Shimura modular curves and asymptotic symmetric tensor rank of multiplication in any finite field

Stéphane Ballet, Jean Chaumine, Julia Pieltant

Shimura modular curves and asymptotic symmetric tensor rank of multiplication in any finite field

Stéphane Ballet[1], Jean Chaumine[2], and Julia Pieltant[3]

[1] Aix-Marseille Université, CNRS IML FRE 3529
Case 930, 13288 Marseille Cedex 9, France
stephane.ballet@univ-amu.fr
[2] Université de la Polynésie Française, GAATI EA 3893
B.P. 6570, 98702 Faa'a, Tahiti, France
jean.chaumine@upf.pf
[3] INRIA Saclay, LIX, École Polytechnique, 91128 Palaiseau Cedex, France
pieltant@lix.polytechnique.fr

Abstract. We obtain new asymptotical bounds for the symmetric tensor rank of multiplication in any finite extension of any finite field $\mathbb{F}_q$. In this aim, we use the symmetric Chudnovsky-type generalized algorithm applied on a family of Shimura modular curves defined over $\mathbb{F}_{q^2}$ attaining the Drinfeld-Vlăduţ bound and on the descent of this family over the definition field $\mathbb{F}_q$.

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

1 Introduction

1.1 General context

The determination of the tensor rank of multiplication in finite fields is a problem which has been widely studied over the past decades both for its theoretical and practical importance. Besides it allows one to obtain multiplication algorithms with a low bilinear complexity, which determination is of crucial significance in cryptography, it has also its own interest in algebraic complexity theory. The pioneer work of D.V. and G.V. Chudnovsky [15] resulted in the design of a Karatsuba-like algorithm where the interpolation is done on points of algebraic curves with a sufficient number of rational points over the ground field. Following these footsteps, several improvements and generalizations of this algorithm leading to ever sharper bounds have been proposed since by various authors [9, 1, 14, 19], and have required to investigate and combine different techniques and objects from algebraic geometry such as evaluations on places of arbitrary degree, generalized evaluations, towers of algebraic function fields... Furthermore, a lot of connexions with other topics have been made : Shparlinski, Tsfasman and Vlăduţ [21] have first developed a correspondence between decompositions

of the tensor of multiplication and a family of linear codes with good parameters that they called *(exact) supercodes*. These codes, renamed *multiplication friendly codes*, had recently be more extensively studied and exploited by Cascudo, Cramer, Xing and Yang [13] to obtain good asymptotic results on the tensor rank. Moreover they combined their notion of multiplication friendly codes with two newly introduced primitives for function fields over finite fields [11], namely the torsion limit and systems of Riemann-Roch equations, to get news results not only on asymptotic tensor rank but also on linear secret sharing systems and frameproof codes. This stresses that the tensor rank determination problem has just as many mathematical interests as consequences and applications in various domains of computer science.

1.2 Tensor rank of multiplication

Let $q = p^s$ be a prime power, $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_{q^n}$ be the degree n extension of $\mathbb{F}_q$. The multiplication of two elements of $\mathbb{F}_{q^n}$ is an $\mathbb{F}_q$-bilinear application from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ onto $\mathbb{F}_{q^n}$. Then it can be considered as an $\mathbb{F}_q$-linear application from the tensor product $\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ onto $\mathbb{F}_{q^n}$. Consequently it can be also considered as an element T of $(\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n})^\star \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$, namely an element of ${\mathbb{F}_{q^n}}^\star \otimes_{\mathbb{F}_q} {\mathbb{F}_{q^n}}^\star \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$. More precisely, when T is written

$$T = \sum_{i=1}^{r} x_i^\star \otimes y_i^\star \otimes c_i, \tag{1}$$

where the r elements $x_i^\star$ and the r elements $y_i^\star$ are in the dual ${\mathbb{F}_{q^n}}^\star$ of $\mathbb{F}_{q^n}$ and the r elements c_i are in $\mathbb{F}_{q^n}$, the following holds for any $x, y \in \mathbb{F}_{q^n}$:

$$x \cdot y = \sum_{i=1}^{r} x_i^\star(x) y_i^\star(y) c_i.$$

Unfortunately, the decomposition (1) is not unique.

Definition 1. *The minimal number of summands in a decomposition of the tensor T of the multiplication is called the bilinear complexity of the multiplication and is denoted by $\mu_q(n)$:*

$$\mu_q(n) = \min \left\{ r \;\middle|\; T = \sum_{i=1}^{r} x_i^\star \otimes y_i^\star \otimes c_i \right\}.$$

However, the tensor T admits also a symmetric decomposition:

$$T = \sum_{i=1}^{r} x_i^\star \otimes x_i^\star \otimes c_i. \tag{2}$$

Definition 2. *The minimal number of summands in a symmetric decomposition of the tensor T of the multiplication is called the symmetric bilinear complexity of the multiplication and is denoted by $\mu_q^{\mathrm{sym}}(n)$:*

$$\mu_q^{\mathrm{sym}}(n) = \min\left\{ r \;\middle|\; T = \sum_{i=1}^{r} x_i^\star \otimes x_i^\star \otimes c_i \right\}.$$

One easily gets that $\mu_q(n) \leq \mu_q^{\mathrm{sym}}(n)$. We know some cases where $\mu_q(n) = \mu_q^{\mathrm{sym}}(n)$ but to the best of our knowledge, no example is known where we can prove that $\mu_q(n) < \mu_q^{\mathrm{sym}}(n)$. However, better upper bounds have been established in the asymmetric case and this may suggest that in general the asymmetric bilinear complexity of the multiplication and the symmetric one are distinct. In any case, at the moment, we must consider separately these two quantities. Remark that from an algorithmic point on view, as well as for some specific applications, a symmetric bilinear algorithm can be more interesting than an asymmetric one, unless if *a priori*, the constant factor in the bilinear complexity estimation is a little worse. In this note we study the asymptotic behavior of the symmetric bilinear complexity of the multiplication. More precisely we study the two following quantities:

$$M_q^{\mathrm{sym}} = \limsup_{k\to\infty} \frac{\mu_q^{\mathrm{sym}}(k)}{k}, \tag{3}$$

$$m_q^{\mathrm{sym}} = \liminf_{k\to\infty} \frac{\mu_q^{\mathrm{sym}}(k)}{k}. \tag{4}$$

1.3 Known results

The bilinear complexity $\mu_q(n)$ of the multiplication in the n-degree extension of a finite field $\mathbb{F}_q$ is known for certain values of n. In particular, S. Winograd [24] and H. 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 [15] applied to elliptic curves, M.A. Shokrollahi has shown in [20] that the symmetric bilinear complexity of multiplication is equal to $2n$ for $\frac{1}{2}q+1 < n < \frac{1}{2}(q+1+\epsilon(q))$ where ϵ is the function defined by:

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

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

Recently in [3], [4], [9], [8], [7], [6] and [5] the study made by M.A. Shokrollahi has been generalized to algebraic function fields of genus g.

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

Theorem 3. *Let $q = p^r$ be a power of the prime p. The symmetric tensor rank $\mu_q^{\mathrm{sym}}(n)$ of multiplication in any finite field $\mathbb{F}_{q^n}$ is linear with respect to the extension degree; more precisely, there exists a constant C_q such that:*

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

General forms for C_q have been established since, depending on the cases where q is a prime or a prime power, a square or not... In order to obtain these good estimates for the constant C_q, S. Ballet has given in [3] 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 [9] the algorithm using places of degree one and two. The best finalized version of this algorithm in this direction is a generalization introduced by N. Arnaud in [1] and developed later by M. Cenk and F. Özbudak in [14]. This generalization uses several coefficients, instead of just the first one in the local expansion at each place on which we perform evaluations. Recently, Randriambolona introduced in [19] a new generalization of the algorithm, which allows asymmetry in the construction.

From the results of [3] and the generalized symmetric algorithm, we obtain (cf. [3], [9]):

Theorem 4. *Let q be a prime power and let $n > 1$ be an integer. Let $F/\mathbb{F}_q$ be an algebraic function field of genus g and N_k be the number of places of degree k in $F/\mathbb{F}_q$. If $F/\mathbb{F}_q$ is such that $2g + 1 \leq q^{\frac{n-1}{2}}(q^{\frac{1}{2}} - 1)$ then:*

1) if $N_1 > 2n + 2g - 2$, then

$$\mu_q^{\mathrm{sym}}(n) \leq 2n + g - 1,$$

2) if there exists a non-special divisor of degree $g-1$ and $N_1 + 2N_2 > 2n + 2g - 2$, then

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + 3g,$$

3) if $N_1 + 2N_2 > 2n + 4g - 2$, then

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + 6g.$$

Theorem 5. *Let q be a square ≥ 25. Then*

$$m_q^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{\sqrt{q} - 3}\right).$$

Moreover, let us recall a very useful lemma due to D.V. and G.V. Chudnovsky [15] and Shparlinski, Tsfasman and Vlăduţ [21, Lemma 1.2 and Corollary 1.3].

Lemma 6. *For any prime power q and for all positive integers n and m, one has*

$$\mu_q(m) \leq \mu_q(mn) \leq \mu_q(n) \cdot \mu_{q^n}(m),$$
$$m_q \leq m_{q^n} \cdot \mu_q(n)/n,$$
$$M_q \leq M_{q^n} \cdot \mu_q(n).$$

Note that these inequalities are also true in the symmetric case. Recall the following definitions that will be useful in the sequel. Let $F/\mathbb{F}_q$ be a function field over the finite field $\mathbb{F}_q$ and $N_1(F)$ be the number of places of degree one of $F/\mathbb{F}_q$. Let us define:

$$N_q(g) = \max\left\{ N_1(F) \,\middle|\, F \text{ is a function field over } \mathbb{F}_q \text{ of genus } g \right\}$$

and

$$A(q) = \limsup_{g \to +\infty} \frac{N_q(g)}{g}.$$

We know that (Drinfeld-Vlăduţ bound):

$$A(q) \leq q^{\frac{1}{2}} - 1,$$

the bound being reached if and only if q is a square.

2 New upper bounds for $m_q^{\mathbf{sym}}$ and $M_q^{\mathbf{sym}}$

In this section, we give upper bounds for the asymptotical quantities M_q^{sym} and m_q^{sym} which are defined respectively by (3) and (4). As was noted in [11, p. 694] and more precisely in [12, Section 5] (cf. also [18]), Theorems 3.1 and 3.9 in [21] are not completely correct. We are going to repair that in the following two propositions.

Proposition 7. *Let q be a prime power such that $A(q) > 2$. Then*

$$m_q^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{A(q) - 2}\right).$$

Proof. Let $\{F_s/\mathbb{F}_q\}_s$ be a sequence of algebraic function fields defined over $\mathbb{F}_q$. Let us denote by g_s the genus of $F_s/\mathbb{F}_q$ and by $N_1(s)$ the number of places of degree 1 of $F_s/\mathbb{F}_q$. Suppose that the sequence $\left(F_s/\mathbb{F}_q\right)_s$ was chosen such that:

1. $\lim_{s\to+\infty} g_s = +\infty$,
2. $\lim_{s\to+\infty} \frac{N_1(s)}{g_s} = A(q)$.

Let ϵ be any real number such that $0 < \epsilon < \frac{A(q)}{2} - 1$. Let us define the following integer

$$n_s = \left\lfloor \frac{N_1(s) - 2g_s(1+\epsilon)}{2} \right\rfloor.$$

Let us remark that

$$N_1(s) = g_s A(q) + o(g_s),$$

$$\text{so } N_1(s) - 2(1+\epsilon)g_s = g_s\left(A(q) - 2(1+\epsilon)\right) + o(g_s).$$

Then the following holds:

1. there exists an integer s_0 such that for any $s \geq s_0$ the integer n_s is strictly positive,
2. for any real number c such that $0 < c < A(q) - 2(1+\epsilon)$ there exists an integer s_1 such that for any integer $s \geq s_1$ the following holds: $n_s \geq \frac{c}{2} g_s$, hence n_s tends to $+\infty$,
3. there exists an integer s_2 such that for any integer $s \geq s_2$ the following holds: $2g_s + 1 \leq q^{\frac{n_s-1}{2}} \left(q^{\frac{1}{2}} - 1\right)$ and consequently there exists a place of degree n_s (cf. [22, Corollary 5.2.10 (c) p. 207]),
4. the following inequality holds: $N_1(s) > 2n_s + 2g_s - 2$ and consequently, using Theorem 4 we conclude that $\mu_q^{\mathrm{sym}}(n_s) \leq 2n_s + g_s - 1$.

Consequently,

$$\frac{\mu_q^{\mathrm{sym}}(n_s)}{n_s} \leq 2 + \frac{g_s - 1}{n_s},$$

so

$$m_q^{\mathrm{sym}} \leq 2 + \lim_{s \to +\infty} \frac{2g_s - 2}{N_1(s) - 2(1+\epsilon)g_s - 2} \leq 2\left(1 + \frac{1}{A(q) - 2(1+\epsilon)}\right).$$

This inequality holding for any $\epsilon > 0$ sufficiently small, we then obtain the result. □

Corollary 8. *Let $q = p^m$ be a prime power such that $q \geq 4$. Then*

$$m_{q^2}^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{q-3}\right).$$

Note that this corollary lightly improves Theorem 5. Now in the case of arbitrary q, we obtain:

Corollary 9. *For any $q = p^m > 3$,*

$$m_q^{\mathrm{sym}} \leq 3\left(1 + \frac{1}{q-3}\right).$$

Proof. For any $q = p^m > 3$, we have $q^2 = p^{2m} \geq 16$ and thus Corollary 8 gives $m_{q^2}^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{q-3}\right)$. Then, by Lemma 6, we have

$$m_q^{\mathrm{sym}} \leq m_{q^2}^{\mathrm{sym}} \cdot \mu_q^{\mathrm{sym}}(2)/2$$

which gives the result since $\mu_q^{\mathrm{sym}}(2) = 3$ for any q. □

Now, we are going to show that for M_q^{sym} the same upper bound as for m_q^{sym} can be proved though only in the case of q being an even power of a prime. However, we are going to prove that in the case of q being an odd power of a prime, the difference between the two bounds is very slight.

Proposition 10. *Let $q = p^m$ be a prime power such that $q \geq 4$. Then*

$$M_{q^2}^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{q-3}\right).$$

Proof. Let $q = p^m$ be a prime power such that $q \geq 4$. Let us consider two cases. First, we suppose that $q = p$. Moreover, firstly, let us consider the characteristic p such that $p \neq 11$. Then it is known ([23] and [21]) that the curve $X_k = X_0(11\ell_k)$, where ℓ_k is the kth prime number, has a genus $g_k = \ell_k$ and satisfies $N_1(X_k(\mathbb{F}_{q^2})) \geq (q-1)(g_k+1)$ where $N_1(X_k(\mathbb{F}_{q^2}))$ denotes the number of rational points over $\mathbb{F}_{q^2}$ of the curve X_k. Let us consider a sufficiently large n. There exist two consecutive prime numbers ℓ_k and ℓ_{k+1} such that $(p-1)(\ell_{k+1}+1) > 2n + 2\ell_{k+1} - 2$ and $(p-1)(\ell_k+1) \leq 2n + 2\ell_k - 2$. Let us consider the algebraic function field $F_{k+1}/\mathbb{F}_{p^2}$ associated to the curve X_{k+1} of genus ℓ_{k+1} defined over $\mathbb{F}_{p^2}$. Let $N_i(F_k/\mathbb{F}_{p^2})$ be the number of places of degree i of $F_k/\mathbb{F}_{p^2}$. Then we get $N_1(F_{k+1}/\mathbb{F}_{p^2}) \geq (p-1)(\ell_{k+1}+1) > 2n + 2\ell_{k+1} - 2$. Moreover, it is known that $N_n(F_{k+1}/\mathbb{F}_{p^2}) > 0$ for any integer n sufficiently large. We also know that $\ell_{k+1} - \ell_k \leq \ell_k^{0,525}$ for any integer $k \geq k_0$ where k_0 can be effectively determined by [2]. Then there exists a real number $\epsilon > 0$ such that $\ell_{k+1} - \ell_k = \epsilon\ell_k \leq \ell_k^{0,525}$ namely $\ell_{k+1} \leq (1+\epsilon)\ell_k$. It is sufficient to choose ϵ such that $\epsilon\ell_k^{0,475} \leq 1$. Consequently, for any integer n sufficiently large, this algebraic function field $F_{k+1}/\mathbb{F}_{p^2}$ satisfies Theorem 4, and so $\mu_{p^2}^{\mathrm{sym}}(n) \leq 2n + \ell_{k+1} - 1 \leq 2n + (1+\epsilon)\ell_k - 1$ with $\ell_k \leq \frac{2n}{p-3} - \frac{p+1}{p-3}$. Thus, as $n \to +\infty$ then $\ell_k \to +\infty$ and $\epsilon \to 0$, so we obtain $M_{p^2}^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{p-3}\right)$. Note that for $p = 11$, Proposition 4.1.20 in [23] enables us to obtain $g_k = \ell_k + O(1)$.

Now, let us study the more difficult case where $q = p^m$ with $m > 1$. We use the Shimura curves as in [21]. Recall the construction of this good family. Let L be a totally real abelian over $\mathbb{Q}$ number field of degree m in which p is inert, thus the residue class field $\mathcal{O}_L/(p)$ of p, where $\mathcal{O}_L$ denotes the ring of integers of L, is isomorphic to the finite field $\mathbb{F}_q$. Let $\wp$ be a prime of L which does not divide p and let B be a quaternion algebra for which

$$B \otimes_{\mathbb{Q}} \mathbb{R} = \mathrm{M}_2(\mathbb{R}) \otimes \mathbb{H} \otimes \cdots \otimes \mathbb{H}$$

where $\mathbb{H}$ is the skew field of Hamilton quaternions. Let B be also unramified at any finite place if $(m-1)$ is even; let B be also unramified outside infinity and $\wp$ if $(m-1)$ is odd. Then, over L one can define the Shimura curve by its complex points $X_\Gamma(\mathbb{C}) = \Gamma \setminus \mathfrak{h}$, where $\mathfrak{h}$ is the Poincaré upper half-plane and Γ is the group of units of a maximal order $\mathcal{O}$ of B with totally positive norm modulo its center. Hence, the considered Shimura curve admits an integral model over L and it is well known that its reduction $X_{\Gamma,p}(\mathbb{F}_{p^{2m}})$ modulo p is good and is defined over the residue class field $\mathcal{O}_L/(p)$ of p, which is isomorphic to $\mathbb{F}_q$ since p is inert in L. Moreover, by [17], the number $N_1(X_{\Gamma,p}(\mathbb{F}_{q^2}))$ of $\mathbb{F}_{q^2}$-points of $X_{\Gamma,p}$ is such that $N_1(X_{\Gamma,p}(\mathbb{F}_{q^2})) \geq (q-1)(g+1)$, where g denotes the genus of $X_{\Gamma,p}(\mathbb{F}_{q^2})$. Let now ℓ be a prime which is greater than the maximum order of stabilizers Γ_z, where $z \in \mathfrak{h}$ is a fixed point of Γ and let $\wp \nmid \ell$. Let $\Gamma_0(\ell)_\ell$ be the

following subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$:

$$\Gamma_0(\ell)_\ell = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_\ell)\,;\, c \equiv 0 \pmod{\ell} \right\}.$$

Suppose that ℓ splits completely in L. Then there exists an embedding $L \to \mathbb{Q}_\ell$ where $\mathbb{Q}_\ell$ denotes the usual ℓ-adic field, and since $B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{M}_2(\mathbb{Q}_\ell)$, we have a natural map:

$$\phi_\ell : \Gamma \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Let Γ_ℓ be the inverse image of $\Gamma_0(\ell)_\ell$ in Γ under ϕ_ℓ. Then Γ_ℓ is a subgroup of Γ of index ℓ. We consider the Shimura curve X_ℓ with

$$X_\ell(\mathbb{C}) = \Gamma_\ell \setminus \mathfrak{h}.$$

It admits an integral model over L and so can be defined over L. Hence, its reduction $X_{\ell,p}$ modulo p is good and it is defined over the residue class field $\mathcal{O}_L/(p)$ of p, which is isomorphic to $\mathbb{F}_q$ since p is inert in L. Moreover the supersingular $\mathbb{F}_p$-points of $X_{\Gamma,p}$ split completely in the natural projection

$$\pi_\ell : X_{\ell,p} \to X_{\Gamma,p}.$$

Thus, the number of rational points of $X_{\ell,p}(\mathbb{F}_{q^2})$ verifies:

$$N_1(X_{\ell,p}(\mathbb{F}_{q^2})) \geq \ell(q-1)(g+1).$$

Moreover, since ℓ is greater than the maximum order of a fixed point of Γ on $\mathfrak{h}$, the projection π_ℓ is unramified and thus by Hurwitz formula,

$$g_\ell = 1 + \ell(g-1)$$

where g_ℓ is the genus of X_ℓ (and also of $X_{\ell,p}$).

Note that since the field L is abelian over $\mathbb{Q}$, there exists an integer N such that the field L is contained in a cyclotomic extension $\mathbb{Q}(\zeta_N)$ where ζ_N denotes a primitive root of unity with minimal polynomial Φ_N. Let us consider the reduction $\Phi_{N,\ell}$ of Φ_N modulo the prime ℓ. Then, the prime ℓ is totally split in the integer ring of L if and only if the polynomial $\Phi_{N,\ell}$ is totally split in $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$ i.e. if and only if $\mathbb{F}_\ell$ contains the Nth roots of unity which is equivalent to $N \mid \ell - 1$. Hence, any prime ℓ such that $\ell \equiv 1 \pmod{N}$ is totally split in $\mathbb{Q}(\zeta_N)$ and then in L. Since ℓ runs over primes in an arithmetical progression, the ratio of two consecutive prime numbers $\ell \equiv 1 \pmod{N}$ tends to one.

Then for any real number $\epsilon > 0$, there exists an integer k_0 such that for any integer $k \geq k_0$, $\ell_{k+1} \leq (1+\epsilon)\ell_k$ where ℓ_k and ℓ_{k+1} are two consecutive prime numbers congruent to one modulo N. Then there exists an integer n_ϵ such that for any integer $n \geq n_\epsilon$, the integer k such that the two following inequalities hold

$$\ell_{k+1}(q-1)(g+1) > 2n + 2g_{\ell_{k+1}} - 2$$

and

$$\ell_k(q-1)(g+1) \leq 2n + 2g_{\ell_k} - 2,$$

satisfies $k \geq k_0$; where $g_{\ell_i} = 1 + \ell_i(g-1)$ for any integer i. Let us consider the algebraic function field $F_k/\mathbb{F}_{q^2}$ defined over the finite field $\mathbb{F}_{q^2}$ associated to the Shimura curve X_{ℓ_k} of genus g_{ℓ_k}. Let $N_i(F_k/\mathbb{F}_{q^2})$ be the number of places of degree i of $F_k/\mathbb{F}_{q^2}$. Then $N_1(F_{k+1}/\mathbb{F}_{q^2}) \geq \ell_{k+1}(q-1)(g+1) > 2n + 2g_{\ell_{k+1}} - 2$ where g is the genus of the Shimura curve $X_{\Gamma,p}(\mathbb{F}_{q^2})$. Moreover, it is known that there exists an integer n_0 such that for any integer $n \geq n_0$, $N_n(F_{k+1}/\mathbb{F}_{q^2}) > 0$. Consequently, for any integer $n \geq \max(n_\epsilon, n_0)$ this algebraic function field $F_{k+1}/\mathbb{F}_{q^2}$ satisfies Theorem 4 and so

$$\mu_{q^2}^{\mathrm{sym}}(n) \leq 2n + g_{\ell_{k+1}} - 1 \leq 2n + \ell_{k+1}(g-1) \leq 2n + (1+\epsilon)\ell_k(g-1)$$

with $\ell_k < \frac{2n}{(q-1)(g+1)-2(g-1)}$. Thus, for any real number $\epsilon > 0$ and for any $n \geq \max(n_\epsilon, n_0)$, we obtain $\mu_{q^2}^{\mathrm{sym}}(n) \leq 2n + \frac{2n(1+\epsilon)(g-1)}{(q-1)(g+1)-2(g-1)}$ which gives $M_{q^2}^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{q-3}\right)$. □

Proposition 11. *Let $q = p^m$ be a prime power with odd m such that $q \geq 5$. Then*

$$M_q^{\mathrm{sym}} \leq 3\left(1 + \frac{2}{q-3}\right).$$

Proof. It is sufficient to consider the same families of curves than in Proposition 10. These families of curves $\{X_k\}$ are defined over the residue class field of p which is isomorphic to $\mathbb{F}_q$. Hence, we can consider the associated algebraic function fields $F_k/\mathbb{F}_q$ defined over $\mathbb{F}_q$. If $q = p$, we have $N_1(F_{k+1}/\mathbb{F}_{p^2}) = N_1(F_{k+1}/\mathbb{F}_p) + 2N_2(F_{k+1}/\mathbb{F}_p) \geq (p-1)(\ell_{k+1}+1) > 2n + 2\ell_{k+1} - 2$ since $F_{k+1}/\mathbb{F}_{p^2} = F_{k+1}/\mathbb{F}_p \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$. Then, for any real number $\epsilon > 0$ and for any integer n sufficiently large, we have $\mu_p^{\mathrm{sym}}(n) \leq 3n + 3g_{\ell_{k+1}} \leq 3n + 3(1+\epsilon)\ell_k$ by Theorem 4 since $N_n(F_{k+1}/\mathbb{F}_{q^2}) > 0$. Then, by using the condition $\ell_k \leq \frac{2n}{p-3} - \frac{p+1}{p-3}$, we obtain $M_p^{\mathrm{sym}} \leq 3\left(1 + \frac{2}{p-3}\right)$. If $q = p^m$ with odd m, we have $N_1(F_{k+1}/\mathbb{F}_{q^2}) = N_1(F_{k+1}/\mathbb{F}_q) + 2N_2(F_{k+1}/\mathbb{F}_q) \geq \ell_{k+1}(q-1)(g+1) > 2n + 2g_{\ell_{k+1}} - 2$ since $F_{k+1}/\mathbb{F}_{q^2} = F_{k+1}/\mathbb{F}_q \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$. Then, for any real number $\epsilon > 0$ and for any integer n sufficiently large as in Proof of Proposition 10, we have $\mu_q^{\mathrm{sym}}(n) \leq 3n + 3g_{\ell_{k+1}} \leq 3n + 3(1+\epsilon)\ell_k(g-1)$ by Theorem 4 since $N_n(F_{k+1}/\mathbb{F}_{q^2}) > 0$. Then, by using the condition $\ell_k < \frac{2n}{(q-1)(g+1)-2(g-1)}$ we obtain $M_q^{\mathrm{sym}} \leq 3\left(1 + \frac{2}{q-3}\right)$. □

Remark 12. Note that in [13, Lemma IV.4], Elkies gives another construction of a family $\{\chi_s\}_{s=1}^{\infty}$ of Shimura curves over $\mathbb{F}_q$ satisfying for any prime power q and for any integer $t \geq 1$ the following conditions:

(i) the genus $g(F_s)$ tends to $+\infty$ as s tends to $+\infty$, where F_s stands for the function field $\mathbb{F}_q(\chi_s)$,
(ii) $\lim_{s\to+\infty} g(F_s)/g(F_{s-1}) = 1$,
(iii) $\lim_{s\to+\infty} B_{2t}(F_s)/g(F_s) = (q^t-1)/(2t)$, where $B_{2t}(F_s)$ stands for the number of places of degree $2t$ in F_s.

However, this construction is not sufficiently explicit to enable Cascudo and al. [12] (and [13]) to derive the best bounds in all the cases (cf. Section 3). Indeed, let us recall the construction of Elkies.

Let $q = p^r$ be a prime power and put $f = rt$. Let K be a totally real number field such that $K/\mathbb{Q}$ is a Galois extension of degree f and p is totally inert in K. Let B be a quaternion algebra over K such that the set S of non-archimedean primes of K that are ramified in B is Galois invariant. Note that B can be constructed by taking S to be either the empty set for odd f, or the set of primes lying over p for even f (see [21]).

Let $\ell \neq p$ be a rational prime outside S such that ℓ is totally inert in K (note that in [21], ℓ is chosen such that it is completely splitting). Consider the Shimura curve $X_0^B(\ell) := \Gamma_0(\ell\mathcal{O}_K)\backslash\mathfrak{h}$, where $\mathfrak{h}$ is the upper half-plane and $\Gamma_0(\ell\mathcal{O}_K)$ is the subgroup of the unit group of the maximal order of B mapping to upper triangle matrices modulo $\ell\mathcal{O}_K$. Then $X_0^B(\ell)$ is defined over the rational field $\mathbb{Q}$ and has a good reduction modulo p. Thus, the reduction of $X_0^B(\ell)$ is defined over $\mathbb{F}_p$, and therefore over $\mathbb{F}_q$ as well. This curve has at least $(p^f - 1)g_\ell$ supersingular points over $\mathbb{F}_{p^{2f}} = \mathbb{F}_{q^{2t}}$, where g_ℓ is the genus of $X_0^B(\ell)$. One knows that the ratio g_ℓ/ℓ^f tends to a fixed number a when ℓ tends to $+\infty$. Now let $\{\ell_s\}_{s=1}^{+\infty}$ be the set of consecutive primes such that ℓ_s are totally inert in K and $\ell_s \notin \mathsf{S}$. By Chebotarev's density theorem, we have $\ell_s/\ell_{s-1} \to 1$ as s tends to $+\infty$. Hence, $g_{\ell_s}/g_{\ell_{s-1}} \to 1$ as s tends to $+\infty$.

For the family of function fields $\{F_s/\mathbb{F}_q\}$ of the above Shimura curves, the number $N_{2t}(F_s)$ of $\mathbb{F}_{q^{2t}}$-rational places of F_s satisfies

$$\lim_{g(F_s)\to+\infty} \frac{N_{2t}(F_s)}{g(F_s)} = p^f - 1 = q^t - 1.$$

Moreover, (i) and (ii) are satisfied as well.

By the identity $N_{2t}(F_s) = \sum_{i|2t} iB_i(F_s)$, we get

$$\begin{aligned}\liminf_{g(F_s)\to+\infty} \frac{1}{g(F_s)} \sum_{i=1}^{2t} \frac{iB_i(F_s)}{q^t-1} &\geq \liminf_{g(F_s)\to+\infty} \frac{1}{g(F_s)} \sum_{i|2t} \frac{iB_i(F_s)}{q^t-1} \\ &= \liminf_{g(F_s)\to+\infty} \frac{N_{2t}(F_s)}{g(F_s)(q^t-1)} = 1.\end{aligned}$$

Thus, the inequality

$$\liminf_{g(F_s)\to+\infty} \frac{1}{g(F_s)} \sum_{i=1}^{2t} \frac{iB_i(F_s)}{q^t-1} \geq 1$$

is satisfied and consequently (iii) is also satisfied by [13, Lemma IV.3].

3 Comparison with the current best asymptotical bounds

In this section, we recall the results obtained in [13, Theorem IV.6 and IV.7] and [12, Theorem 5.18] which are known to give the best current estimates for M_q^{sym}, and compare these bounds to those established in Propositions 10 and 11.

3.1 Comparison with the bounds in [13]

In [13], the authors establish the following results:

Theorem 13. *For any prime power $q \geq 2$, one has*

$$M_q^{\mathrm{sym}} \leq \mu_q^{\mathrm{sym}}(2t)\frac{q^t-1}{t(q^t-5)} \tag{5}$$

for any $t \geq 1$ as long as $q^t - 5 > 0$, and

$$M_{q^2}^{\mathrm{sym}} \leq \mu_{q^2}^{\mathrm{sym}}(t)\frac{2(q^t-1)}{t(q^t-5)} \tag{6}$$

for any $t \geq 1$ as long as $q^t - 5 > 0$.

Let us show that our results are better than those of this theorem except for some small values of q.

Bounds over $\mathbb{F}_q$. The estimates obtained in [13, Corollary IV.8.] show that (5) gives better bounds than Proposition 11 for any $q \leq 13$. Indeed, one has:

q	5	7	8	9	11	13
M_q^{sym} [13, Cor. IV.8]	4.8	3.82	3.74	3.68	3.62	3.59
M_q^{sym} [Prop. 11]	6	4.5	4.2	4	3.75	3.6

However, as soon as $q \geq 15$, our estimate is sharper than (5). Indeed, for $q \geq 15$, Proposition 11 gives:

$$M_q^{\mathrm{sym}} \leq 3.5.$$

On the other hand, since $\mu_q^{\mathrm{sym}}(2t) \geq 4t-1$, the best estimate that can be obtained with Bound (5) is:

$$M_q^{\mathrm{sym}} \leq (4t-1)\cdot\frac{q^t-1}{t(q^t-5)} = \left(4-\frac{1}{t}\right)\cdot\left(1+\frac{4}{q^t-5}\right). \tag{7}$$

Thus one must have $4-\frac{1}{t} < 3.5$ to obtain a better estimate than 3.5, which requires $t = 1$. In this case, (7) becomes:

$$M_q^{\mathrm{sym}} \leq 3\left(1+\frac{4}{q-5}\right)$$

which is less precise than the bound of Proposition 11 for any $q \geq 15$.

Bounds over $\mathbb{F}_{q^2}$. For $q = 4$, Proposition 10 gives $M_{q^2}^{\mathrm{sym}} \leq 4$, which is less sharp than Bound (6) applied with $t = 4$, which leads to $M_{q^2}^{\mathrm{sym}} \leq 3.56$.

However, for any $q \geq 5$, Proposition 10 gives better bounds than (6). Indeed, since $\mu_{q^2}^{\mathrm{sym}}(t) \geq 2t-1$, the best estimate that can be obtained with (6) is:

$$M_{q^2}^{\mathrm{sym}} \leq 2(2t-1)\cdot\frac{q^t-1}{t(q^t-5)} = \left(4-\frac{2}{t}\right)\cdot\left(1+\frac{4}{q^t-5}\right). \tag{8}$$

Since Proposition 10 gives $M_{q^2}^{\mathrm{sym}} \leq 3$ for any $q \geq 5$, it is necessary to have $4 - \frac{2}{t} < 3$ to obtain a better bound with (8), which requires $t = 1$. This is impossible for $q = 5$ since Bound (6) is undefined in this case, and for $q > 5$ and $t = 1$, (8) becomes:

$$M_{q^2}^{\mathrm{sym}} \leq 2\left(1 + \frac{4}{q-5}\right)$$

which is less sharp than the bound obtained from Proposition 10.

3.2 Comparison with the bounds in [12]

In [12] (which is an extended version of [11]), the authors establish the following asymptotic bounds:

Theorem 14. *For a prime power q, one has*

$$M_q^{\mathrm{sym}} \leq \begin{cases} \mu_q^{\mathrm{sym}}(2t)\frac{q^t-1}{t(q^t-2-\log_q 2)}, & \text{if } 2|q \\ \mu_q^{\mathrm{sym}}(2t)\frac{q^t-1}{t(q^t-2-2\log_q 2)}, & \text{otherwise} \end{cases}$$

for any $t \geq 1$ as long as $q^t - 2 - \log_q 2 > 0$ for even q; and $q^t - 2 - 2\log_q 2 > 0$ for odd q.

This bound always beats the one of Proposition 11 for arbitrary q (for example, by setting $t = 1$ and $\mu_q^{\mathrm{sym}}(2t) = 4t - 1$). Nevertheless, if we focus on the case of $M_{q^2}^{\mathrm{sym}}$, then the bound of Proposition 10 is better as soon as $q > 5$ since in this case, it gives:

$$M_{q^2}^{\mathrm{sym}} < 3$$

which can not be reached with the bound of Theorem 3.2, since the best that one can get is:

$$M_q^{\mathrm{sym}} \leq \begin{cases} \left(4 - \frac{1}{t}\right)\left(1 + \frac{1+\log_q 2}{q^t-2-\log_q 2}\right), & \text{if } 2|q \\ \left(4 - \frac{1}{t}\right)\left(1 + \frac{1+2\log_q 2}{q^t-2-2\log_q 2}\right), & \text{otherwise} \end{cases}$$

which obviously can not be < 3.

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. Roger Baker, Glyn Harman, and János Pintz. The difference between consecutive primes, II. In *Proceedings of the London Mathematical Society*, volume 83(3), pages 532–562, 2001.
3. 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.

4. 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.
5. Stéphane Ballet. On the tensor rank of the multiplication in the finite fields. *Journal of Number Theory*, 128:1795–1806, 2008.
6. 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.
7. 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.
8. 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.
9. 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.
10. Ulrich Baum and Amin Shokrollahi. An optimal algorithm for multiplication in $\mathbb{F}_{256}/\mathbb{F}_4$. *Applicable Algebra in Engineering, Communication and Computing*, 2(1):15–20, 1991.
11. Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. The torsion-limit for algebraic function fields and its application to arithmetic secret sharing. In *Proceedings of 31st Annual IACR CRYPTO, Santa Barbara, Ca., USA*, volume 6841 of *Lecture Notes in Computer Science*, pages 685–705, 2011.
12. Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. Torsion limits and Riemann-Roch systems for function fields and applications. *ArXiv e-prints*, http://arxiv.org/abs/1207.2936v1, 2012.
13. Ignacio Cascudo, Ronald Cramer, Chaoping Xing, and An Yang. Asymptotic bound for multiplication complexity in the extensions of small finite fields. *IEEE Transactions on Information Theory*, 58(7):4930–4935, 2012.
14. Murat Cenk and Ferruh Özbudak. On multiplication in finite fields. *Journal of Complexity*, 26(2):172–186, 2010.
15. David Chudnovsky and Gregory Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4:285–316, 1988.
16. Hans F. de Groote. Characterization of division algebras of minimal rank and the structure of their algorithm varieties. *SIAM Journal on Computing*, 12(1):101–117, 1983.
17. Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *Journal of the Faculty of Science. University of Tokyo. Section IA. Mathematics*, 28:721–724, 1981.
18. Julia Pieltant. *Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis*. PhD thesis, Université d'Aix-Marseille, Institut de Mathématiques de Luminy, 2012.
19. Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *Journal of Complexity*, 28:489–517, 2012.
20. Amin Shokrollahi. Optimal algorithms for multiplication in certain finite fields using algebraic curves. *SIAM Journal on Computing*, 21(6):1193–1198, 1992.
21. Igor Shparlinski, Michael Tsfasman, and Serguei Vlăduţ. Curves with many points and multiplication in finite fields. In H. Stichtenoth and M.A. Tsfasman, editors,

Coding Theory and Algebraic Geometry, number 1518 in Lectures Notes in Mathematics, pages 145–169, Berlin, 1992. Springer-Verlag. Proceedings of AGCT-3 Conference, June 17-21, 1991, Luminy.

22. Henning Stichtenoth. *Algebraic Function Fields and Codes*. Number 314 in Lectures Notes in Mathematics. Springer-Verlag, 1993.
23. Michael Tsfasman and Serguei Vlăduţ. Asymptotic properties of zeta-functions. *Journal of Mathematical Sciences*, 84(5):1445–1467, 1997.
24. Shmuel Winograd. On multiplication in algebraic extension fields. *Theoretical Computer Science*, 8:359–377, 1979.