Tower of algebraic function fields with maximal Hasse-Witt invariant and tensor rank of multiplication in any extension of $\mathbb{F}_2$ and $\mathbb{F}_3$

Stéphane Ballet

Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France.

Julia Pieltant[1,*]

Inria – Saclay Île-de-France, LIX, École Polytechnique, 91128 Palaiseau Cedex, France.

Abstract

Up until now, it was recognized that a detailed study of the p-rank in towers of function fields is relevant for their applications in coding theory and cryptography. In particular, it appears that having a large p-rank may be a barrier for a tower to lead to competitive bounds for the symmetric tensor rank of multiplication in every extension of the finite field $\mathbb{F}_q$, with q a power of p. In this paper, we show that there are two exceptional cases, namely the extensions of $\mathbb{F}_2$ and $\mathbb{F}_3$. In particular, using the definition field descent on the field with 2 or 3 elements of a Garcia-Stichtenoth tower of algebraic function fields which is asymptotically optimal in the sense of Drinfel'd-Vlăduţ and has maximal Hasse-Witt invariant, we obtain a significant improvement of the uniform bounds for the symmetric tensor rank of multiplication in any extension of $\mathbb{F}_2$ and $\mathbb{F}_3$.

Keywords: Algebraic function field, tower of function fields, tensor rank, algorithm, finite field.

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, as shown by the growing number of publications on this topic including amoung others [12], [18], [2], [11], [5], [16].

[*] Corresponding author.

Email addresses: stephane.ballet@univ-amu.fr (Stéphane Ballet), pieltant@lix.polytechnique.fr (Julia Pieltant)

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

[1] Present address: *CNRS LTCI, Télécom ParisTech , 46 rue Barrault, 75634 Paris Cedex 13, France.*

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.

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. The multiplication in the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$ is a bilinear map from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ into $\mathbb{F}_{q^n}$, thus it corresponds to a tensor $t \in \mathbb{F}^\star_{q^n} \bigotimes \mathbb{F}^\star_{q^n} \bigotimes \mathbb{F}_{q^n}$ where $\mathbb{F}^\star_{q^n}$ 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

$$t = \sum_{\ell=1}^{\lambda} a_\ell \otimes b_\ell \otimes c_\ell$$

where $a_\ell \in \mathbb{F}^\star_{q^n}$, $b_\ell \in \mathbb{F}^\star_{q^n}$, $c_\ell \in \mathbb{F}_{q^n}$, then

$$x \cdot y = t(x \otimes y) = \sum_{\ell=1}^{\lambda} a_\ell(x) b_\ell(y) c_\ell. \qquad (1)$$

Every expression (1) is called a bilinear multiplication algorithm $\mathscr{U}$ (resp. a symmetric bilinear multiplication algorithm if $a_\ell = b_\ell$ for all $\ell \in \{1, \ldots, \lambda\}$). The integer λ is called the tensor rank (resp. symmetric tensor rank) of the algorithm $\mathscr{U}$, or the bilinear complexity (resp. symmetric bilinear complexity) of the algorithm $\mathscr{U}$.
Let us set

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

respectively

$$\mu_q^{\mathsf{sym}}(n) := \min_{\mathscr{U}^{\mathsf{sym}}} \mu(\mathscr{U}^{\mathsf{sym}}),$$

where $\mathscr{U}$ is running over all bilinear multiplication algorithms (resp. $\mathscr{U}^{\mathsf{sym}}$ is runnig over all symmetric such algorithms) in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
It is interesting to study the minimal length of a symmetric multiplication algorithm since it turns out that it plays an important role in several other areas such as Riemann-Roch system of equations, arithmetic secret sharing, multiplication-friendly codes, etc, as mentioned in [9].

1.3. *Basic notions related to function fields and notation*

Let $\mathbf{F}/\mathbb{F}_q$ be an algebraic function field of one variable of genus g, with constant field $\mathbb{F}_q$. For any integer $k \geq 1$, we denote by $\mathsf{P}_k(\mathbf{F}/\mathbb{F}_q)$ the set of places of degree k, by $\mathsf{B}_k(\mathbf{F}/\mathbb{F}_q)$ the cardinality of this set and by $\mathsf{P}(\mathbf{F}/\mathbb{F}_q) = \cup_k \mathsf{P}_k(\mathbf{F}/\mathbb{F}_q)$ the set of all places in $\mathbf{F}/\mathbb{F}_q$. For any place P, we define F_P to be the residue class field of P and $\mathscr{O}_P$ its valuation ring. Every element $t \in P$ such that $P = t\mathscr{O}_P$ is called a local parameter for P. The support of $\mathscr{D} = \sum_P a_P P$ is the set of the places P such that $a_P \neq 0$. For any divisor $\mathscr{D}$ of $\mathbf{F}/\mathbb{F}_q$, the Riemann-Roch $\mathbb{F}_q$-vector-space associated to $\mathscr{D}$ is the set

$$\mathscr{L}(\mathscr{D}) = \{f \in \mathbf{F}/\mathbb{F}_q \mid \mathscr{D} + (f) \geq 0\} \cup \{0\}.$$

The Riemann-Roch Theorem states that the dimension $\dim \mathscr{D}$ of the vector space $\mathscr{L}(\mathscr{D})$ is related to the degree of the divisor $\mathscr{D}$ and to the genus of $\mathbf{F}/\mathbb{F}_q$ by:

$$\dim \mathscr{D} = \deg \mathscr{D} - g + 1 + \dim(\kappa - \mathscr{D}), \tag{2}$$

where κ denotes a canonical divisor of $\mathbf{F}/\mathbb{F}_q$. In this relation, the complementary term $\mathrm{i}(\mathscr{D}) := \dim(\kappa - \mathscr{D})$ is called the index of speciality of $\mathscr{D}$. Note that in any case, we have $\mathrm{i}(\mathscr{D}) \geq 0$. In particular, a divisor $\mathscr{D}$ is called a non-special divisor when the index of speciality $\mathrm{i}(\mathscr{D})$ is zero and $\mathscr{D}$ is called a special divisor if $\mathrm{i}(\mathscr{D}) > 0$.

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 [20] and de Groote [13] 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 Chudnovsky-Chudnovsky algorithm [12] applied to elliptic curves, Shokrollahi has shown in [17] 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:

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

Eventually, the original algorithm of D.V. and G.V. Chudnovsky introduced in [12] leads to the following theorem by [3]:

Theorem 1. *Let q be a prime power. The tensor rank $\mu_q(n)$ of multiplication in any finite extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ is linear with respect to the extension degree; more precisely, there exists a constant C_q such that for any n, it holds that:*

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

Moreover, one can give explicit values for C_q; in particular for $q=2$ or $q=3$:

Proposition 2. *The best known values for the constant C_q defined in the previous theorem are:*

$$C_q = \begin{cases} 19.6 & \text{if } q=2 \quad [11], [5] \\ \\ 27 & \text{if } q=3 \quad [3] \end{cases}$$

Remark. The estimate $C_2 = 19.6$ is obtained by combining the general uniform bound $\mu_2^{\mathrm{sym}}(n) \leq \frac{477}{26}n + \frac{45}{2}$ from [5] for n greater than 19, and the values of $\mu_2^{\mathrm{sym}}(n)$ given in [11, Table 1] for $n \leq 18$ (see Appendix).

Let us present the best finalized version of this algorithm in its symmetrical version, which is a generalization of the algorithm of Chudnovsky-Chudnovsky type introduced by Arnaud in [2] and developed later by Cenk and Özbudak in [11]. 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 symmetric bilinear complexity involves the complexity notion $\widehat{M}_q(u)$ introduced by Cenk and Özbudak in [11] and defined as follows:

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

Note that in [16], Randriambololona gives an even more general version of the Chudnovsky-Chudnovsky algorithm, which encompass the case of non-necessarily symmetric algorithms. This generalization is not relevant here, since we focus on the symmetric tensor rank; thus we introduce the generalized symmetric algorithm Chudnovsky-Chudnovsky type described in [11].

Theorem 4. *Let*

- *q be a prime power,*
- *$\mathbf{F}/\mathbb{F}_q$ be an algebraic function field,*
- *Q be a degree n place of $\mathbf{F}/\mathbb{F}_q$,*
- *$\mathscr{D}$ be a divisor of $\mathbf{F}/\mathbb{F}_q$,*
- *$\mathscr{P} = \{P_1, \ldots, P_N\}$ be a set of N places of arbitrary degree,*
- *$t_1, \ldots, t_N$ be local parameters for $P_1, \ldots, P_N$ respectively,*
- *$u_1, \ldots, u_N$ be positive integers.*

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

a) the map

$$\mathsf{Ev}_Q : \left| \begin{array}{ccc} \mathscr{L}(\mathscr{D}) & \rightarrow & \mathbb{F}_{q^n} \simeq \mathrm{F}_Q \\ f & \longmapsto & f(Q) \end{array} \right.$$

is onto,

b) the map

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

is injective, where each application φ_i is defined by

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

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

Then

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

In particular, we will consider in this paper a specialization of this algorithm which is described in Section 4 and requires the additional hypothesis that there exists a non-special divisor of degree $g-1$; this will motivate the study of ordinary towers.

1.4.2. Asymptotic bounds for the extensions of $\mathbb{F}_2$ *and* $\mathbb{F}_3$

The following asymptotic bound for the bilinear complexity was introduced in [18]:

$$\mathrm{M}_q^{\mathrm{sym}} := \limsup_{k\to\infty} \frac{\mu_q^{\mathrm{sym}}(k)}{k}.$$

Recently, with the help of the torsion-limit technique and Riemann-Roch systems, Cascudo, Cramer and Xing improved in [9] the upper bounds for $\mathrm{M}_q^{\mathrm{sym}}$ in the case where q is small ($q \in \{2,3,4,5\}$). In particular, from optimal towers with asymptotically few 2-torsion points relatively to the genus they obtained:

$$\mathrm{M}_2^{\mathrm{sym}} \leq 7.23 \qquad \text{and} \qquad \mathrm{M}_3^{\mathrm{sym}} \leq 5.45.$$

1.5. Motivations – New results established in this paper

As mentioned in [9] by Cascudo, Cramer and Xing, and in [7] by Bassa and Beelen, it is widely accepted that towers of algebraic function fields having a large p-rank are less efficient for certain applications to information theory.

Indeed, for example, in [7], it reads: *"A detailed study of the p-rank in towers is relevant for their applications, see [8]. For example, although both of the towers introduced in [15] and [14] have the same limit and hence are equally influential for applications in coding theory, a detailed study of their p-rank reveals that in fact the latter* [2] *is more appropriate for other kinds of applications, e.g. secure multiparty computation and fast bilinear multiplication."* In particular, it appears that having a large p-rank may be a barrier for a tower to lead to competitive bounds for the symmetric tensor rank of multiplication in every extension of the finite field $\mathbb{F}_q$, with q a power of p. In this paper, we show that there are two exceptional cases, namely the extensions of $\mathbb{F}_2$ and $\mathbb{F}_3$. More precisely, we will show that an ordinary tower may lead to better uniform results for the tensor rank of multiplication in any extension of $\mathbb{F}_2$ and $\mathbb{F}_3$ than a non-ordinary one because of the link between maximal p-rank and existence of a non-special divisor of degree $g-1$. Indeed, we know that the existence of a non-special divisor of degree $g-1$ in the function field $\mathbf{F}/\mathbb{F}_q$ is of crucial importance in the performance of Chudnovsky-Chudnovsky type algorithms over $\mathbb{F}_q$ designed from $\mathbf{F}/\mathbb{F}_q$

[2] which turns out not to be ordinary, according to [9]

[4], [16]. When the definition field $\mathbb{F}_q$ is such that $q \geq 4$, then according to [4] there always exists a non-special divisor of degree $g-1$. Nevertheless, the problem persists in the case where the definition field is $\mathbb{F}_2$ or $\mathbb{F}_3$. In [5], to avoid this obstacle, we substituted non-special divisors of degree $g-1$ for zero-dimensional divisors whose degree is as close as possible to $g-1$, in the descent over $\mathbb{F}_2$ of the original Garcia-Stichtenoth tower presented in [14] and defined over $\mathbb{F}_{16}$; non-special divisors of degree $g-1$ being the borderline case of zero-dimensional divisors. However, Bassa and Beelen established in [7] that the second optimal Garcia-Stichtenoth tower introduced in [15] and defined over $\mathbb{F}_{q^2}$ is ordinary. On the other hand, it was shown in [6] that there always exists a non-special divisor of degree $g-1$ in any ordinary function field. In this article, we combine these two results to a modified version of the optimal tower studied by Bassa and Beelen which improves the results obtained in [5]. Namely we define intermediate steps for the tower and descend the definition field from $\mathbb{F}_{16}$ to $\mathbb{F}_2$, and from $\mathbb{F}_9$ to $\mathbb{F}_3$ respectively, which lead us to the two following bounds:

$$\mu_2^{\mathrm{sym}}(n) \leq 15.23n + \frac{9}{2} \qquad \text{and} \qquad \mu_3^{\mathrm{sym}}(n) \leq 7.732n.$$

Note that the difficulty to obtain non-asymptotic estimations of the 2-torsion points in all steps of the tower used in [9] is an obstruction to obtain uniform bounds as we get in this paper.

2. Definitions and related properties of the p-rank

Definition 5. *The p-rank $\gamma(\mathbf{F})$, also called Hasse-Witt invariant, of a function field $\mathbf{F}$ with constant field $\overline{\mathbb{F}_p}$, the algebraic closure of the finite field $\mathbb{F}_p$, is defined as the dimension over $\mathbb{F}_p$ of the group of divisor classes of degree zero of order p.*
If the function field is defined over a finite field $\mathbb{F}_q$, we define its p-rank as the p-rank of the function field $\mathbf{F}\overline{\mathbb{F}_q}$, obtained by extending the constant field to the algebraic closure of $\mathbb{F}_q$.

It can be shown that :

Proposition 6. *If $\mathbf{F}/\mathbb{F}_q$ be a function field of genus $g(\mathbf{F})$, then $0 \leq \gamma(\mathbf{F}) \leq g(\mathbf{F})$.*

Definition 7. *A function field $\mathbf{F}/\mathbb{F}_q$ is called ordinary if $\gamma(\mathbf{F}) = g(\mathbf{F})$.*
A tower of function fields $\mathscr{T} = \left(\mathbf{F}_n/\mathbb{F}_q\right)_{n\in\mathbb{N}}$ is said ordinary if for any $n \geq 0$, $\mathbf{F}_n$ is such that $\gamma(\mathbf{F}_n) = g(\mathbf{F}_n)$, i.e. if any step of the tower is an ordinary function field.

Let us recall the following result from [6]:

Corollary 8. *If $\mathbf{F}$ is an ordinary function field of genus $g > 0$ defined over $\mathbb{F}_2$ or over $\mathbb{F}_3$, then there is always a degree $g-1$ zero-dimensional divisor in $\mathbf{F}$.*

Moreover, directly from Definition 5, we can deduce the following lemma:

Lemma 9. *Let $r \geq 0$ be an integer. If we set $\mathbf{F}/\mathbb{F}_{q^r} := \mathbf{H}/\mathbb{F}_q \otimes \mathbb{F}_{q^r}$, then $\mathbf{H}/\mathbb{F}_q$ is ordinary if and only if $\mathbf{F}/\mathbb{F}_{q^r}$ is ordinary.*

PROOF. Note that the genus does not change under constant field extension or descent. It follows from Definition 5 that p-rank does not change under constant field extension or descent since the p-rank of a function field $\mathbf{F}/\mathbb{F}_q$ defined over a finite field $\mathbb{F}_q$ is equal to the p-rank of $\mathbf{F}\overline{\mathbb{F}_q}$. □

To conclude this section, we recall the following result which is proven in [7, Lemma 6, 2.]:

Lemma 10. *If $\mathbf{H}/\mathbf{F}$ is a finite extension of function fields with same constant field $\mathbb{F}_q$, then*

$$g(\mathbf{H})-\gamma(\mathbf{H})\geq g(\mathbf{F})-\gamma(\mathbf{F}).$$

In particular, if $\mathbf{H}$ is ordinary then so is $\mathbf{F}$.

3. Good ordinary sequences of function fields defined over $\mathbb{F}_2$ or $\mathbb{F}_3$

In this section, we present sequences of algebraic function fields defined over $\mathbb{F}_2$ or $\mathbb{F}_3$, constructed from the well-known Garcia-Stichtenoth tower defined in [15], which will be used to obtain new bounds for the tensor rank of multiplication.

3.1. *Definition of the Garcia-Stichtenoth's tower*

Let us consider a finite field $\mathbb{F}_{q^2}$ with $q=p^r$, for p a prime number and r an integer. We consider the Garcia-Stichtenoth's elementary abelian tower T_0 over $\mathbb{F}_{q^2}$ constructed in [15] and defined by the sequence $(\mathbf{F}_0,\mathbf{F}_1,\mathbf{F}_2,\ldots)$ where

$$\mathbf{F}_0:=\mathbb{F}_{q^2}(x_0)$$

is the rational function field over $\mathbb{F}_{q^2}$, and for any $i\geq 0$, $\mathbf{F}_{i+1}:=\mathbf{F}_i(x_{i+1})$ with x_{i+1} satisfying the following equation:

$$x_{i+1}^q+x_{i+1}=\frac{x_i^q}{x_i^{q-1}+1}.$$

Let us denote by g_i the genus of $\mathbf{F}_i$ in $T_0/\mathbb{F}_{q^2}$ and recall the following formulæ:

$$g_i=\begin{cases}(q^{\frac{i+1}{2}}-1)^2 & \text{for odd } i,\\ (q^{\frac{i}{2}}-1)(q^{\frac{i+2}{2}}-1) & \text{for even } i.\end{cases}\tag{3}$$

Thus, according to these formulæ, it is straightforward that the genus of any step of the tower satisfies:

$$(q^{\frac{i}{2}}-1)(q^{\frac{i+1}{2}}-1)<g(\mathbf{F}_i)<(q^{\frac{i+2}{2}}-1)(q^{\frac{i+1}{2}}-1).\tag{4}$$

Moreover, a tighter upper bound will be useful and can be obtained by expanding expressions in (3):

$$g(\mathbf{F}_i)\leq q^{i+1}-2q^{\frac{i+1}{2}}+1.\tag{5}$$

If the characteristic $p=2$ and $r=2$, i.e. $q=4$, then we can densify the Garcia-Stichtenoth's tower with steps defined over the finite field $\mathbb{F}_{q^2}$ by considering the following completed tower:

$$T_1/\mathbb{F}_{16}\ :\qquad \mathbf{F}_{0,0}\subseteq \mathbf{F}_{0,1}\subseteq \mathbf{F}_{0,2}=\mathbf{F}_{1,0}\subseteq \mathbf{F}_{1,1}\subseteq \mathbf{F}_{1,2}=\mathbf{F}_{2,0}\subseteq\cdots$$

such that $\mathbf{F}_i\subseteq \mathbf{F}_{i,s}\subseteq \mathbf{F}_{i+1}$ for any integer $s\in\{0,1,2\}$, with $\mathbf{F}_{i,0}:=\mathbf{F}_i$ and $\mathbf{F}_{i,2}:=\mathbf{F}_{i+1}$. Indeed:

Proposition 11. *There exists a tower T_1 defined over $\mathbb{F}_{16}$ whose recursive equation is defined over $\mathbb{F}_2$. More precisely, the tower T_1 is the densified Garcia-Stichtenoth's tower over $\mathbb{F}_{16}$ and is defined by $T_1=\left(\mathbf{F}_{i,s}\right)_{\substack{\mathrm{i}\geq 0\\ s\in\{0,1\}}}$ where for any $i\geq 0$:*

$$\mathbf{F}_{i,0}:=\mathbf{F}_i\qquad \textit{and}\qquad \mathbf{F}_{i,1}:=\mathbf{F}_i(t_{i+1})$$

with t_{i+1} satisfying the equation:

$$t_{i+1}^2+t_{i+1}=\frac{x_i^4}{x_i^3+1}\quad \textit{for } i=0,\ldots,n-1. \tag{6}$$

PROOF. Let x_0 be a transcendental element over $\mathbb{F}_2$ and let us set

$$\mathbf{F}_0:=\mathbb{F}_{16}(x_0).$$

We define recursively for $i\geq 0$

(i) x_{i+1} such that $x_{i+1}^4+x_{i+1}=\frac{x_i^4}{x_i^3+1}$ for $i=0,\ldots,n-1$,

(ii) t_{i+1} such that $t_{i+1}^2+t_{i+1}=\frac{x_i^4}{x_i^3+1}$ for $i=0,\ldots,n-1$,
(or alternatively $t_{i+1}=x_{i+1}^2+x_{i+1}$).

Thus, we can define recursively the tower T_1 by setting:

$$\mathbf{F}_{i,1}=\mathbf{F}_{i,0}(t_{i+1})=\mathbf{F}_i(t_{i+1})\qquad \text{and}\qquad \mathbf{F}_{i+1,0}=\mathbf{F}_{i+1}=\mathbf{F}_i(x_{i+1}).$$

□

Let us remark that it is possible to densify the general Garcia-Stichtenoth's tower over $\mathbb{F}_{q^2}$ for any characteristic p and for any integer r since each extension $\mathbf{F}_{i+1}/\mathbf{F}_i$ is Galois of degree $q=p^r$ with full constant field $\mathbb{F}_{q^2}$. However, in the general case the equation (6) for the intermediate steps is not defined over $\mathbb{F}_p$ but over $\mathbb{F}_q$. For example, for $p=3$ and $r=2$, we obtain an equation which is defined over $\mathbb{F}_9$.

Notation. In the sequel, we will denote by $\mathrm{B}_k(\mathbf{F}/K)$ the number of places of degree k of an algebraic function field $\mathbf{F}/K$ defined over a finite field K; we will also denote by $g_{i,s}$ the genus of $\mathbf{F}_{i,s}/\mathbb{F}_{16}$ in $T_1/\mathbb{F}_{16}$.

3.2. Descent of the definition field of the Garcia-Stichtenoth's tower on the fields $\mathbb{F}_2$ and $\mathbb{F}_3$

First we state that when $q = 3$, one can descend the definition field of the tower $T_0/\mathbb{F}_{q^2}$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ since the recursive equation defining the tower has coefficients lying in $\mathbb{F}_q$. Thus, we have the following result:

Proposition 12. *If $q = p = 3$, there exists a tower $E/\mathbb{F}_q$ defined over $\mathbb{F}_q$ given by a sequence:*

$$\mathbf{G}_0 \subseteq \mathbf{G}_1 \subseteq \mathbf{G}_2 \subseteq \mathbf{G}_3 \subseteq \cdots$$

defined over the constant field $\mathbb{F}_q$ and related to the tower $T_0/\mathbb{F}_{q^2}$ by

$$\mathbf{F}_i = \mathbb{F}_q \mathbf{G}_i \quad \textit{for all } i,$$

namely $\mathbf{F}_i/\mathbb{F}_{q^2}$ is the constant field extension of $\mathbf{G}_i/\mathbb{F}_q$.

Now, we are interested in 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, for the tower $T_1/\mathbb{F}_{q^2}$, one can not establish a general result but one can prove that it is possible in the case where the characteristic is 2 and $r = 2$, i.e. $q = 4$. Note that in order to simplify the presentation, we are going to set the results by using the variable p.

Proposition 13. *If $p = 2$ and $q = p^2$, 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 $T_2/\mathbb{F}_p$ given by a sequence:*

$$\mathbf{H}_{0,0} \subseteq \mathbf{H}_{0,1} \subseteq \mathbf{H}_{0,2} = \mathbf{H}_{1,0} \subseteq \mathbf{H}_{1,1} \subseteq \mathbf{H}_{1,2} = \mathbf{H}_{2,0} \subseteq \cdots$$

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

$$\mathbf{F}_{i,s} = \mathbb{F}_{q^2} \mathbf{H}_{i,s} \quad \textit{for all } i \geq 0 \textit{ and } s \in \{0,1,2\},$$

namely $\mathbf{F}_{i,s}/\mathbb{F}_{q^2}$ is the constant field extension of $\mathbf{H}_{i,s}/\mathbb{F}_p$.

PROOF. It is a straightforward consequence of Proposition 11. □

In order to draw consequences for the previously descended towers, let us recall the known results concerning the number of places of degree one of the tower $T_0/\mathbb{F}_{q^2}$, established in [15] and [1].

Proposition 14. *If $q = p^r \geq 2$, then for any $n > 2$:*

$$\mathrm{B}_1(\mathbf{F}_n/\mathbb{F}_{q^2}) = \begin{cases} q^n(q^2 - q) + 2q^2 & \textit{if } p = 2, \\ q^n(q^2 - q) + 2q & \textit{if } p > 2. \end{cases}$$

Now, we deduce some straightforward properties concerning the towers $T_2/\mathbb{F}_2$ and $E/\mathbb{F}_3$.

Proposition 15. *Let $q = p^2 = 4$. For any integers $i \geq 0$ and $s \in \{0,1,2\}$, the algebraic function field $\mathbf{H}_{i,s}/\mathbb{F}_p$ in the tower $T_2/\mathbb{F}_p$ has $\mathrm{B}_1(\mathbf{H}_{i,s}/\mathbb{F}_p)$ places of degree one, $\mathrm{B}_2(\mathbf{H}_{i,s}/\mathbb{F}_p)$ places of degree two and $\mathrm{B}_4(\mathbf{H}_{i,s}/\mathbb{F}_p)$ places of degree four and satisfies:*

(i) $\mathbf{H}_i/\mathbb{F}_p \subseteq \mathbf{H}_{i,s}/\mathbb{F}_p \subseteq \mathbf{H}_{i+1}/\mathbb{F}_p$ *with* $\mathbf{H}_{i,0} = \mathbf{H}_i$ *and* $\mathbf{H}_{i,2} = \mathbf{H}_{i+1}$*,*

(ii) the genus $g_{i,s}$ *of* $\mathbf{H}_{i,s}/\mathbb{F}_p$ *satisfies:*

(ii.a) $g_{i,s} \leq \frac{g_{i+1}}{p^{2-s}}$ *(ii.b)* $g_{i,s} \leq p^{s-2}(q^{i+2} - 2q^{\frac{i}{2}+1}) + p^{s-2}$

(iii) $\mathrm{B}_1(\mathbf{H}_{i,s}/\mathbb{F}_p) + 2\mathrm{B}_2(\mathbf{H}_{i,s}/\mathbb{F}_p) + 4\mathrm{B}_4(\mathbf{H}_{i,s}/\mathbb{F}_p) \geq q^i(q^2 - q)p^s$.

Moreover, $\mathbb{F}_p$ *is algebraically closed in each algebraic function field* $\mathbf{H}_{i,s}$ *of the tower* $T_2/\mathbb{F}_p$*.*

Remark. Bound (ii.a) is tighter than Bound (ii.b), but when we will need an estimate for $g_{i,s}$ which does not depend on the parity of the step i of the tower, Bound (ii.b) will be useful.

PROOF. Property (i) follows directly from Proposition 13. Each extension $\mathbf{H}_{i+1}/\mathbf{H}_{i,s}$ is a Galois extension of degree $[\mathbf{H}_{i+1} : \mathbf{H}_{i,s}] = 2^{2-s}$. Moreover, according to [19, Prop. 3.7.8] the full constant field of $\mathbf{H}_{i,s}$ is $\mathbb{F}_p$ since at least one place of $\mathbf{H}_0$ is totally ramified in $\mathbf{H}_{i,s}$. Indeed, the place at infinity of $\mathbf{F}_0$ is totally ramified in the tower $T_0/\mathbb{F}_{q^2}$. Hence, the same holds for the place at infinity of $\mathbf{H}_0$ in $T_2/\mathbb{F}_p$. Since the algebraic function field $\mathbf{F}_{i,s}$ is a constant field extension of $\mathbf{H}_{i,s}$, for any two integers $i \geq 0$ and $s \in \{0, 1, 2\}$, $\mathbf{F}_{i,s}$ and $\mathbf{H}_{i,s}$ have the same genus, so by the Hurwitz Genus Formula [19], one has:

$$g_{i,s} \leq \frac{g_{i+1}}{p^{2-s}} \tag{7}$$

with $g(\mathbf{H}_{i+1}/\mathbb{F}_p) = g(\mathbf{F}_{i+1}/\mathbb{F}_{q^2}) = g_{i+1}$ given by (3). Finally, applying Bound (5) on g_{i+1}, we get (ii.b). Moreover, for $\alpha \in \mathbb{F}_{q^2}\backslash\{\omega \in \mathbb{F}_{q^2} \mid \omega^q + \omega = 0\}$, let P_α denote the place of degree one in the rational function field $\mathbf{F}_0$ which is the zero of $x_0 - \alpha$, then P_α splits completely in $\mathbf{F}_{i+1}/\mathbf{F}_0$ by [15, Lemma 3.9]. Let us set $d := [\mathbf{F}_{i+1} : \mathbf{F}_0]$ and $d' := [\mathbf{F}_{i+1} : \mathbf{F}_{i,s}]$. If ℓ denotes the number of places of $\mathbf{F}_{i,s}$ lying over the place P_α of $\mathbf{F}_0$, it is well known that $\ell \leq \frac{d}{d'}$ with equality holding if and only if P_α splits completely in $\mathbf{F}_{i+1}/\mathbf{F}_0$; so $\ell = \frac{d}{d'} = [\mathbf{F}_{i,s} : \mathbf{F}_0]$ which proves that the place P_α splits completely also in $\mathbf{F}_{i,s}/\mathbf{F}_0$. Thus, there are exactly $q^i p^s$ places of degree one above P_α in $\mathbf{F}_{i,s}$, so there are at least $q^i(q^2 - q)p^s$ places of degree one in $\mathbf{F}_{i,s}$, since $\left|\mathbb{F}_{q^2}\backslash\{\omega \in \mathbb{F}_{q^2} \mid \omega^q + \omega = 0\}\right| = q^2 - q$.

To conclude, we deduce from [15] (where the same formula with $s = 0$ is proven for $\mathbf{F}_{i,0}$) that the number of places of degree one of $\mathbf{F}_{i,s}/\mathbb{F}_{q^2}$ is such that $\mathrm{B}_1(\mathbf{F}_{i,s}/\mathbb{F}_{q^2}) \geq (q^2 - q)q^i p^s$. Eventually, $\mathbf{F}_{i,s}$ being a degree four constant field extension of $\mathbf{H}_{i,s}$, it is clear that for any two integers $i \geq 0$ and $s \in \{0, 1, 2\}$, it holds that

$$\mathrm{B}_1(\mathbf{H}_{i,s}/\mathbb{F}_p) + 2\mathrm{B}_2(\mathbf{H}_{i,s}/\mathbb{F}_p) + 4\mathrm{B}_4(\mathbf{H}_{i,s}/\mathbb{F}_p) \geq (q^2 - q)q^i p^s.$$

□

Similar results than those of Proposition 15 can be obtained for the tower $E/\mathbb{F}_3$, namely:

Proposition 16. *Let $q = p = 3$. For any integer $i \geq 0$, the algebraic function field $\mathbf{G}_i/\mathbb{F}_q$ in the tower $E/\mathbb{F}_q$ has the same genus g_i than the corresponding step $\mathbf{F}_i/\mathbb{F}_{q^2}$ of the tower $T_0/\mathbb{F}_{q^2}$. Moreover, the number of places of degree one and two of each function field $\mathbf{G}_i/\mathbb{F}_q$ is related to the number of rational places of $\mathbf{F}_i/\mathbb{F}_{q^2}$ by:*

$$\mathrm{B}_1(\mathbf{F}_i/\mathbb{F}_{q^2}) = \mathrm{B}_1(\mathbf{G}_i/\mathbb{F}_q) + 2\mathrm{B}_2(\mathbf{G}_i/\mathbb{F}_q)$$

thus, the following bound holds:

$$\mathrm{B}_1(\mathbf{G}_i/\mathbb{F}_q) + 2\mathrm{B}_2(\mathbf{G}_i/\mathbb{F}_q) \geq q^i(q^2 - q). \tag{8}$$

To conclude this section, let us recall that in [7], the authors established the ordinarity of the classical tower over $\mathbb{F}_{q^2}$:

Theorem 17. *For any prime power q, the tower $T_0/\mathbb{F}_{q^2}$ is ordinary.*

Thus, we can deduce that the ordinarity of $T_0/\mathbb{F}_{q^2}$ provides the same property to the towers $T_2/\mathbb{F}_2$ and $E/\mathbb{F}_3$:

Proposition 18. *The towers $T_2/\mathbb{F}_2$ and $E/\mathbb{F}_3$ are ordinary.*

PROOF. Since constant field descent preserves ordinarity from Lemma 9, the tower $E/\mathbb{F}_3$ is ordinary and so are the steps $\mathbf{F}_{i,0}$ of the tower $T_2/\mathbb{F}_2$. Moreover Lemma 10 implies that the intermediate steps $\mathbf{F}_{i,1}$ are also ordinary since each one belongs to a finite extension $\mathbf{F}_{i+1,0}/\mathbf{F}_{i,1}$ with same constant field, where $\mathbf{F}_{i+1,0}$ is ordinary. □

A straightforward consequence of this last proposition and Corollary 8 is the following result:

Corollary 19. *For any function field $\mathbf{F}$ in the towers $T_2/\mathbb{F}_2$ and $E/\mathbb{F}_3$, there exists a non-special divisor of degree $g(\mathbf{F}) - 1$.*

4. New bounds for the tensor rank

4.1. Preliminary results

To obtain our new estimates for $\mu_2^{\mathrm{sym}}(n)$ and $\mu_3^{\mathrm{sym}}(n)$ from the towers described in the previous section, we will need some technical results which are proven below.

Theorem 20. *Let n and d be two fixed integers. Let $\mathbf{F}/\mathbb{F}_q$ be an algebraic function field of genus g with at least B_k places of degree k for any $k|d$. If the three following conditions are satisfied:*

(a) $\mathrm{B}_n(\mathbf{F}/\mathbb{F}_q) > 0$,

(b) there exists a non-special divisor of degree $g - 1$,

(c) $\sum_{k|d} k(B_k + b_k) \geq 2n + 2g - 1$, *where the integers b_k are chosen such that* $0 \leq b_k \leq B_k$,

then

$$\mu_q^{\mathrm{sym}}(n) \le \sum_{k|d} \mu_q^{\mathrm{sym}}(k)(B_k + b_k) + \sum_{k|d} \mu_q^{\mathrm{sym}}(k) b_k,$$

so

$$\mu_q^{\mathrm{sym}}(n) \le \eta \left(\sum_{k|d} k(B_k + b_k) + \sum_{k|d} k b_k \right) \qquad \textit{with } \eta := \max_{k|d} \frac{\mu_q^{\mathrm{sym}}(k)}{k}.$$

PROOF. The algorithm recalled in Theorem 4 is applied on a set $\mathscr{P} = \cup_{k|d} \mathscr{P}_k$ with $\mathscr{P}_k$ a subset of $\mathsf{P}_k(\mathbf{F}/\mathbb{F}_q)$ with cardinality B_k. Among each $P \in \mathscr{P}_k$, b_k are used with multiplicity $u = 2$; all such places form a subset $\mathscr{R}$ of $\mathscr{P}$. The others $B_k - b_k$ places of $\mathscr{P}_k$ are used with multiplicity $u = 1$. From the existence of a non-special divisor $\mathscr{G}$ of degree $g - 1$ provided by Hypothesis (b) and the existence of a place Q of degree n, one constructs an effective divisor $\mathscr{D}$ such that $\deg \mathscr{D} = n + g - 1$ and $\dim \mathscr{D} = n$. Precisely, one can choose any divisor $\mathscr{D}$ which is equivalent to $Q + \mathscr{G}$, but whose support is disjoint from the support of $Q + \mathscr{G}$. For such a divisor $\mathscr{D}$, the map Ev_Q is bijective: indeed its kernel $\mathscr{L}(\mathscr{D} - Q)$ is trivial since $\mathscr{D} - Q$ is equivalent to $\mathscr{G}$ which is non-special of degree $g - 1$ and so is zero-dimensional; thus Ev_Q is injective and actually bijective by dimension reasons. Moreover, from Hypothesis (c) it holds that $\mathscr{L}\Big(2\mathscr{D} - \big(\sum_{P \in \mathscr{P}} P + \sum_{R \in \mathscr{R}} R\big)\Big) = \{0\}$ since

$$\deg\left(2\mathscr{D} - (\sum_{P \in \mathscr{P}} P + \sum_{R \in \mathscr{R}} R) \right) = 2 \deg \mathscr{D} - \sum_{k|d} k(B_k + b_k) < 0$$

thus $\mathsf{Ev}_{\mathscr{P}}$ is injective.

From [11], it holds that $\widehat{M}_q(2) \le 3$, so Theorem 4 then gives the following bound:

$$\mu_q^{\mathrm{sym}}(n) \le \sum_{P \in \mathscr{P}} \mu_q^{\mathrm{sym}}(\deg P) + 2 \sum_{R \in \mathscr{R}} \mu_q^{\mathrm{sym}}(\deg R).$$

Rearranging summation to group places with the same degree, we get the result. □

Here we state two special cases of Theorem 20 which are adapted to the study of the tensor rank on $\mathbb{F}_2$ and $\mathbb{F}_3$ respectively. The first one is adapted to the case where places of degree one, two and four are taking into account:

Proposition 21. *Let $p = 2$. If $\mathbf{F}/\mathbb{F}_2$ is an algebraic function field of genus g with at least B_k places of degree k for k =1, 2 and 4, such that the three following conditions are satisfied:*

(a) $\mathrm{B}_n(\mathbf{F}/\mathbb{F}_2) > 0$,

(b) there exists a non-special divisor of degree $g - 1$,

(c) $\sum_{k|4} k(B_k + b_k) \ge 2n + 2g - 1$, *where the integers b_k are chosen such that* $0 \le b_k \le B_k$,

then

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{9}{2}(n+g+1) + \frac{9}{4}\sum_{k|4} k b_k.$$

PROOF. It is a straightforward consequence of Theorem 20 with $q = p = 2$ and $d = 4$. We recall that $\mu_2^{\mathrm{sym}}(2) = 3$ and $\mu_2^{\mathrm{sym}}(4) \leq 9$; so we obtain $\eta = \max_{k|4} \frac{\mu_2^{\mathrm{sym}}(k)}{k} \leq \max\left\{1; \frac{3}{2}; \frac{9}{4}\right\} = \frac{9}{4}$ and the result follows from a choice of the B_k's and the b_k's such that $\sum_{k|4} k(B_k + b_k) = 2n + 2g - 1 + \epsilon$, with $\epsilon \in \{0, 1, 2, 3\}$: we must consider the less favorable case where there only exists places of degree four and so we have to choose $\epsilon = 3$. □

This second specialization corresponds to the case where only places of degree one and two are considered:

Proposition 22. *Let $q = 3$. If $\mathbf{F}/\mathbb{F}_3$ is an algebraic function field of genus g with at least B_k places of degree k for k =1, 2 such that the three following conditions are satisfied:*

(a) $\mathrm{B}_n(\mathbf{F}/\mathbb{F}_3) > 0$,

(b) there exists a non-special divisor of degree $g-1$,

(c) $\sum_{k|2} k(B_k + b_k) \geq 2n + 2g - 1$, *where the integers b_k are chosen such that* $0 \leq b_k \leq B_k$,

then

$$\mu_3^{\mathrm{sym}}(n) \leq 3(n+g) + \frac{3}{2}\sum_{k|2} k b_k.$$

PROOF. The same proof than the previous one with $q = 3$ and $d = 2$, and so $\eta = \frac{3}{2}$ in Theorem 20 gives the result. □

Lemma 23. *Let $q = 4 = p^2$ and $n \geq 19$. There exists a step $\mathbf{H}_{i,s}/\mathbb{F}_2$ of the tower $T_2/\mathbb{F}_2$ such that the three conditions of Proposition 21 are satisfied with $b_1 = b_2 = b_4 = 0$. Moreover, if Condition (c) is satisfied then the two others also are.*

PROOF. Thanks to Corollary 19, Condition (b) is satisfied for any step of the tower. For $i \leq \frac{n-13}{4}$, it holds that $p^{2i+6} \leq p^{\frac{n-1}{2}}$. Then we get that $p^{2i+6}\left(1 - \frac{1}{p^{i+2}} + \frac{1}{p^{2i+3}}\right) \leq p^{\frac{n-1}{2}} p^2(\sqrt{p} - 1)$, since $1 - \frac{1}{p^{i+2}} + \frac{1}{p^{2i+3}} \leq 1 \leq p^2(\sqrt{p} - 1)$. It follows that $p^{2i+4} - p^{i+2} + p \leq p^{\frac{n-1}{2}}(\sqrt{p} - 1)$, which leads to $2g_{i,s} + 1 \leq p^{\frac{n-1}{2}}(\sqrt{p} - 1)$ according to Proposition 15 (ii.b) with $s \in \{0, 1\}$ (one can always assume that $s \neq 2$ since $\mathbf{H}_{i,2} = \mathbf{H}_{i+1,0}$). Hence, from [19, Corollary 5.2.10] Condition (a) is satisfied for any step $\mathbf{H}_{i,s}$ such that $i \leq \frac{n-13}{4}$.
On the other hand, for i such that $i > \log_q(n) - \frac{1}{2}$, one has $q^{i+1-\frac{1}{2}} \geq n + 1$, so $q^{i+1}p^{s-1}(q-3) \geq n + 1$ since $p^{s-1} \geq q^{-\frac{1}{2}} = p^{-1}$, which gives that $q^{i+1}p^s(q-3) \geq 2n + 2$ and so $q^{i+1}p^s(q-1-2) + q^{\frac{i-1}{2}p^s} \geq 2n + 2$. Thus it holds that:

$q^{i+1}p^s(q-1) \geq 2n+2+2q^{i+1}p^s - q^{\frac{i-1}{2}}p^s = 2n+2p^{s-2}(q^{i+2}-q^{\frac{i}{2}+1})+2$.
Eventually, one gets that $q^{i+1}p^s(q-1) \geq 2n+2p^{s-2}(q^{i+2}-q^{\frac{i}{2}+1})+2p^{s-2}-1$ since $2p^{s-2}-1 \leq 2$ for $s \in \{0,1\}$, and Condition (c) is satisfied according to the inequalities (ii.b) and (iii) established in Proposition 15.
Thus, for $n \geq 21$ one can find at least one integer i in the interval $\left]\log_q(n)-\frac{1}{2}; \frac{n-13}{4}\right]$, and so a corresponding step of the tower $\mathbf{H}_{i,0}$ for which Proposition 21 holds. Note that in any case, Condition (a) is satisfied for lower steps than Condition (c), so it may happened that the first suitable step that satisfy both conditions is not $\mathbf{H}_{i,0}$ itself but one of the previous step.
Moreover one can check that for $n = 19$, $\mathbf{H}_1$ is the first suitable step of the tower to apply Proposition 21 with $b_1 = b_2 = b_4 = 0$. Indeed, it holds that $g(\mathbf{H}_1/\mathbb{F}_2) = 9$ so Condition (a) is satisfied and since $\mathrm{B}_1(\mathbf{H}_1/\mathbb{F}_2) = 4$, $\mathrm{B}_2(\mathbf{H}_1/\mathbb{F}_2) = 2$ and $\mathrm{B}_4(\mathbf{H}_1/\mathbb{F}_2) = 12$, Condition (c) is also satisfied for $\mathbf{H}_1$ but it is not the case for $\mathbf{H}_{0,1}$. Similarly for $n = 20$, $\mathbf{H}_1$ does not satisfy Condition (c), but $\mathbf{H}_{1,1}$ does satisfy both Conditions (a) and (c) since $g(\mathbf{H}_{1,1}/\mathbb{F}_2) = 21$, $\mathrm{B}_1(\mathbf{H}_{1,1}/\mathbb{F}_2) = 4$, $\mathrm{B}_2(\mathbf{H}_{1,1}/\mathbb{F}_2) = 2$ and $\mathrm{B}_4(\mathbf{H}_{1,1}/\mathbb{F}_2) = 25$. □

Lemma 24. *Let $q = 3$ and $n \geq 13$. There exists a step $\mathbf{G}_i/\mathbb{F}_3$ of the tower $E/\mathbb{F}_3$ such that the three conditions of Proposition 22 are satisfied with $b_1 = b_2 = 0$. Moreover, if Condition (c) is satisfied then the two others also are.*

PROOF. Thanks to Corollary 19, Condition (b) is satisfied for any step of the tower. For $i \leq \frac{n-5}{2}$, Condition (a) is satisfied since one has: $q^i \leq \frac{q^{\frac{n-4}{2}}}{\sqrt{q}} \leq \frac{q^{\frac{n-4}{2}}}{\sqrt{q}+1} = q^{\frac{n-4}{2}}\frac{\sqrt{q}-1}{2}$ and so $(q^{\frac{i+2}{2}}-1)(q^{\frac{i+1}{2}}-1) \leq q^{\frac{n-1}{2}}\frac{\sqrt{q}-1}{2}$ which gives that the inequality $2g_i+1 \leq q^{\frac{n-1}{2}}(\sqrt{q}-1)$ of [19, Corollary 5.2.10] holds according to (4).
On the other hand, when $i \geq 2\log_q\left(\frac{n}{2}-1\right)$, Condition (c) is satisfied. Indeed, for such i one has: $q^{\frac{i}{2}} \geq \frac{n}{2}-1$, so $4q^{\frac{i}{2}} \geq 2n-5$, which gives that $4q^{\frac{i}{2}}+2q \geq 2n+1$. Adding $2q^{i+1}$, which equals $(q^2-q)q^i$, to both sides it follows that: $(q^2-q)q^i+2q \geq 2n+2q^{i+1}-4q^{\frac{i}{2}}+1 = 2n+2(q^{i+1}-2q^{\frac{i}{2}}+1)-1$. Thus from (8) and (5) we get that inequality of Condition (c) holds with $b_1 = b_2 = 0$.
To conclude, one can see that for $n \geq 13$, the interval $\left[2\log_q\left(\frac{n}{2}-1\right); \frac{n-5}{2}\right]$ contains at least an integer i and so $\mathbf{G}_i/\mathbb{F}_3$ is a suitable step of the tower; moreover the smallest such integer is the smallest $i \geq 2\log_q\left(\frac{n}{2}-1\right)$, i.e. the smallest one for which Condition (c) is satisfied. □

Till the end of this section, we will deal with the following notations:

$$n_{2,i,s} \overset{\text{def}}{:=} \max\left\{m \,\middle|\, 2m+2g(\mathbf{H}_{i,s})-1 \leq \sum_{k|4} k\mathrm{B}_k(\mathbf{H}_{i,s}/\mathbb{F}_2)\right\}$$

and

$$n_{3,i} \overset{\text{def}}{:=} \max\left\{m \,\middle|\, 2m+2g(\mathbf{G}_i)-1 \leq \sum_{k|2} k\mathrm{B}_k(\mathbf{G}_i/\mathbb{F}_3)\right\}.$$

Let us explain the relevance of these definitions, focusing on the case of the role of $n_{3,i}$ in the tower $E/\mathbb{F}_3$ (the same holds for the tower $T_2/\mathbb{F}_2$ when one replaces

$n_{3,i}$ by $n_{2,i,s}$). The integer $n_{3,i}$ is the biggest one for which it holds that:

$$\sum_{k|2} k\mathrm{B}_k(\mathbf{G}_i/\mathbb{F}_3) \geq 2n_{3,i} + 2g_i - 1$$

i.e. $\mathbb{F}_{q^{n_{3,i}}}$ is the biggest extension of $\mathbb{F}_3$ for which $\mathbf{G}_i/\mathbb{F}_3$ could be a suitable step of the tower to apply Proposition 22 with $b_1 = b_2 = 0$. If $n > n_{3,i}$, then

$$\sum_{k|2} k\mathrm{B}_k(\mathbf{G}_i/\mathbb{F}_3) < 2n + 2g_i - 1$$

but one has

$$\sum_{k|2} k\mathrm{B}_k(\mathbf{G}_i/\mathbb{F}_3) + 2(n - n_{3,i}) \geq 2n + 2g_i - 1$$

which means that $\mathbf{G}_i$ is still a suitable step of tower to apply Theorem 22 if we can choose the b_k's such that $\sum_{k|2} kb_k \geq 2(n - n_{3,i})$.

Thus, we are interested in the determination of a lower bound for $n_{3,i}$ and $n_{2,i,s}$. It is the purpose of the two following lemmas:

Lemma 25. *If $p = 2$ and $q = p^2 = 4$, then* $n_{2,i,s} \geq q^{i+1}p^s + q^{\frac{i}{2}+1}p^s - 1$.

PROOF. According to Proposition 15 (iii) and (ii.a), and Formula (5), we get:

$$\begin{aligned}
\sum_{k|4} k\mathrm{B}_k(\mathbf{H}_{i,s}/\mathbb{F}_2) - 2g(\mathbf{H}_{i,s}) + 1 &\geq (q^2 - q)q^i p^s - 2p^{s-2}(q^{i+2} - 2q^{\frac{i}{2}+1} + 1) + 1 \\
&= q^{i+2}p^s - q^{i+1}p^s - p^{s-1}(q^{i+2} - 2q^{\frac{i}{2}+1} + 1) + 1 \\
&= q^{i+2}p^{s-1}(p-1) - q^{i+1}p^s + q^{\frac{i}{2}+1}p^s - p^{s-1} + 1 \\
&\geq q^{i+1}p^{s-1}(q-p) + q^{\frac{i}{2}+1}p^s - 1 \\
&\qquad\qquad \text{since } s \in \{0,1,2\} \text{ and } p - 1 = 1 \\
&= q^{i+1}p^s + q^{\frac{i}{2}+1}p^s - 1.
\end{aligned}$$

□

Lemma 26. *If $q = 3$, then* $n_{3,i} \geq 4q^{\frac{i+1}{2}} - 1$.

PROOF. Proposition 16 and Formula (5) give:

$$\begin{aligned}
\sum_{k|2} k\mathrm{B}_k(\mathbf{G}_i/\mathbb{F}_3) - 2g(\mathbf{G}_i) + 1 &\geq q^i(q^2 - q) - 2(q^{i+1} - 2q^{\frac{i+1}{2}} + 1) + 1 \\
&\geq q^{i+1}(q-1) - 2q^{i+1} + 4q^{\frac{i+1}{2}} - 1 \\
&= q^{i+1}(q-3) + 4q^{\frac{i+1}{2}} - 1 = 4q^{\frac{i+1}{2}} - 1.
\end{aligned}$$

□

Now, we establish a lower bound for the gap between the genus of two successive steps of each tower $T_2/\mathbb{F}_2$ and $E/\mathbb{F}_3$:

Lemma 27. *(i) If* $q = p^2 = 4$ *then* $\Delta g_{i,s} \overset{def}{:=} g(\mathbf{H}_{i,s+1}) - g(\mathbf{H}_{i,s}) \geq p^s(2q^i - 3q^{\frac{i}{2}})$.

(ii) If $p = q = 3$ *then* $\Delta g_i \overset{def}{:=} g(\mathbf{G}_{i+1}) - g(\mathbf{G}_i) \geq (q-1)(q^{i+1} - q^{\lceil i/2 \rceil})$.

PROOF. (i) For any $s \in \{0,1\}$, since $[\mathbf{H}_{i,s+1} : \mathbf{H}_{i,s}] = p$ the Hurwitz Genus Formula gives that $g_{i,s+1} - 1 \geq p(g_{i,s} - 1)$ and it follows that $g_{i,s+1} - g_{i,s} \geq (p-1)(g_{i,s} - 1)$.
If $s = 0$, then $g_{i,s} - 1 = g_i - 1$ and according to (4), it holds that $g_i - 1 \geq (q^{\frac{i}{2}} - 1)(q^{\frac{i+1}{2}} - 1)$. Thus, we get $g_i \geq \sqrt{q}q^i - (1 + \sqrt{q})q^{\frac{i}{2}} = 2q^i - 3q^{\frac{i}{2}}$, which gives that $g_{i,s+1} - g_{i,s} \geq 2q^i - 3q^{\frac{i}{2}} = p^s(2q^i - 3q^{\frac{i}{2}})$.
If $s = 1$, then $g_{i,s+1} - g_{i,s} \geq (p-1)(g_{i,s} - 1)$ holds, with $g_{i,s} - 1 = g_{i,1} - 1 \geq p(g_i - 1)$ from Hurwitz Genus Formula. Thus we get $g_{i,s+1} - g_{i,s} \geq (p-1)p(g_i - 1) \geq (p-1)p(2q^i - 3q^{\frac{i}{2}}) = p^s(2q^i - 3q^{\frac{i}{2}})$.

(ii) From Formulæ (3), we get

$$g_i = \begin{cases} (q-1)\left(q^{i+1} - q^{\frac{i}{2}}\right) & \text{for even } i, \\ (q-1)\left(q^{i+1} - q^{\frac{i+1}{2}}\right) & \text{for odd } i, \end{cases}$$

which gives the result.

□

4.2. Main results

Theorem 28. *It holds that*

$$\mu_2^{\mathrm{sym}}(n) \leq \underbrace{\frac{1035}{68}}_{<15.221} n + \frac{9}{2} \qquad \textit{and} \qquad \mu_3^{\mathrm{sym}}(n) \leq \underbrace{\frac{1933}{250}}_{=7.732} n.$$

PROOF. We first set $p = 2$ and $q = p^2$. Note that for $n \leq 18$, the result already holds from Section 1.4.1 and [11, Table 1] (see Appendix). So, fix $n \geq 19$ and choose $i \geq 0$ and $s \in \{0,1\}$ such that

$$\sum_{k|4} k B_k(\mathbf{H}_{i,s+1}/\mathbb{F}_p) \geq 2n + 2g_{i,s+1} - 1$$

but

$$\sum_{k|4} k B_k(\mathbf{H}_{i,s}/\mathbb{F}_p) < 2n + 2g_{i,s} - 1.$$

We can apply Proposition 21 in the two following ways:

(a) on $\mathbf{H}_{i,s+1}/\mathbb{F}_p$ with $b_1 = b_2 = b_4 = 0$, which gives:

$$\mu_2^{\text{sym}}(n) \leq \frac{9}{2}\left(n + g_{i,s+1} + 1\right)$$

(b) on $\mathbf{H}_{i,s}/\mathbb{F}_p$ with the b_k's chosen such that $\sum_{k|4} kb_k := 2(n - n_{2,i,s})$ **if** $2(n - n_{2,i,s}) \leq \sum_{k|4} k\mathrm{B}_k(\mathbf{H}_{i,s}/\mathbb{F}_p)$, which leads to:

$$\mu_2^{\text{sym}}(n) \leq \frac{9}{2}\left(n + g_{i,s} + 1\right) + \frac{9}{4}\sum_{k|4} kb_k.$$

Rewriting those two bounds respectively as:

$$\mu_2^{\text{sym}}(n) \leq \frac{9}{2}(n - n_{2,i,s}) + \frac{9}{2}(n_{2,i,s} + g_{i,s} + 1) + \frac{9}{2}\Delta g_{i,s}$$

and

$$\mu_2^{\text{sym}}(n) \leq 9(n - n_{2,i,s}) + \frac{9}{2}(n_{2,i,s} + g_{i,s} + 1)$$

we see that the second one is better than the other as soon as $n - n_{2,i,s} < \Delta g_{i,s}$, under the assumption that $2(n - n_{2,i,s}) \leq \sum_{k|4} k\mathrm{B}_k(\mathbf{H}_{i,s}/\mathbb{F}_p)$. So if $D_{2,i,s}$ is such that $D_{2,i,s} \leq \Delta g_{i,s}$ and $2D_{2,i,s} \leq \sum_{k|4} k\mathrm{B}_k(\mathbf{H}_{i,s}/\mathbb{F}_p)$, then when $n - n_{2,i,s} < D_{2,i,s}$, the second bound is better and can be reached since we can choose the b_k's such that $\sum_{k|4} kb_k := 2(n - n_{2,i,s})$. The particular case where $n = n_{2,i,s} + D_{2,i,s}$ will give us an upper bound for $\mu_2^{\text{sym}}(n)$ as follows: define the function $\Phi_2(x) := \min_{i,s} \Phi_{2,i,s}(x)$, with

$$\Phi_{2,i,s}(x) = \begin{cases} 9(x - n_{2,i,s}) + \frac{9}{2}(n_{2,i,s} + g_{i,s} + 1) & \text{if } x - n_{2,i,s} < D_{2,i,s} \\ \frac{9}{2}\left(x + g_{i,s+1} + 1\right) & \text{else,} \end{cases}$$

then $\mu_2^{\text{sym}}(n)$ is bounded above by any linear function whose graph lies above all the points $\left\{\left(n_{2,i,s} + D_{2,i,s}, \Phi_p(n_{2,i,s} + D_{2,i,s})\right)\right\}_{i,s}$.
We fix $X := n_{2,i,s} + D_{2,i,s}$ where

$$D_{2,i,s} := \min\left\{p^s(2q^i - 3q^{\frac{i}{2}})\,;\, \frac{1}{2}q^i(q^2 - q)p^s\right\} = p^s(2q^i - 3q^{\frac{i}{2}})$$

so that one has $D_{2,i,s} \leq \Delta g_{i,s}$ from Lemma 27, and $D_{2,i,s} \leq \frac{1}{2}\sum_{k|4} k\mathrm{B}_k(\mathbf{H}_{i,s}/\mathbb{F}_p)$ according to Theorem 15. Thus, for any i, s, $\Phi_2(X) \leq \frac{9}{2}\left(1 + \frac{g_{i,s+1}}{X}\right)X + \frac{9}{2}$.

One has

$$\begin{aligned}
\frac{g_{i,s+1}}{X} &\leq \frac{p^s(q^{i+2}-3q^{\frac{i}{2}+1})+p^{s-1}}{q^{i+1}p^s+q^{\frac{i}{2}+1}p^s-1+p^s(2q^i-3q^{\frac{i}{2}})} \\
&= \frac{q^{i+1}p^s(q-3q^{\frac{i}{2}}+q^{-i-1}p^{-1})}{q^{i+1}p^s(1+2q^{-1}+q^{-\frac{i}{2}}-3q^{-\frac{i}{2}-1}-q^{-i-1}p^{-s})} \\
&= \frac{q-3p^i+q^{-i-1}p^{-1}}{1+2q^{-1}+p^{-i}-\underbrace{(3q^{-\frac{i}{2}-1}-q^{-i-1}p^{-s})}_{\leq 7/16}} \\
&\leq \frac{q-3p^i+q^{-i-1}p^{-1}}{1+2q^{-1}+p^{-i}-\frac{7}{16}}
\end{aligned}$$

which gives that $\dfrac{g_{i,s+1}}{X} \leq \dfrac{81}{34}$, so

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{9}{2}\left(1+\frac{81}{34}\right)n+\frac{9}{2} = \frac{1035}{68}n+\frac{9}{2}.$$

Now we consider the case $q = p = 3$. Since the result already holds for $n < 13$ from [11, Table 1] (see Appendix), fix $n \geq 13$, and choose $i \geq 0$ such that

$$\sum_{k|2} k\mathrm{B}_k(\mathbf{G}_{i+1}/\mathbb{F}_q) \geq 2n+2g_{i+1}-1$$

but

$$\sum_{k|2} k\mathrm{B}_k(\mathbf{G}_i/\mathbb{F}_q) < 2n+2g_i-1.$$

We can apply Proposition 22 in the two following ways:

(a) on $\mathbf{G}_{i+1}/\mathbb{F}_q$ with $b_1 = b_2 = 0$, which gives:

$$\mu_3^{\mathrm{sym}}(n) \leq 3\,(n+g_{i+1})$$

(b) on $\mathbf{G}_i/\mathbb{F}_q$ with the b_k's chosen such that $\sum_{k|2} kb_k := 2(n-n_{3,i})$ **if** $2(n-n_{3,i}) \leq \sum_{k|2} k\mathrm{B}_k(\mathbf{G}_i/\mathbb{F}_q)$, which leads to:

$$\mu_3^{\mathrm{sym}}(n) \leq 3(n+g_i)+\frac{3}{2}\sum_{k|2} kb_k.$$

Rewriting those two bounds respectively as:

$$\mu_3^{\mathrm{sym}}(n) \leq 3(n-n_{3,i})+3(n_{3,i}+g_i)+3\Delta g_i$$

and

$$\mu_3^{\mathrm{sym}}(n) \leq 6(n-n_{3,i})+3(n_{3,i}+g_i)$$

we see that the second one is better than the other when $n - n_{3,i} < \Delta g_i$, under the assumption that $2(n - n_{3,i}) \leq \sum_{k|2} k\mathrm{B}_k(\mathbf{G}_i/\mathbb{F}_q)$. So if $D_{3,i}$ is such that $D_{3,i} \leq \Delta g_i$ and $2D_{3,i} \leq \sum_{k|2} k\mathrm{B}_k(\mathbf{G}_i/\mathbb{F}_q)$, then when $2(n - n_{3,i}) < D_{3,i}$, the second bound is better and can be reached since we can choose the b_k's such that $\sum_{k|2} kb_k := 2(n - n_{3,i})$. The particular case where $n = n_{3,i} + D_{3,i}$ will give us an upper bound for $\mu_3^{\mathrm{sym}}(n)$ as follows: define the function $\Phi_3(x) := \min_i \Phi_{3,i}(x)$, with

$$\Phi_{3,i}(x) = \begin{cases} 6(x - n_{3,i}) + 3(n_{3,i} + g_i) & \text{if } x - n_{3,i} < D_{3,i} \\ \\ 3\,(x + g_{i+1}) & \text{else,} \end{cases}$$

then $\mu_3^{\mathrm{sym}}(n)$ is bounded above by any linear function whose graph lies above all the points $\left\{\left(n_{3,i} + D_{3,i}, \Phi_3(n_{3,i} + D_{3,i})\right)\right\}_i$.
We fix $X := n_{3,i} + D_{3,i}$ where

$$D_{3,i} := \min\left\{(q-1)(q^{i+1} - q^{\lceil i/2 \rceil})\,;\ \frac{1}{2}q^i(q^2 - q)\right\}.$$

Thus, for any $i \geq 2$, $D_{3,i} = (q-1)(q^{i+1} - q^{\lceil i/2 \rceil})$; and it holds that

$$\Phi_3(X) \leq 3\left(1 + \frac{g_{i+1}}{X}\right)X.$$

One has:

$$\begin{aligned} \frac{g_{i+1}}{X} &\leq \frac{(q^{\frac{i+3}{2}} - 1)(q^{\frac{i+2}{2}} - 1)}{4q^{\frac{i+1}{2}} - 1 + (q-1)(q^{i+1} - q^{\lceil i/2 \rceil})} \\ &= \frac{q^{i+\frac{5}{2}} - q^{\frac{i+2}{2}}(1 + \sqrt{q}) + 1}{q^{i+2} + 4q^{\frac{i+1}{2}} - q^{i+1} - (q-1)q^{\lceil i/2 \rceil} - 1} \\ &\leq \frac{q^{i+2}\left(\sqrt{q} - q^{-\frac{i+2}{2}}(1 + \sqrt{q}) + q^{-i-2}\right)}{q^{i+2}\left(1 + 4q^{-\frac{i+3}{2}} - q^{-1} - (q-1)q^{-\frac{i+3}{2}} - q^{-i-2}\right)} \end{aligned}$$

which gives that:

$$\frac{g_{i+1}}{X} \leq \frac{\sqrt{q} - q^{-\frac{i+2}{2}}(1 + \sqrt{q}) + q^{-i-2}}{1 - q^{-1} - (q-1)q^{-\frac{i+3}{2}} - q^{-i-2}}$$

so since $i \geq 2$:

$$\frac{g_{i+1}}{X} \leq \frac{\sqrt{q} - q^{-2}(1 + \sqrt{q}) + q^{-4}}{1 - q^{-1} - (q-1)q^{-\frac{5}{2}} - q^{-4}}.$$

Finally, with $q = 3$, one gets:

$$\mu_3^{\mathrm{sym}}(n) \leq \underbrace{3\left(1 + \frac{\sqrt{3} - \frac{1}{9}(1 + \sqrt{3}) + 3^{-4}}{\frac{2}{3} - 2 \cdot 3^{-\frac{5}{2}} - 3^{-4}}\right)}_{\simeq 7.7314} n \leq \underbrace{\frac{1933}{250}}_{=7.732} n.$$

□

Remark. In the case of $\mathbb{F}_2$, the descent of the tower T_0 defined over $\mathbb{F}_{q^2}$ with $q = 2$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q = \mathbb{F}_2$ is not sufficient to obtain a competitive bound for the tensor rank. Indeed, in this case, we get:

$$\mu_2^{\mathrm{sym}}(n) \leq 22.5n + \frac{9}{2}.$$

Corollary 29. *The following new estimates hold:*

$$C_2 = 15.46 \qquad \textit{and} \qquad C_3 = 7.732.$$

PROOF. The estimate for C_3 is straightforward since $\frac{1933}{250} = 7.732$; for C_2, it follows from Theorem 28 for n greater than 19 and [11, Table 1] for $n \leq 18$ (see Appendix). □

APPENDIX

To be selfcontained we recall here the values from [11, Table 1] which are used througout this paper, namely bounds for $\mu_2^{\mathrm{sym}}(n)$ and $\mu_3^{\mathrm{sym}}(n)$ for $2 \leq n \leq 18$:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mu_2^{\mathrm{sym}}(n) \leq$	3	6	9	13	15	22	24	30	33	39	42	48	51	54	60	67	69
$\mu_3^{\mathrm{sym}}(n) \leq$	3	6	9	12	15	19	21	26	27	34	36	42	45	50	54	58	62

Acknowledgments

The first author wishes to thank Inria for funding his venue at Saclay where this work was partly done while he was visiting the GRACE team at LIX.

The second author was partially supported by the Labex Mathematics Hadamard (LMH) through its International PostDoctoral Scholarschip program.

References

[1] Aleshnikov, I., Kumar, V. P., Shum, K. W., Stichtenoth, H., 2001. On the splitting of places in a tower of function fields meeting the Drinfeld-Vlăduţ bound. IEEE, Transations on Information Theory 47 (4), 1613–1619.

[2] Arnaud, N., 2006. Évaluations dérivées, multiplication dans les corps finis et codes correcteurs. Ph.D. thesis, Université de la Méditerranée, Institut de Mathématiques de Luminy.

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

[4] Ballet, S., Le Brigand, D., 2006. 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.

[5] Ballet, S., Pieltant, J., 2011. On the tensor rank of multiplication in any extension of $\mathbb{F}_2$. Journal of Complexity 27, 230–245.

[6] Ballet, S., Ritzenthaler, C., Rolland, R., 2010. On the existence of dimension zero divisors in algebraic function fields defined over $\mathbb{F}_q$. Acta Arithmetica 143 (4), 377–392.

[7] Bassa, A., Beelen, P., 2010. The Hasse-Witt invariant in some towers of function fields over finite fields. Bull. Braz. Math. Soc. (N.S.) 41 (4), 567–582.

[8] Cascudo, I., Cramer, R., Xing, C., 2009. Torsion-limits for towers and asymptotically good special codes in secure computation and complexity. manuscript.

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

[10] Cenk, M., Özbudak, F., 2008. Efficient multiplication in $\mathbb{F}_{3^{lm}}$, $m \geq 1$ and $5 \leq l \leq 18$. In: Vaudenay, S. (Ed.), Progress in Cryptology – AFRICACRYPT 2008. Vol. 5023 of Lecture Notes in Computer Science. pp. 406–414.

[11] Cenk, M., Özbudak, F., 2010. On multiplication in finite fields. Journal of Complexity 26 (2), 172–186.

[12] Chudnovsky, D. V., Chudnovsky, G. V., 1988. Algebraic complexities and algebraic curves over finite fields. Journal of Complexity 4, 285–316.

[13] de Groote, H. F., 1983. Characterization of division algebras of minimal rank and the structure of their algorithm varieties. SIAM Journal on Computing 12 (1), 101–117.

[14] Garcia, A., Stichtenoth, H., 1995. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. Inventiones Mathematicae 121, 211–222.

[15] Garcia, A., Stichtenoth, H., 1996. On the asymptotic behaviour of some towers of function fields over finite fields. J. Number Theory 61 (2), 248–273.

[16] Randriambololona, H., 2012. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. Journal of Complexity 28, 489–517.

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

[18] Shparlinski, I., Tsfasman, M., Vlăduţ, S., 1992. Curves with many points and multiplication in finite fields. Coding Theory and Algebraic Geometry (Luminy 1991). Lectures Notes in Mathematics, 151. Springer-Verlag, Berlin, pp. 145–169.

[19] Stichtenoth, H., 1993. Algebraic Function Fields and Codes. No. 314 in Lectures Notes in Mathematics. Springer-Verlag.

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