}{d}(x - n_0^k) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}\left(2n_0^k + g(F_{k+1}) + \alpha_q + d - 1\right), \text{ else.} \end{cases}$$

We define the function $\Phi$ for all $x \geq N$ as the minimum of the functions $\Phi_i$ for which $x$ is in the domain of $\Phi_i$. This function is piecewise linear with two kinds of pieces: those which have slope $\frac{2\mu_q^{\mathrm{sym}}(d)}{d}$ and those which have slope $\frac{2\mu_q^{\mathrm{sym}}(d)}{d} + 2\gamma_{q,d}$. Moreover, the graph of the function $\Phi$ lies below any straight line that lies above all the points $\big(n_0^i + \frac{1}{2}(D_i - d + 1), \Phi(n_0^i + \frac{1}{2}(D_i - d + 1))\big)$, since these are the *vertices* of the graph. Let $X := n_0^i + \frac{1}{2}(D_i - d + 1)$, then

$$\begin{aligned} \Phi(X) &= \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(X + \frac{g(F_{i+1})}{2}\right) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1) \\ &= \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(1 + \frac{g(F_{i+1})}{2X}\right)X + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1). \end{aligned}$$

If we can give a bound for $\Phi(X)$ which is independent of $i$, then it will provide a bound for $\mu_q(n)$ for all $n \geq N$, since $\mu_q(n) \leq \Phi(n)$.

## 3. Good sequences of function fields

3.1. **Garcia-Stichtenoth tower of Artin-Schreier algebraic function field extensions.** We present now a modified Garcia-Stichtenoth's tower (cf. [15], [2], [8]) having good properties. Let us consider a finite field $\mathbb{F}_{q^2}$ with $q = p^r \geq 4$ and $r$ an integer. We consider the Garcia-Stichtenoth's elementary abelian tower $T_1$ over $\mathbb{F}_{q^2}$ constructed in [15] and defined by the sequence $(F_1, F_2, F_3, \ldots)$ 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*:

$$g_k = \begin{cases} q^k + q^{k-1} - q^{\frac{k+1}{2}} - 2q^{\frac{k-1}{2}} + 1 & \text{if } k \equiv 1 \mod 2, \\ q^k + q^{k-1} - \frac{1}{2}q^{\frac{k}{2}+1} - \frac{3}{2}q^{\frac{k}{2}} - q^{\frac{k}{2}-1} + 1 & \text{if } k \equiv 0 \mod 2. \end{cases} \tag{7}$$

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 [2] such that $F_k \subseteq F_{k,s} \subseteq F_{k+1}$ for any integer $s \in \{0, \ldots, r\}$, with $F_{k,0} = F_k$ 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 $F_{k,s}/\mathbb{F}_{q^2}$ 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 3.1.** *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 $N_{k,s}$ places of degree one in $F_{k,s}/\mathbb{F}_{q^2}$ (respectively $N_{k,s} := B_1(G_{k,s}/\mathbb{F}_q) + 2B_2(G_{k,s}/\mathbb{F}_q)$ where $B_i(G_{k,s}/\mathbb{F}_q)$ denote the number of places of degree $i$ in $G_{k,s}/\mathbb{F}_q$) 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 $G_k \subseteq G_{k,s} \subseteq G_{k+1}$, with $G_{k,0} := G_k$ 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) $N_{k,s} \geq (q^2 - 1)q^{k-1}p^s$.*

Now, we are interested to search the descent of the definition field of the tower $T_2/\mathbb{F}_{q^2}$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_p$ if it is possible. In fact, one cannot establish a general result but one can prove that it is possible in the case of characteristic 2 which is given by the following result obtained in [9].

**Proposition 3.2.** *Let $p = 2$. If $q = p^2$, the descent of the definition field of the tower $T_2/\mathbb{F}_{q^2}$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_p$ is possible. More precisely, there exists a tower $T_4/\mathbb{F}_p$ defined over $\mathbb{F}_p$ given by a sequence:*

$$T_4/\mathbb{F}_p = H_{1,0} \subseteq H_{1,1} \subseteq H_{1,2} = H_{2,0} \subseteq H_{2,1} \subseteq H_{2,2} = H_{3,0} \subseteq \cdots$$

*defined over the constant field* $\mathbb{F}_p$ *and related to the towers* $T_1/\mathbb{F}_{q^2}$ *and* $T_2/\mathbb{F}_q$ *by*

$$F_{k,s} = \mathbb{F}_{q^2} H_{k,s} \text{ for all } k \text{ and } s = 0, 1, 2,$$
$$G_{k,s} = \mathbb{F}_q H_{k,s} \text{ for all } k \text{ and } s = 0, 1, 2,$$

*namely* $F_{k,s}/\mathbb{F}_{q^2}$ *is the constant field extension of* $G_{k,s}/\mathbb{F}_q$ *and* $H_{k,s}/\mathbb{F}_p$ *and* $G_{k,s}/\mathbb{F}_q$ *is the constant field extension of* $H_{k,s}/\mathbb{F}_p$.

Moreover, from [9], the following properties holds for this tower $T_3/\mathbb{F}_p$:

**Proposition 3.3.** *Let* $q = p^2 = 4$. *For any integers* $k \geq 1$ *and* $s \in \{0, 1, 2\}$, *the algebraic function field* $H_{k,s}/\mathbb{F}_p$ *in the tower* $T_3/\mathbb{F}_p$ *with genus* $g_{k,s} := g(H_{k,s}/\mathbb{F}_p)$ *and* $B_i(H_{k,s}/\mathbb{F}_p)$ *places of degree* $i$, *is such that:*
*(1)* $H_k/\mathbb{F}_p \subseteq H_{k,s}/\mathbb{F}_p \subseteq H_{k+1}/\mathbb{F}_p$ *with* $H_{k,0} = H_k$ *and* $H_{k,2} = H_{k+1}$,
*(2)* $g_{k,s} \leq \frac{g_{k+1}}{p^{2-s}} + 1$ *with* $g_{k+1} \leq q^{k+1} + q^k$,
*(3)* $B_1(H_{k,s}/\mathbb{F}_p) + 2B_2(H_{k,s}/\mathbb{F}_p) + 4B_4(H_{k,s}/\mathbb{F}_p) \geq (q^2 - 1)q^{k-1}p^s$.

3.2. **Garcia-Stichtenoth tower of Kummer function field extensions.** In this section we present a Garcia-Stichtenoth's 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 [16]:

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

The tower $T/\mathbb{F}_q$ is represented by the sequence of function fields $(L_0, L_1, L_2, \ldots)$ where $L_n = \mathbb{F}_q(x_0, x_1, \ldots, x_n)$ and $x_{i+1}^2 = (x_i^2 + 1)/2x_i$ holds for each $i \geq 0$. Note that $L_0$ 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-Vlăduţ bound. Moreover, for any integer $k$, $L_k/\mathbb{F}_{p^2}$ is the constant field extension of $L_k/\mathbb{F}_p$.

From [4], we know that the genus $g(L_k)$ of the steps $L_k/\mathbb{F}_{p^2}$ and $L_k/\mathbb{F}_p$ is given by:

$$g(L_k) = \begin{cases} 2^{k+1} - 3 \cdot 2^{\frac{k}{2}} + 1 & \text{if } k \equiv 0 \mod 2, \\ 2^{k+1} - 2 \cdot 2^{\frac{k+1}{2}} + 1 & \text{if } k \equiv 1 \mod 2. \end{cases} \tag{8}$$

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

$$B_1(L_k/\mathbb{F}_{p^2}) \geq 2^{k+1}(p - 1) \tag{9}$$

and

$$B_1(L_k/\mathbb{F}_p) + 2B_2(L_k/\mathbb{F}_p) \geq 2^{k+1}(p - 1). \tag{10}$$

3.3. **Some preliminary results.** Here we establish some technical results about genus and number of places of each step of the towers $T_2/\mathbb{F}_{q^2}$, $T_3/\mathbb{F}_q$, $T_4/\mathbb{F}_2$, $T/\mathbb{F}_{p^2}$ and $T/\mathbb{F}_p$ defined in Sections 3.1 and 3.2. These results will allow us to determine a suitable step of the tower to apply the algorithm on.

3.3.1. *About the Garcia-Stichtenoth's tower of Artin-Schreier extensions.* In this section, $q = p^r$ is a power of the prime $p$. We denote by $g_{k,s}$ the genus of the corresponding steps of the towers $T_2/\mathbb{F}_{q^2}$, $T_3/\mathbb{F}_q$ and $T_4/\mathbb{F}_2$; recall that $g_k = g_{k,0} = g_{k-1,r}$. We also set

$$\Delta g_{k,s} := g_{k,s+1} - g_{k,s}.$$

**Lemma 3.4.** *Let $q \geq 4$. We have the following bounds for the genus of each step of the towers $T_2/\mathbb{F}_{q^2}$, $T_3/\mathbb{F}_q$ and $T_4/\mathbb{F}_2$ (we set $q = 4$ and $p = r = 2$ in the special case of this tower):*

*i)* $g_k > q^k$ *for all* $k \geq 4$,
*moreover for the tower $T_4/\mathbb{F}_2$, one has $g_k > pq^{k-1}$ for all $k \geq 3$,*

*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* $s \in \{0, \ldots, r\}$,

*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* $s \in \{0, \ldots, r\}$.

**Proof.**

i) According to Formula (7), 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 $g_k > q^k$.
Hence, the second bound for the tower $T_4/\mathbb{F}_2$ is already proved for $k \geq 4$, and for $k = 3$, one has $g_3 - pq^2 = q^3 - 2q + 1 - pq^2 = 25$ so this bound holds also for $k = 3$.

ii) It follows from Formula (7) 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 (7), 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 3.1 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 (7). Thus, we get

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

iv) It follows from ii) since Proposition 3.1 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 $k \geq 2$.

□

Now we set $N_{k,s} := B_1(F_{k,s}/\mathbb{F}_{q^2}) = B_1(G_{k,s}/\mathbb{F}_q) + 2B_2(G_{k,s}/\mathbb{F}_q)$.

**Lemma 3.5.** *Let $D_{k,s} := (p-1)p^s q^k$. For any $k \geq 1$ and $s \in \{0, \ldots, r-1\}$, one has:*

*i) $\Delta g_{k,s} \geq D_{k,s}$ if $k \geq 4$,*
*ii) $N_{k,s} \geq D_{k,s}$.*

**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 $g_{k,s+1} - g_{k,s} \geq (p-1)p^s(g_k - 1)$. Thus we have $g_{k,s+1} - g_{k,s} \geq (p-1)p^s q^k$, from Lemma 3.4 i) since $q > 3$ and $k \geq 4$.
ii) According to Proposition 3.1, one has

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

□

**Lemma 3.6.** *For all $k \geq 1$ and $s \in \{0, \ldots, r\}$, one has*

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

**Proof.** From Proposition 3.1 and Lemma 3.4 iii), we get

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

□

Now we recall similar technical results about genus and number of places of each step of the tower $T_4/\mathbb{F}_2$ defined in Section 3.1. In order to simplify the presentation, we still use the variables $p$ and $q$.

**Lemma 3.7.** *Let $q = p^2 = 4$. For all $k \geq 1$ and $s \in \{0, 1\}$, we set $D_{k,s} := \frac{3}{2}p^{s+1}q^{k-1}$. Then we have*

*i) $\Delta g_{k,s} \geq \lambda D_{k,s}$, with $\lambda := \frac{4\gamma_{2,4}}{\mu_2^{\mathrm{sym}}(4)} \leq \frac{3}{2}$ (see Section 2.1),*
*ii) $B_1(H_{k,s}/\mathbb{F}_p) + 2B_2(H_{k,s}/\mathbb{F}_p) + 4B_4(H_{k,s}/\mathbb{F}_p) \geq D_{k,s}$.*

**Proof.**

i) We apply Genus Hurwitz Formula as in the proof of Lemma 3.5 to obtain $g_{k,s+1} - g_{k,s} \geq (p-1)p^s(g_k - 1)$, so we get $\Delta g_{k,s} \geq (p-1)p^{s+1}q^{k-1}$ from Lemma 3.4 i) for $k \geq 3$, which gives the results. For $k = 1$ and 2, we check that the result is still valid since $g_1 = 0$, $g_{1,1} = 2$, $g_2 = 6$, $g_{2,1} = 23$ and $g_3 = 57$.

ii) It is obvious since $q^2 - 1 > \frac{3}{2}p$ and since from Proposition 3.3 we have $B_1(H_{k,s}/\mathbb{F}_2) + 2B_2(H_{k,s}/\mathbb{F}_2) + 4B_4(H_{k,s}/\mathbb{F}_2) \geq (q^2-1)q^{k-1}p^s$.

□

**Lemma 3.8.** *Let $q = p^2 = 4$. For all $k \geq 1$ and $s \in \{0, 1, 2\}$, we have*

$$\sup\Big\{n \in \mathbb{N} \,\Big|\, \sum_{i=1,2,4} iB_i(H_{k,s}/\mathbb{F}_2) \geq 2n + g_{k,s} + 5\Big\} \geq 5p^sq^{k-1} - \frac{5}{2}.$$

**Proof.** From Proposition 3.3 and Lemma 3.4 iii), we get

$$\begin{aligned}\sum_{i=1,2,4} iB_i(H_{k,s}/\mathbb{F}_2) - g_{k,s} - 5 &\geq (q^2-1)q^{k-1}p^s - q^{k-1}(q+1)p^s - 5 \\ &= p^sq^{k-1}(q+1)(q-2) - 5\end{aligned}$$

thus we get the result since $q = 4$. □

3.3.2. *About the Garcia-Stichtenoth's tower of Kummer extensions.* In this section, $p$ is an odd prime. We denote by $g_k$ the genus of the step $L_k$ and we fix

$$N_k := B_1(L_k/\mathbb{F}_{p^2}) = B_1(L_k/\mathbb{F}_p) + 2B_2(L_k/\mathbb{F}_p)$$

and

$$\Delta g_k := g_{k+1} - g_k.$$

The following lemma is straightforward according to Formulae (8):

**Lemma 3.9.** *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 3.10.** *For all $k \geq 0$, 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 (9) and (10) which gives $N_k \geq 2^{k+2}$. □

**Lemma 3.11.** *Let $L_k$ be a step of one of the towers $T/\mathbb{F}_{p^2}$ or $T/\mathbb{F}_p$. One has:*

$$\sup\big\{n \in \mathbb{N} \mid N_k \geq 2n + g_k - 1\big\} \geq 2^k(p-2) + 2^{\frac{k+1}{2}}, \text{ if } p > 5$$

*and*

$$\sup\left\{n \in \mathbb{N} \mid N_k \geq 2n + g_k + 2\right\} \geq 2^k(p-2) + 2^{\frac{k+1}{2}} - 1, \text{ if } p = 5 \text{ or } 3.$$

**Proof.** From Bounds (9) and (10) for $N_k$ and Lemma 3.9 i), we get

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

Similarly, we get

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

which gives the result for $p = 5$ or 3. □

3.4. **Existence of a good step in each tower.** The following lemmas prove the existence of a « good » step of the towers defined in Sections 3.1 and 3.2, that is to say a step that will be optimal for the bilinear complexity of multiplication in a degree $n$ extension of $\mathbb{F}_q$, for any integer $n$.

**Lemma 3.12.** *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 the following conditions are verified:*

*(1) there exists a place of $F_{k,s}/\mathbb{F}_{q^2}$ of degree $n$,*
*(2) $B_1(F_{k,s}/\mathbb{F}_{q^2}) \geq 2n + g_{k,s} - 1$.*
*Moreover, the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified.*

**Proof.** Note that $n \geq 13$ since $q \geq 4$ and $n \geq \frac{1}{2}(q^2 + 1 + 2q) \geq 12.5$. First, we prove that for $1 \leq k \leq n-2$ and $s \in \{0, \ldots, r\}$, there exists a place of $F_{k,s}/\mathbb{F}_{q^2}$ of degree $n$. Indeed, for such an integer $k$, one has $q^{n-k-1} \geq q > 2 \times \frac{5}{3} \geq 2\frac{q+1}{q-1}$, so $q^{n-k}p^{-s} > 2\frac{q+1}{q-1}$ since $1 \geq p^{-s} \geq q^{-1}$, which gives $2q^{k-1}(q+1)p^s < q^{n-1}(q-1)$. Thus Lemma 3.4 iii) implies that $2g_{k,s} + 1 \leq q^{n-1}(q-1)$, which ensures that there exists a place of $F_{k,s}/\mathbb{F}_{q^2}$ of degree $n$. On the other hand, we prove that for $k \geq K(n) + 1$, with $K(n) := \log_q\left(\frac{2n}{(q+1)(q-2)}\right)$, Condition (2) is satisfied. Indeed, for such integers $k$, one has $\frac{2n}{(q+1)(q-2)} \leq q^{k-1}$, so $2n - 1 \leq q^{k-1}(q+1)(q-2)p^s$. Hence, one gets $2n + q^{k-1}(q+1)p^s - 1 \leq (q^2-1)q^{k-1}p^s$, which gives the result according to Lemma 3.4 iii) and Proposition 3.1 (3). To conclude, note that there exists at least one step $F_{k,s}/\mathbb{F}_{q^2}$ satisfying both Conditions (1) and (2) since for $n \geq 13$ and $q \geq 4$, $n - K(n) - 3 \geq 13 - (\log_4(2 \cdot 13)) - 3 > 1$. Moreover, remark that Condition (1) is satisfied from the step $F_{1,0}/\mathbb{F}_{q^2}$, so the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified. □

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

**Lemma 3.13.** *Let $n \geq \frac{1}{2}(q+1+\epsilon(q))$ be an integer. If $q = p^r > 5$, then there exists a step $G_{k,s}/\mathbb{F}_q$ of the tower $T_3/\mathbb{F}_q$ such that the following conditions are verified:*
*(1) there exists a place of $G_{k,s}/\mathbb{F}_q$ of degree $n$,*
*(2) $B_1(G_{k,s}/\mathbb{F}_q) + 2B_2(G_{k,s}/\mathbb{F}_q) \geq 2n + g_{k,s} - 1$.*
*Moreover, the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified.*

**Proof.** Here we have $n \geq 7$ since $q \geq 7$ and $n \geq \frac{1}{2}(q+1+\epsilon(q)) \geq 6.5$. First, we prove that for $1 \leq k \leq \frac{n}{2} - 2$ and $s \in \{0, \dots, r\}$, there exists a place of $G_{k,s}/\mathbb{F}_q$ of degree $n$, by showing that $2g_{k,s} + 1 \leq q^{\frac{n-1}{2}}(\sqrt{q}-1)$. Indeed, the function $q \mapsto \frac{\sqrt{q}-1}{q+1} \cdot q^{\frac{n-1}{2}-k}$ is increasing, so one has $\frac{\sqrt{q}-1}{q+1} \cdot q^{\frac{n-1}{2}-k} \geq \frac{\sqrt{7}-1}{8} \cdot 7^{\frac{n-1}{2}-k}$ since $q \geq 7$. Thus for any $k \leq \frac{n}{2} - 2$, we get $\frac{\sqrt{q}-1}{q+1} \cdot q^{\frac{n-1}{2}-k} \geq \frac{7^{\frac{3}{2}}(\sqrt{7}-1)}{8} > 2$. It follows that $2q^k(q+1) < q^{\frac{n-1}{2}}(\sqrt{q}-1)$, so $2q^{k-1}(q+1)p^s < q^{\frac{n-1}{2}}(\sqrt{q}-1)$ since $p^s \leq q$, and we get $2q^{k-1}(q+1)p^s + 1 \leq q^{\frac{n-1}{2}}(\sqrt{q}-1)$ which ensures that there exists a place of $F_{k,s}/\mathbb{F}_{q^2}$ of degree $n$, according to Lemma 3.4 iii). On the other hand, we can proceed as the preceding proof to prove that for $k \geq K(n) + 1$, with $K(n) := \log_q\left(\frac{2n}{(q+1)(q-2)}\right)$, Condition (2) is satisfied. To conclude, note that there exists at least one step $G_{k,s}/\mathbb{F}_q$ satisfying both Conditions (1) and (2) since for $n \geq 7$ and $q \geq 7$, $\frac{n}{2} - K(n) - 3 \geq \frac{7}{2} - \log_7\left(\frac{2\times 7}{8\times 5}\right) - 3 > 1$. Moreover, remark that Condition (1) is satisfied from the step $G_{1,0}/\mathbb{F}_q$, so the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified. □

In the special case where $q = 4$, Condition (2) needs to be slightly stronger:

**Lemma 3.14.** *Let $n \geq 10$ be an integer. If $q = p^2 = 4$, then there exists a step $G_{k,s}/\mathbb{F}_4$ of the tower $T_3/\mathbb{F}_4$ such that the following conditions are verified:*
*(1) there exists a place of $G_{k,s}/\mathbb{F}_4$ of degree $n$,*
*(2) $B_1(G_{k,s}/\mathbb{F}_4) + 2B_2(G_{k,s}/\mathbb{F}_4) \geq 2n + g_{k,s} + 2$.*
*Moreover, the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified.*

**Proof.** We can proceed as in the previous proof with minor changes. Indeed, we first have that $2g_{k,s} + 1 \leq q^{\frac{n-1}{2}}(\sqrt{q}-1)$ for $1 \leq k \leq \frac{n-9/2}{2}$ and $s \in \{0, 1\}$, since in this case $\frac{\sqrt{q}-1}{q+1} \cdot q^{\frac{n-1}{2}-k} = \frac{1}{5}2^{n-1-2k} \geq \frac{2^{7/2}}{5} > 2$, which proves that Condition (1) is verified according to Lemma 3.4 iii). Moreover, Condition (2) is satisfied for $k \geq K(n) + 1$ with $K(n) := \log_4\left(\frac{2n+2}{(q+1)(q-2)}\right)$, and one can check that $\frac{n}{2} - K(n) - \frac{9}{4} - 1 \geq \frac{10}{2} - \frac{9}{4} - \log_4\left(\frac{20}{10}\right) > 1$. □

This is a similar result for the tower $T_4/\mathbb{F}_2$:

**Lemma 3.15.** *For any integer $n \geq 12$ there exists a step $H_{k,s}/\mathbb{F}_2$ of the tower $T_4/\mathbb{F}_2$, with genus $g_{k,s} \geq 2$, such that both following conditions are verified:*

*(1) there exists a place of degree $n$ in $H_{k,s}/\mathbb{F}_2$,*
*(2) $B_1(H_{k,s}/\mathbb{F}_2) + 2B_2(H_{k,s}/\mathbb{F}_2) + 4B_4(H_{k,s}/\mathbb{F}_2) \geq 2n + g_{k,s} + 5$.*

*Moreover, the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified.*

**Proof.** According to [7, Lemma 2.6], if $n \geq 12$ then there exists a step $H_{k,s}/\mathbb{F}_2$ of the tower $T_4/\mathbb{F}_2$, with $k \geq 2$ (so, in particular $g_{k,s} \geq g_2 = 6$) such that there exists a place of $H_{k,s}/\mathbb{F}_2$ of degree $n$ and $B_1(H_{k,s}/\mathbb{F}_2) + 2B_2(H_{k,s}/\mathbb{F}_2) + 4B_4(H_{k,s}/\mathbb{F}_2) \geq 2n + 2g_{k,s} + 7$. Thus we get the result since $2n + 2g_{k,s} + 7 \geq 2n + g_{k,s} + 5$. □

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

**Lemma 3.16.** *Let $p \geq 3$ and $n \geq \frac{1}{2}\left(p^2 + 1 + \epsilon(p^2)\right)$. There exists a step $L_k/\mathbb{F}_{p^2}$ of the tower $T/\mathbb{F}_{p^2}$, with genus $g_k \geq 2$, such that the following conditions are verified:*

*(1) there exists a place of $L_k/\mathbb{F}_{p^2}$ of degree $n$,*
*(2) $B_1(L_k/\mathbb{F}_{p^2}) \geq 2n + g_k - 1$.*

*Moreover the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified.*

**Proof.** Note that $n \geq \frac{1}{2}(3^2 + 1 + 2 \cdot 3) = 8$. 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 satisfied. Indeed, for such an integer $k$, one has $2^{k+1} \leq 2^{n-1} < p^{n-1}$, since $p > 2$. Thus $2 \cdot 2^{k+1} < p^{n-1}(p-1)$ since $2 \leq p-1$ and we get the result from Lemma 3.9 ii).
We prove now that for $k \geq \log_2\left(\frac{n}{2}\right)$, Condition (2) is verified. Indeed, for such an integer $k$, we have $2^{k+2} \geq 2n$, so $2^{k+2} \geq 2n - 2 \cdot 2^{\frac{k+1}{2}}$. Hence we get $2^{k+1}(p-2) \geq 2n - 2 \cdot 2^{\frac{k+1}{2}}$ since $p \geq 3$ and then we obtain $2^{k+1}(p-1) \geq 2n + 2^{k+1} - 2 \cdot 2^{\frac{k+1}{2}}$. Thus we have $B_1(L_k/\mathbb{F}_{p^2}) \geq 2n + g_k - 1$ according to Bound (9) and Lemma 3.9 i).
Hence, we have proved that for any integers $n \geq 8$ and $k \geq 2$ such that $\log_2\left(\frac{n}{2}\right) \leq k \leq n-2$, both Conditions (1) and (2) are verified. Moreover, note that for any $n \geq 8$, there exists an integer $k \geq 2$ in the interval $\left[\log_2\left(\frac{n}{2}\right); n-2\right]$ since $n - 2 - \log_2\left(\frac{n}{2}\right) \geq 6 - \log_2(4) > 1$. To conclude, remark that Condition (1) is satisfied from the step $L_0/\mathbb{F}_{p^2}$, so the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified; moreover, for $k \geq 2$, $g_k \geq g_2 = 3$. □

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

**Lemma 3.17.** *Let $p > 5$ and $n \geq \frac{1}{2}(p + 1 + \epsilon(p))$. There exists a step $L_k/\mathbb{F}_p$ of the tower $T/\mathbb{F}_p$, with genus $g_k \geq 2$, such that the following conditions are verified:*

*(1) there exists a place of $L_k/\mathbb{F}_p$ of degree $n$,*
*(2) $B_1(L_k/\mathbb{F}_p) + 2B_2(L_k/\mathbb{F}_p) \geq 2n + g_k - 1$.*

*Moreover the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified.*

**Proof.** Note that $n \geq \frac{1}{2}(7 + 1 + \epsilon(7)) = 7$. 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 (1) is satisfied. Indeed, for such an integer $k$, one has $2^{k+2} \leq 2^{n-1} = 4^{\frac{n-1}{2}}$, so $2 \cdot 2^{k+1} < p^{\frac{n-1}{2}}$ since $p > 4$. Hence we get $2 \cdot 2^{k+1} < p^{\frac{n-1}{2}}(\sqrt{p} - 1)$, which gives the result from Lemma 3.9 ii).
On the other hand, we proceed as the preceding proof to prove that for $k \geq \log_2\left(\frac{n}{2}\right)$, Condition (2) is verified. Moreover, note that for any $n \geq 7$, there exists an integer $k \geq 2$ in the interval $\left[\log_2\left(\frac{n}{2}\right); n - 3\right]$ since $n - 3 - \log_2\left(\frac{n}{2}\right) \geq 4 - \log_2(3.5) > 1$. To conclude, remark that Condition (1) is satisfied from the step $L_0/\mathbb{F}_p$, so the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified; moreover, for $k \geq 2$, $g_k \geq g_2 = 3$. □

This is a similar result for the tower $T/\mathbb{F}_p$ for $p = 3$ or 5:

**Lemma 3.18.** *If $p = 5$ and $n \geq \frac{1}{2}(5 + 1 + \epsilon(5)) = 5$ or $p = 3$ and $n \geq 11$, then there exists a step $L_k/\mathbb{F}_p$ of the tower $T/\mathbb{F}_p$, with genus $g_k \geq 2$, such that the following conditions are verified:*

*(1) there exists a place of $L_k/\mathbb{F}_p$ of degree $n$,*
*(2) $B_1(L_k/\mathbb{F}_p) + 2B_2(L_k/\mathbb{F}_p) \geq 2n + g_{k,s} + 2$.*

*Moreover the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified.*

**Proof.** We first consider the case $p = 5$ and $n \geq 5$. Since $p > 4$, the first part of the preceding proof shows 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 (1) is satisfied. Now, we prove that for $k \geq \log_2\left(\frac{n}{3}\right)$, Condition (2) is satisfied. Indeed for such an integer $k$, one has $2^{k+1}(p - 2) + 2^{\frac{k+3}{2}} \geq 2n + 2\sqrt{\frac{2n}{3}} > 2n + 3$ since $n \geq 5$. Thus we get $2^{k+1}(p - 1) > 2n + (2^{k+1} - 2^{\frac{k+3}{2}} + 1) + 2$, which gives the result according to Bound (9) and Lemma 3.9 i). Hence, we have proved that for any integers $n \geq 5$ and $k \geq 2$ such that $\log_2\left(\frac{n}{3}\right) \leq k \leq n - 3$, both Conditions (1) and (2) are verified. Moreover, note that for any $n \geq 5$, there exists an integer $k \geq 2$ in the interval $\left[\log_2\left(\frac{n}{3}\right); n - 3\right]$ since $n - 3 - \log_2\left(\frac{n}{3}\right) \geq 2 - \log_2\left(\frac{n}{3}\right) > 1$. To conclude, remark that Condition (1) is satisfied from the step $L_0/\mathbb{F}_{p^2}$, so the first step

for which both Conditions (1) and (2) are verified is the first step for which (2) is verified; moreover, for $k \geq 2$, $g_k \geq g_2 = 3$.

Now we consider the case $p = 3$ and $n \geq 11$. We first prove that for all integers $k$ such that $2 \leq k \leq \log_2(3^{\frac{n-1}{2}}) - 3$, we have $2g_k + 1 \leq 3^{\frac{n-1}{2}}(\sqrt{3} - 1)$, so Condition (1) is satisfied. Indeed, for such an integer $k$, one has $2^{k+3} \leq 3^{\frac{n-1}{2}}$, so $2 \cdot 2^{k+1} \leq \frac{1}{2} \cdot 3^{\frac{n-1}{2}} < 3^{\frac{n-1}{2}}(\sqrt{3} - 1)$ which gives the result from Lemma 3.9 ii). On the other hand, we prove that for $k \geq \log_2(n)$, Condition (2) is satisfied. Indeed for such an integer $k$, one has $2^{k+1}(p-2) + 2^{\frac{k+3}{2}} = 2^{k+1} + 2^{\frac{k+3}{2}} \geq 2n + 2\sqrt{2n} > 2n + 3$ since $n \geq 11$. Thus we get $2^{k+1}(p-1) > 2n + (2^{k+1} - 2^{\frac{k+3}{2}} + 1) + 2$, which gives the result according to Bound (9) and Lemma 3.9 i). Hence, we have proved that for any integers $n \geq 11$ and $k \geq 2$ such that $\log_2(n) \leq k \leq \log_2(3^{\frac{n-1}{2}}) - 3$, both Conditions (1) and (2) are verified. Moreover, note that for any $n \geq 11$, there exists an integer $k \geq 2$ in the interval $\left[\log_2(n); \log_2(3^{\frac{n-1}{2}}) - 3\right]$ since $\log_2(3^{\frac{n-1}{2}}) - 3 - \log_2(n) \geq \log_2(3^5) - 3 - \log_2(11) > 1$. To conclude, remark that Condition (1) is satisfied from the step $L_0/\mathbb{F}_{p^2}$, so the first step for which both Conditions (1) and (2) are verified is the first step for which (2) is verified; moreover, for $k \geq 2$, $g_k \geq g_2 = 3$. □

## 4. New uniform bounds for the tensor rank

**Theorem 4.1.** *For any integer $n \geq 2$, we have*

$$\mu_2(n) \leq \frac{189}{22}n + 18.$$

**Proof.** Let $q := p^2 = 4$ and $n \geq 2$. We apply the general method described in Section 2.1 on the tower $T_4/\mathbb{F}_q$ with $d = 4$, $\gamma_{2,4} \leq \frac{3}{2}$ (see Proof of Corollary 2.4) and $\lambda := \frac{4\gamma_{2,4}}{\mu_2^{\mathrm{sym}}(4)} \leq \frac{2}{3}$, since $\mu_2^{\mathrm{sym}}(4) = 9$.
We set $X = n_0^{k,s} + \frac{1}{2}(D_{k,s} - 3)$ where $D_{k,s} = \frac{3}{2}p^{s+1}q^{k-1}$. Lemmas 3.7 and 3.15 ensure that Hypotheses (A) to (E) are satisfied, so we have:

$$\begin{aligned}\Phi(X) &= \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(1 + \frac{g(H_{k,s+1})}{2X}\right)X + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1) \\ &= \frac{9}{2}\left(1 + \frac{g(H_{k,s+1})}{2X}\right)X + 18.\end{aligned}$$

From Lemmas 3.4 iii) and 3.8 it follows that:

$$\begin{aligned}\frac{g(H_{k,s+1})}{2X} &\leq \frac{q^{k-1}(q+1)p^{s+1}}{2n_0^{k,s}+D_{k,s}-3}\\ &\leq \frac{q^{k-1}(q+1)p^{s+1}}{5p^{s+1}q^{k-1}-5+\frac{3}{2}p^{s+1}q^{k-1}-3}\\ &= \frac{q+1}{\frac{13}{2}-\frac{8}{q^{k-1}p^{s+1}}}.\end{aligned}$$

Since $k \geq 2$, one has $\frac{g(H_{k,s+1})}{2X} \leq \frac{10}{11}$ which leads to $\mu_q(n) \leq \frac{9}{2}\left(1+\frac{10}{11}\right)n + 18$ and gives the result. □

**Theorem 4.2.** *Let $p$ be a prime and $q := p^r$. For any $n \geq 2$, we have:*

*(a) if $q \geq 4$, then*

$$\mu_{q^2}(n) \leq 2\left(1+\frac{p}{q-2+(p-1)\frac{q}{q+1}}\right)n - 1,$$

*(b) if $p \geq 3$, then*

$$\mu_{p^2}(n) \leq 2\left(1+\frac{2}{p-1}\right)n - 1,$$

*(c) if $q > 5$, then*

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

*(d) if $p > 5$, then*

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

**Proof.**

(a) Let $n \geq \frac{1}{2}(q^2+1+\epsilon(q^2))$. We apply the general method described in Section 2.1 on the tower $T_2/\mathbb{F}_{q^2}$ with $d=1$, $\gamma_{q^2,1} \leq 1$ (see Proof of Corollary 2.3) and $\lambda := \frac{\gamma_{q^2,1}}{\mu_{q^2}^{\mathrm{sym}}(1)} \leq 1$.

We set $X = n_0^{k,s} + \frac{1}{2}D_{k,s}$ where $D_{k,s} = (p-1)p^sq^k$. Lemmas 3.5 and 3.12 ensure that Hypotheses (A) to (E) are satisfied. Note that we can always choose a step $F_{k,s+1}$ with $k \geq 4$ (so in particular $g_{k,s+1} \geq 2$), even if doing so we may have a non-optimal bound for some small $n$.
Thus we have:

$$\Phi(X) = 2\left(1+\frac{g(F_{k,s+1})}{2X}\right)X - 1$$

From Lemmas 3.4 iii) and 3.6 it follows that:

$$\begin{aligned}\frac{g(F_{k,s+1})}{2X} &\leq \frac{q^{k-1}(q+1)p^{s+1}}{2n_0^{k,s}+D_{k,s}}\\ &\leq \frac{q^{k-1}(q+1)p^{s+1}}{(q+1)q^{k-1}p^s(q-2)+(p-1)p^sq^k}\\ &= \frac{p}{q-2+(p-1)\frac{q}{q+1}}\end{aligned}$$

which gives the result.

(b) Let $n \geq \frac{1}{2}(p^2+1+\epsilon(p^2))$. We apply the general method described in Section 2.1 on the tower $T/\mathbb{F}_{p^2}$ with $d=1$, $\gamma_{p^2,1} \leq 1$ and $\lambda := \frac{\gamma_{p^2,1}}{\mu_{p^2}(1)} \leq 1$.
We set $X = n_0^k + \frac{1}{2}D_k$ where $D_k = 2^{k+1} - 2^{\frac{k+1}{2}}$. Lemmas 3.10 and 3.16 ensure that Hypotheses (A) to (E) are satisfied.
Thus we have:

$$\Phi(X) = 2\left(1+\frac{g(L_{k+1})}{2X}\right)X - 1$$

From Lemmas 3.9 ii) and 3.11 it follows that:

$$\begin{aligned}\frac{g(L_{k+1})}{2X} &\leq \frac{2^{k+2}}{2n_0^{k,s}+D_{k,s}}\\ &\leq \frac{2^{k+2}}{2^{k+1}(p-2)+2\frac{k+3}{2}+2^{k+1}-2^{\frac{k+1}{2}}}\\ &= \frac{2}{p-1+2^{-\frac{k-1}{2}}-2^{-\frac{k+1}{2}}}\end{aligned}$$

which gives the result, since $2^{-\frac{k-1}{2}} - 2^{-\frac{k+1}{2}} \geq 0$.

(c) Let $n \geq \frac{1}{2}(q+1+\epsilon(q))$. We apply the general method described in Section 2.1 on the tower $T_3/\mathbb{F}_q$ with $d=2$, $\gamma_{q,2} \leq \frac{1}{2}$ (see Proof of Corollary 2.3) and $\lambda := \frac{2\gamma_{q,2}}{\mu_q^{\mathrm{sym}}(2)} \leq \frac{1}{3}$ since $\mu_q^{\mathrm{sym}}(2) \geq 3$.
We set $X = n_0^{k,s} + \frac{1}{2}(D_{k,s}-1)$ where $D_{k,s} = (p-1)p^sq^k$. Lemmas 3.5 and 3.13 ensure that Hypotheses (A) to (E) are satisfied. Note that we can always choose a step $F_{k,s+1}$ with $k \geq 4$ (so in particular $g_{k,s+1} \geq 2$), even if doing so we may have a non-optimal bound for some small $n$.
Thus we have:

$$\Phi(X) = 3\left(1+\frac{g(G_{k,s+1})}{2X}\right)X.$$

We proceed as in (a) to get $\frac{g(G_{k,s+1})}{2X} \leq \frac{p}{q-2+(p-1)\frac{q}{q+1}}$ which gives the result. (Note that $\lambda \leq 1$ so Lemma 3.5 implies that Hypothesis (D) of

Section 2.1 is satisfied.)

(d) Let $n \geq \frac{1}{2}(p+1+\epsilon(p))$. We apply the general method described in Section 2.1 on the tower $T/\mathbb{F}_p$ with $d=2$, $\gamma_{p,2} \leq \frac{1}{2}$ (see Proof of Corollary 2.3) and $\lambda := \frac{2\gamma_{p,2}}{3} \leq \frac{1}{3}$.
We set $X = n_0^k + \frac{1}{2}(D_k - 1)$ where $D_k = 2^{k+1} - 2^{\frac{k+1}{2}}$. Lemmas 3.10 and 3.17 ensure that Hypotheses (A) to (E) are satisfied.
Thus we have:

$$\Phi(X) \quad = \quad 3\left(1 + \frac{g(L_{k+1})}{2X}\right) X$$

We proceed as in (b) to get $\frac{g(L_{k+1})}{2X} \leq \frac{2}{p-1}$ which gives the result. (Note that $\lambda \leq 1$ so Lemma 3.10 implies that Hypothesis (D) of Section 2.1 is satisfied.) □

**Theorem 4.3.** *For any $n \geq 2$, we have*

$$\mu_3(n) \leq 6n, \qquad \mu_4(n) \leq \frac{87}{19}n, \qquad \textit{and} \qquad \mu_5(n) \leq \frac{9}{2}n.$$

**Proof.** For the bounds over $\mathbb{F}_3$ and $\mathbb{F}_5$, we proceed as in the proof of Theorem 4.2 (d), since Lemma 3.18 ensures that the method is still valid in this cases. Thus we get

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

Note that with our method, we prove the bound for $\mu_3(n)$ for $n \geq 11$ according to Lemma 3.18, but that this bound holds also for $n \leq 10$, according to Table 1 in [12].

The bound over $\mathbb{F}_4$ is obtained for $n \geq 10$ with the same reasoning as in the proof of Theorem 4.2 (c): let $q := 4$ and $n \geq 10 > \frac{1}{2}(q+1+\epsilon(q))$, we apply the general method described in Section 2.1 on the tower $T_3/\mathbb{F}_4$ with $d=2$, $\gamma_{4,2} \leq 1$ (see Proof of Corollary 2.3) and $\lambda := \frac{2\gamma_{4,2}}{\mu_4^{\mathrm{sym}}(2)} \leq \frac{2}{3}$ since $\mu_4^{\mathrm{sym}}(2) \geq 3$. We set $X = n_0^{k,s} + \frac{1}{2}(D_{k,s} - 1)$ where $D_{k,s} = (p-1)p^s q^{k-1}$. Lemmas 3.5 and 3.14 ensure that Hypotheses (A) to (E) are satisfied. Note that we can always choose a step $F_{k,s+1}$ with $k \geq 4$ (so in particular $g_{k,s+1} \geq 2$), even if doing so we may have a non-optimal bound for some small $n$. Thus we have:

$$\Phi(X) \quad = \quad 3\left(1 + \frac{g(G_{k,s+1})}{2X}\right) X$$

which gives $\frac{g(G_{k,s+1})}{2X} \leq \frac{p}{q-2+(p-1)\frac{q}{q+1}}$. (Note that $\lambda \leq 1$ so Lemma 3.5 implies that Hypothesis (D) of Section 2.1 is satisfied.) To conclude, remark that our bound is still valid for $\mu_4(n)$ when $4.5 = \frac{1}{2}(q+1+\epsilon(q)) \leq n < 10$

according to the known estimates for $\mu_4^{\mathrm{sym}}(n)$ (recalled in [12, Table 1]). □

## 5. Asymptotic bounds

So far we gave upper bounds for the tensor rank of multiplication that hold uniformly for any extension of finite fields. Now, introducing the quantity

$$M_q = \limsup_{n\to\infty} \frac{\mu_q(n)}{n}$$

and letting the degree of the extension go to infinity, these bounds then turn into the following asymptotic estimates:

**Proposition 5.1.** *We have*

$$M_2 \le \frac{189}{22} \approx 8.591, \qquad M_3 \le 6, \qquad M_4 \le \frac{87}{19} \approx 4.579, \qquad M_5 \le 4.5,$$

*and for $p$ a prime and $q = p^r$,*

*(a) if $q \ge 4$, then* $M_{q^2} \le 2\left(1 + \frac{p}{q-2+(p-1)\frac{q}{q+1}}\right)$,

*(b) if $p \ge 3$, then* $M_{p^2} \le 2\left(1 + \frac{2}{p-1}\right)$,

*(c) if $q > 5$, then* $M_q \le 3\left(1 + \frac{p}{q-2+(p-1)\frac{q}{q+1}}\right)$,

*(d) if $p > 5$, then* $M_p \le 3\left(1 + \frac{2}{p-1}\right)$.

**Proof.** Let $n \to \infty$ in Theorems 4.1, 4.2, and 4.3. □

It is interesting to compare these asymptotic bounds with other known similar results, such as the ones in [11]. We see the bound on $M_2$ in Proposition 5.1 is less sharp than the one in [11], while the bounds on $M_3$, $M_4$, and $M_5$ are better.

However, in such a comparison, one should keep in mind other features of these various bounds. On one hand, the bounds in [11] hold not only for the general bilinear complexity, but also for the symmetric bilinear complexity. On the other hand, the constructions leading to Proposition 5.1 were not aimed solely at maximizing asymptotics:

- they give uniform bounds, that hold for any given extension of finite fields (so, not only asymptotically)
- they come from towers of curves given by explicit equations, so at least in principle, it should be possible to write explicitly the multiplication algorithms reaching these bounds.

Now, if one relaxes these last two conditions, it is possible to give substantially better asymptotic bounds, especially for $q$ small. For this we will borrow the following lemma from [11] (with a very slight modification):

**Lemma 5.2** (compare [11], Lemma IV.4)**.** *Let $q$ be a prime power and $t \geq 1$ an integer such that $q^t$* is a square *(so $q$ itself is a square, or $t$ is even). Then there exists a family $(F_s/\mathbb{F}_q)_{s\geq 1}$ of function fields such that, as $s$ goes to infinity, we have:*

*(i)* $g_s \to \infty$
*(ii)* $g_{s+1}/g_s \to 1$
*(iii)* $B_t(F_s)/g_s \to (q^{t/2}-1)/t$

*where $g_s$ is the genus of $F_s/\mathbb{F}_q$.*

For the details of the proof we refer to [11], where it is in fact credited to Elkies, who proceeded by modifying the construction of Shimura curves previously introduced in [19].

As a matter of fact, the version of the lemma originally stated in [11] requires $t$ even, while we allow $t$ odd provided $q$ is a square. However our increased generality is only apparent, because it is readily seen that the aforementioned proof of Elkies also gives the version we stated. Alternatively, when $q$ is a square, we can replace $q$ and $t$ with $q^{1/2}$ and $2t$ to reduce to the case $t$ even, and conclude with a base field extension argument.

**Theorem 5.3.** *Let $q$ be a prime power and $t \geq 1$ an integer such that $q^t \geq 9$ is a square. Then*

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

*Proof.* Let $(F_s/\mathbb{F}_q)_{s\geq 1}$ be the family of function fields given by Lemma 5.2 for $q$ and $t$. Given an integer $n$, let $s(n)$ be the smallest integer such that

$$tB_t(F_{s(n)}/\mathbb{F}_q) - g_{s(n)} \geq 2n+8.$$

Such an integer exists because of conditions (i) and (iii) in Lemma 5.2 and our hypothesis $q^t \geq 9$, and it goes to infinity with $n$. More precisely, minimality of $s(n)$ and conditions (iii) and (ii) give, respectively:

- $tB_t(F_{s(n)}/\mathbb{F}_q) - g_{s(n)} \geq 2n+8 > tB_t(F_{s(n)-1}/\mathbb{F}_q) - g_{s(n)-1}$
- $tB_t(F_{s(n)}/\mathbb{F}_q) = (q^{t/2}-1)g_{s(n)} + o(g_{s(n)})$
- $g_{s(n)-1} = g_{s(n)} + o(g_{s(n)})$

hence the estimate

$$(q^{t/2}-2)g_{s(n)} + o(g_{s(n)}) = 2n + o(n)$$

which can be restated finally as

$$g_{s(n)} = \frac{2n}{q^{t/2}-2} + o(n)$$

and

$$B_t(F_{s(n)}/\mathbb{F}_q) = \frac{2n}{t}\left(1+\frac{1}{q^{t/2}-2}\right) + o(n).$$

The estimate on $g_{s(n)}$ implies $2g_{s(n)}+1 \leq q^{(n-1)/2}(q^{1/2}-1)$ as soon as $n$ is big enough. We can then use Theorem 1.3 with $F_{s(n)}/\mathbb{F}_q$, setting $m = n$,

$l = 1$, $N_t = n_{t,1} = B_t(F_{s(n)}/\mathbb{F}_q)$, and $n_{d,u} = 0$ for all other values of $d$ and $u$. This gives

$$\mu_q(n) \leq \mu_q(t) B_t(F_{s(n)}/\mathbb{F}_q)$$

and the conclusion follows. □

**Corollary 5.4.** *We have:*

$$M_2 \leq 35/6 \approx 5.833$$
$$M_3 \leq 36/7 \approx 5.143$$
$$M_4 \leq 30/7 \approx 4.286$$

*Proof.* Apply Theorem 5.3 with $q = 2$, $t = 6$, $\mu_2(6) \leq 15$; with $q = 3$, $t = 4$, $\mu_3(4) \leq 9$; and with $q = 4$, $t = 4$, $\mu_4(4) \leq 8$. □

**Corollary 5.5.** *For any $q \geq 3$ we have $M_q \leq 3\left(1 + \frac{1}{q-2}\right)$. In particular:*

$$M_5 \leq 4$$
$$M_7 \leq 3.6$$
$$M_8 \leq 3.5$$

*Proof.* Apply Theorem 5.3 with $t = 2$, $\mu_q(2) = 3$. □

## References


[1] 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.

[2] 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.

[3] Stéphane Ballet. On the tensor rank of the multiplication in the finite fields. *Journal of Number Theory*, 128:1795–1806, 2008.

[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] Stéphane Ballet and Robert Rolland. Families of curves over any finite field attaining the generalized Drinfeld-Vladut bound. *Publ. Math. Univ. Franche-Comté Besançon Algèbr. Theor. Nr.*, pages 5–18, 2011.

[10] Ulrich Baum and Amin Shokrollahi. An optimal algorithm for multiplication in $\mathbb{F}_{256}/\mathbb{F}_4$. *Applicable Algebra in Engineering, Communication and Computing*, 2(1):15–20, 1991.

[11] 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.

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

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

[14] Hans F. 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.

[15] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Inventiones Mathematicae*, 121:211–222, 1995.

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

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

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

[19] Igor Shparlinski, Michael Tsfasman, and Serguei Vlăduţ. Curves with many points and multiplication in finite fields. In H. Stichtenoth and M.A. Tsfasman, editors, *Coding Theory and Algebraic Geometry*, number 1518 in Lectures Notes in Mathematics, pages 145–169, Berlin, 1992. Springer-Verlag. Proceedings of AGCT-3 Conference, June 17-21, 1991, Luminy.

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

Inria Saclay, LIX, École Polytechnique, 91128 Palaiseau Cedex, France
*E-mail address*: pieltant@lix.polytechnique.fr

ENST ("Telecom ParisTech"), 46 rue Barrault, F-75634 Paris Cedex 13, France
*E-mail address*: randriam@telecom-paristech.fr