Journal of Complexity 27 (2011) 230–245

Contents lists available at ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

On the tensor rank of multiplication in any extension of $\mathbb{F}_2$

Stéphane Ballet, Julia Pieltant *

Institut de Mathématiques de Luminy, case 930, F13288 Marseille cedex 9, France
eRISCS Groupe de Recherche "Informatique des Systèmes Communicants Sécurisés", France

ARTICLE INFO

Article history:
Received 16 March 2010
Accepted 26 January 2011
Available online 3 February 2011

Keywords:
Algebraic function fields
Tower of function fields
Tensor rank
Algorithm
Finite fields

ABSTRACT

In this paper, we obtain new bounds for the tensor rank of multiplication in any extension of $\mathbb{F}_2$. In particular, it also enables us to obtain the best known asymptotic bound. To this aim, we use the generalized algorithm of type Chudnovsky with derivative evaluations on places of degree one, two and four applied on the descent over $\mathbb{F}_2$ of a Garcia–Stichtenoth tower of algebraic function fields defined over $\mathbb{F}_{2^4}$.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

1.1. General context

The determination problem of the tensor rank of multiplication in finite fields has been widely studied over the past 20 years. This problem is worthwhile both because of its theoretical interest and because it has several applications in the area of information theory such as cryptography and coding theory. In particular, Shparlinski et al. have developed a correspondence between bilinear multiplication algorithms and linear codes with good parameters [20]. Their work is an achievement of the brilliant idea introduced by D.V. and G.V. Chudnovsky in [14]. Recently, Cenk and Özbudak have presented in [13] the best general version of Chudnovsky–Chudnovsky's algorithm and shown its significance in cryptography.

The theory of bilinear complexity of multiplication is a part of algebraic complexity theory. For a more extensive presentation of the background and the framework of this topic, we refer the reader to the classic book [12] by Bürgisser et al.

* Corresponding author at: Institut de Mathématiques de Luminy, case 930, F13288 Marseille cedex 9, France.
E-mail addresses: stephane.ballet@univmed.fr (S. Ballet), julia.pieltant@univmed.fr (J. Pieltant).

0885-064X/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.jco.2011.01.008

1.2. Tensor rank of multiplication

Let $\mathbb{F}_q$ be a finite field with q elements where q is a prime power and let $\mathbb{F}_{q^n}$ be a $\mathbb{F}_q$-extension of degree n. We denote by m the multiplication in the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$. The multiplication m is a bilinear map from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ into $\mathbb{F}_{q^n}$, thus it corresponds to a linear map M from the tensor product $\mathbb{F}_{q^n} \bigotimes \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ into $\mathbb{F}_{q^n}$. One can also represent M by a tensor $t_M \in \mathbb{F}^*_{q^n} \bigotimes \mathbb{F}^*_{q^n} \bigotimes \mathbb{F}_{q^n}$ where $\mathbb{F}^*_{q^n}$ denotes the dual of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Hence the product of two elements x and y of $\mathbb{F}_{q^n}$ is the convolution of this tensor with $x \otimes y \in \mathbb{F}_{q^n} \bigotimes \mathbb{F}_{q^n}$. If

$$t_M = \sum_{l=1}^{\lambda} a_l \otimes b_l \otimes c_l \tag{1}$$

where $a_l \in \mathbb{F}^*_{q^n}$, $b_l \in \mathbb{F}^*_{q^n}$, $c_l \in \mathbb{F}_{q^n}$, 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 $\mathcal{U}$. The integer λ is called the bilinear complexity $\mu(\mathcal{U})$ of $\mathcal{U}$.

Let us set

$$\mu_q(n) = \min_{\mathcal{U}} \mu(\mathcal{U}),$$

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

Then $\mu_q(n)$ corresponds to the minimum possible number of summands in any tensor decomposition of type (1), which is the rank of the tensor of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The tensor rank $\mu_q(n)$ is also called the bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

1.3. 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 in $F/\mathbb{F}_q$. Recall that this valuation does not depend on the choice of the local parameter. Let $f \in F \setminus \{0\}$, 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 $\mathcal{D} = \sum_P a_P P$ in 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 $x \in F \setminus \{0\}$.

1.4. Known results

1.4.1. General 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, Winograd [22] and de Groote [16] 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 [14] applied to elliptic curves, Shokrollahi has shown in [19] that the 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:

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

Moreover, Baum and Shokrollahi have succeeded in [11] to construct effective optimal algorithms of type Chudnovsky in the elliptic case.

Recently in [2,3,10,7,6,5,4] the study made by 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 [14] leads to the following theorem:

Theorem 1.1. *Let $q = p^r$ be a power of the prime p. The tensor rank $\mu_q(n)$ 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:*

$$\mu_q(n) \leq C_q n.$$

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:*

$$C_q = \begin{cases} \text{if } q = 2 & \text{then } 54 & [2] \\ \text{else if } q = 3 & \text{then } 27 & [2] \\ \text{else if } q = p \geq 5 & \text{then } 3\left(1 + \dfrac{4}{q-3}\right) & [5] \\ \text{else if } q = p^2 \geq 25 & \text{then } 2\left(1 + \dfrac{2}{\sqrt{q}-3}\right) & [5] \\ \text{else if } q = p^{2k} \geq 16 & \text{then } 2\left(1 + \dfrac{p}{\sqrt{q}-3}\right) & [3] \\ \text{else if } q \geq 16 & \text{then } 3\left(1 + \dfrac{2p}{q-3}\right) & [10,7,6] \\ \text{else if } q > 3 & \text{then } 6\left(1 + \dfrac{p}{q-3}\right) & [3]. \end{cases}$$

In order to obtain these good estimates for the constant C_q, Ballet has given in [2] some easy to verify conditions allowing the use of the D.V. and G.V. Chudnovsky algorithm. Then Ballet and Rolland have generalized in [10] the algorithm using places of degree one and two.

Let us present the last version of this algorithm, which is a generalization of the algorithm of type Chudnovsky introduced by Arnaud in [1] and Cenk and Özbudak in [13]. This generalization uses several coefficients in the local expansion at each place P_i instead of just the first one. Due to the way to obtain the local expansion of a product from the local expansion of each term, the bound for the bilinear complexity involves the complexity notion $\widehat{M_q}(u)$ introduced by Cenk and Özbudak in [13] and defined as follows:

Definition 1.3. We denote by $\widehat{M_q}(u)$ the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain coefficients of the product of two arbitrary u-term polynomials modulo x^u in $\mathbb{F}_q[x]$.

Let us recall that for all prime powers q, we trivially have $\widehat{M_q}(2) \leq 3$.

Now we introduce the generalized algorithm of type Chudnovsky described in [13].

Theorem 1.4. *Let*

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

$$Ev_Q : \begin{cases} \mathcal{L}(\mathcal{D}) \to \mathbb{F}_{q^n} \simeq F_Q \\ f \longmapsto f(Q) \end{cases}$$

is onto,

(b) *the map*

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

is injective, where the map φ_i is defined by

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

with $f = f(P_i) + f'(P_i)t_i + f''(P_i)t_i^2 + \cdots + f^{(k)}(P_i)t_i^k + \cdots$, 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

$$\mu_q(n) \leq \sum_{i=1}^{N} \mu_q(\deg P_i)\widehat{M}_{q^{\deg P_i}}(u_i).$$

First of all, note that we can define the map Ev_Q since Q is not in the support of $\mathcal{D}$. Indeed, for such a place Q, we have $\mathcal{L}(\mathcal{D}) \subseteq \mathcal{O}_Q$, so Ev_Q is the restriction of the projection $\pi : \mathcal{O}_Q \to F_Q$. Moreover, the application $Ev_{\mathcal{P}}$ can be defined since $\mathcal{L}(2\mathcal{D}) \subseteq \mathcal{O}_{P_i}$ for all integers $i \in \{1, \ldots, n\}$, so the local expansion of $f \in \mathcal{L}(2\mathcal{D})$ at any place $P_i \in \mathcal{P}$ exists from [18, (1.4)]. Indeed, this follows from the fact that the intersection $\mathcal{P} \cap \operatorname{supp} \mathcal{D}$ is empty, so $v_{P_i}(f) \geq 0$ and the coefficients of the local expansion of f at P_i can be defined inductively.

Let us remark that the algorithm given in [14] by D.V. and G.V. Chudnovsky is the case $\deg P_i = 1$ and $u_i = 1$ for $i = 1, \ldots, N$. The generalization introduced here is useful: it allows us to use certain places many times, thus less places are necessary to get the injectivity of $Ev_{\mathcal{P}}$. In particular, we have the following results, obtained by Arnaud in [1].

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 $F/\mathbb{F}_q$,*
- *$\mathcal{D}$ be a divisor of $F/\mathbb{F}_q$,*
- *$\mathcal{P} = \{P_1, \ldots, P_{N_1}, P_{N_1+1}, \ldots, P_{N_1+N_2}\}$ be a set of N_1 places of degree one and N_2 places of degree two,*
- *$0 \leq l_1 \leq N_1$ and $0 \leq l_2 \leq N_2$ be two 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*

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

is onto,

(b) *the map*

$$Ev_{\mathcal{P}} : \begin{cases} \mathcal{L}(2\mathcal{D}) \to \mathbb{F}_q^{N_1} \times \mathbb{F}_q^{l_1} \times \mathbb{F}_{q^2}^{N_2} \times \mathbb{F}_{q^2}^{l_2} \\ f \mapsto \big(f(P_1), \ldots, f(P_{N_1}), f'(P_1), \ldots, f'(P_{l_1}), \\ \quad f(P_{N_1+1}), \ldots, f(P_{N_1+N_2}), f'(P_{N_1+1}), \ldots, f'(P_{N_1+l_2})\big) \end{cases}$$

is injective.

Then

$$\mu_q(n) \le N_1 + 2l_1 + 3N_2 + 6l_2.$$

Proof. Up to reindexing the places, the result follows from Theorem 1.4 applied with $N = N_1 + N_2$, $\deg P_i = 1$ for $i = 1, \ldots, N_1$, $\deg P_i = 2$ for $i = N_1 + 1, \ldots, N$, and

$$u_i = \begin{cases} 2, & \text{if } 1 \le i \le l_1 \text{ or } N_1 + 1 \le i \le N_1 + l_2, \\ 1, & \text{else.} \end{cases}$$

Recall that for all prime powers q, we have $\mu_q(2) = 3$ and $\widehat{M_q}(2) \le 3$.

Then applying Theorem 1.4, we get:

$$\begin{aligned} \mu_q(n) &\le \sum_{i=1}^{l_1} \mu_q(1)\widehat{M_q}(2) + \sum_{i=l_1+1}^{N_1} \mu_q(1)\widehat{M_q}(1) + \sum_{i=N_1+1}^{N_1+l_2} \mu_q(2)\widehat{M_{q^2}}(2) + \sum_{i=N_1+l_2+1}^{N} \mu_q(2)\widehat{M_{q^2}}(1) \\ &\le 3l_1 + N_1 - l_1 + 9l_2 + 3(N_2 - l_2) \\ &= N_1 + 2l_1 + 3N_2 + 6l_2. \quad \square \end{aligned}$$

Moreover, from the last corollary applied on Garcia–Stichtenoth towers, Arnaud obtained the two following bounds.

Theorem 1.6. *Let $q = p^r \ge 4$ be a prime power. Then*

$$\text{(i) } \mu_{q^2}(n) \le 2\left(1 + \frac{p}{q - 3 + (p-1)\left(1 - \frac{1}{q+1}\right)}\right) n,$$

$$\text{(ii) } \mu_q(n) \le 3\left(1 + \frac{2p}{q - 3 + 2(p-1)\left(1 - \frac{1}{q+1}\right)}\right) n.$$

1.4.2. Asymptotic bounds for the extensions of $\mathbb{F}_2$

From the asymptotic point of view, let us recall that Shparlinski et al. have given in [20] many interesting remarks on the algorithm of D.V. and G.V. Chudnovsky. In particular, they considered the following asymptotic bounds for the bilinear complexity

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

and

$$m_q = \liminf_{k\to\infty} \frac{\mu_q(k)}{k}.$$

In [20], they claim that $M_2 \le 27$, but it is possible to obtain easily a better bound for M_2 from one of the bounds of Arnaud. Indeed, by using Bound (ii) of Theorem 1.6, we obtain:

Proposition 1.7.

$$M_2 \le \frac{297}{13} \approx 22.85.$$

Proof. For all $m \ge 1$, we have

$$\mu_q(n) \le \mu_q(mn) \le \mu_q(m) \cdot \mu_{q^m}(n).$$

Thus for $q = 2$ and $m = 2$ we get $\mu_2(n) \leq \mu_2(2) \cdot \mu_4(n)$. Remembering that $\mu_2(2) = 3$ and applying Bound (ii) of Theorem 1.6, we obtain

$$\mu_2(n) \leq 3 \cdot 3 \left(1 + \frac{4}{1 + 2\left(1 - \frac{1}{5}\right)}\right) n = \frac{297}{13} n. \quad \square$$

Remark. Using Bound (i) from Theorem 1.6, we obtain $M_2 \leq 38$. Indeed, for all $m \geq 1$, we have

$$\mu_q(n) \leq \mu_q(mn) \leq \mu_q(m) \cdot \mu_{q^m}(n).$$

Thus for $q = 2$ and $m = 4$ we get $\mu_2(n) \leq \mu_2(4) \cdot \mu_{16}(n)$. Remembering that $\mu_2(4) \leq 9$ and applying Bound (i) of Theorem 1.6, we obtain

$$\mu_2(n) \leq 9 \cdot 2 \left(1 + \frac{2}{2 - \frac{1}{5}}\right) n = 38n.$$

1.5. New results established in this paper

Our main result concerns an improvement of the asymptotic bound for the tensor rank of multiplication in any extension of $\mathbb{F}_2$. More precisely, we prove that:

$$M_2 \leq \frac{477}{26} \approx 18.35.$$

This result comes from a new bound for the tensor rank of multiplication in any extension of $\mathbb{F}_2$ that we also obtain in this paper, namely:

$$\mu_2(n) \leq \frac{477}{26} n + \frac{45}{2}.$$

In Section 2, we recall some results about a modified Garcia–Stichtenoth tower [17] studied in [3,10,7,5]. Specially, we present the descent of the definition field of this Garcia–Stichtenoth tower on the field $\mathbb{F}_2$ obtained in [9] and study some of its properties which will be useful in Section 3. In Section 3, we specialize the generalized algorithm of type Chudnovsky by using places of degree one, two and four with derivative evaluations. In order to obtain new bounds for the bilinear complexity, we apply this specialized algorithm to suitable steps of the tower presented in Section 2. In particular, in Section 4 these new bounds lead to an improvement of known results on the asymptotic tensor rank of multiplication in the extensions of $\mathbb{F}_2$.

2. A good sequence of function fields defined over $\mathbb{F}_2$

In this section, we present a sequence of algebraic function fields defined over $\mathbb{F}_2$ constructed and studied in [9], which will be used to obtain the new bounds for the tensor rank of multiplication in the extensions of $\mathbb{F}_2$.

2.1. Definition of Garcia–Stichtenoth towers

First, we present a modified Garcia–Stichtenoth tower (cf. [17,3,10]) having good properties. Let us consider a finite field $\mathbb{F}_{q^2}$ with $q = p^r$, for p a prime number and r an integer. Let us consider the Garcia–Stichtenoth elementary abelian tower T_0 over $\mathbb{F}_{q^2}$ constructed in [17] and defined by the sequence $(F_1, F_2, \ldots)$ where

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

and z_{k+1} satisfies the equation:

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

with

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

Moreover $F_1 := \mathbb{F}_{q^2}(x_0)$ 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 in $T_0/\mathbb{F}_{q^2}$, we recall the following *formulae*:

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

If $r > 1$, we consider the completed Garcia–Stichtenoth tower

$$T_1/\mathbb{F}_{q^2} = F_{1,0} \subseteq F_{1,1} \subseteq \cdots \subseteq F_{1,r} = F_{2,0} \subseteq F_{2,1} \subseteq \cdots \subseteq F_{2,r} = F_{3,0} \subseteq \cdots$$

considered in [3] such that $F_k \subseteq F_{k,s} \subseteq F_{k+1}$ for any integer s such that $s = 0, \ldots, r$, with $F_{k,0} = F_k$ and $F_{k,r} = F_{k+1}$. Let us denote by $g_{k,s}$ the genus of $F_{k,s}/\mathbb{F}_{q^2}$ in $T_1/\mathbb{F}_{q^2}$ and by $N_i(F_{k,s}/\mathbb{F}_{q^2})$ the number of places of degree i of $F_{k,s}/\mathbb{F}_{q^2}$ in $T_1/\mathbb{F}_{q^2}$. Recall that each extension $F_{k,s}/F_k$ is Galois of degree p^s with full constant field $\mathbb{F}_{q^2}$. Moreover, we know by [7] that the descent of the definition field of the tower $T_1/\mathbb{F}_{q^2}$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ is possible. More precisely, there exists a tower $T_2/\mathbb{F}_q$ defined over $\mathbb{F}_q$ given by a sequence:

$$T_2/\mathbb{F}_q = G_{1,0} \subseteq G_{1,1} \subseteq \cdots \subseteq G_{1,r} = G_{2,0} \subseteq G_{2,1} \subseteq \cdots \subseteq G_{2,r} = G_{3,0} \subseteq \cdots$$

defined over the constant field $\mathbb{F}_q$ and related to the tower $T_1/\mathbb{F}_{q^2}$ 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 $G_{k,s}/\mathbb{F}_q$.

2.2. Descent of the definition field of a Garcia–Stichtenoth tower on the field $\mathbb{F}_2$

Now, we are interested to search the descent of the definition field of the tower $T_1/\mathbb{F}_{q^2}$ 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]. Note that in order to simplify the presentation, we are going to set the results by using the variable p and to give the proofs to be self-contained.

Proposition 2.1. *Let $p = 2$. If $q = p^2$, the descent of the definition field of the tower $T_1/\mathbb{F}_{q^2}$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_p$ is possible. More precisely, there exists a tower $T_3/\mathbb{F}_p$ defined over $\mathbb{F}_p$ given by a sequence:*

$$T_3/\mathbb{F}_p = H_{1,0} \subseteq H_{1,1} \subseteq H_{1,2} = H_{2,0} \subseteq H_{2,1} \subseteq H_{2,2} = H_{3,0} \subseteq \cdots$$

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

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

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 $H_{k,s}/\mathbb{F}_p$.

Proof. In the proof, we use $p = 2$. Let x_1 be a transcendent element over $\mathbb{F}_2$ and let us set

$$H_1 = \mathbb{F}_2(x_1), \qquad G_1 = \mathbb{F}_4(x_1), \qquad F_1 = \mathbb{F}_{16}(x_1).$$

We define recursively for $k \geq 1$

(1) z_{k+1} such that $z_{k+1}^4 + z_{k+1} = x_k^5$,
(2) t_{k+1} such that $t_{k+1}^2 + t_{k+1} = x_k^5$
(or alternatively $t_{k+1} = z_{k+1}(z_{k+1} + 1)$),
(3) $x_{k+1} = z_{k+1}/x_k$,

(4) $H_{k,1} = H_{k,0}(t_{k+1}) = H_k(t_{k+1}), H_{k+1,0} = H_{k+1} = H_k(z_{k+1}), G_{k,1} = G_{k,0}(t_{k+1}) = G_k(t_{k+1}),$ $G_{k+1,0} = G_{k+1} = G_k(z_{k+1}), F_{k,1} = F_{k,0}(t_{k+1}) = F_k(t_{k+1}), F_{k+1,0} = F_{k+1} = F_k(z_{k+1}).$

By [7], the tower $T_1 = (F_{k,i})_{k\geq 1, i=0,1}$ is the densified Garcia–Stichtenoth tower over $\mathbb{F}_{16}$ and the two other towers T_2 and T_3 are respectively the descent of T_1 over $\mathbb{F}_4$ and over $\mathbb{F}_2$. □

Now, we recall different properties concerning the tower $T_3/\mathbb{F}_2$.

Proposition 2.2. *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 $T_3/\mathbb{F}_p$ has a genus $g(H_{k,s}/\mathbb{F}_p) = g_{k,s}$ with $N_1(H_{k,s}/\mathbb{F}_p)$ places of degree one, $N_2(H_{k,s}/\mathbb{F}_p)$ places of degree two and $N_4(H_{k,s}/\mathbb{F}_p)$ places of degree 4 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) *$g(H_{k,s}/\mathbb{F}_p) \leq \frac{g(H_{k+1}/\mathbb{F}_p)}{p^{2-s}} + 1$ with $g(H_{k+1}/\mathbb{F}_p) = g_{k+1} \leq q^{k+1} + q^k$,*
(3) *$N_1(H_{k,s}/\mathbb{F}_p) + 2N_2(H_{k,s}/\mathbb{F}_p) + 4N_4(H_{k,s}/\mathbb{F}_p) \geq (q^2 - 1)q^{k-1}p^s$.*

Proof. The property (1) follows directly from Proposition 2.1. Moreover, by Theorem 2.2 in [3], we have $g(F_{k,s}) \leq \frac{g(F_{k+1})}{p^{2-s}} + 1$ with $g(F_{k+1}) = g_{k+1} \leq q^{k+1} + q^k$. Then, as the algebraic function field $F_{k,s}$ is a constant field extension of $H_{k,s}$, for any integers k and s the algebraic function fields $F_{k,s}$ and $H_{k,s}$ have the same genus. So, the inequality satisfied by the genus $g(F_{k,s})$ is also true for the genus $g(H_{k,s})$. Moreover, the number of places of degree one $N_1(F_{k,s}/\mathbb{F}_{q^2})$ of $F_{k,s}/\mathbb{F}_{q^2}$ is such that $N_1(F_{k,s}/\mathbb{F}_{q^2}) \geq (q^2 - 1)q^{k-1}p^s$. Then, as the algebraic function field $F_{k,s}$ is a constant field extension of $H_{k,s}$ of degree 4, it is clear that for any integers k and s, we have

$$N_1(H_{k,s}/\mathbb{F}_p) + 2N_2(H_{k,s}/\mathbb{F}_p) + 4N_4(H_{k,s}/\mathbb{F}_p) \geq (q^2 - 1)q^{k-1}p^s. \quad \square$$

2.3. Some preliminary results

Here we establish some technical results about genus and number of places of each step of the tower $T_3/\mathbb{F}_2$ defined in Section 2.2. These results will allow us to determine a suitable step of the tower to apply the algorithm on. In order to simplify the presentation, we still use the variables p and q.

Lemma 2.3. *Let $q = p^2 = 4$. We have the following bounds for the genus of each step of the tower $T_3/\mathbb{F}_p$:*

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

Proof. (i) According to Formula (3) recalled in Section 2.1, we know that if $k \equiv 1 \bmod 2$, 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 $q = 4$ and $k \geq 4$, we have $q^{\frac{k-1}{2}} - q - 2 > 0$, thus $g_k > q^k$.

Else if $k \equiv 0 \bmod 2$, then

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

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

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

(iii) If $s = 2$, then according to Proposition 2.2, we have

$$g_{k,s} = g_{k+1} \leq q^{k+1} + q^k = q^{k-1}(q+1)p^2.$$

Else, $s < 2$ and Proposition 2.2 says that $g_{k,s} \leq \frac{g_{k+1}}{p^{2-s}} + 1$. 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

$$\begin{aligned} g_{k,s} &\leq \frac{q^{k+1} + q^k - q + 1}{p^{2-s}} + 1 \\ &= q^{k-1}(q+1)p^s - p^s + p^{s-2} + 1 \\ &\leq q^{k-1}(q+1)p^s + p^{s-2} \\ &\leq q^{k-1}(q+1)p^s \quad \text{since } 0 \leq p^{s-2} < 1 \text{ and } g_{k,s} \in \mathbb{N}. \end{aligned}$$

(iv) It follows from (ii) since Proposition 2.2 gives $g_{k,s} \leq \frac{g_{k+1}}{p^{2-s}} + 1$, so $g_{k,s} \leq \frac{q^k(q+1) - \sqrt{q}q^{\frac{k+1}{2}}}{p^{2-s}} + 1$ which gives the result since $p^{2-s} \leq q^{\frac{k}{2}}$ for all $k \geq 2$. □

Lemma 2.4. *Let $q = p^2 = 4$. For all $k \geq 1$ and $0 \leq s \leq 2$, we set $D_{k,s} := p^{s+1}q^{k-1}$. Then we have*

(i) $\Delta g_{k,s} := g_{k,s+1} - g_{k,s} \geq D_{k,s}$,
(ii) $N_1(H_{k,s}/\mathbb{F}_p) + 2N_2(H_{k,s}/\mathbb{F}_p) + 4N_4(H_{k,s}/\mathbb{F}_p) > 2D_{k,s}$.

Proof. (i) From Hurwitz Genus Formula, we know that $g_{k,s+1} - 1 \geq p(g_{k,s} - 1)$ for any integer $k \geq 1$ and $s = 0, 1$, 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 for $k \geq 4$ we have $g_{k,s+1} - g_{k,s} \geq (p-1)p^s q^k$ because $g_k > q^k$ according to Lemma 2.3(i).

(ii) It is obvious since $q^2 - 1 > p^2$ and since from Proposition 2.2 we have $N_1(H_{k,s}/\mathbb{F}_2) + 2N_2(H_{k,s}/\mathbb{F}_2) + 4N_4(H_{k,s}/\mathbb{F}_2) \geq (q^2 - 1)q^{k-1}p^s$. □

Lemma 2.5. *Let $q = p^2 = 4$ and $N_i(k, s) := N_i(H_{k,s}/\mathbb{F}_p)$. For all $k \geq 1$ and $s = 0, 1, 2$, we have*

$$\sup\left\{n \in \mathbb{N} \mid 2n \leq N_1(k,s) + 2N_2(k,s) + 4N_4(k,s) - 2g_{k,s} - 7\right\} \geq \frac{5}{2}q^{k-1} - \frac{7}{2}.$$

Proof. From Proposition 2.2 and Lemma 2.3(iii), we get

$$\begin{aligned} N_1(k,s) + 2N_2(k,s) + 4N_4(k,s) - 2g_{k,s} - 7 &\geq (q^2-1)q^{k-1}p^s - 2q^{k-1}(q+1)p^s - 7 \\ &= p^s q^{k-1}(q+1)(q-3) - 7 \end{aligned}$$

thus we have $\sup\{n \in \mathbb{N} \mid 2n \leq N_1(k,s) + 2N_2(k,s) + 4N_4(k,s) - 2g_{k,s} - 7\} \geq \frac{1}{2}p^s q^{k-1}(q+1)(q-3) - \frac{7}{2}$ and we get the result since $q = 4$ and $s \geq 0$. □

Lemma 2.6. *Let n be an integer ≥ 2. Then there exists a step $H_{k,s}/\mathbb{F}_2$ of the tower $T_3/\mathbb{F}_2$ introduced in Section 2.2 such that both following conditions are verified:*

(1) *there exists a place of degree n in $H_{k,s}/\mathbb{F}_2$,*
(2) $N_1(H_{k,s}/\mathbb{F}_2) + 2N_2(H_{k,s}/\mathbb{F}_2) + 4N_4(H_{k,s}/\mathbb{F}_2) \geq 2n + 2g_{k,s} + 7$.

Moreover, the first step for which both conditions are verified is the first step for which (2) is verified.

Proof. Let $q = p^2 = 4$. Fix $n \geq 28$. We first show that for all integers k such that $2 \leq k \leq \frac{1}{4}(n-12)$, we have $2g_{k,s} + 1 \leq p^{\frac{n-1}{2}}\left(p^{\frac{1}{2}} - 1\right)$ for any $s \in \{0, 1, 2\}$, so Condition (1) is verified according to Corollary 5.2.10 in [21]. Indeed for such an integer k, we have $6 \leq \frac{n}{2} - 2k$ i.e. $p^6 \leq p^{\frac{n}{2}-2k}$. Since $5p^{\frac{7}{2}} \leq p^6$, we

get $5p^{\frac{7}{2}} \leq p^{\frac{n}{2}-2k}$ or equivalently $5p^{2k+1} \leq p^{\frac{n-1}{2}-2}$, which leads to $5p^{2k+1} \leq p^{\frac{n-1}{2}}\left(p^{\frac{1}{2}}-1\right)$. Now, let us show that $2g_{k,s}+1 \leq 5p^{2k+1}$. According to Lemma 2.3(iv), since $k \geq 2$ we have for $s = 0, 1, 2$:

$$\begin{aligned}
2g_{k,s}+1 &\leq 2\frac{q^k(q+1)-q^{\frac{k}{2}}(q-1)}{p^{2-s}}+1\\
&= 2\left(q^{k-1}(q+1)-q^{\frac{k}{2}}\frac{q-1}{q}\right)p^s+1\\
&= 2q^{k-1}(q+1)p^s-2q^{\frac{k}{2}}\frac{q-1}{q}p^s+1\\
&\leq 2q^{k-1}(q+1)p^s \quad \text{since } 2q^{\frac{k}{2}}\frac{q-1}{q}p^s \geq 1\\
&= 2p^{2(k-1)}(p^2+1)p^s\\
&= 5p^{2k-1}p^s \quad \text{since } p=2
\end{aligned}$$

which gives the result since $p^s \leq p^2$.

We prove now that for $k \geq \frac{1}{2}\log_p\left(\frac{4}{5}(2n+6)\right)$, Condition (2) is verified. Indeed, for such an integer k, we have $2n+6 \leq \frac{5}{4}p^{2k}$, so $2n+6 \leq \frac{5}{4}p^{2k}p^s$ for $s = 0, 1, 2$. Since $p = 2$, we have $\frac{5}{4}p^{2k}p^s = \left(p^4-1-p(p^2+1)\right)p^{2k-2}p^s$, so we get

$$2n+p^{2k-1}(p^2+1)p^s+6 \leq (p^4-1)p^{2k-2}p^s. \tag{4}$$

Recall that we got $2g_{k,s}+1 \leq p^{2k-1}(p^2+1)p^s$ in the first part of the proof, so $2n+2g_{k,s}+7 \leq 2n+p^{2k-1}(p^2+1)p^s+6$ and (4) gives the result since we know from Proposition 2.2 that $N_1(H_{k,s}/\mathbb{F}_p)+2N_2(H_{k,s}/\mathbb{F}_p)+4N_4(H_{k,s}/\mathbb{F}_p) \geq (q^2-1)q^{k-1}p^s$.

Finally, we have proved that for any integers $n \geq 28$ and $k \geq 2$ such that $\frac{1}{2}\log_p\left(\frac{4}{5}(2n+6)\right) \leq k \leq \frac{1}{4}(n-12)$, both Conditions (1) and (2) are verified. Note that for any $n \geq 28$, we have $\frac{1}{2}\log_p\left(\frac{4}{5}(2n+6)\right) > 2$. Moreover the size of the interval $\left[\frac{1}{2}\log_p\left(\frac{4}{5}(2n+6)\right); \frac{1}{4}(n-12)\right]$ is bigger than 1 as soon as $n \geq 28$, and this size increases with n. Hence, for any integer $n \geq 28$, we know that there is an integer $k > 2$ in this interval and so there exists a corresponding step $H_{k,s}$. Moreover, the first step $H_{k,s}$, that is to say the smallest couple of integers (k, s), for which both Conditions (1) and (2) are verified, is the first step for which Condition (2) is verified, since for all integers $k \leq \frac{1}{4}(n-12)$ there is a place of degree n in $H_{k,s}/\mathbb{F}_2$. To conclude, we complete the proof by computing, for the first steps of the tower, the number of places of degree one, two, four and n for $n < 28$. Using the KASH packages [15], we obtain the following results:

(a) $g(H_1/\mathbb{F}_2) = 0$, $N_1(H_1/\mathbb{F}_2) = 3$, $N_2(H_1/\mathbb{F}_2) = 1$ and $N_4(H_1/\mathbb{F}_2) = 3$. Hence Condition (2) holds for all $n \leq 5$; moreover we check that $N_3(H_1/\mathbb{F}_2) > 0$ and $N_5(H_1/\mathbb{F}_2) > 0$. So for any integer $n \leq 5$, the first step that verifies both Conditions (1) and (2) is $H_1/\mathbb{F}_2$.

(b) $g(H_{1,1}/\mathbb{F}_2) = 2$, $N_1(H_{1,1}/\mathbb{F}_2) = 3$, $N_2(H_{1,1}/\mathbb{F}_2) = 1$ and $N_4(H_{1,1}/\mathbb{F}_2) = 7$. Hence Condition (2) holds for all $n \leq 11$; moreover we check that $N_i(H_{1,1}/\mathbb{F}_2) > 0$ for all integers i such that $6 \leq i \leq 11$. So for any integer n such that $6 \leq n \leq 11$, the first step that verifies both Conditions (1) and (2) is $H_{1,1}/\mathbb{F}_2$.

(c) $g(H_2/\mathbb{F}_2) = 6$, $N_1(H_2/\mathbb{F}_2) = 3$, $N_2(H_2/\mathbb{F}_2) = 1$ and $N_4(H_2/\mathbb{F}_2) = 15$. Hence Condition (2) holds for all $n \leq 23$; moreover we know that $N_i(H_2/\mathbb{F}_2) > 0$ for all integers i such that $12 \leq i \leq 23$ since we have $2g(H_2/\mathbb{F}_2)+1 \leq 2^{\frac{i-1}{2}}(\sqrt{2}-1)$. Indeed $2g(H_2/\mathbb{F}_2)+1 = 13$ and $2^{\frac{i-1}{2}}(\sqrt{2}-1) \geq 2^{\frac{12-1}{2}}(\sqrt{2}-1) \geq 18$ for all integers i such that $12 \leq i \leq 23$. So for any integer n such that $12 \leq n \leq 23$, the first step that verifies both Conditions (1) and (2) is $H_2/\mathbb{F}_2$.

(d) $g(H_{2,1}/\mathbb{F}_2) = 23$, $N_1(H_{2,1}/\mathbb{F}_2) = 4$, $N_2(H_{2,1}/\mathbb{F}_2) = 1$ and $N_4(H_{2,1}/\mathbb{F}_2) = 28$. Hence Condition (2) holds for all $n \leq 32$; moreover we know that $N_i(H_2/\mathbb{F}_2) > 0$ for all integers i such that $24 \leq i \leq 27$ since we have $2g(H_{2,1}/\mathbb{F}_2)+1 \leq 2^{\frac{n-1}{2}}(\sqrt{2}-1)$. Indeed $2g(H_{2,1}/\mathbb{F}_2)+1 = 47$

and $2^{\frac{i-1}{2}}(\sqrt{2}-1) \geq 2^{\frac{24-1}{2}}(\sqrt{2}-1) \geq 1199$ for all integers i such that $24 \leq i \leq 27$. So for any integer n such that $24 \leq n \leq 27$, the first step that verifies both Conditions (1) and (2) is $H_{2,1}/\mathbb{F}_2$.

Note that, as in the first part of the proof, we have to use the step $(k, s+1)$ because Condition (2) is not verified for the step (k, s). □

Finally, we establish the following lemma which ensures us that given a finite set of places $\mathcal{P}$ and a divisor $\mathcal{D}$, up to equivalence we can suppose that the support of $\mathcal{D}$ does not contain any place in $\mathcal{P}$.

Lemma 2.7. *Let $F/\mathbb{F}_q$ be an algebraic function field and $\mathcal{P} := \{P_1, \ldots, P_N\}$ be a set of places of arbitrary degrees in $F/\mathbb{F}_q$. For any divisor $\mathcal{D}$, there exists a divisor $\mathcal{D}'$ such that $\mathcal{D}$ and $\mathcal{D}'$ are equivalents and $\mathcal{P} \cap \operatorname{supp} \mathcal{D} = \varnothing$.*

Proof. Let us consider the integers $n_1, \ldots, n_N$ defined by $n_i = 0$ if $P_i \notin \operatorname{supp} \mathcal{D}$ and $n_i = -\operatorname{ord}_{P_i} \mathcal{D}$ if $P_i \in \operatorname{supp} \mathcal{D}$. According to Strong Approximation Theorem (cf. [21, Theorem 1.6.5]), there exists an element $x \in F/\mathbb{F}_q$ such that for all integers $i \in \{1, \ldots, N\}$, $v_{P_i}(x) = n_i$ and for any place $P \notin \mathcal{P}$, $v_P(x) \geq 0$. Thus we have for all integers $i \in \{1, \ldots, N\}$, $\operatorname{ord}_{P_i}\big(\mathcal{D} + (x)\big) = \operatorname{ord}_{P_i} \mathcal{D} + n_i = 0$ i.e. the intersection $\mathcal{P} \cap \operatorname{supp}\big(\mathcal{D} + (x)\big)$ is empty, so $\mathcal{D}' := \mathcal{D} + (x)$ is a suitable $\mathcal{D}$-equivalent divisor. □

3. New bounds for the tensor rank

3.1. Adapted algorithm of type Chudnovsky and associated complexity

In this section, we use places of degree one, two and four to obtain new results for the tensor rank of multiplication in any extension of the finite field $\mathbb{F}_2$.

First of all, we specialize the general algorithm presented in Theorem 1.4 for places of degree one, two and four by using first derivative evaluations, i.e. with $u_i \leq 2$ for $i = 1, \ldots, N$.

Proposition 3.1. *Let*

- *q be a prime power,*
- *$F/\mathbb{F}_q$ be an algebraic function field,*
- *Q be a degree n place of $F/\mathbb{F}_q$,*
- *$\mathcal{D}$ be a divisor of $F/\mathbb{F}_q$,*
- *$\mathcal{P} = \{P_1, \ldots, P_{N_1}, P_{N_1+1}, \ldots, P_{N_1+N_2}, P_{N_1+N_2+1}, \ldots, P_{N_1+N_2+N_4}\}$ be a set of N_1 places of degree one, N_2 places of degree two and N_4 places of degree four.*
- *$0 \leq l_1 \leq N_1$, $0 \leq l_2 \leq N_2$ and $0 \leq l_4 \leq N_4$ be three 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*

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

is onto,

(b) *the map*

$$Ev_{\mathcal{P}} : \begin{cases} \mathcal{L}(2\mathcal{D}) \to \mathbb{F}_q^{N_1} \times \mathbb{F}_q^{l_1} \times \mathbb{F}_{q^2}^{N_2} \times \mathbb{F}_{q^2}^{l_2} \times \mathbb{F}_{q^4}^{N_4} \times \mathbb{F}_{q^4}^{l_4} \\ f \mapsto \big(f(P_1), \ldots, f(P_{N_1}), f'(P_1), \ldots, f'(P_{l_1}), f(P_{N_1+1}), \ldots, \\ \quad f(P_{N_1+N_2}), f'(P_{N_1+1}), \ldots, f'(P_{N_1+l_2}), f(P_{N_1+N_2+1}), \ldots, \\ \quad f(P_{N_1+N_2+N_4}), f'(P_{N_1+N_2+1}), \ldots, f'(P_{N_1+N_2+l_4})\big) \end{cases}$$

is injective.

Then

$$\mu_q(n) \leq N_1 + 2l_1 + 3N_2 + 6l_2 + \mu_q(4)\big(N_4 + 2l_4\big).$$

Proof. Up to reindexing the places, the result follows from Theorem 1.4 applied with $N = N_1 + N_2 + N_4$, $\deg P_i = 1$ for $i = 1, \ldots, N_1$, $\deg P_i = 2$ for $i = N_1 + 1, \ldots, N_1 + N_2$, $\deg P_i = 4$ for

$i = N_1 + N_2 + 1, \ldots, N$ and

$$u_i = \begin{cases} 2, & \text{if } 1 \le i \le l_1, \text{ or } N_1 + 1 \le i \le N_1 + l_2, \text{ or } N_1 + N_2 + 1 \le i \le N_1 + N_2 + l_4, \\ 1, & \text{else.} \end{cases}$$

Recall that for all prime powers q, $\mu_q(2) = 3$ and $\widehat{M_q}(2) \le 3$.

Applying Theorem 1.4, we get:

$$\begin{aligned} \mu_q(n) &\le \sum_{i=1}^{l_1} \mu_q(1)\widehat{M_q}(2) + \sum_{i=l_1+1}^{N_1} \mu_q(1)\widehat{M_q}(1) + \sum_{i=N_1+1}^{N_1+l_2} \mu_q(2)\widehat{M_{q^2}}(2) \\ &\quad + \sum_{i=N_1+l_2+1}^{N_1+N_2} \mu_q(2)\widehat{M_{q^2}}(1) + \sum_{i=N_1+N_2+1}^{N_1+N_2+l_4} \mu_q(4)\widehat{M_{q^4}}(2) + \sum_{i=N_1+N_2+l_4+1}^{N} \mu_q(4)\widehat{M_{q^4}}(1) \\ &\le 3l_1 + N_1 - l_1 + 9l_2 + 3(N_2 - l_2) + 3\mu_q(4)l_4 + \mu_q(4)(N_4 - l_4) \\ &= N_1 + 2l_1 + 3N_2 + 6l_2 + \mu_q(4)(N_4 + 2l_4). \quad \square \end{aligned}$$

Remark. Note that if l_1, l_2 and l_4 are three integers such that the map $Ev_{\mathcal{P}}$ is injective, then for any other integers L_1, L_2 and L_4 such that $l_1 \le L_1 \le N_1$, $l_2 \le L_2 \le N_2$ and $l_4 \le L_4 \le N_4$ the injectivity of the map is still valid but we obtain a bigger bound for the bilinear complexity. Consequently, we will try to use the optimal integers l_1, l_2 and l_4, that is to say the smallest integers for which the map $Ev_{\mathcal{P}}$ is injective. In particular, if $l_1 = l_2 = l_4 = 0$ is a suitable choice, then we can multiply in $\mathbb{F}_{q^n}$ without using derivative evaluations.

Theorem 3.2. *Let q be a prime power. Let $F/\mathbb{F}_q$ be an algebraic function field of genus g and N_i be a number of places of degree i in $F/\mathbb{F}_q$. Let l_1, l_2, l_4 be three integers such that $0 \le l_1 \le N_1$, $0 \le l_2 \le N_2$ and $0 \le l_4 \le N_4$. If*

(i) $N_n > 0$ $\left(\text{or } 2g + 1 \le q^{\frac{n-1}{2}}\left(q^{\frac{1}{2}} - 1\right)\right)$,

(ii) $N_1 + l_1 + 2(N_2 + l_2) + 4(N_4 + l_4) > 2n + 2g + 6$,

then

$$\mu_q(n) \le \frac{\mu_q(4)}{2}\big(n + g + 5\big) + \mu_q(4)l_4.$$

In particular,

$$\mu_2(n) \le \frac{9}{2}\big(n + g + 5\big) + 9l_4.$$

Proof. Let Q be a place of degree n in $F/\mathbb{F}_q$, which exists since (i). We can build a divisor $\mathcal{D}$ such that the map Ev_Q defined previously is onto. Indeed from Corollary 3.4 in [8], there exists a zero dimensional divisor $\mathcal{R}$ of degree $g - 5$. Let $\mathcal{D}$ be a divisor such that $\mathcal{D} \sim \mathcal{K} + Q - \mathcal{R}$, with $\mathcal{K}$ a canonical divisor. According to Lemma 2.7, we can choose $\mathcal{D}$ such that $Q \notin \operatorname{supp} \mathcal{D}$. Such a divisor $\mathcal{D}$ verifies $\deg \mathcal{D} = n + g + 3$ and by Riemann–Roch Theorem, we have $\dim(\mathcal{D} - Q) = 4$ since $i(\mathcal{D} - Q) = \dim(\mathcal{K} - \mathcal{D} + Q) = \dim \mathcal{R} = 0$. Moreover, by Riemann–Roch Theorem we get $\dim \mathcal{D} \ge n + 4$. Consequently, Ev_Q is onto since the dimension of its image verifies

$$\dim \operatorname{Im}(Ev_Q) = \dim \mathcal{D} - \dim(\mathcal{D} - Q) \ge n.$$

Let us set $N := N_1 + l_1 + 2(N_2 + l_2) + 4(N_4 + l_4)$. According to (ii), we know that $N > 2n + 2g + 6$ so without any loss of generality we can assume that $N = 2n + 2g + 7 + \epsilon$ with $\epsilon = 0, 1, 2, 3$. Let $\mathcal{P}$ be a set of N_1 places of degree one, N_2 places of degree two and N_4 places of degree four. According to Lemma 2.7, we can suppose that no place in $\mathcal{P}$ is in the support of $\mathcal{D}$. Note that we can apply Proposition 3.1 with the set of places $\mathcal{P}$ by using l_1 derivative evaluations on places of degree one, l_2

derivative evaluations on places of degree two and l_4 derivative evaluations on places of degree four. Indeed, let us denote by $\mathcal{A}$ the divisor $\mathcal{A} := \sum_{i=1}^{N_1+N_2+N_4} P_i + \sum_{i=1}^{l_1} P_i + \sum_{i=1}^{l_2} P_{N_1+i} + \sum_{i=1}^{l_4} P_{N_1+N_2+i}$, then we have $\deg \mathcal{A} = N$, so $\deg(2\mathcal{D} - \mathcal{A}) < 0$ by (ii) and $\ker Ev_{\mathcal{P}} = \mathcal{L}(2\mathcal{D} - \mathcal{A})$ is trivial. Thus, we get $\mu_q(n) \leq N_1 + 2l_1 + 3N_2 + 6l_2 + \mu_q(4)(N_4 + 2l_4)$ by Proposition 3.1. Now let us remark that this bound depends on the number of places of each degree we use in the second evaluation: the higher the degrees are, the bigger the bound is. Consequently, we must consider that $N_1 = N_2 = 0$ corresponding to the *worst case*. Then we obtain $\mu_q(n) \leq \mu_q(4)\left(\frac{N}{4} + l_4\right)$, which gives the result since $\frac{N}{4} \leq \frac{2n+2g+10}{4} = \frac{1}{2}(n+g+5)$. In particular, for $q = 2$ we get

$$\mu_2(n) \leq \frac{9}{2}\left(n+g+5\right) + 9l_4$$

since $\mu_2(4) = 9$. □

3.2. Tensor rank in any extension of $\mathbb{F}_2$

Now we apply the results of the preceding section to the tower of Garcia–Stichtenoth $T_3/\mathbb{F}_2$ presented in Section 2.2. We obtain two kinds of results: one which uses derivative evaluations and an other which does not. We will see later that we obtain a better bound for M_2 using derivative evaluations but this utilization is more complicated in practice and leads to an increase of linear complexity which can be inconvenient; so we present both techniques. Moreover, although the best results are obtained using derivative evaluations, we still get an improvement of the best known bound for M_2 using simple evaluations.

3.2.1. Bound for the tensor rank without using derivative evaluation

First of all, we apply the bound of Theorem 3.2 on the tower $T_3/\mathbb{F}_2$ with $l_1 = l_2 = l_4 = 0$.

Theorem 3.3. *For any integer $n \geq 2$, we have*

$$\mu_2(n) \leq \frac{45}{2}n + 85.5.$$

Proof. Let $q = p^2 = 4$ and let us consider the sequence of algebraic function fields $T_3 = \left\{H_{k,s}/\mathbb{F}_2\right\}$ introduced in Section 2.2. We set $M_{k,s} := N_1(H_{k,s}/\mathbb{F}_2) + 2N_2(H_{k,s}/\mathbb{F}_2) + 4N_4(H_{k,s}/\mathbb{F}_2)$. For any integer n, we know by Lemma 2.6 that there exists a step of the tower T_3 on which we can apply Theorem 3.2. Let $H_{k,s}/\mathbb{F}_2$ be the first step of the tower that suits the hypothesis of Theorem 3.2 with $l_1 = l_2 = l_4 = 0$. According to Lemma 2.6, this step is determined by the smallest integers k and s such that $2n \leq M_{k,s} - 2g_{k,s} - 7$, so $2n > M_{k,s-1} - 2g_{k,s-1} - 7$. For any integer $k \geq 1$ and for any integer $s = 0, 1, 2$, we have $g_{k,s} \leq q^{k-1}(q+1)p^s$ by Lemma 2.3(iii). Moreover, since $M_{k,s-1} \geq (q^2-1)q^{k-1}p^{s-1}$ by Proposition 2.2, we obtain $2n > (q^2 - 2q - 3)q^{k-1}p^{s-1} - 7$. Then since $q = 4$, we have $q^2 - 2q + 3 = (q+1)(q-3) = q+1$, which leads to $2np > (q+1)q^{k-1}p^s - 7p \geq g_{k,s} - 7p$ and it follows that $g_{k,s} \leq 2np + 7p$, so

$$\mu_2(n) \leq \frac{9}{2}\left(n + g_{k,s} + 5\right) \leq \frac{9}{2}n\,(1+2p) + \frac{9}{2}(7p+5)$$

by Theorem 3.2, which gives the result since $p = 2$. □

3.2.2. Bound for the tensor rank using derivative evaluations

Here, we apply results of Theorem 3.2 with an optimal number of derivative evaluations.

Theorem 3.4. *For any integer $n \geq 2$, we have*

$$\mu_2(n) \leq \frac{477}{26}n + \frac{45}{2}.$$

Proof. For any integer n, we know by Lemma 2.6 that there exists a step of the tower $T_3/\mathbb{F}_2$ on which we can apply Theorem 3.2 with $l_1 = l_2 = l_4 = 0$. We set $M_{k,s} := N_1(H_{k,s}/\mathbb{F}_2) + 2N_2(H_{k,s}/\mathbb{F}_2) +$

$4N_4(H_{k,s}/\mathbb{F}_2)$ for any step $H_{k,s}/\mathbb{F}_2$, with $k \geq 0$ and $s = 0, 1$. Let $H_{k,s+1}/\mathbb{F}_2$ be the first step of the tower that suits the hypothesis of Theorem 3.2 with $l_1 = l_2 = l_4 = 0$ i.e. k and s are integers such that $M_{k,s+1} > 2n + 2g_{k,s+1} + 6$ and $M_{k,s} \leq 2n + 2g_{k,s} + 6$. We denote by $n_0^{k,s}$ the biggest integer such that $M_{k,s} > 2n_0^{k,s} + 2g_{k,s} + 6$ i.e. $n_0^{k,s} := \sup\left\{n \in \mathbb{N} \mid 2n \leq M_{k,s} - 2g_{k,s} - 7\right\}$. To multiply in $\mathbb{F}_{2^n}$, we have the following alternative:

(a) to use the algorithm on the step $H_{k,s+1}$. In this case, a bound for the bilinear complexity is given by Theorem 3.2 applied with $l_1 = l_2 = l_4 = 0$:

$$\mu_2(n) \leq \frac{9}{2}(n + g_{k,s+1} + 5) = \frac{9}{2}(n_0^{k,s} + g_{k,s} + 5) + \frac{9}{2}(n - n_0^{k,s} + \Delta g_{k,s}).$$

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

(b) to use the algorithm on the step $H_{k,s}$ with derivative evaluations on l_1 places of degree one, l_2 places of degree two and l_4 places of degree four, where l_i satisfies $l_i \leq N_i(H_{k,s}/\mathbb{F}_2)$ for $i = 1, 2, 4$ and $M_{k,s} + l_1 + 2l_2 + 4l_4 > 2n + 2g_{k,s} + 6$. One can check that this condition is verified as soon as $l_1 + 2l_2 + 4l_4 \geq 2(n - n_0^{k,s})$, so Theorem 3.2 gives $\mu_2(n) \leq \frac{9}{2}\left(n + g_{k,s} + 5\right) + 9l_4$. Without any loss of generality, we can suppose that $l_1 + 2l_2 + 4l_4 = 2(n - n_0^{k,s}) + \epsilon$ with $\epsilon = 0, 1, 2, 3$. Moreover, we must consider that $l_1 = l_2 = 0$, which corresponds to the *worst case*. Thus we have $4l_4 = 2(n - n_0^{k,s}) + \epsilon \leq 4\left(\left[\frac{1}{2}(n - n_0^{k,s})\right] + 2\right)$ with $[\cdot]$ denoting the floor function, and we obtain the following bound for the bilinear complexity:

$$\begin{aligned}\mu_2(n) &\leq \frac{9}{2}(n + g_{k,s} + 5) + 9\left(\left[\frac{1}{2}(n - n_0^{k,s})\right] + 2\right)\\ &\leq \frac{9}{2}(n_0^{k,s} + g_{k,s} + 5) + 9(n - n_0^{k,s} + 2).\end{aligned}$$

Thus, if the integers l_i such that $l_1+2l_2+4l_4 = 2(n-n_0^{k,s})+\epsilon$ with $\epsilon = 0, 1, 2, 3$, verify $l_i \leq N_i(H_{k,s}/\mathbb{F}_2)$ for $i = 1, 2, 4$, i.e. $2(n-n_0^{k,s})+\epsilon \leq M_{k,s}$ then case (b) gives a better bound as soon as $\Delta g_{k,s} > n-n_0^{k,s}+4$.

For $x \in \mathbb{R}^+$ such that $M_{k,s+1} > 2[x] + 2g_{k,s+1} + 6$ and $M_{k,s} \leq 2[x] + 2g_{k,s} + 6$, we define the function $\Phi_{k,s}(x)$ as follows:

$$\Phi_{k,s}(x) = \begin{cases} 9(x - n_0^{k,s}) + \dfrac{9}{2}(n_0^{k,s} + g_{k,s} + 5) + 18 & \text{if } x - n_0^{k,s} + 4 < D_{k,s} \\ \dfrac{9}{2}(x - n_0^{k,s}) + \dfrac{9}{2}(n_0^{k,s} + g_{k,s} + 5 + \Delta g_{k,s}) & \text{else.}\end{cases}$$

Recall that $D_{k,s}$ was defined in Lemma 2.4 as $p^{s+1}q^{k-1}$.

Note that if $x - n_0^{k,s} + 4 < D_{k,s}$, then according to Lemma 2.4 we have both

$$x - n_0^{k,s} + 4 < \Delta g_{k,s},$$

so case (b) gives a better bound for the bilinear complexity, and

$$2(x - n_0^{k,s}) + \epsilon < 2D_{k,s} \leq M_{k,s} \quad \text{for } \epsilon = 0, 1, 2, 3,$$

so we can proceed as in case (b) since there are enough places of each degree to use derivative evaluations on l_1 places of degree one, l_2 places of degree two and l_4 places of degree four with $l_1 + 2l_2 + 4l_4 = 2(n - n_0^{k,s}) + \epsilon$.

We define the function Φ for all $x \geq 0$ as the minimum of the functions $\Phi_{k,s}$ for which x is in the domain of $\Phi_{k,s}$. This function is piecewise linear with two kinds of pieces: those which have slope $\frac{9}{2}$ and those which have slope 9. 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 $\left(n_0^{k,s} + D_{k,s} - 4, \Phi(n_0^{k,s} + D_{k,s} - 4)\right)$, since these are the *vertices* of the graph. Let $X := n_0^{k,s} + D_{k,s} - 4$,

then

$$\Phi(X) = \frac{9}{2}(X + g_{k,s+1} + 5) = \frac{9}{2}\left(1 + \frac{g_{k,s+1}}{X}\right)X + \frac{45}{2}.$$

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

Lemmas 2.3(iii) and 2.5 give

$$\begin{aligned}\frac{g_{k,s+1}}{X} &\le \frac{q^{k-1}(q+1)p^{s+1}}{\frac{5}{2}q^{k-1} - \frac{7}{2} + p^{s+1}q^{k-1} - 4}\\ &= \frac{q+1}{\frac{5}{2p^{s+1}} + 1 - \frac{15}{2q^{k-1}p^{s+1}}}\\ &\le \frac{5}{\frac{13}{8} - \frac{15}{4\cdot 4^{k-1}}}\\ &\le \frac{40}{13}.\end{aligned}$$

Thus, the graph of the function Φ lies below the line $y = \frac{9}{2}\left(1 + \frac{40}{13}\right)x + \frac{45}{2}$. In particular, we get

$$\Phi(n) \le \frac{9}{2}\left(1 + \frac{40}{13}\right)n + \frac{45}{2}. \quad \square$$

4. New asymptotic bounds for the tensor rank

Without using derivative evaluation, we obtain from Theorem 3.3 the following bound for M_2:

$$M_2 \le 22.5,$$

which is better than the best known bound recalled in Proposition 1.7.

However, it follows from Theorem 3.4 that we obtain a better bound for M_2 by using derivative evaluations, namely:

Theorem 4.1.

$$M_2 \le \frac{477}{26} \approx 18.35.$$

References

[1] Nicolas Arnaud, Évaluations dérivées, multiplication dans les corps finis et codes correcteurs, Ph.D. 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 (1999) 364–377.
[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 (2003) 472–478.
[4] Stéphane Ballet, On the tensor rank of the multiplication in the finite fields, Journal of Number Theory 128 (2008) 1795–1806.
[5] Stéphane Ballet, Jean Chaumine, On the bounds of the bilinear complexity of multiplication in some finite fields, Applicable Algebra in Engineering, Communication and Computing 15 (2004) 205–211.
[6] Stéphane Ballet, 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 of Number Theory 116 (2006) 293–310.
[7] Stéphane Ballet, Dominique Le Brigand, 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, vol. 21, Société Mathématique de France, sér. Séminaires et Congrès, 2009, pp. 187–203.
[8] Stéphane Ballet, Christophe Ritzenthaler, Robert Rolland, On the existence of dimension zero divisors in algebraic function fields defined over $\mathbb{F}_q$, Acta Arithmetica 143 (4) (2010) 377–392.
[9] Stéphane Ballet, Robert Rolland, Families of curves over any finite field attaining the generalized Drinfeld–Vladut bound, Publ. Math. Univ. Franche-Comté Besançon Algèbr. Theor. Nr. (2011) 5–18.

[10] Stéphane Ballet, Robert Rolland, Multiplication algorithm in a finite field and tensor rank of the multiplication, Journal of Algebra 272 (1) (2004) 173–185.
[11] Ulrich Baum, Amin Shokrollahi, An optimal algorithm for multiplication in $\mathbb{F}_{256}/\mathbb{F}_4$, Applicable Algebra in Engineering, Communication and Computing 2 (1) (1991) 15–20.
[12] Peter Bürgisser, Michael Clausen, Amin Shokrollahi, Algebraic Complexity Theory, in: Grundlehren der Mathematischen Wissenchaften, vol. 315, Springer, 1997.
[13] Murat Cenk, Ferruh Özbudak, On multiplication in finite fields, Journal of Complexity (2009) doi:10.1016/j.jco.2009.11.002.
[14] David Chudnovsky, Gregory Chudnovsky, Algebraic complexities and algebraic curves over finite fields, Journal of Complexity 4 (1988) 285–316.
[15] Mario Daberkow, Claus Fieker, Jürgen Klüners, Michael E. Pohst, Roegner Katherine, Klaus Wildanger, KANT V4, Journal of Symbolic Computation 24 (1997) 267–283.
[16] Hans de Groote, Characterization of division algebras of minimal rank and the structure of their algorithm varieties, SIAM Journal on Computing 12 (1) (1983) 101–117.
[17] Arnaldo Garcia, Henning Stichtenoth, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, Inventiones Mathematicae 121 (1995) 211–222.
[18] Harald Niederreiter, Chaoping Xing, Algebraic Geometry in Coding Theory & Cryptography, Princeton University Press, 2009.
[19] Amin Shokhrollahi, Optimal algorithms for multiplication in certain finite fields using algebraic curves, SIAM Journal on Computing 21 (6) (1992) 1193–1198.
[20] Igor Shparlinski, Michael Tsfasman, Serguei Vladut, Curves with many points and multiplication in finite fields, in: H. Stichtenoth, M.A. Tsfasman (Eds.), Coding Theory and Algebraic Geometry, in: Lectures Notes in Mathematics, vol. 1518, Springer-Verlag, Berlin, 1992, pp. 145–169. Proceedings of AGCT-3 Conference, June 17–21, 1991, Luminy.
[21] Henning Stichtenoth, Algebraic Function Fields and Codes, second ed., in: Graduate Texts in Mathematics, vol. 254, Springer, 2008.
[22] Shmuel Winograd, On multiplication in algebraic extension fields, Theoretical Computer Science 8 (1979) 359–377.