ON THE TENSOR RANK OF MULTIPLICATION IN ANY EXTENSION OF $\mathbb{F}_2$

STÉPHANE BALLET AND JULIA PIELTANT

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. In 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 $\mathbb{F}_{2^4}$.

1. Introduction

1.1. **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 ordinary 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 multiplicative 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 $\mathbb{F}_q$.

1.2. **Known results.**

1.2.1. *General results.* From the existence of towers of algebraic function fields satisfying good properties, it was proved:

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:*

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

Date: April 22, 2010.
2000 *Mathematics Subject Classification.* Primary 14H05; Secondaries 11Y16, 12E20.
Key words and phrases. Algebraic function fields, tower of function fields, tensor rank, algorithm, finite fields.

where C_q is the constant defined by:

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

In order to obtain these good estimates for the constant C_q, S. Ballet has given in [2] 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 [7] 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 N. Arnaud in [1] and M. Cenk and F. Özbudak in [10]. 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 M. Cenk and F. Özbudak in [10] and defined as follows:

Definition 1.2. *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 $\mathbb{F}_q[x]$.*

Now we introduce the generalized algorithm of type Chudnovsky described in [10].

Theorem 1.3. *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 application

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

is onto,

b) the application

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

is injective, where the application φ_i is defined by

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

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

Then

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

Let us remark that the algorithm given in [11] 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, in [1] N. Arnaud has presented a simplified version of this algorithm where all integers $u_i = 2$ and places are of degree one and two. Applying his algorithm on Garcia-Stichtenoth towers, he obtained the two following bounds.

Theorem 1.4. *Let $q = p^r \geq 4$ be a prime power. Then*

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

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

1.2.2. *Asymptotic bounds for the extensions of $\mathbb{F}_2$.* From the asymptotic point of view, let us recall that I. Shparlinski, M. Tsfasman and S. Vladut have given in [13] 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 [13], they claim that $M_2 \leq 27$ but I. Cascudo, R. Cramer and C. Xing recently noticed in [9] a gap in the proof about $M_2 \leq 27$ established by I. Shparlinsky, M. Tsfasman and S. Vladut. Consequently, we can consider this bound as not proved. Anyway, it is possible to obtain easily a better bound for M_2 from one of the bounds of N. Arnaud. Indeed, by using Bound (ii) of Theorem 1.4 we obtain:

Proposition 1.5.

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

1.3. **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 this aim, we use a modified Garcia-Stichtenoth's tower [12] studied in [3], [7], [6] and [4]. Specially, we apply an adapted version of the generalized algorithm of type Chudnosky which involves only places of degree one, two and four with derivative evaluations to the descent of the definition field of this Garcia-Stichtenoth's tower on the field $\mathbb{F}_2$ obtained in [8].

2. New bounds for the tensor rank

2.1. **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 1.3 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 2.1. *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 application

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

is onto,

b) the application

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

is injective.

Then

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

This specialization yields the followings bounds for the tensor rank of multiplication in any extension of $\mathbb{F}_2$:

Theorem 2.2. *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 $0 \leq l_1 \leq N_1$, $0 \leq l_2 \leq N_2$ and $0 \leq l_4 \leq N_4$. If*

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

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

then

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

In particular,

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

2.2. **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 [8]. We obtain two kinds of result: one which uses derivative evaluations and an other which does not. In fact 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 technics. 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.

2.2.1. *Bound for the tensor rank without using derivative evaluation.* First of all, we apply the bound of Theorem 2.2 on the tower $T_3/\mathbb{F}_2$ with $l_1 = l_2 = l_4 = 0$. This yields:

Theorem 2.3. *For any integer $n \geq 2$, we have*

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

2.2.2. *Bound for the tensor rank using derivative evaluations.* Here, we apply results of Theorem 2.2 with an optimal number of derivative evaluations.

Theorem 2.4. *For any integer $n \geq 2$, we have*

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

3. New asymptotic bounds for the tensor rank

Without using derivative evaluation, we obtain from Theorem 2.3 the following bound for M_2:

$$M_2 \leq 22.5,$$

which is better than the best known bound recalled in Proposition 1.5.

However, by using derivative evaluations, we obtain a better bound for M_2, namely:

Theorem 3.1.

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

Proof. It follows from Theorem 2.4. □

References

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

[2] Stéphane Ballet. Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$. *Finite Fields and Their Applications*, 5:364–377, 1999.

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

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

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

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

[7] Stéphane Ballet and Robert Rolland. Multiplication algorithm in a finite field and tensor rank of the multiplication. *Journal of Algebra*, 272(1):173–185, 2004.

[8] Stéphane Ballet and Robert Rolland. Families of curves over any finite field with a class number greater than the Lachaud - Martin-Deschamps bounds. ArXiv:0906.5432v1, 2009.

[9] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. Torsion-limits for tower and asymptotically good special codes in secure computation and complexity. 2009.

[10] Murat Cenk and Ferruh Özbudak. On multiplication in finite fields. *Journal of Complexity*, doi:10.1016/j.jco.2009.11.002, 2009.

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

[12] 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.

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

Institut de Mathématiques de Luminy, case 930, F13288 Marseille cedex 9, France

eRISCS Groupe de Recherche "Informatique des Systèmes Communicants Sécurisés"
E-mail address: stephane.ballet@univmed.fr

Institut de Mathématiques de Luminy, case 930, F13288 Marseille cedex 9, France

eRISCS Groupe de Recherche "Informatique des Systèmes Communicants Sécurisés"
E-mail address: julia.pieltant@univmed.fr