On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry

Stéphane Ballet, Julia Pieltant, Jean Chaumine, Matthieu Rambaud, Hugues Randriambololona, Rolland Robert

ON THE TENSOR RANK OF MULTIPLICATION IN FINITE EXTENSIONS OF FINITE FIELDS AND RELATED ISSUES IN ALGEBRAIC GEOMETRY

STÉPHANE BALLET, JEAN CHAUMINE, JULIA PIELTANT, MATTHIEU RAMBAUD, HUGUES RANDRIAMBOLOLONA, AND ROBERT ROLLAND

Abstract. In this paper, we give a survey of the known results concerning the tensor rank of the multiplication in finite extensions of finite fields, enriched with some not published recent results as well as analyzes enhancing the qualitative understanding of the domain. In particular, we identify and clarify certain results not completely proved and we emphasis the link with open problems in number theory, algebraic geometry, and coding theory.

Contents

1. Introduction 2
1.1. Tensor rank and multiplication algorithm 3
1.2. Organization of the paper 5
2. Old classical results 6
3. The approach via algebraic curves 7
3.1. The D.V. Chudnovsky and G.V. Chudnovsky algorithm (CCMA) 8
3.2. The linearity of the bilinear complexity of the multiplication 9
4. The approach via codes 11
4.1. Connection with codes and asymptotic lower bounds 11
4.2. Supercodes 12
5. Generalizations of the algorithm of Chudnovsky-Chudnovsky 13
5.1. Motivation 13
5.2. Evaluation at places of higher degree and with multiplicities 14
5.3. Discussion on symmetry 15
5.4. The current generalized CCMA 16
6. Choice of the curves 19
6.1. Motivation and notations 19
6.2. Explicit towers, densification and descent 20
6.3. Modular and Shimura curves 21
6.3.1. Intertwinning two recursive towers into a dense family 22
6.3.2. Problems of descent on Shimura curves and open questions 23
6.3.3. References and historical notes for section 6 25
7. Obtaining a divisor of optimal degree for symmetric algorithms 26
7.1. Bounding the 2-torsion 26
7.2. Direct construction 28

Date: September 17, 2019.
2010 *Mathematics Subject Classification.* Primary 14H05; Secondary 12E20.
Key words and phrases. finite field, tensor rank of the multiplication, function field.

8. Asymptotic upper bounds 29
8.1. Upper bounds on m_q and M_q 30
8.2. Upper bounds on m_q^{sym} and M_q^{sym} 31
9. Uniform bounds 37
9.1. Some exact values for $\mu_q^{\mathrm{sym}}(n)$ 37
9.2. Upper bounds for $\mu_q^{\mathrm{sym}}(n)$ and $\mu_q^{\mathrm{sym}}(l,r)$ 38
9.3. Upper bounds for $\mu_q(n)$ and $\mu_q(l,r)$ 42
10. Effective construction of bilinear multiplication algorithms 44
10.1. Non-asymptotic construction 44
10.1.1. Classical multiplication algorithms 44
10.1.2. Parallel algorithms designed for multiplication and exponentiation 46
10.2. Asymptotic construction 47
11. Appendix: proof of Theorem 8.21, Theorem 8.9 and Proposition 6.11.2 48
11.1. Repairing (and extending) the criterion of Cascudo & al 49
11.2. Deriving the bounds from the previous theorem and other criterions from the litterature 50
References 51

1. Introduction

This article proposes a survey on the tensor rank of the multiplication in finite fields. It is an update of the previous survey [26] published about ten years ago. The deep improvements done since then require a complete rewrite of the survey highlighting the current state of the art. In particular, we present the new techniques introduced in recent years. The growing importance of this topic has attracted many mathematicians and computer scientists who developed new ideas and obtained new results. At the same time, we report a number of non-trivial errors and solutions which testify to the vividness of the domain and the community concerned. The finite fields are an important area. They arise in many fields applications, particularly in areas related to information theory. In particular, the complexity of the multiplication in the finite fields is a central problem. It is a part of the algebraic complexity for which the best general reference is [36]. It turns out that studying this problem has raised many issues of number theory and algebraic geometry. Notably, it has revealed deep links between these different domains. So, one of the objectives of this article is also to explicit these links and to present current related open problems. In the same time we prove some new results not yet published.

Let us describe more precisely the problem: we suppose that we have the multiplication in a finite field $\mathbb{F}_q$ and we want to construct an algorithm of multiplication in the extension $\mathbb{F}_{q^n}$ which is the least expansive in terms of operations in $\mathbb{F}_q$. Let us remark that from this point of view the multiplication in $\mathbb{F}_{q^n}$ is the multiplication of two polynomials of degree $< n$ with coefficients in $\mathbb{F}_q$. We then distinguish in the algorithm two types of operations: those which are linear with respect to the variables that one multiply and those which are bilinear with respect to the two variables. More precisely, let $\mathcal{B} = \{e_1, ..., e_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. If

$x = \sum_{i=1}^{n} x_i e_i$ et $y = \sum_{i=1}^{n} y_i e_i$ then a direct computation gives:

$$z = xy = \sum_{h=1}^{n} z_h e_h = \sum_{h=1}^{n} \Big(\sum_{i,j=1}^{n} t_{ijh} x_i x_j \Big) e_h, \tag{1}$$

where

$$e_i e_j = \sum_{h=1}^{n} t_{ijh} e_h,$$

$t_{ijh} \in \mathbb{F}_q$ being constants. Then the problem of the algebraic complexity consists on determining the minimal number of elementary operations in $\mathbb{F}_q$ required to compute the product of two elements $x, y \in \mathbb{F}_{q^n}$. We can distinguish the following operations:

- addition : $(\alpha, \beta) \mapsto \alpha + \beta$ où $\alpha, \beta \in \mathbb{F}_q$,
- scalar multiplication : $x_i \mapsto \alpha \cdot x_i$ where $\alpha, x_i \in \mathbb{F}_q$, and α is a constant,
- non-scalar or bilinear multiplication : $(x_i, y_j) \mapsto x_i \cdot y_j$ where $x_i, y_j \in \mathbb{F}_q$ depend on the elements x and y of $\mathbb{F}_{q^n}$ which are multiplied.

So, to obtain the product xy by the direct computation, one counts:

- $n^3 - n$ additions,
- n^3 scalar multiplications,
- n^2 non-scalar or bilinear multiplications.

The bilinear complexity of the algorithm of multiplication is given by the number of used bilinear multiplications. This complexity corresponds to the rank of the tensor of multiplication corresponding to this algorithm in $\mathbb{F}_{q^n}$ as vector space over $\mathbb{F}_q$, as will be explained in the next section.

The bilinear complexity of multiplication in finite fields $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is obtained by a tensor (resp. an algorithm) of minimal rank (resp. of minimal bilinear complexity). The survey emphases the study of this minimal complexity.

In this paper, it is a question of introducing the problem of the tensor rank of the multiplication in finite fields and of giving a statement of the results obtained in this part of algebraic complexity theory, as well as related issues.

1.1. **Tensor rank and multiplication algorithm.** Let us recall the notions of multiplication algorithm and associated bilinear complexity.

Definition 1.1. *Let K be a field and $E_0, \ldots, E_s$ be finite dimensional K-vector spaces. A non zero element $t \in E_0 \otimes \cdots \otimes E_s$ is said to be an elementary tensor, or a tensor of rank 1, if it can be written in the form $t = e_0 \otimes \cdots \otimes e_s$ for some $e_i \in E_i$. More generally, the rank of an arbitrary $t \in E_0 \otimes \cdots \otimes E_s$ is defined as the minimal length of a decomposition of t as a sum of elementary tensors.*

Definition 1.2. *If*

$$\alpha \ : \ E_1 \times \cdots \times E_s \longrightarrow E_0$$

is an s-linear map, the s-linear complexity of α is defined as the tensor rank of the element

$$\tilde{\alpha} \in E_0 \otimes E_1^\vee \otimes \cdots \otimes E_s^\vee$$

where $E_i^\vee$ denotes the dual of E_i as vector space over K for any integer i, naturally deduced from α. In particular, the 2-linear complexity is called the bilinear complexity.

Definition 1.3. *Let $\mathcal{A}$ be a finite-dimensional K-algebra. We denote by*

$$\mu(\mathcal{A}/K)$$

the bilinear complexity of the multiplication map

$$m_{\mathcal{A}} \ : \ \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$$

considered as a K-bilinear map.
In particular, if $\mathcal{A} = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$, we set:

$$\mu_q(m) = \mu(\mathbb{F}_{q^m}/\mathbb{F}_q).$$

More concretely, $\mu(\mathcal{A}/K)$ is the smallest integer n such that there exist linear forms $\phi_1, \ldots, \phi_n, \psi_1, \ldots, \psi_n \ : \ \mathcal{A} \longrightarrow K$, and elements $w_1, \ldots, w_n \in \mathcal{A}$, such that for all $x, y \in \mathcal{A}$ one has

$$xy = \phi_1(x)\psi_1(y)w_1 + \cdots + \phi_n(x)\psi_n(y)w_n, \tag{2}$$

since such an expression is the same thing as a decomposition

$$t_M = \sum_{i=1}^{n} w_i \otimes \phi_i \otimes \psi_i \in \mathcal{A} \otimes \mathcal{A}^\vee \otimes \mathcal{A}^\vee \tag{3}$$

for the multiplication tensor of $\mathcal{A}$.

Definition 1.4. *We call multiplication algorithm of length n for $\mathcal{A}/K$ a collection of ϕ_i, ψ_i, w_i that satisfy (2) or equivalently a tensor decomposition*

$$t_M = \sum_{i=1}^{n} w_i \otimes \phi_i \otimes \psi_i \in \mathcal{A} \otimes \mathcal{A}^\vee \otimes \mathcal{A}^\vee$$

for the multiplication tensor of $\mathcal{A}$. Such an algorithm is said symmetric if $\phi_i = \psi_i$ for all i (this can happen only if $\mathcal{A}$ is commutative).

Hence, when $\mathcal{A}$ is commutative, it is interesting to study the minimal length of a symmetric multiplication algorithm.

Definition 1.5. *Let $\mathcal{A}$ be a finite-dimensional commutative K-algebra. The symmetric bilinear complexity*

$$\mu^{\mathrm{sym}}(\mathcal{A}/K)$$

is the minimal length of a symmetric multiplication algorithm.
In particular, if $\mathcal{A} = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$, we set:

$$\mu_q^{\mathrm{sym}}(m) = \mu^{\mathrm{sym}}(\mathbb{F}_{q^m}/\mathbb{F}_q).$$

Here are some basic properties of these quantities, taken from [72, Lemma 1.10]:

Lemma 1.6. *(a) If $\mathcal{A}$ is a finite-dimensional K-algebra and L an extension field of K, and if we let $\mathcal{A}_L = \mathcal{A} \otimes_K L$ considered as an L-algebra, then*

$$\mu(\mathcal{A}_L/L) \leq \mu(\mathcal{A}/K).$$

Moreover, if $\mathcal{A}$ is commutative, we also have

$$\mu^{\mathrm{sym}}(\mathcal{A}_L/L) \leq \mu^{\mathrm{sym}}(\mathcal{A}/K).$$

(b) If $\mathcal{A}$ is a finite-dimensional L-algebra, where L is an extension field of K, then $\mathcal{A}$ can also be considered as a K-algebra, and

$$\mu(\mathcal{A}/K) \leq \mu(\mathcal{A}/L)\mu(L/K).$$

Moreover, if $\mathcal{A}$ is commutative, we also have

$$\mu^{\mathrm{sym}}(\mathcal{A}/K) \leq \mu^{\mathrm{sym}}(\mathcal{A}/L)\mu^{\mathrm{sym}}(L/K).$$

(c) If $\mathcal{A}$ and $\mathcal{B}$ are two finite-dimensional K-algebras,

$$\mu(\mathcal{A} \times \mathcal{B}/K) \leq \mu(\mathcal{A}/K) + \mu(\mathcal{B}/K).$$

Moreover, if $\mathcal{A}$ and $\mathcal{B}$ are commutative, we also have

$$\mu^{\mathrm{sym}}(\mathcal{A} \times \mathcal{B}/K) \leq \mu^{\mathrm{sym}}(\mathcal{A}/K) + \mu^{\mathrm{sym}}(\mathcal{B}/K).$$

(d) If $\mathcal{A}$ and $\mathcal{B}$ are two finite-dimensional K-algebras,

$$\mu(\mathcal{A} \otimes_K \mathcal{B}/K) \leq \mu(\mathcal{A}/K)\mu(\mathcal{B}/K).$$

Moreover, if $\mathcal{A}$ and $\mathcal{B}$ are commutative, we also have

$$\mu^{\mathrm{sym}}(\mathcal{A} \otimes_K \mathcal{B}/K) \leq \mu^{\mathrm{sym}}(\mathcal{A}/K)\mu(\mathcal{B}/K).$$

In particular, the following lemma of Shparlinski, Tsfasman, and Vladut [78, Lemma 1.2], is especially useful. Actually, the right-hand inequality was already stated in the original paper of D.V. Chudnovsky and G.V.Chudnovsky [44, eq. (6.2)], so the new contribution of I. Shparlinski, M. Tsfasman, and S. Vladut is the left-hand inequality. This will be important when we will consider asymptotic complexities in Lemma 8.1.

Lemma 1.7. *For all m, n we have*

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

Actually the same holds for symmetric complexity.

Lemma 1.8. *For all m, n we have*

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

Proof. The left-hand inequalities $\mu_q(n) \leq \mu_q(mn)$ and $\mu_q^{\mathrm{sym}}(n) \leq \mu_q^{\mathrm{sym}}(mn)$ are consequences of the inclusion $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^{mn}}$. Then, for the right-hand inequalities $\mu_q(mn) \leq \mu_q(m) \cdot \mu_{q^m}(n)$ and $\mu_q^{\mathrm{sym}}(mn) \leq \mu_q^{\mathrm{sym}}(m) \cdot \mu_{q^m}^{\mathrm{sym}}(n)$, we apply Lemma 1.6(b) with $\mathcal{A} = \mathbb{F}_{q^{mn}}$, $L = \mathbb{F}_{q^m}$, and $K = \mathbb{F}_q$. □

1.2. **Organization of the paper.** In Section 2, we present the classical results via the approach using the multiplication by polynomial interpolation. In Section 3, we give an historical record of results obtained from the pioneer works due to D.V. and G.V. Chudnovsky in [44] and later I. Shparlinski, M. Tsfasman and S. Vladut in [78]. In particular, we present the original algorithm. This modern approach uses the interpolation over algebraic curves defined over finite fields. This approach, which we recount the first success as well as the rocks on which the pionners came to grief, enables to end at a first complete proof of the linearity of the bilinear complexity of multiplication by S. Ballet in [6]. In Section 4, we present the code approach for the bilinear complexity and explain the connexion between the bilinear complexity of multiplication and the so-called (exact) supercodes, or equivalently multiplication friendly codes in the lexicon of certain authors. Then, in Section 5, we present the different generalizations of the original D.V. and G.V.

Chudnovsky algorithm, in particular the most successful version of the algorithm of Chudnovsky–Chudnovsky type at the present time, due to H. Randriambololona in [72]. This part explains the links with algebraic geometry. In Section 8, we recall the known results on the asymptotic bounds about the symmetric and asymmetric bilinear complexity that have been established through the last 30 years. Then, in a same way, in Section 9, we give uniform bounds about the symmetric and asymmetric bilinear complexity. Finally, in Section 10 we present methods about the effective construction of bilinear multiplication algorithms in finite fields.

2. Old classical results

Let

$$P(u) = \sum_{i=0}^{n} a_i u^i$$

be a monic irreducible polynomial of degree n with coefficients in a field F. Let

$$R(u) = \sum_{i=0}^{n-1} x_i u^i$$

and

$$S(u) = \sum_{i=0}^{n-1} y_i u^i$$

be two polynomials of degree $\leq n-1$ where the coefficients x_i and y_i are indeterminates.

C. Fiduccia and Y. Zalcstein (cf. [55], [36] p.367 Prop. 14.47) have studied the general problem of computing the coefficients of the product $R(u) \times S(u)$ and they have shown that at least $2n-1$ multiplications are needed. When the field F is infinite, an algorithm reaching exactly this bound was previously given by A. Toom in [80]. S. Winograd described in [87] all the algorithms reaching the bound $2n-1$. Moreover, S. Winograd proved in [88] that up to some transformations every algorithm for computing the coefficients of $R(u) \times S(u) \mod P(u)$ which is of bilinear complexity $2n-1$, necessarily computes the coefficients of $R(u) \times S(u)$, and consequently uses one of the algorithms described in [87]. These algorithms use interpolation techniques and cannot be performed if the cardinality of the field F is $< 2n-2$. In conclusion, we have the following result:

Theorem 2.1. *If the cardinality of F is $< 2n-2$, every algorithm computing the coefficients of $R(u) \times S(u) \mod P(u)$ has a bilinear complexity $> 2n-1$.*

Applying the results of S. Winograd and H. De Groote [47] and Theorem 2.1 to the multiplication in a finite extension $\mathbb{F}_{q^n}$ of a finite field $\mathbb{F}_q$ we obtain:

Theorem 2.2. *The bilinear complexity $\mu_q(n)$ of the multiplication in the finite field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ verifies*

$$\mu_q(n) \geq 2n-1,$$

with equality holding if and only if

$$n \leq \frac{q}{2} + 1.$$

This result does not give any estimate of an upper bound for $\mu_q(n)$, when n is large. In [62], A. Lempel, G. Seroussi and S. Winograd proved that $\mu_q(n)$ has a quasi-linear upper bound. More precisely:

Theorem 2.3. *The bilinear complexity of the multiplication in the finite field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ verifies:*

$$\mu_q(n) \leq f_q(n)n,$$

where $f_q(n)$ is a very slowly growing function defined recursively by

$$f_q(n) = 2f_q((\lceil \log_q(2(q-1)n) \rceil),$$

$n \geq 4$, $q \geq 2$.
For $n < 4$, $f_q(n)$ is defined as follows:

$$f_q(n) = \begin{cases} 1, & n = 1,\ q \geq 2, \\ \dfrac{3}{2}, & n = 2,\ q \geq 2, \\ \dfrac{5}{3}, & n = 3,\ q \geq 4, \\ 2, & n = 3,\ 2 \leq q \leq 3. \end{cases}$$

Corollary 2.4. *Asymptotically,*

$$f_q(n) < \underbrace{\log_q \log_q \cdots \log_q}_{k \text{ times}}(n)$$

for any $k \geq 1$.

Furthermore, extending and using more efficiently the technique developed in [35], N. Bshouty and M. Kaminski showed that

$$\mu_q(n) \geq 3n - o(n)$$

for $q \geq 3$. The proof of the above lower bound on the complexity of straight-line algorithms for polynomial multiplication is based on the analysis of Hankel matrices representing bilinear forms defined by linear combinations of the coefficients of the polynomial product.

3. The approach via algebraic curves

We have seen in the previous section that if the number of points of the ground field is too low, we cannot perform the multiplication by the Winograd interpolation method. D.V. and G.V. Chudnovsky have designed in [44] an algorithm where the interpolation is done on points of an algebraic curve over the ground-field with a sufficient number of rational points. We will denote by CCMA this Chudnovsky–Chudnovsky Multiplication Algorithm. Using this algorithm, D.V. and G.V. Chudnovsky claimed that the bilinear complexity of the multiplication in finite extensions of a finite field is asymptotically linear but later I. Shparlinski, M. Tsfasman and S. Vladut in [78] noted that they only proved that the quantity $m_q = \liminf_{k\to\infty} \frac{\mu_q(k)}{k}$ is bounded which does not enable to prove the linearity. To prove the linearity, it is also necessary to prove that $M_q = \limsup_{k\to\infty} \frac{\mu_q(k)}{k}$ is bounded which is the main aim of their paper. However, I. Cascudo, R. Cramer and C. Xing recently detected a mistake in the proof of I. Shparlinski, M. Tsfasman and S. Vladut. Unfortunately, this mistake that we will explain in details in this section, also had an effect on their improved estimations of m_q.

After the above pioneer research, S. Ballet obtained in [6] (cf. also [5]) the first upper bounds uniformly with respect to q for $\mu_q(n)$. The algorithm CCMA being clearly symmetric, these first uniform bounds also concerned $\mu_q^{\mathrm{sym}}(n)$. Moreover, these bounds not being affected by the same mistake enable at the same time to prove the linearity of the bilinear complexity of the multiplication in finite extensions of a finite field since it obviously implied that M_q was finite. Subsequently, critical improvements were introduced: in [5][6], S. Ballet introduces simple numerical conditions on algebraic curves of an arbitrary genus g giving a sufficient condition for the application of the algorithm CCMA (existence of places of certain degree, of non-special divisors of degree $g-1$) generalizing the result of A. Shokrollahi [77] for the elliptic curves; in [5][6] S. Ballet introduces the use of towers of algebraic functions fields and their densification in [8]; in [25] S. Ballet and R. Rolland introduce the use of places of higher degree; in [25] S. Ballet and R. Rolland introduce the descent over $\mathbb{F}_q$ of the definition field $\mathbb{F}_{q^2}$ of a densified tower defined over $\mathbb{F}_{q^2}$ for any finite field $\mathbb{F}_q$ with a caracteristic $p = 2$ and in [19], S. Ballet, D. Le Brigand and R. Rolland generalize the method for any finite field; in [9] , S. Ballet derive optimal criterions for direct construction of the divisors satisfying the needed conditions and in [42][43], J. Chaumine proves that these criterions are always satisfied in the elliptic case, so improving the result of A. Shokrollahi [77]; in [18], thanks to an existence theorem of non-special divisors of degree $g-1$, S. Ballet and D. Le Brigand improve sufficient conditions for the application of the algorithm CCMA for the extensions of arbitrary finite fields; in [1], N. Arnaud introduces the use of local expansion, called derivated evaluation; in [20] [66] S. Ballet and Julia Pieltant introduce the use of divisors of degree zero thanks to a existence result obtained in [24] by S. Ballet, C. Ritzenthaler and R. Rolland and combine it with local expansion. Then M. Cenk and F. Özbudak [40], and H. Randriambololona [72] gave improvements by using of local expansion and high degree places. These can be combined with the following other independent ingredients, also proposed in [72]: allowing asymmetry in the interpolation procedure, which establishes the announced Shparlinski-Tsfasman-Vladut estimates for m_q and M_q; and using the best bilinear complexities recursively, an idea that was then also used in [15]. Last, two ideas can be used in order to deal with symmetric complexities: bounds involving the 2-torsion [89][70][37][38], and direct construction of the divisors satisfying the needed conditions [73][71][72]. Ultimately this allows to obtain for most cases the Shparlinski-Tsfasman-Vladut estimates also for m_q^{sym} and M_q^{sym}, as well as other related estimates for symmetric complexity.

3.1. **The D.V. Chudnovsky and G.V. Chudnovsky algorithm (CCMA).** In this section, we recall the brilliant idea of D.V. Chudnovsky and G.V. Chudnovsky and give their main result. First, we present the original CCMA, which was established in 1987 in [44].

Theorem 3.1. *Let*

- $F/\mathbb{F}_q$ *be an algebraic function field,*
- Q *be a degree* n *place of* $F/\mathbb{F}_q$*,*
- $\mathcal{D}$ *be a divisor of* $F/\mathbb{F}_q$*,*
- $\mathscr{P} = \{P_1, \ldots, P_N\}$ *be a set of places of degree* 1*.*

We suppose that Q*,* $P_1, \ldots, P_N$ *are not in the support of* $\mathcal{D}$ *and that:*

(a) the evaluation map

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

is onto (where F_Q is the residue class field of Q),

(b) the application

$$Ev_{\mathscr{P}} : \left| \begin{array}{ccc} \mathcal{L}(2\mathcal{D}) & \to & \mathbb{F}_q^N \\ f & \mapsto & (f(P_1), \ldots, f(P_N)) \end{array} \right.$$

is injective.

Then

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

We presented this result as it was formulated in [44], in terms of the bilinear complexity $\mu_q(n)$. However closer inspection of the method shows that it produces symmetric algorithms, so the conclusion also holds for the *symmetric* bilinear complexity:

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

3.2. **The linearity of the bilinear complexity of the multiplication.** As seen previously, I. Shparlinski, M. Tsfasman and S. Vladut have given in [78] many interesting remarks on CCMA and the bilinear complexity. In particular, they have considered asymptotic bounds[1] for the bilinear complexity in order to prove the linearity of this complexity from CCMA. Following these authors, let us define

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

and

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

Moreover, we also have to consider the symmetric variants of these quantities which were not considered by I. Shparlinski, M. Tsfasman and S. Vladut, but were first introduced by H. Randriambololona in [72], and have become equally important since then:

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

and

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

It is clear that we have:

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

and

$$m_q \leq m_q^{\mathrm{sym}}.$$

It is not obvious at all that either of these values is finite. Note that if M_q (resp. M_q^{sym}) is finite, then bilinear complexity (resp. the symmetric bilinear complexity)

[1]The families of curves used by the pioneers only gave asymptotic bounds. M. Tsfasman in a private communication asked for the question of finding uniform bounds to R. Rolland.

of multiplication is linear in the degree of extension, namely there exists a constant $C_q \geq M_q$ (resp. $C_q^{sym} \geq M_q^{\mathrm{sym}}$) such that for any integer $n > 1$,

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

From Theorem 3.1, D.V. Chudnovsky and G.V. Chudnovsky derive [44, Theorem 7.7][2]: for $q \geq 25$ a square, as $n \to \infty$, we have

$$\mu_q^{\mathrm{sym}}(n) \leq 2\left(1 + \frac{1}{\sqrt{q}-3}\right) \cdot n + o(n). \tag{4}$$

However, as pointed out by I. Shparlinski, M. Tsfasman and S. Vladut, the proof given for Bound (4) is quite sketchy, with some important details missing. This made them question its validity.

More precisely, relying on Ihara's work [61], D.V. Chudnovsky and G.V. Chudnovsky consider Shimura modular curves having an asymptotically maximal number of points over $\mathbb{F}_q$, and in the final step of their argument, they assert that, for some given constant C and for all integers n large enough, they can choose curves in this family of genus $g = C \cdot n + o(n)$. Although it follows from [61] that this is possible for infinitely many n, D.V. Chudnovsky and G.V. Chudnovsky need it to hold for *all* n, for which they do not give justification. Because of this, I. Shparlinski, M. Tsfasman and S. Vladut explain that one should consider that, although D.V. Chudnovsky and G.V. Chudnovsky state an estimate for the limsup M_q, their proof is valid only for the liminf m_q.

But then, with [78, Claim, p. 163], I. Shparlinski, M. Tsfasman and S. Vladut precisely describe a family of Shimura curves that satisfy the conditions needed by D.V. Chudnovsky and G.V. Chudnovsky, which essentially completes the proof of (4). Unfortunately, at the same time, I. Shparlinski, M. Tsfasman and S. Vladut also propose to replace (4) with a sharper bound, and in doing so they introduce in the proof an unproved argument. The gap in their proof was found by I. Cascudo, R. Cramer and C. Xing (cf. personal communication in 2009 and [38, Section V]). They present the gap as follows: *the mistake in* [78] *from 1992 is in the proof of their Lemma 3.3, page 161, the paragraph following formulas about the degrees of the divisor. It reads: "Thus the number of linear equivalence classes of degree a for which either Condition α or Condition β fails is at most $D_{b'} + D_b$." This is incorrect; D_b should be multiplied by the torsion. Hence the proof of their asympotic bound is incorrect.* ». Note that a synthesis work enabling to fill the gap let in the proof of D.V and G. V. Chudnovsky with the approach of Shparlinski, Tsfasman and Vladut is possible but not direct. Anyway, independently, by using the strategy of D.V and G. V. Chudnovsky applied to the first tower[3] of Garcia-Stichtenoth [57] attaining the Drinfeld-Vladut bound, joint to a result concerning the existence of non-special divisors of degree $g - 1$, S. Ballet gives in [6] the first complete proof of the linearity of the bilinear complexity of the multiplication. More precisely, it was done by determining directly upper bounds for C_q^{sym}. From there, different

[2]This result is originally formulated for $\mu_q(n)$. Although at this time most authors did not distinguish in the notation between bilinear complexity and symmetric bilinear complexity, it was known that the CCMA naturally produces symmetric algorithms (cf. [44, Definition p. 154 and Remark 2.2] and also more precisely [6, Proof of Theorem 1.1]), so the estimate also holds for the symmetric bilinear complexity $\mu_q^{\mathrm{sym}}(n)$.

[3]The advantage of this tower of algebraic function fields is that firstly one knows explicitly the number of rational points and the the genus for each step, secondly the ratio of rational points over the genus is very good.

works were done to improve the asymptotic bounds (cf. Section 8) and the uniform bounds (cf. Section 9).

4. The approach via codes

Initially, just after the pioneer work of D.V. and G.V. Chudnovsky [44], I. Shparlinski, M. Tsfasman and S. Vladut in [78] specified the link between certain codes and multiplication tensors. Then, they introduced the notion of exact supercodes also called multiplication friendly codes.

4.1. **Connection with codes and asymptotic lower bounds.** First, let us recall the link between the linear error-correcting codes and the decomposition of multiplication tensors.

Let us recall the following classical definition:

Definition 4.1. *A linear error-correcting code C over $\mathbb{F}_q$ of length N, dimension n and Hamming distance d is called an $[N,n,d]_q$-code. The rate $\frac{n}{d}$ of such a code is denoted by R and its relative minimum distance $\frac{d}{n}$ by δ.*

By [78], it is possible to construct a code using decomposition of t_M into a sum of rank one tensors. Indeed, if

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

where $a_l \in \mathbb{F}_{q^n}^*$, $b_l \in \mathbb{F}_{q^n}^*$, $c_l \in \mathbb{F}_{q^n}$, then one defines an $\mathbb{F}_q$-linear map

$$\begin{array}{rccc} \phi: & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_q^N \\ & x & \longmapsto & (a_1(x), \ldots, a_N(x)). \end{array}$$

From [78], it follows that:

Proposition 4.2. *The $\mathbb{F}_q$-vector space $C = \operatorname{Im}\phi$ is an $[N,n,d]_q$-code such that $d \geq n$.*

Corollary 4.3. *Any decomposition of length N of a tensor of multiplication in the finite field $\mathbb{F}_{q^n}$ gives an $[N,n,d]_q$-code such that $d \geq n$. In particular, if $N_q(n)$ is the minimum length of a linear $[N,n,n]_q$-code then the tensor rank $\mu_q(n)$ of multiplication in the finite field $\mathbb{F}_{q^n}$ is such that $\mu_q(n) \geq N_q(n)$.*

Let us recall that there exists a continuous decreasing function $\alpha_q^{\mathrm{lin}}(\delta)$ on the segment $[0, 1-\frac{1}{q}]$ which corresponds to the bound for the rate R of the linear codes over $\mathbb{F}_q$ with relative minimum distance at least δ (cf [82, 1.3.1]). Hence:

Corollary 4.4. *One has:*

$$m_q \geq \delta_q^{-1},$$

where δ_q is the unique solution of the equation $\alpha_q^{\mathrm{lin}}(\delta) = \delta$.

Any upper bound for $\alpha_q^{\mathrm{lin}}(\delta)$ gives an upper bound for δ_q and thus a lower bound for m_q. So, from this corollary, it follows that we can obtain lower bounds of the asymptotic quantity m_q from asymptotic parameters of codes. Now, let us summarize the known lower bounds concerning this quantity, namely the lower bound of m_2 obtained by R. Brockett, M. Brown and D. Dobkin in [32, 31] by using the bound of "four" [82, 1.3.2] for asymptotic parameters of binary codes, and the lower bound of m_q for $q > 2$ given by I. Shparlinski, M. Tsfasman and S. Vladut in

[78] by using the asymptotic Plotkin bound [82, 1.3.2]. Note that this last bound is a straightforward consequence of Proposition 4.3 established by D.V. and G.V. Chudnovsky in [44].

Proposition 4.5. *One has:*

$$m_2 \geq 3.52$$

and

$$m_q \geq 2\left(1+\frac{1}{q-1}\right) \text{ for any } q>2.$$

4.2. **Supercodes.** Let us recall the notion of supercode introduced by Shparlinski, Tsfasman and Vladut in [78]. First, let us recall the idea leading to the emergence of the notion of supercode. By Section 4.1, any decomposition of the tensor t_M into a sum of N summands of rank one enables us to obtain an $[N,n,d]_q$-code. In fact, the notion of supercode follows from the question to know when it is possible conversely to construct such a decomposition from a linear $[N,n,\geq n]_q$-code.

Definition 4.6. *Let $S \subseteq \mathbb{F}_{q^n} \oplus \mathbb{F}_q^N$ be an $\mathbb{F}_q$-linear subspace. S is called an $[N,n]_q$-supercode if the following conditions are satisfied:*

1) the first projection

$$\pi_1 : \mathbb{F}_{q^n} \oplus \mathbb{F}_q^N \longrightarrow \mathbb{F}_{q^n}$$

restricted to S is surjective.

2) let $S^2 = \{s_1 s_2 \,|\, s_1, s_2 \in S\}$ where the multiplication is that in $\mathbb{F}_q$-algebra $\mathbb{F}_{q^n} \oplus \mathbb{F}_q^N$ and let $< S^2 >$ be the subspace in $\mathbb{F}_{q^n} \oplus \mathbb{F}_q^N$ spanned by S^2. The second projection

$$\pi_2 : \mathbb{F}_{q^n} \oplus \mathbb{F}_q^N \longrightarrow \mathbb{F}_q^N$$

restricted to $< S^2 >$ is injective.

From Definition 4.6, it is now possible to obtain the following more restrictive notion, almost equivalent to the notion of symmetric decomposition of a multiplication tensor.

Definition 4.7. *An $[N,n]_q$-supercode S is said exact if π_1 is an isomorphism, i.e. if $\dim S = n$.*

Proposition 4.8. *Let S be an $[N,n]_q$-supercode and let $C = \pi_2(S)$, then:*

(1) C is an $[N,\geq n,\geq n]$-code.

(2) If S is exact then C is an $[N,n,\geq n]$-code.

(3) Any supercode contains an exact sub-supercode.

In fact, the notion of exact supercode is equivalent to that of symmetric decomposition of t_M into a sum of N rank one tensors, up to the representation of $\mathbb{F}_{q^n}$ (i.e modulo the following equivalence relation):

Definition 4.9. *Let $\sigma_1 = \sum_{i=1}^N u_i \otimes u_i \otimes w_i$ and $\sigma_2 = \sum_{i=1}^N v_i \otimes v_i \otimes z_i$ be two symmetric decompositions of t_M. We call σ_1 and σ_2 equivalent if $u_i = v_i$ for every i.*

Now, by considering the equivalence relation of Definition 4.9, we obtain the following result.

Theorem 4.10. *There is a bijection between the set of exact supercodes and the set of equivalence classes of symmetric decompositions of t_M.*

Then, by [78, Proposition 1.11 and Corollary 1.13], we obtain:

Corollary 4.11. *(1) Any exact supercode $S \subset \mathbb{F}_{q^n} \oplus \mathbb{F}_q^N$ yields a symmetric multiplication algorithm of bilinear complexity N and conversely.*
(2) Any supercode $S \subset \mathbb{F}_{q^n} \oplus \mathbb{F}_q^N$ yields a symmetric multiplication algorithm of bilinear complexity $\leq N$.

Note that I. Shparlinski, M. Tsfasman and S. Vladut in [78] gave an explicit construction of a symmetric tensor t_M of length N performing the multiplication in a finite field $\mathbb{F}_{q^n}$ from an exact supercode $S \subset \mathbb{F}_{q^n} \oplus \mathbb{F}_q^N$. Conversely, from an arbitrary symmetric decomposition, they explicitly obtain an exact supercode by [78, Proposition 1.11].

Remark 4.12. *Note that certain authors use the notion of multiplication friendly code which is equivalent to the notion of exact supercode. In particular, the results obtained by using the notion of multiplication friendly code only concern the symmetric bilinear complexity.*

Open problems 4.13. How can one characterize those $[N, \geq k, \geq k]$-codes which are projections of supercodes?

5. Generalizations of the algorithm of Chudnovsky-Chudnovsky

5.1. **Motivation.** When using the original Chudnovsky-Chudnovsky method, one sees that the bounds that can be obtained on the bilinear complexity, as well as their effectivity or the practical implementation of the corresponding multiplication algorithms, highly depend on the choice of the geometric data on which Theorem 3.1 is applied. For instance, in order to get the best possible bounds, one needs curves having sufficiently many rational points with the smallest possible genus. This works well when one is considering a base field that is not too small, and of square order, so the celebrated Drinfeld-Vladut bound can be attained (see section 6 for details). But in other situations, the original Chudnovsky-Chudnovsky method presents certain limitations. Several improvements were then proposed to overcome these limitations.

In order to better understand these improvements, we will thus distinguish *two steps* in the construction of multiplication algorithms. The *first step* is to state a "generic" CCMA, which takes as input some geometric data (a function field or a curve, some places or points on it, and some divisors that satisfy adequate conditions), and gives as output an effective multiplication algorithm, or at least an upper bound on some bilinear complexity. The *second step* then is to specify the geometric objects on which this generic CCMA will be applied: choice of the curves, existence of the divisors, etc.

Concerning the *first step* (generic statement of the CCMA), successive generalizations were proposed by various authors, using several independent ingredients, among which we can cite:

- evaluation at places of higher degree and/or with multiplicities
- symmetric/asymmetric versions of the algorithm optimized for symmetric/asymmetric bilinear complexity respectively
- formulation adapted for an iterative use.

In this section we give more details on these lines of improvements, with emphasis on the first two (in sections 5.2 and 5.3), and we present the best finalized version

of the CCMA [72, Theorem 3.5], which combines them all. We then explain how intermediate historical contributions can be retrieved as particular cases.

Concerning the *second step* (specification of the geometric objects), the most important ingredients are:

- careful choice of the curves, either explicit recursive towers, their densification and descent of base field (see section 6.2 for details), or more abstract modular, Shimura, or Drinfled modular curves (see section 6.3)
- techniques to ensure the existence, or even to effectively construct the divisor needed to perform interpolation, of best possible degree; this is especially important in the context of symmetric algorithms (see section 7).

Of course these two steps that we distinguished are closely intertwined: a suitably generalized generic CCMA will allow a broader choice for the geometric objects, hence lead to better bounds or a more effective implementation. In the other direction, it can happen that some geometric conditions (e.g. existence of points of given degree or of suitable divisors) can be replaced with simple numerical criteria, and get included in the statement of the generic CCMA.

5.2. **Evaluation at places of higher degree and with multiplicities.** Here one can cite several successive contributions.

- First S. Ballet and R. Rolland have generalized in [25] the algorithm using places of degree 1 and 2.
- Then N. Arnaud [1] introduced, as in the interpolation of Lagrange-Sylvester, the use of derivatives (evaluation with multiplicities) to improve the interpolation process.
- These ideas are combined and extended in the work of M. Cenk and F. Özbudak in [40]. This generalization uses several coefficients in the local expansion at each place P_i instead of just the first one. Due to the way it is obtained, their bound for the bilinear complexity involves a sum of local contributions, each of which is written as a product of two separate factors: one factor accounts for the degree of the place, the other factor accounts for the multiplicity.
- Last H. Randriambololona [72] refined this method by introducing a single quantity that combines both degree and multiplicity at the same time and leads to the sharpest bounds as presently known.

This quantity introduced in [72] can be defined in two variants, one for the bilinear complexity, the other for the symmetric bilinear complexity:

Definition 5.1. *For any integers $m, \ell \geq 1$ we consider the $\mathbb{F}_q$-algebra $\mathbb{F}_{q^m}[t]/(t^\ell)$ of polynomials in one indeterminate with coefficients in $\mathbb{F}_{q^m}$, truncated at order ℓ, and we denote by*

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

its bilinear complexity over $\mathbb{F}_q$, and by

$$\mu_q^{\mathrm{sym}}(m, \ell) = \mu^{\mathrm{sym}}((\mathbb{F}_{q^m}[t]/(t^\ell))/\mathbb{F}_q)$$

its symmetric bilinear complexity over $\mathbb{F}_q$.

Note that for $\ell = 1$, we have $\mu_q(m, 1) = \mu_q(m)$ and $\mu_q^{\mathrm{sym}}(m, 1) = \mu_q^{\mathrm{sym}}(m)$. While for $m = 1$, we have $\mu_q(1, \ell) = \widehat{M}_q(\ell)$ as defined by M. Cenk and F. Özbudak

in [40] (we could set likewise $\mu_q^{\mathrm{sym}}(1,\ell) = \widehat{M}_q^{\mathrm{sym}}(\ell)$, although this quantity is not considered in [40]).

The generalized evaluation maps that appear in the generalized CCMA can be described either in the language of modern algebraic geometry, as done in [72], or in the language of algebraic function fields, as done in previous works. Actually these two languages are equivalent, so we explain how to pass from one to the other.

Suppose we are given:

- a curve X over $\mathbb{F}_q$ (which corresponds to a function field $F/\mathbb{F}_q$)
- a closed point P on X of degree m (which corresponds to a place of F of degree m)
- an integer ℓ.

This allows to consider the thickened point $P^{[\ell]}$ on X, which is the closed subscheme defined by the sheaf of ideals $(\mathcal{I}_P)^\ell$.

Now, for any divisor $\mathcal{D}$ on X, we can define a generalized evaluation map, that evaluates sections of $\mathcal{D}$ at P with multiplicity ℓ. In geometric terms, this is just the natural restriction map

$$\varphi_{\mathcal{D},P,\ell} : \mathcal{L}(\mathcal{D}) \longrightarrow O_X(\mathcal{D})|_{P^{[\ell]}}.$$

After possibly replacing $\mathcal{D}$ with a linearly equivalent divisor, we will assume P is not in the support of $\mathcal{D}$. We then have a natural identification $\mathcal{O}_X(\mathcal{D})|_{P^{[\ell]}} = \mathcal{O}_{P^{[\ell]}}$. Then, thanks to [72, Lemma 3.4], we have an isomorphism of algebras

$$\mathcal{O}_{P^{[\ell]}} \simeq \mathbb{F}_{q^m}[t]/(t^\ell)$$

where t corresponds to a local parameter t_P at P, and $\mathbb{F}_{q^m}$ is identified with the residue field of P. Last, in order to make everything explicit for computations, we can use the natural linear isomorphism

$\mathbb{F}_{q^m}[t]/(t^\ell) \simeq (\mathbb{F}_{q^m})^\ell$ identifying a polynomial $a_0 + a_1 t + \cdots + a_{\ell-1}t^{\ell-1}$ with its coefficients $(a_0, a_1, \ldots, a_{\ell-1})$. Combining all this, the generalized evaluation map becomes

$$\varphi_{\mathcal{D},P,\ell} : \left| \begin{array}{ccc} \mathcal{L}(\mathcal{D}) & \longrightarrow & (\mathbb{F}_{q^m})^\ell \\ f & \mapsto & (f(P), f'(P), \ldots, f^{(\ell-1)}(P)) \end{array} \right. \tag{5}$$

where the $f^{(k)}(P)$ are the coefficients of the local expansion

$$f = f(P) + f'(P)t_P + f''(P)t_P^2 + \cdots + f^{(k)}(P)t_P^k + \cdots$$

of f at P with respect to t_P. Sometimes this is also called a "derived evaluation map", although one should be careful that for $k \geq 2$ these $f^{(k)}(P)$ are not precisely derivatives in the usual sense (at best they are "$\frac{1}{k!}$ times the derivative").

5.3. **Discussion on symmetry.** In the broader context of bilinear algorithms over finite fields, the distinction between (general) bilinear complexity and symmetric bilinear complexity, together with some of the mathematical issues related specifically to the construction of symmetric algorithms, were first discussed in 1984 by Seroussi and Lempel with [76].

Focusing now on works based on the Chudnovsky-Chudnovsky method, it turns out that until 2011, all results (including those in [44][78][26][40][71]) were stated in terms of μ_q only (not μ_q^{sym}), although by construction the method always produced symmetric algorithms. Of course this does not mean that the authors were not aware of the distinction: indeed, for instance, I. Shparlinski, M. Tsfasman and S.

Vladut explicitely mentioned the issue when they observed [78, p. 154] that their notion of supercode corresponds only to symmetric algorithms.

However the situation became unsatisfactory when I. Cascudo, R. Cramer and C. Xing discovered the gap in the construction of the divisor in [78], as already discussed in section 3. Indeed, it turns out that the difficulty of this construction, which they analyze in terms of the 2-torsion in the divisor class group of the curve (see section 7.1), is closely related to the symmetry requirement for the algorithm.

Finally, things were clarified by H. Randriambololona in [72]. Along with the contributions already discussed in section 5.2, this work introduced two further improvements to the method:

- one that solves the difficulty with the construction of the divisor in the symmetric case, at least for curves with sufficiently many rational points (see section 7.2 for details)
- another one that produces asymmetric algorithms instead, by allowing asymmetry in the CCMA; this is advantageous because asymmetric interpolation allows more freedom in the choice of the divisors, and ultimately, can lead to sharper bounds.

As a consequence of these developments, whenever possible, the generalized CCMA should be stated in two versions, one for bilinear complexity, the other for symmetric bilinear complexity. Likewise, the numerical bounds should be stated in two versions, accordingly.

Beside bilinear complexity μ_q and symmetric bilinear complexity μ_q^{sym}, other refinements were introduced and studied in [76] and [74, Appendix A]: these are trisymmetric bilinear complexity μ_q^{tri}, and normalized trisymmetric bilinear complexity μ_q^{nrm}.

It should be noted that it can happen that these quantities are not well defined for some values of q and n. More precisely, [74, Prop. A.14] shows that $\mu_q^{\mathrm{tri}}(n)$ is well defined for all values of q and n except precisely for $q = 2$, $n \geq 3$. Likewise [74, Prop. A.19] shows that $\mu_q^{\mathrm{nrm}}(n)$ is well defined for all values of q and n except precisely for $q = 2$, $n \geq 3$ and for $q = 4$, $n \geq 2$.

In any case, when well defined, one has

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

Also, [76, Th. 2] gives $\mu_q^{\mathrm{tri}}(n) \leq 4\,\mu_q^{\mathrm{sym}}(n)$ for $q \neq 2$, $\mathrm{char}(\mathbb{F}_q) \neq 3$, and [74, Prop. A.19] gives $\mu_q^{\mathrm{nrm}}(n) \leq 2\,\mu_q^{\mathrm{tri}}(n)$ for $q \neq 7$ and $\mu_7^{\mathrm{nrm}}(n) \leq 3\,\mu_7^{\mathrm{tri}}(n)$. Joint with the linearity of μ_q^{sym}, this gives the linearity of μ_q^{nrm} and μ_q^{tri} for most q.

But beside this, very few is known about these quantities.

Open problems 5.2. What are the exact values of $\mu_q^{\mathrm{nrm}}(n)$ and $\mu_q^{\mathrm{tri}}(n)$ for small q and n?

Can some of the inequalities between $\mu_q(n)$, $\mu_q^{\mathrm{sym}}(n)$, $\mu_q^{\mathrm{tri}}(n)$ and $\mu_q^{\mathrm{nrm}}(n)$ be strict? If so, for which values of n?

Can one give better asymptotic bounds on them?

5.4. **The current generalized CCMA.** Now we can state H. Randriambolona 's result [72, Theorem 3.5], which provides the current most general CCMA. It makes

use of the most elaborate form of derived evaluation, and it gives bounds both for asymmetric complexity and for symmetric complexity.

As already explained, this result was originally presented in the language of modern algebraic geometry, but here we give the equivalent translation in the language of function fields.

Theorem 5.3. *Let*

- q *be a prime power,*
- $F/\mathbb{F}_q$ *be an algebraic function field,*
- Q *be a place of* $F/\mathbb{F}_q$*, of degree* $n = \deg Q$
- ℓ *be a positive integer*
- $\mathcal{D}_1, \mathcal{D}_2$ *be two divisors of* $F/\mathbb{F}_q$*,*
- $\mathscr{P} = \{P_1, \ldots, P_N\}$ *be a set of places of arbitrary degree* $d_i = \deg P_i$*,*
- $u_1, \ldots, u_N$ *be positive integers.*

We suppose that Q *and all the places in* $\mathscr{P}$ *are not in the support of* $\mathcal{D}_1$ *and* $\mathcal{D}_2$*, and that:*

(a) the maps

$$\varphi_{\mathcal{D}_1,Q,\ell} : \mathcal{L}(\mathcal{D}_1) \longrightarrow (\mathbb{F}_{q^n})^\ell$$

and

$$\varphi_{\mathcal{D}_2,Q,\ell} : \mathcal{L}(\mathcal{D}_2) \longrightarrow (\mathbb{F}_{q^n})^\ell$$

are onto,

(b) the map

$$Ev_{\mathscr{P},\underline{u}} : \left| \begin{array}{ccc} \mathcal{L}(\mathcal{D}_1+\mathcal{D}_2) & \longrightarrow & \left(\mathbb{F}_{q^{d_1}}\right)^{u_1} \times \left(\mathbb{F}_{q^{d_2}}\right)^{u_2} \times \cdots \times \left(\mathbb{F}_{q^{\deg d_N}}\right)^{u_N} \\ f & \longmapsto & \big(\varphi_1(f), \varphi_2(f), \ldots, \varphi_N(f)\big) \end{array} \right.$$

is injective,

where the applications $\varphi_{\mathcal{D}_1,P,\ell}$*,* $\varphi_{\mathcal{D}_2,P,\ell}$*, and* $\varphi_i = \varphi_{\mathcal{D}_1+\mathcal{D}_2,P_i,u_i}$ *are the derived evaluation maps from* (5)*. Then*

$$\mu_q(n,\ell) \leq \sum_{i=1}^{N} \mu_q(d_i, u_i).$$

Moreover, if $\mathcal{D}_1 = \mathcal{D}_2$*, the same holds for the symmetric bilinear complexity:*

$$\mu_q^{\mathrm{sym}}(n,\ell) \leq \sum_{i=1}^{N} \mu_q^{\mathrm{sym}}(d_i, u_i).$$

Existence of the objects satisfying the conditions above is ensured by the following numerical criteria:

- *a sufficient condition for the existence of* Q *of degree* n *is that* $2g+1 \leq q^{(n-1)/2}(q^{1/2}-1)$*, where* g *is the genus of* F
- *a sufficient condition for (a) is that the divisors* $\mathcal{D}_1 - \ell Q$ *and* $\mathcal{D}_2 - \ell Q$ *are nonspecial:*
  $$i(\mathcal{D}_1 - \ell Q) = i(\mathcal{D}_2 - \ell Q) = 0$$
  where i *denotes index of speciality*
- *a necessary and sufficient condition for (b) is that the divisor* $\mathcal{D}_1 + \mathcal{D}_2 - \mathcal{G}$ *is zero-dimensional:*
  $$\dim \mathcal{L}(\mathcal{D}_1 + \mathcal{D}_2 - \mathcal{G}) = 0$$
  where $\mathcal{G} = u_1 P_1 + \cdots + u_N P_N$*.*

The fact that $\mu_q(n,\ell)$ (resp. $\mu_q^{\mathrm{sym}}(n,\ell)$) appears on the left-hand side of the inequalities allows to apply the result recursively. For $n=1$ it also provides bounds for the quantity $\widehat{M}_q(\ell)$ of M. Cenk and F. Özbudak (resp. for $\widehat{M}_q^{\mathrm{sym}}(\ell)$).

However in most applications we are interested mostly in the case $\ell=1$. If we restate the result in this particular case, and focus only on the symmetric part, this generalized version of CCMA algorithm then specializes to the following statement (special case of [72, Theorem 3.5]), which suffices for most applications:

Corollary 5.4. *Let*

- q *be a prime power,*
- $F/\mathbb{F}_q$ *be an algebraic function field,*
- Q *be a place of* $F/\mathbb{F}_q$*, of degree* $n=\deg Q$ *and residue field* $F_Q\simeq\mathbb{F}_{q^n}$
- $\mathcal{D}$ *be a divisor of* $F/\mathbb{F}_q$*,*
- $\mathscr{P}=\{P_1,\dots,P_N\}$ *be a set of places of arbitrary degree* $d_i=\deg P_i$*,*
- $u_1,\dots,u_N$ *be positive integers.*

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

(a) the evaluation map

$$\varphi_{\mathcal{D},Q}:\left|\begin{array}{ccc}\mathcal{L}(\mathcal{D}) & \longrightarrow & \mathbb{F}_{q^n}\\ f & \mapsto & f(Q)\end{array}\right.$$

is onto

(b) the map

$$Ev_{\mathscr{P},\underline{u}}:\left|\begin{array}{ccc}\mathcal{L}(2\mathcal{D}) & \longrightarrow & \left(\mathbb{F}_{q^{d_1}}\right)^{u_1}\times\left(\mathbb{F}_{q^{d_2}}\right)^{u_2}\times\cdots\times\left(\mathbb{F}_{q^{\deg d_N}}\right)^{u_N}\\ f & \longmapsto & \big(\varphi_1(f),\varphi_2(f),\dots,\varphi_N(f)\big)\end{array}\right.$$

is injective, where $\varphi_i=\varphi_{2\mathcal{D},P_i,u_i}$ *is the derived evaluation map from* (5)*.*

Then

$$\mu_q^{\mathrm{sym}}(n)\le\sum_{i=1}^{N}\mu_q^{\mathrm{sym}}(d_i,u_i).$$

This can be specialized still further. Indeed, first observe that for all d,u we have the easy inequality

$$\mu_q^{\mathrm{sym}}(d,u)\le\mu_q^{\mathrm{sym}}(d)\widehat{M}_{q^d}^{\mathrm{sym}}(u). \tag{6}$$

This follows directly from Lemma 1.6(b) applied with $\mathcal{A}=\mathbb{F}_{q^d}[t]/(t^u)$, $L=\mathbb{F}_{q^d}$, $K=\mathbb{F}_q$. We deduce:

Corollary 5.5. *Under the same hypotheses as Corollary 5.4, we have*

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

Corollary 5.5 can be seen as a symmetric variant of M. Cenk and F. Özbudak's version of the CCMA [40]. It is weaker than Corollary 5.4, since the inequality $\mu_q^{\mathrm{sym}}(d,u)\le\mu_q^{\mathrm{sym}}(d)\widehat{M}_{q^d}^{\mathrm{sym}}(u)$ can be strict.

One should be careful that all bilinear complexities in the original statement of [40] (including the one for multiplicities) have to be replaced by symmetric bilinear complexities in order to get this valid symmetric reformulation.

Going further back in time, let us then remark that the algorithm given in [44] by D.V. and G.V. Chudnovsky corresponds to the case $d_i = 1$ and $u_i = 1$ for $i = 1, \ldots, N$. The first generalization introduced by S. Ballet and R. Rolland in [25] concerns the case $d_i = 1$ or 2 and $u_i = 1$ for $i = 1, \ldots, N$. Next, the generalization introduced by N. Arnaud in [1] concerns the case $d_i = 1$ or 2 and $u_i = 1$ or 2 for $i = 1, \ldots, N$. In particular, as a corollary of Theorem 5.3, we have the following result obtained by N. Arnaud in [1] by gathering the places used with the same multiplicity; namely he sets $\ell_j := |\{P_i \mid \deg P_i = j \text{ and } u_i = 2\}|$ for $j = 1$ and 2 and with $\mathcal{D} = \mathcal{D}_1 = \mathcal{D}_2$.

Corollary 5.6. *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* $F/\mathbb{F}_q$*,*
- $\mathscr{P} = \{P_1, \ldots, P_{N_1}, P_{N_1+1}, \ldots, P_{N_1+N_2}\}$ *be a set of* N_1 *places of degree one and* N_2 *places of degree two,*
- $0 \leq \ell_1 \leq N_1$ *and* $0 \leq \ell_2 \leq N_2$ *be two integers.*

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

(a) the map

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

is onto,

(b) the map

$$Ev_{\mathscr{P}} : \left| \begin{array}{ccl} \mathcal{L}(2\mathcal{D}) & \to & \mathbb{F}_q^{N_1} \times \mathbb{F}_q^{\ell_1} \times \mathbb{F}_{q^2}^{N_2} \times \mathbb{F}_{q^2}^{\ell_2} \\ f & \mapsto & \big(f(P_1), \ldots, f(P_{N_1}), f'(P_1), \ldots, f'(P_{\ell_1}), \\ & & \quad f(P_{N_1+1}), \ldots, f(P_{N_1+N_2}), f'(P_{N_1+1}), \ldots, f'(P_{N_1+\ell_2})\big) \end{array} \right.$$

is injective.

Then

$$\mu_q^{\mathrm{sym}}(n) \leq N_1 + 2\ell_1 + 3N_2 + 6\ell_2.$$

I

6. Choice of the curves

6.1. **Motivation and notations.** As seen in Section 3 and 5, until now, the best method to quantify the bilinear complexity of multiplication in finite fields is the CCMA algorithm based upon the interpolation over algebraic curves defined over a finite field. So in this context, to get the best bounds on the upper-limit complexities M_q and M_q^{sym} or the upper bounds C_q and C_q^{sym} defined in Section 3.2, it is necessary to use sufficiently many different curves so as to deal with the worst cases. So let us give a name to the following requirement, formalized in [78, Claim p163]:

Definition 6.1. *Let* X_s/k *be a family of curves over a field* k *with genera* g_s*. We say that the family* $(X_s)_s$ *is dense if and only if the genera* g_s *tend to infinity and the ratio of two successive genera* g_{s+1}/g_s *tends to 1.*

As introduced in the last section, multiplication algorithms by interpolation on algebraic curves often require many points of higher degree $r \geq 2$. So let us study the best possible asymptotic ratios β_r of the number of places of degree r divided by

the genus. The first definition is due to M. Tsfasman [81] (cf. also [27, definitions 1.1, 1.2 and 1.3]).

Definition 6.2. *Let $\mathcal{X}/\mathbb{F}_q = (X_s/\mathbb{F}_q)$ be a sequence of curves $X_s/\mathbb{F}_q$ defined over a finite field $\mathbb{F}_q$ of genus $g_s = g(X_s/\mathbb{F}_q)$. We suppose that the sequence of the genus g_s is an increasing sequence growing to infinity. Then the sequence $\mathcal{X}/\mathbb{F}_q$ is said to be asymptotically exact if for all $m \geq 1$ the limit $\beta_r(\mathcal{X}) = \lim_{s\to\infty} \frac{B_r(X_s)}{g_s}$, where $B_r(X_s)$ denotes the number of closed points of degree r of the curve X_s, exists.*

Definition 6.3. *Let $r \geq 1$ be an integer and q a prime power. For X a curve over $\mathbb{F}_q$, let $B_r(X)$ denote the number of closed points of degree r. For an asymptotically exact sequence of curves $\mathcal{X} = (X_s)$, let us define*

$$\beta_r(\mathcal{X}) = \lim_{s\to\infty} \frac{B_r(X_s)}{g_s}.$$

Then, we respectively define :

$$A_r(q)(\textit{resp. } A'_r(q)) = \limsup_{\mathcal{X}} \beta_r(\mathcal{X}),$$

$\mathcal{X}$ running over all asymptotically exact sequences of curves (resp. dense asymptotically exact sequences of curves).

Remark 6.4. *Note that the quantity $A_1(q)$ is the classical Ihara Constant $A(q)$ defined by Y. Ihara in* [61]. *The order r Ihara constants $A_r(q)$ were in particular defined in* [27, definitions 1.3]. *Concerning the quantities $A'_r(q)$, note that the dense Ihara constant $A'_1(q)$ was first introduced (and noted $A'(q)$) by H. Randriambololona in* [71] *(cf. also* [75]*). The order r dense Ihara constants $A'_r(q)$ were first introduced (and noted $\widetilde{A}_r(q)$) by M. Rambaud in* [69].

The following is possibly well-known. It essentially follows from [39, Lemma IV.3], itself based on the generalized bound of Drinfeld-Vladuts (cf. [81, Theorem 1], see also [27, Definitions 1.2 and 1.3]).

Theorem 6.5. *Let $(X_s/\mathbb{F}_q)$ be a family of curves over a finite field $\mathbb{F}_q$, with genera g_s tending to infinity. Let $r \geq 1$ be an integer, $B_r(X_s)$ the number of closed points of degree r and $\mid X_s(\mathbb{F}_{q^r}) \mid$ the number of points of X_s in the extension $\mathbb{F}_{q^r}$. Then the following assertions are equivalent :*

(i) $$\lim_{s\to\infty} \frac{|X_s(\mathbb{F}_{q^r})|}{g_s} = \sqrt{q^r} - 1,$$

(ii) $$\lim_{s\to\infty} \frac{B_r(X_s)}{g_s} = \frac{\sqrt{q^r} - 1}{r}.$$

As a corollary of Theorem 1 in [81], the following holds:

Theorem 6.6.

$$A'_r(q) \leq A_r(q) \leq \frac{\sqrt{q^r} - 1}{r}. \tag{7}$$

6.2. **Explicit towers, densification and descent.** The pioneer papers [44] [78] having for objectives to prove the linearity (cf. Section 3.2) of this complexity with respect to the extension degree, required the use of infinite families of curves with many rational points relatively to the genus. However, the first exhibited families of curves (of type modular and Shimura) enable them to obtain uniquely

purely asymptotic bounds. So, the objective of [5] (cf. also [6] and footnote 1 page 9) was to give the first uniform upper bounds with respect to q. In this aim, it was necessary to use more explicit families of curves. The first tower of algebraic function fields of Garcia-Stichtenoth [57] fulfilled the required conditions: knowledge of fundamental invariants, namely the genus and the number of rational points of each step of the tower, which attains the Drinfeld-Vladut bound. From a general point of view, to obtain the best bounds by CCMA, we need to use families of curves of genus increasing the more slowly possible (cf. Section 5.1 and Theorem 9.5 in Section 9.2). But, a tower of algebraic function fields is composed of successive algebraic function fields whose genera increase as the extension degree between two consecutive steps by the Hurwitz formula. For example, the first Garcia-Stichtenoth tower defined over $\mathbb{F}_{q^2}$ is an Artin-Schreier tower whose ratio of two consecutive genus is $\frac{g_{i+1}}{g_i} \geq q$ where q is an arbitrary prime power. In this case, an interesting strategy to improve the bounds obtained with this type of tower consisted on densifying this tower by adding intermediate steps (cf. [7]). It is easily possible in this case, even without knowing the recursive equation of intermediate steps because the tower is a Galois tower. When the used towers $\mathcal{X}/\mathbb{F}_q$ are such that the value of $\beta_1(\mathcal{X})$ is not sufficiently large (which is the case when the finite fields of definition are small or when the best known lower bound of the Ihara constant $A_r(q)$ associated to the definition field $\mathbb{F}_q$ is not sufficiently large), it is necessary to use places of degree > 1 because of the Drinfeld-Vladut bound (cf. [25], [20]). So, we need families of curves reaching the Drinfeld-Vladut Bound of order $r > 1$ (cf. [26] and Assertion (ii) in Theorem 6.5). Until now, the only way to obtain such families is the technic of the descent of families of algebraic function fields defined over $\mathbb{F}_{q^r}$ on the definition field $\mathbb{F}_q$, which was introduced in [25]. Of course, the descent of the original tower of Garcia-Stichtenoth is always possible since the coefficients of the recursive equation lie in $\mathbb{F}_q$. However, the problem arises as soon as we introduce intermediate steps. So, in [25], the descent was made explicit only for the characteristic two and $r = 2$ because in this case the descended tower conserves the property to be Galois. Then, the generalization for any characteristic with $r = 2$ was realized in [19] by using two different techniques: theoretically by using the action of the Galois group of $\mathbb{F}_{q^2}/\mathbb{F}_q$ on the intermediate steps of the tower defined on $\mathbb{F}_{q^2}$ or by finding explicit equations of the intermediate steps. Then, having used all the possibilities of the towers, it became necessary to use families of algebraic function fields more dense than the towers. In this aim, it was natural to come back to the study of families of modular and Shimura curves, which is the subject of the following section.

6.3. **Modular and Shimura curves.** The previous section motivates the search for dense families of curves becoming optimal after a base field extension of (small) degree r.

Firstly, the towers of Garcia-Stichtenoth [57][58] being actually defined over their prime field $\mathbb{F}_p$, then for any base extension degree r, there exists *non-dense* towers reaching the previous bound (see next section):

$$A_r(q) = \frac{\sqrt{q^r} - 1}{r} \text{ as long as } q^r \text{ is a square.} \tag{8}$$

Now, in the particular case of *quadratic extensions* $r = 2$, the celebrated results of [61] and [83] (cf. also [78]) state that (see also the two original approaches of [49, Theorem IV.4.5]), for all prime power q, there exists *dense* families of *Shimura modular curves* over $\mathbb{F}_q$ that become optimal over $\mathbb{F}_{q^2}$. See also [85] for an introduction (in characteristic zero). Notice that classical modular curves over prime fields $\mathbb{F}_p$ are a particular case of Shimura curves. Summing up, the Shimura curves mentionned above match the bound of Drinfeld-Vladuts over $\mathbb{F}_{q^2}$, which reads:

$$A'_1(q^2) = q - 1. \tag{9}$$

Plus, taking into consideration that these curves are defined over $\mathbb{F}_q$, Theorem 6.5 implies :

$$A'_2(q) = \frac{q-1}{2}. \tag{10}$$

6.3.1. *Intertwinning two recursive towers into a dense family.* A recursive construction to obtain a dense family of curves consists in *intertwinning two towers of modular curves defined over the same basis*. Let us illustrate this with the classical modular curves $X_0(N)$. Let l be a prime number, then we know from Igusa that there exists —canonical— models $X_0(l^i)_{\mathbb{Q}}$ over $\mathbb{Q}$ for any $i \geq 0$, which have good reduction at any $p \neq l$, and are asymptotically optimal over $\mathbb{F}_{p^2}$. The curves $X_0(l^i)_{\mathbb{Q}}$ form a tower over $\mathbb{Q}$ that is recursively determined from the two first steps (actually the first step is enough, see historical notes and references below). More precisely, the tower is deduced by iterated fiber products from the two following data:

- the canonical morphisms over $\mathbb{Q}$
$$X_0(l^2) \to X_0(l) \to X_0(1)$$
- the Atkin-Lehner involutions w_i on $X_0(l^i)_{\mathbb{Q}}$ for $i = 0, 1, 2$

Remark 6.7. *Actually the first step are enough to deduce the whole tower recursively (see historical notes and references below). Namely, one needs only the covering map $X_0(l) \to X_0(1)$ and the Atkin-Lehner involutions w_i, for $i = 0, 1$. Caution must be taken since the fiber product of the first step $X_0(l)$ with its Atkin-Lehner twist —in addition to be highly singular— contains a second irreducible component in addition to $X_0(l^2)$. This comes from degree reasons,* [69, VI §2.3 & §3.2] *(or modular interpretation reasons, if one prefers).*

The genera in a single tower $X_0(l^i)_{\mathbb{F}_p}$ for any p are tightly controled by the prime powers l^i:

$$l^i(1 + 1/l)/12 + o(g_i) \leq g_i \leq l^i(1 + 1/l)/12 \tag{11}$$

(see [82, 4.1] or [48, Th 3.1.1 & p107]). So this single tower does not form a dense family.

Now let $l' \neq l$ be another prime and consider the recursive tower $X_0(l'^j)_{\mathbb{Q}}$. Both towers are defined over the same basis $X_0(1)$, and, by taking fiber products over $X_0(1)$, we obtain:

$$X_0(l^i)_{\mathbb{Q}} \times X_0(l'^j)_{\mathbb{Q}} = X_0(l^i l'^j)_{\mathbb{Q}}$$

for any i and j. By doing so for every indexes i and j we obtain the family $\left\{X_0(l^i l'^j)_{\mathbb{Q}}\right\}_{i,j}$: let us call this family the "intertwinning" of the two recursive

towers. This family has good reduction at any prime $p \neq l, l'$ and is asymptotically optimal. The genera in this family are now closely controled by the prime products $l^i l'^j$, as follows from

$$l^i l'^j (1+1/l)(1+1/l')/12 + o(g_{i,j}) \leq g_{i,j} \leq l^i l'^j (1+1/l)(1+1/l')/12 \; . \tag{12}$$

The key observation is that the family of integers $l^i l'^j$ is *dense*, i.e. its growth rate tends to zero. So that the intertwinned family $\left\{X_0(l^i l'^j)_{\mathbb{Q}}\right\}_{i,j}$ is dense.

6.3.2. *Problems of descent on Shimura curves and open questions.* Let us shift to Shimura curves and consider three specific recursive towers $X_0(\mathfrak{p}^i)$ defined over the same basis $X_0(1)$ of genus zero. Let $F = \mathbb{Q}[cos(2\pi/7)]$ be the totally real number field of degree three, $\mathfrak{p}_2$ and $\mathfrak{p}_3$ the prime ideals over the inert primes (2) and (3) and $\mathfrak{p}_7$ the prime ideal over the split prime (7). Let B be the quaternion algebra over F, which is ramified exactly at two of the three real places and no finite place. B contains one unique conjugacy class of Eichler orders of given level. In particular, "the" maximal order $\mathcal{O}$ has its group of units $\mathcal{O}^1$ which embeds into $\mathrm{PSL}_2(\mathbb{R})$ onto the celebrated $(2,3,7)$ triangle group (it is the hyperbolic group of smallest covolume). The Shimura curve $X_0(1)_{\mathbb{C}}$ uniformized by this group has a canonical model over F of genus zero with three rational points, which precisely arise from the elliptic points, of orders 2, 3 and 7. Above this base curve one has notably the three towers $X_0(\mathfrak{p}^i)$ where $\mathfrak{p} = \mathfrak{p}_2, \mathfrak{p}_3$ and $\mathfrak{p}_7$, which have canonical models over F. They have good reduction at every prime $\mathfrak{p}'$ of F different from $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_7$ and, if furthermore $\mathfrak{p}' = (p)$ comes from an inert prime, then the reductions $X_0(\mathfrak{p}^i)_{\mathbb{F}_{p^3}}$ modulo $\mathfrak{p}$ have an *asymptotically optimal* number of points over $\mathbb{F}_{p^6}$ (see [49, Th IV.4.5], which is established from two independent methods).

Now, intertwinning the two towers $X_0(\mathfrak{p}_2^i)$ and $X_0(\mathfrak{p}_7^j)$ over $X_0(1)$ gives a dense family $\left\{X_0(\mathfrak{p}_2^i \mathfrak{p}_7^j)_F\right\}_{i,j}$ over F, with genera tightly controled by the products $8^i.7^j$:

$$g_{i,j} = 7^{j-2}(8^{i-1}6/7 + 1/7) \text{ for } i \geq 1 \text{ and } j \geq 2 \tag{13}$$

(and similar formulas for smaller i or j: see [69, IV Corollary 2.12]). In particular it has good reduction modulo $p_3 = (3)$ and yields an asymptotically optimal dense family $X_0(\mathfrak{p}_2^i \mathfrak{p}_7^j)_{\mathbb{F}_{3^3}}$ over $\mathbb{F}_{3^3}$ with many points in $\mathbb{F}_{3^6}$. Now, the interesting problem for bilinear multiplication over $\mathbb{F}_3$ is: *can we descend this family over* $\mathbb{F}_3$ *?* Much of the work towards this result has been done, since it is proven in [69, VI §5.2] that the two first steps of the reductions modulo $\mathfrak{p}' = p_3$ of the two towers descend over $\mathbb{F}_3$. But recall that, over F, these two first steps are sufficient to build the whole family. So, the problem of descent of the family over $\mathbb{F}_3$ falls back to the following general question:

Open problems 6.8.

Conjecture 6.8.1. *Are good reductions of towers of Shimura curves recursive ?*

We are confident that this point falls back to the modular interpretation of *integral models* of Shimura curves —and not only models over number fields, such as F—, which should be also well known to specialists.

Additional evidence supports the descent question that we are concerned with, since it is also established in [69, Th. V.5.14] that the family $\left\{X_0(\mathfrak{p}_2^i \mathfrak{p}_7^j)_F\right\}_{i,j}$ descends over $\mathbb{Q}$, and that strong numerical evidence (the number of points) suggests that the third steps also descend ([69, VI §5.2]).

Recapitulating: descent of the previous family, as would be implied e.g. by Conjecture 6.8.1, would provide a dense family over $\mathbb{F}_3$ with many points of degree 6, which would thus establish:

$$A'_6(3) = \frac{3^3 - 1}{6} \tag{14}$$

which is (prematurely) claimed as "Theorem B" in [69].

Likewise, intertwinning the two towers $X_0(\mathfrak{p}_3^i)$ and $X_0(\mathfrak{p}_7^j)$ over $X_0(1)$ gives a dense family $\left\{X_0(\mathfrak{p}_3^i\mathfrak{p}_7^j)_F\right\}_{i,j}$ over F, with genera tightly controled by the products $27^i.7^j$, good reduction modulo $p_2 = (2)$ over $\mathbb{F}_{2^3}$ and asymptotically many points in $\mathbb{F}_{2^6}$.

Open problems 6.9. Similarly, we are concerned with descent of this dense family over $\mathbb{F}_2$, which if true would thus yield the value $A'_6(2) = \frac{2^3-1}{6}$. Let us assume that the previous Conjecture 6.8.1 is true: then this would already imply that the tower $X_0(\mathfrak{p}_7^j)$ descends over $\mathbb{F}_2$. So, we would then be left to show that the two first steps of the tower $X_0(\mathfrak{p}_3^i)$ also descend. More precisely:

Conjecture 6.9.1. *The following morphisms descend over $\mathbb{F}_2$: the canonical branched cover $X_0(\mathfrak{p}_3^2)_{\mathbb{F}_{2^3}} \longrightarrow X_0(\mathfrak{p}_3)_{\mathbb{F}_{2^3}}$, and the Atkin Lehner involution on $X_0(\mathfrak{p}_3^2)_{\mathbb{F}_{2^3}}$.*

Finally, notice that the first step of this tower $X_0(\mathfrak{p}_3)_{\mathbb{Q}} \longrightarrow X_0(1)_{\mathbb{Q}}$ was explicitly computed over $\mathbb{Q}$ in [54]: a Belyi map of degree 27. So, if it was true that good reduction of towers of Shimura curves were also recursive from the first step (see Remark 6.7), then one would be left with the easier problem of finding a good reduction modulo (3) of this Belyi map of degree 27.

Open problems 6.10. From a more general point of view, the so far known families of curves attaining the Drinfeld Vladuts bound over q are all defined over fields of square cardinal $q = p^(2t)$. The following conjecture states (under an equivalent form) that for all square q, there exists such a dense optimal family over $\mathbb{F}_q$ which descend over the prime field $\mathbb{F}_p$.

Conjecture 6.10.1. *Let p be a prime number and $2t \geq 4$ an even integer. Then the following equality holds:*

$$A'_r(q) = \frac{p^t - 1}{2t}. \tag{15}$$

Said otherwise: there exists a family $(X_s/\mathbb{F}_{p^{2t}})_{s\geq 1}$ of curves over $\mathbb{F}_p$ with (increasing) genera g_s tending to infinity such that

(i) X_s is, actually, defined over the prime field $\mathbb{F}_p$;
(ii) $\lim_{s\to\infty} \frac{g_{s+1}}{g_s} = 1$ (maximal density condition)
(iii) $\lim_{s\to\infty} \frac{|X_s(\mathbb{F}_{p^{2t}})|}{g_s} = p^t - 1$ (Ihara constant over $\mathbb{F}_{p^{2t}}$)

Open problems 6.11. The following conjecture was proposed in [70], to which we added a density requirement.

Conjecture 6.11.1. *Let $p > 2$ be an odd prime. Then there exists a sequence of numbers $(N_s)_s$, with $\lim_{s\to\infty} \frac{N_{s+1}}{N_s} = 1$ (density condition), such that Hecke operator $T_p(N_s)$ acting on the space of weight 2 cusp forms $S_2(\Gamma_0(N_s))$, has an odd determinant.*

Its consequence would be the asymptotic vanishing of two-torsion in classical modular curves:

Proposition 6.11.1. *Under Conjecture 6.11.1, then there exists a dense family of (classical modular) curves* $\{X_0(N_s)/\mathbb{F}_p\}_s$ *such that*

$$\big(\mathrm{Cl}_0(X_0(N_s))\big)(\mathbb{F}_{p^2})[2] = \{0\}$$

(i.e. that have no two torsion in their class group.)

This proposition is stated as Conjecture I 2.8 in [69]. Here, a detailed proof that it results from Conjecture 6.11.1 is given: in the discussion above Conjecture I 2.8 and, also, in §II.5 (for the key formula (2.6)). The following practical consequence will be proven in the Annex.

Proposition 6.11.2. *Let* p *be a prime number such that Conjecture 6.11.1 holds for* p*, and* r *an integer such that* $\big\{q = p \text{ and } r = 2\big\}$ *or* $\big\{q = p^2 \text{ and } r = 1\big\}$*, then formula (a) in Theorem 8.21 also holds.*

6.3.3. *References and historical notes for section 6.*

Recursive modular towers: The recursivity of towers of classical modular curves was pointed in the seminal paper of N. Elkies [51, pp 1-3], where more details and a proof over $\mathbb{C}$ can be found. The proof carries over the canonical models over $\mathbb{Q}$ since the moduli interpretation in terms of elliptic curves is the same. N. Elkies also claims –and uses– that towers of Shimura curves are recursive. The proof of this fact is formally analogous: see [49, Proposition IV.5.1]. But actually, extra care must be taken with the irreducibility of the tensor products involved: [69, VI §2.3 & §3.2], because the moduli interpretation is much more complicated. *Intertwinning two towers* over the same basis: this construction is already mentionned in [51, top of page 7]. The crucial observation that the resulting family is dense was pointed to us by N. Elkies in August 2015.

Recursivity from the first step: The fact that the first step of modular towers is actually enough to construct them recursively is already pointed in [51, footnote 4] and [53, p8], and brought to our attention by N. Elkies in 2017.

About conjecture 6.10.1: this conjecture was essentially stated as a Lemma IV.4 in [39] . For their proof, the authors claim that some specific Shimura curves, with Galois invariant parameters, descend over the rationals. This claim is unfortunately false: in [23, §3] we exhibited counterexamples to this claim, which evidence more generally that Shimura curves do not descend over their field of moduli. Consequences of Conjecture 6.10.1 on upper-limit asymptotic complexities are given M. Rambaud in [69, Table 2.2], lines "Conj Y". Notice that they improve a bit those claimed by [39], displayed in footnote 11 page 36.

More on explicit computations: Since the seminal works of [83] and [61] on Shimura curves with many points, many equations of curves of genus zero and one were computed in [52], [59] and [79]. Further examples of recursive towers of Shimura curves can be found in: [49, IV Example 5.3]; [60]; [69, VI §3] (defined over a totally real field of narrow class number two, with a record number of points over F_{5^4} in genus 5). The (nonexplicit) list of Shimura curves of genus less than two can be found in [86]. From this data and the recent tools for Belyi maps developped in [64], one could access the dozen of recursive towers whose first step are covering map of $\mathbb{P}^1$ of degree ≤ 9 ramified above three points. Finally, when the first step is

over a *genus one* curve, then a first example was computed in C. Levrat's masters thesis [63].

7. Obtaining a divisor of optimal degree for symmetric algorithms

Using the numerical criteria at the end of Theorem 5.3, in the symmetric case $\mathcal{D}_1 = \mathcal{D}_2$, we meet the following problem: given

- q a prime power
- $F/\mathbb{F}_q$ a function field, of genus g
- $\mathcal{Q}$ a divisor of $F/\mathbb{F}_q$, of degree $n = \deg \mathcal{Q}$
- $\mathcal{G}$ a divisor of $F/\mathbb{F}_q$, of degree $N = \deg \mathcal{G}$

does there exist a divisor $\mathcal{D}$ such that the two conditions

$$i(\mathcal{D} - \mathcal{Q}) = 0 \tag{16}$$

and

$$\dim \mathcal{L}(2\mathcal{D} - \mathcal{G}) = 0 \tag{17}$$

are both satisfied?

Clearly the answer will depend on n and N. By Riemann-Roch's theorem, condition (16) implies $\deg \mathcal{D} - n \geq g - 1$ and condition (17) implies $2 \deg \mathcal{D} - N \leq g - 1$, so combining both we see

$$N \geq 2n + g - 1 \tag{18}$$

is a necessary condition for the existence of a solution.

Observe that, in order to get the algorithm of best complexity for given n, we need N to be as small as possible.

In their original paper [44], D.V. Chudnovsky and G.V. Chudnovsky introduced a simple cardinality and degree argument, later made more explicit by S. Ballet in [6], which proved the existence of a solution under the less optimal condition

$$N \geq 2n + 2g - 1. \tag{19}$$

As explained in section 3.2, Shparlinski-Tsfasman-Vladut tried to improve the original bound of Chudnovsky-Chudnovsky by proving the existence of $\mathcal{D}$ under the optimal condition (18), instead of (19). For this they had to adapt the cardinality argument, but they failed to notice the consequence of the existence of 2-torsion in the class group when dealing with (17).

In order to repair their proof, two approaches were devised:

- choose curves with 2-torsion as small as possible
- directly construct $\mathcal{D}$ under condition (18).

7.1. Bounding the 2-torsion.

Bounds on torsion in the class group were first introduced in a very similar context, that of frameproof codes (also called linear intersecting codes), by C. Xing [89]. Indeed, in order to obtain a s-frameproof code of high rate, one needs, given a divisor $\mathcal{G}$, to prove the existence of a divisor $\mathcal{D}$ of high degree such that

$$\dim \mathcal{L}(s\mathcal{D} - \mathcal{G}) = 0. \tag{20}$$

C. Xing proved the existence of such a $\mathcal{D}$ using a cardinality argument similar to that of Chudnovsky-Chudnovsky and Shparlinski-Tsfasman-Vladut, while correctly recognizing the difficulty with s-torsion. His result on the rate of s-frameproof codes thus includes a term accounting for the size of the s-torsion subgroup. Actually, C.

Xing used the well known upper bound s^{2g} for the size of the s-torsion subgroup in the Jacobian of curve of genus g.

It is natural to ask for better bounds, especially in the asymptotic case $g \to \infty$. This problem was formalized and studied, independently,

- by H. Randriambolona, through the quantity $\delta_s^-(q)$ in [70]
- by I. Cascudo, R. Cramer and C. Xing, through the torsion-limit $J_r(q,a)$ in [37][38].

One of the questions asked by H. Randriambolona in [70] is the following: for given q and s, can one find an infinite sequence of curves having many rational points (ideally, matching the Ihara constant $A(q)$), but whose class group has few s-torsion?

How asymptotically small this s-torsion can be is measured by the following quantity:

Definition 7.1. *Let $\delta_s^-(q)$ be the smallest real number such that there exists a sequence $(\mathcal{X}_k)_{k\geq 1}$ of curves over $\mathbb{F}_q$, of increasing genus $g_k = g(\mathcal{X}_k)$, having an asymptotically number of rational points:*

$$\lim_{k\to\infty} \frac{|\mathcal{X}_k(\mathbb{F}_q)|}{g_k} = A(q)$$

and such that the cardinal of the s-torsion subgroup $\mathcal{J}_k(\mathbb{F}_q)[s]$ of the group of rational points over $\mathbb{F}_q$ of the Jacobian $\mathcal{J}_k = \mathcal{J}(\mathcal{X}_k)$ satisfies

$$\lim_{k\to\infty} \frac{\log_s |\mathcal{J}_k(\mathbb{F}_q)[s]|}{g_k} = \delta_s^-(q).$$

Open problems 7.2. Estimation of the quantity $\delta_s^-(q)$ for an infinite sequence of curves attaining the Drinfeld-Vladut bound. H. Randriambololona conjectures that $\delta_s^-(q) = 0$ for all s and q, i.e. that there exists curves that have an asymptotically maximal number of points over $\mathbb{F}_q$ and whose class groups have asymptotically negligible s-torsion. Of special importance for us is the case $s = 2$, i.e. the case of 2-torsion. In [70] H. Randriambololona puts focus on classical modular curves, which have an asymptotically maximal number of points over $\mathbb{F}_{p^2}$ (for p prime). The size of the class group of such a curve is given by the determinant of a Hecke operator. This leads to deep number theoretic questions on the parity of these determinants, which remain conjectural at this time.

In [38], I. Cascudo, R. Cramer and C. Xing generalize conditions like (16)(17) or like (20) into what they name Riemann-Roch systems of equations. They adapt the cardinality argument of [44][78][89] in this more general framework. First, for a function field $F/\mathbb{F}_q$, let $\mathcal{J}_F$ be its zero divisor class group. Let then $\mathcal{J}_F[r]$ be its r-torsion subgroup, of cardinality $J_F[r] =\mid \mathcal{J}_F[r] \mid$. Their main result (see [38, Theorem 3.2]) is as follows :

Proposition 7.3. *Let:*

- *q be a prime power*
- *$F/\mathbb{F}_q$ be a function field*
- *h be the class number of F*
- *A_m the number of effective divisors of degree m in the group of divisors $Div(F)$ for $m > 0$*

- $u \geq 1$ *be an integer*
- $\mathcal{Y}_1, \ldots, \mathcal{Y}_u$ *be divisors of* F
- $m_1, \ldots, m_u$ *be nonzero integers.*

Suppose that for some integer $s \in \mathbb{Z}$*, the inequality*

$$h > \sum_{i=1}^{u} A_{r_i(s)} J_F[m_i]$$

holds, where $r_i(s) = m_i s + \deg \mathcal{Y}_i$*. Then the system of conditions*

$$\dim \mathcal{L}(m_1\mathcal{D} + \mathcal{Y}_1) = \cdots = \dim \mathcal{L}(m_u\mathcal{D} + \mathcal{Y}_u) = 0$$

is satisfied by some divisor $\mathcal{D}$ *of degree* s*.*

In order to measure the size of the torsion subgroups, they introduce the notion of torsion-limit:

Definition 7.4. *For each family* $\mathcal{F} = \{F/\mathbb{F}_q\}$ *of function fields with increasing genus* $g(F)$*, we define the asymptotic limit*

$$J_r(\mathcal{F}) = \liminf_{F \in \mathcal{F}} \frac{\log_q J_F[r]}{g(F)}.$$

For a prime power q*, an integer* $r > 1$ *and a real number* $a \leq A(q)$*, let* Υ *be a set of families* $\{\mathcal{F}\}$ *of function fields over* $\mathbb{F}_q$ *such that the genus in each family tends to* ∞ *and the Ihara limit satisfies* $A(\mathcal{F}) \geq a$ *for every* $\mathcal{F} \in \Upsilon$*. Then the asymptotic quantity* $J_r(q, a)$ *is defined by*

$$J_r(q, a) = \liminf_{\mathcal{F} \in \Upsilon} J_r(\mathcal{F}).$$

Thanks to the equivalence between curves and function fields, where the group of rational points of the Jacobian corresponds to the zero divisor class group, we see that this torsion-limit is related to the constant $\delta_r^-(q)$ by the relation:

$$J_r(q, A(q)) = \log_q(r)\delta_r^-(q). \tag{21}$$

This torsion-limit can be introduced as a correcting term in the denominator of the bound claimed by Shparlinski, Tsfasman, and Vladut, as we will see in Section 8.2.

However, another approach is possible namely the direct construction.

7.2. **Direct construction.** The direct construction consists on finding the best divisors D to apply CCMA, i.e divisors D satisfying Conditions (16) and (17) for given q and n. The idea is explicitly introduced by S. Ballet in [9, Theorem 2.2] as we will see more precisely in Section 9.2. Then J. Chaumine proved in [42] (cf. also [43]) that the direct construction is optimal in the elliptic case, improving then the result of A. Shokrollahi [77] as we will see in Section 9.1. Then, H. Randriambolona introduces news ideas which originate in his work [73] for the construction of intersecting codes. The technique was then extended in [71] in order to solve more general Riemann-Roch systems of equations. In the case of the Riemann-Roch system associated with a CCMA, it allows the effective construction of a solution, in most cases up to optimal degree.

The key point is the following result [73, Lemma 9], which can be seen as a numerical variant of a generalized Plücker formula:

Lemma 7.5. *Let X be a curve of genus g over a perfect field K, and let $\mathcal{A}$ be a divisor on X with $\deg \mathcal{A} \leq g-3$ and*

$$\dim \mathcal{L}(\mathcal{A}) = 0.$$

Then for all points $P \in X(K)$ except perhaps for at most $4g$ of them, we have

$$\dim \mathcal{L}(\mathcal{A} + 2P) = 0.$$

In [71] it is shown how the bound $4g$ can be slightly improved when K is a finite field. However the original Lemma 7.5 suffices to prove the following result [71, Corollary 20]:

Proposition 7.6. *Let:*

- *q be a prime power*
- *$F/\mathbb{F}_q$ be a function field, of genus g*
- *$\mathcal{Q}$ be a divisor of $F/\mathbb{F}_q$, of degree $n = \deg \mathcal{Q}$*
- *$\mathcal{G}$ be a divisor of $F/\mathbb{F}_q$, of degree $N = \deg \mathcal{G}$.*

Assume that the number of degree 1 places of F satisfies

$$N_1(F/\mathbb{F}_q) > 5g.$$

Then, provided

$$N \geq 2n + g - 1$$

there exists a divisor $\mathcal{D}$ of $F/\mathbb{F}_q$ such that $\mathcal{D} - \mathcal{Q}$ is nonspecial of degree $g-1$ and $2\mathcal{D} - \mathcal{G}$ is zero-dimensional:

- $\deg \mathcal{D} = n + g - 1$
- $\dim \mathcal{L}(\mathcal{D} - \mathcal{Q}) = 0$
- $\dim \mathcal{L}(2\mathcal{D} - \mathcal{G}) = 0$.

Observe that for a divisor of degree $g-1$, nonspecial and zero-dimensional are equivalent, so here $i(\mathcal{D} - \mathcal{Q}) = 0$ and $\dim \mathcal{L}(\mathcal{D} - \mathcal{Q}) = 0$ are equivalent.

Observe also that Proposition 7.6 gives precisely what was required in the approach of Shparlinski, Tsfasman and Vladut, as described in section 3.2, with $N = 2n + g - 1$, $\mathcal{Q} = Q$, and $\mathcal{G} = P_1 + \cdots + P_N$. The only downside is the condition that F should have sufficiently many rational places.

Beside [71], the proof of this Proposition 7.6 can also be found inside the proof of [72, Theorem 5.2(c)].

8. Asymptotic upper bounds

The asymptotic study of the bilinear complexity of the multiplication consists on evaluating the quantities m_q, M_q, m_q^{sym}, M_q^{sym}. The importance of this study comes from the fact that generally we have better estimations of these quantities than those of the constants C_q and C_q^{sym}. Indeed, the best known families of curves suitable to the application of the D. V. and G. V. Chudnovsky algorithm are known asymptotically, in particular the families of Shimura curves used by I. Shparlinski, M. Tsfasman and S. Vladut in [78]. These latter establish the following general result which we can see as a direct consequence of Lemma 1.7 (or of [78, Lemma 1.2])[4].

[4]Their main motivation to introduce this lemma was, from the finiteness of M_q for q square, to deduce finiteness of M_q for all q.

Lemma 8.1. *For any prime power q and any positive integer n we have*

$$m_q \leq m_{q^n} \cdot \mu_q(n)/n \tag{22}$$

$$M_q \leq M_{q^n} \cdot \mu_q(n). \tag{23}$$

Actually, inequality (22) about m_q is already implicit in the original paper of D. V. Chudnovsky and G. V. Chudnovsky (from [44, eq. (6.2)]). So, here, the important new contribution of I. Shparlinski, M. Tsfasman and S. Vladut is inequality (23) about M_q. Note that these inequalities are also true in the symmetric case, as a consequence of Lemma 1.8:

Lemma 8.2.

$$m_q^{\mathrm{sym}} \leq m_{q^n}^{\mathrm{sym}} \cdot \mu_q^{\mathrm{sym}}(n)/n \tag{24}$$

$$M_q^{\mathrm{sym}} \leq M_{q^n}^{\mathrm{sym}} \cdot \mu_q^{\mathrm{sym}}(n). \tag{25}$$

By using Theorem 2.2 with Lemma 8.1 or Lemma 8.2, we trivially get the following useful corollary:

Corollary 8.3. *For every prime power q, we have $m_q \leq \frac{3}{2} m_{q^2}$, $m_q^{\mathrm{sym}} \leq \frac{3}{2} m_{q^2}^{\mathrm{sym}}$, $M_q \leq 3M_{q^2}$, and $M_q^{\mathrm{sym}} \leq 3M_{q^2}^{\mathrm{sym}}$. If $q \geq 4$, then $m_q \leq \frac{5}{3} m_{q^3}$, $m_q^{\mathrm{sym}} \leq \frac{5}{3} m_{q^3}^{\mathrm{sym}}$, $M_q \leq 5M_{q^3}$, and $M_q^{\mathrm{sym}} \leq 5M_{q^3}^{\mathrm{sym}}$.*

Let us recall that $A(q)$ denotes the Ihara limit defined by $A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g}$ where $N_q(g)$ is the maximum number of rational places over all the algebraic function fields over $\mathbb{F}_q$ of genus g (cf. also Definition 7.1).

8.1. **Upper bounds on m_q and M_q.** Thanks to the asymmetric interpolation allowed by the generalized CCMA (cf. Section 5.3), H. Randriambololona [72, Theorem 6.3 and Theorem 6.4] obtains bounds for m_q and M_q. For m_q, the bound reads:

Theorem 8.4. *Let q be a prime power such that $A(q) > 1$. Then*

$$m_q \leq 2\left(1 + \frac{1}{A(q) - 1}\right). \tag{26}$$

For M_q, it reads:

Theorem 8.5. *Let $q = p^{2r} \geq 9$ be a square prime power. Then*

$$M_q \leq 2\left(1 + \frac{1}{\sqrt{q} - 2}\right). \tag{27}$$

Combined with Lemma 8.1 and $\mu_q(2) = 3$, this implies at once:

Corollary 8.6. *Let $q \geq 3$ be a prime or a nonsquare prime power. Then*

$$m_q \leq 3\left(1 + \frac{1}{q - 2}\right) \tag{28}$$

and

$$M_q \leq 6\left(1 + \frac{1}{q - 2}\right). \tag{29}$$

Moreover, from Theorem 9.18, J. Pieltant and H. Randriambololona deduce the following asymptotic bounds in the general case:

Theorem 8.7.

$$M_3 \leq 6 \quad M_4 \leq \tfrac{87}{19} \simeq 4.579 \quad M_5 \leq 4.5 \quad M_{11} \leq 3.6 \quad M_{13} \leq 3.5.$$

These bounds are the best published current asymptotic bounds in the general case. They are deduced from the best known uniform bounds. Indeed, the purely asymptotic bounds[5] given in Theorem 5.3, Corollary 5.4, Corollary 5.5 of [67] are unproved as established in [23]. In addition, as corollary of uniform bounds in Theorem 9.19 (cf. Section 9.3), H. Randriambololona obtains recently the following result:

Theorem 8.8. *For $p \geq 7$, we have:*

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

Finally, in [69] M. Rambaud obtains the current best general upper-limit asymptotic bound, namely:

Theorem 8.9. *Let q a prime power and $r \geq 1$, $l \geq 1$ be two positive integers. Then, as long as $rlA'_r(q) - 1 > 0$, we have:*

$$M_q \leq \frac{2\mu_q(r,l)}{rl}\left(1 + \frac{1}{rlA'_r(q) - 1}\right).$$

In particular, this result enables to obtain the following value (with $(r,l) = (4,1)$, $\mu_q(r,l) \leq \mu_q^{\mathrm{sym}}(r,l) = 9$ by Table 1 and $A'_r(2) = \frac{3}{4}$ by Formula (7):

Corollary 8.10.

$$M_2 \leq 7.$$

8.2. **Upper bounds on m_q^{sym} and M_q^{sym}.** Initially, by using the original Chudnovsky and Chudnovsky, I. Shparlinski, M. Tsfasman and S. Vladut [78] obtain upper bounds[6] of M_q^{sym} and m_q^{sym} for any q, which are not completely proved

[5]These unproven bounds are:

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

for q be a prime power and $t \geq 1$ an integer such that $q^t \geq 9$ is a square;
and

$$M_2 \leq \frac{35}{6}, \qquad M_3 \leq \frac{36}{7}, \qquad M_4 \leq \frac{30}{7}, \qquad M_5 \leq 4, \qquad M_7 \leq 3.6, \qquad M_8 \leq 3.5.$$

[6]These are following bounds:

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

where $A(q) > 1$ is defined in Proposition 8.14,

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

where q is a perfect square ≥ 9,

$$m_q^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{c\log_2 q - 1}\right),$$

where $q \geq 2^{1/c}$ with c is a positive constant,

$$m_q^{\mathrm{sym}} \leq 2\left(1 + \frac{q^{1/3} + 2}{2q^{2/3} - q^{1/3} - 4}\right),$$

because of the gap mentioned in Section 3.2. H. Randriambololona in [72, Theorem 6.3 and Theorem 6.4] obtains the following results which prove the bounds of Shparlinsky-Tsfasman-Vladut with a slight restriction on the range of the values for $A(q)$ and q. For m_q^{sym}, the bound reads:

Theorem 8.11. *Let q be a prime power such that $A(q) > 5$. Then*

$$m_q^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{A(q) - 1}\right). \tag{30}$$

For M_q^{sym}, it reads:

Theorem 8.12. *Let $q = p^{2r} \geq 49$ be a square prime power. Then*

$$M_q^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{\sqrt{q} - 2}\right). \tag{31}$$

Combined with Lemma 8.2 and $\mu_q^{\mathrm{sym}}(2) = 3$, this implies at once:

Corollary 8.13. *Leq $q \geq 7$ be a prime or a nonsquare prime power. Then*

$$m_q^{\mathrm{sym}} \leq 3\left(1 + \frac{1}{q - 2}\right) \tag{32}$$

and

$$M_q^{\mathrm{sym}} \leq 6\left(1 + \frac{1}{q - 2}\right). \tag{33}$$

In [17], S. Ballet, J. Chaumine and J. Pieltant obtain bounds slightly less accurate than the bounds of the above results but for a slightly larger range of values for $A(q)$ and q. They give the following propositions.

Proposition 8.14. *Let q be a prime power such that $A(q) > 2$. Then*

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

$$m_2^{\mathrm{sym}} \leq \frac{35}{6},$$

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

where $q > 2$,

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

where $q \geq 9$ is a perfect square,

$$M_q^{\mathrm{sym}} \leq 6\left(1 + \frac{1}{q - 2}\right),$$

where $q > 2$, and

$$M_2^{\mathrm{sym}} \leq 27$$

given respectively in [78, Theorem 3.1], [78, Corollary 3.4], [78, Corollary 3.5], [78, Remark 3.6], [78, Corollary 3.7], [78, Corollary 3.8], [78, Theorem 3.9] and [78, Corollary 3.10] for the last two bounds. Note that these bounds are originally formulated with notation m_q and M_q, but for the same reasons that those mentioned in footnote 2 of Section 3.2, these bounds concern the quantities M_q^{sym} and m_q^{sym}. Note that there exist proved bounds exceeding the last bound (cf. Proposition 8.23).

Corollary 8.15. *Let $q = p^{2m}$ be a square prime power such that $q \geq 16$. Then*

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

Note that this corollary slightly improves the range of the bound (4) proved by D.V. and G.V. Chudnovsky. Now in the case of arbitrary q, they obtain:

Corollary 8.16. *For any $q = p^m > 3$,*

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

Moreover, for M_q^{sym} they obtain the same value for the same range than that of m_q^{sym}:

Proposition 8.17. *Let $q = p^{2m}$ be a square prime power such that $q \geq 16$. Then*

$$M_q^{\mathrm{sym}} \leq 2\left(1 + \frac{1}{\sqrt{q} - 3}\right). \tag{34}$$

Proposition 8.18. *Let $q = p^m$ be a prime power with odd m such that $q \geq 5$. Then*

$$M_q^{\mathrm{sym}} \leq 3\left(1 + \frac{2}{q - 3}\right). \tag{35}$$

Remark 8.19. *For q square, Bound (34) is better that Bound (35) except for $q = 16$.*

When q is a prime number, the uniform bounds of Proposition 9.14 obtained in [28, Proposition 10] by S. Ballet and A. Zykin lead to the asymptotic symmetric complexity given in the following proposition:

Proposition 8.20. *Let $p \geq 5$ be a prime number. Then*

$$M_p^{\mathrm{sym}} \leq 3\left(1 + \frac{\frac{4}{3}}{p - 3}\right). \tag{36}$$

The following theorem due to M. Rambaud in [69] generalizes essentially all the known formulas providing the current best symmetric upper-limit asymptotic bounds.

Theorem 8.21. *Let q a prime power and $r \geq 1$, $l \geq 1$ be two positive integers. Then, as long as the respective denominators are positive, we have:*

(a) if $r = 1$ and q is such that $A_1'(q) > 5$

$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1 + \frac{1}{rlA_r'(q) - 1}\right).$$

(b)

$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1 + \frac{2}{rlA_r'(q) - 2}\right).$$

(c) if $2|q$

$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1 + \frac{1 + \log_q(2)}{rlA_r'(q) - 1 - \log_q(2)}\right).$$

(d) if $2 \nmid q$

$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1+\frac{1+2\log_q(2)}{rlA'_r(q)-1-2\log_q(2)}\right).$$

Remark 8.22. *In comparison to the other known results :*

- *Bound (a) encompasses the upper-limit bounds of 8.4 8.6, where it adds multiplicities of evaluation. This additional tool was introduced in* [1] *and improved by* [40]*, then by* [72, Lemma 3.4]*;*
- *Bound (b) allows evaluation on points of arbitrary degree compared to* [17, Proposition 11]*;*
- *Bounds (c) and (d) allow evaluation on points of odd degree r in* [38, Theorem 5.18]*, and adds multiplicities of evaluation. Also, instead of using the formula $A'_r(q) = (\sqrt{q^r}-1)/r$ in loc. cit., which is unproven in the general case, they are replaced here by $A'_r(q)$. Notice that* bounds (b) and (c) give stricly better numerical values than Proposition 8.18 for all values of q *for which Proposition 8.18 holds*[7]*. Indeed, it suffices to use $r = 2$ (and $l = 1$), and to use the known value (10) of $A'_2(q)$ in Section 6.*

The following bounds are deduced from theorem 8.21, except for $q = 25$. We indicate the criterions (a) (b), etc. from which they are deduced, and the parameters (r, l) used. The values $A'_r(q)$ are directly taken from the known values given in Section 6.3.

We detail how the upper bounds of the $\mu_q^{\mathrm{sym}}(r,l)$ are infered, because many where not directly published. Because of their interest, these bounds will be summarized in Section 9.2. To obtain these upper bounds we often use Formula (58) in [72, Lemma 3.2] given by Inequality (6) in Section 5.4:

$$\mu_q^{\mathrm{sym}}(r,l) \leq \mu_{q^r}^{\mathrm{sym}}(1,l)\mu_q^{\mathrm{sym}}(r) \tag{37}$$

in particular

$$\mu_q^{\mathrm{sym}}(2,2) \leq \mu_{q^2}^{\mathrm{sym}}(1,2)\mu_q^{\mathrm{sym}}(2) \leq 3 \times 3 = 9$$

(where the last two values are actually both equal to 3, as shown by S. Winograd.

The biggest emphasis must be put on the following upper bound:

$$\mu_q^{\mathrm{sym}}(2,5) \leq 30$$

which is deduced from formula (37) and from the upper bound:

$$\mu_4^{\mathrm{sym}}(1,5) \leq 10 \tag{38}$$

which was only published in [68, Table 2], in the justification of entry (1,10). It is regrettable that this record bound was not more emphasized in [68]: this has been repaired in [69, Appendix §2.3], where an explicit formula attaining this bound is given. Even more regrettable, the entry for (1,10) in the loc cit [68, Table 1 & Table 2] is grossly false. One should not read $\mu_q^{\mathrm{sym}}(1,10) \leq 30$ but instead $\mu_q^{\mathrm{sym}}(2,5) \leq 30$, as deduced from formula (37) above. This was corrected in [69, Table 3.1]. The error in [68, Table 1 & Table 2] comes from a grossly wrong application of formula (37).

Let us determine the values of the quantities $\mu_q^{\mathrm{sym}}(r,l)$ and $\mu_q(r,l)$ required in order to obtain Proposition 8.23. All these values will be summarized in Sections 9.2 and 9.3.

[7]Proposition 8.18 is let for the simplicity of its expression.

For $q = 2$: from (b) with $(r, l) = (2, 5)$ with $\mu_q^{\mathrm{sym}}(2, 5) \leq 30$ as emphasized above.
For $q = 3$: (b) $(r, l) = (2, 3)$ with

$$\mu_3(2, 3) \leq \mu_9^{\mathrm{sym}}(1, 3)\mu_3^{\mathrm{sym}}(2, 1) \leq \mu_3^{\mathrm{sym}}(1, 3)\mu_3^{\mathrm{sym}}(2, 1) \leq 5 \times 3 = 15$$

where the latter, 3, is from Karatsuba and the former, 5, from [41, Table 1 col. (2.4)] (note that 5 is actually *equal* to the asymmetric complexity, by [29, Table 3]).

For $q = 4$: (c) $(r, l) = (2, 2)$ with $\mu_4(2, 2) \leq 8$ from [72, (88)] (which, as a side remark, we even claim to be an equality, as follows from an unpublished exhaustive search performed while working on [68, §1]).
For $q = 5$: (d) $(r, l) = (2, 2)$ with $\mu_5(2, 2) \leq 8$ ([72, (88)]).
For $q = 7$: (d) $(r, l) = (2, 1)$[8].
For $q = 8$: (c) $(r, l) = (2, 1)$.
For $q = 9$: (d) $(r, l) = (2, 1)$.
For $q = 11$: (d) $(r, l) = (2, 1)$.
For $q = 25$ apply Proposition 8.17 obtained in [17, Proposition 2]. [9].

Proposition 8.23.

$$M_2^{\mathrm{sym}} \leq 10,$$
$$M_3^{\mathrm{sym}} \leq 7.5,$$
$$M_4^{\mathrm{sym}} \leq 5.33,$$
$$M_5^{\mathrm{sym}} \leq 5.21,$$
$$M_7^{\mathrm{sym}} \leq 4.08,$$
$$M_8^{\mathrm{sym}} \leq 3.71,$$
$$M_9^{\mathrm{sym}} \leq 3.77,$$
$$M_{11}^{\mathrm{sym}} \leq 3.56,$$
$$M_{25}^{\mathrm{sym}} \leq 3.$$

These previous asymptotic bounds are the best published current numerical ones in the symmetric case[10].

Now, if equation (14) did hold: $A_6'(3) = \frac{3^3-1}{6} = 13/3$, as would be implied e.g. by Conjecture 6.8.1, then applying criterion (b) to (6,1), using $\mu_3^{\mathrm{sym}}(6, 1) \leq 15$ from [40, table 1], would yield $M_3^{\mathrm{sym}} \leq \dfrac{65}{12} \simeq 5.41$. And likewise for the couple of other bounds mentionned in [69, Table 2.2] on the two lines named "Adding theorem B". Similarly, conjectures 6.9.1, 6.10.1 and 6.11.1 would imply the bounds on the corresponding lines of [69, Table 2.2].

Then, using the general quantities linked to the 2-torsion (cf. Section 7.1), I. Cascudo, R. Cramer, and C. Xing in[38, Theorem 6.27] (cf. also [37]) obtain the following general result:

---

[8]Let us recall that $\mu_q(2, 1) = \mu_q(2) = 3$.

[9]Notice that the authors did not apply themselves their bound to $q = 25$, because it gives a higher value than the one from [38]: they did not know at the time that this latter bound was not actually proved. Note also that this bound is obtained by using the criterium 1) in 9.5 with $a = 0$, obtained in [6, Theorem 1.1].

[10]These bounds improve the following bounds: $M_2^{\mathrm{sym}} \leq \frac{1035}{68} \simeq 15.23$ and $M_3^{\mathrm{sym}} \leq \frac{1933}{250} \simeq 7.74$, obtained for $q = 2$ and for $q = 3$ in [22, Theorem 4.9] (cf. also [21, Theorem 4.9]) and for $q = 4$ in [23, Theorem 1.6 (i)]: $M_4^{\mathrm{sym}} \leq \frac{237}{39} \simeq 6.08$, which already improved the old following results : $M_2^{\mathrm{sym}} \leq \frac{477}{26} \simeq 18.35$ obtained in [20, Theorem 4.1] and the old result $M_3^{\mathrm{sym}} \leq 27$ obtained from [8, Remark of Corollary 3.1].

Theorem 8.24. *Let $\mathbb{F}_q$ be a finite field. If there exists a real number $a \leq A(q)$ with $a \geq 1 + J_2(q, a)$, then*

$$m_q^{sym} \leq 2\left(1 + \frac{1}{a - J_2(q,a) - 1}\right).$$

In particular, if $A(q) \geq 1 - J_2(a, A(q))$, then

$$m_q^{sym} \leq 2\left(1 + \frac{1}{A(q) - J_2(q, A(q)) - 1}\right).$$

Actually, Cascudo, Cramer and Xing stated their result in terms of m_q, not of m_q^{sym}(cf. footnote 2 Section 3.2). Here we stated it in terms of m_q^{sym} because, as already explained, the 2-torsion really enters the play only when we restrict to symmetric algorithms.

In order to be useful, this result should be combined with upper bounds on the torsion-limit. Some upper-bounds of this sort can be easily deduced from Weil's classical results on the torsion in Abelian varieties. However, Cascudo, Cramer and Xing obtain a spectacular improvement using the Deuring-Shafarevich theorem. This allows them to give an upper-bound on the 2-torsion-limit of certain explicit towers (such as the Garcia-Stichtenoth tower), as well as the following general result [38, Theorem 2.3(iii)]:

Theorem 8.25. *Let $q = p^{2t}$ be an even power of a prime p. Then we have*

$$J_p(q, \sqrt{q} - 1) \leq \frac{1}{(\sqrt{q} + 1)\log_p(q)}.$$

Despite this important progress, at this time this approach does not allow to obtain the claimed bounds by Shparlinski-Tsfasman-Vladut bound for symmetric complexity. Indeed, for this, one has to show that the 2-torsion-limit is 0, or equivalently, that $\delta_2^-(q) = 0$ which is the open problem 7.2.

Note that all the upper bounds on M_q^{sym} obtained by I. Cascudo et al in [39] and [38] are unproved because the proofs are based on [39, Lemma IV] which is not completely correct as it is shown in [23, Section 3] (cf. also [69]). However, the bounds are correct under Conjecture 6.10.1 [11].

[11] The following results rely on the above unproven assumption: Theorem IV.6, Theorem IV.7 and the list of specific bounds in Corollary IV.8 of [39]. Also, Theorem 5.18 and the list of bounds in Corollary 5.19 of [37]. More precisely, here is the unproved bounds:

- the symmetric bounds in Theorem IV.6, Theorem IV.7 and the list of specific bounds in Corollary IV.8 of [39]; namely the following:

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

  for any $t \geq 1$ as long as $q^t - 5 > 0$ for q a prime power;

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

  for any $t \geq 1$ as long as $q^{t/2} - 5 > 0$ for q a prime power which is a square.

q	2	3	4	5	7	8	9	11	13
M_q^{sym}	7.47	5.49	4.98	4.8	3.82	3.74	3.68	3.62	3.59

- also, the symmetric bounds in Theorem V.18 and the list of bounds in Corollary V.19 of [38], namely:

q	n	$\mu_q^{\mathrm{sym}}(n)$	$\mu_q(n)$
2	4	9	9
2	6	15	15

TABLE 1. Exact bilinear complexities

9. Uniform bounds

9.1. **Some exact values for $\mu_q^{\mathrm{sym}}(n)$.** Recall that by Theorem 2.2, we have $\mu_q^{\mathrm{sym}}(n) = \mu_q(n) = 2n-1$ if and only if $n \leq \frac{q}{2}+1$. Applying CCMA with well fitted elliptic curves, Shokrollahi in [77] (for the strict inequality) and Chaumine in [43] have shown that:

Theorem 9.1. *If*

$$\frac{1}{2}q + 1 < n \leq \frac{1}{2}(q+1+\epsilon(q)) \tag{39}$$

where ϵ is the function defined by:

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

then the symmetric bilinear complexity $\mu_q^{\mathrm{sym}}(n)$ of the multiplication in the finite extension $\mathbb{F}_{q^n}$ of the finite field $\mathbb{F}_q$ is equal to $2n$. In particular, in this case, we have:

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

Open problems 9.2. We still do not know if the converse is true. More precisely the question is: suppose that $\mu_q(n) = 2n$, are the inequalities (39) true?

Moreover, for the values of n not concerned by Theorems 2.2 and 9.1, very few particular exact values are known and are all obtained in [44]:

Remark 9.3. *The bilinear complexity $\mu_2(4) = 9$ is obtained in* [44, Example 3.2] *by a personal computer program. It is easy to check this value can be obtained by a symmetric tensor corresponding to the iteration of the Karatsuba algorithm. Then $\mu_2(4) = \mu_2^{\mathrm{sym}}(4) = 9$. The bilinear complexity $\mu_2(6) = 15$ is obtained in* [44, Example 3.3] *thanks to Inequality (1.7) of Lemma 8.1 and a lower bound over the length of binary codes of dimension 6 equal to the minimal distance.*

Open problems 9.4. Find exact values for $\mu_q^{\mathrm{sym}}(n)$ and $\mu_q(n)$. Find examples where $\mu_q(n) < \mu_q^{\mathrm{sym}}(n)$.

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

for a prime power q and 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.

q	2	3	4	5
M_q^{sym}	7.23	5.45	4.44	4.34

9.2. **Upper bounds for $\mu_q^{\mathrm{sym}}(n)$ and $\mu_q^{\mathrm{sym}}(l,r)$.** From the results of [6] and the algorithm of Corollary 5.6 with $\ell_1 = \ell_2 = 0$, we obtain (cf. [6], [25]):

Theorem 9.5. *Let q be a prime power and let n be an integer > 1. Let $F/\mathbb{F}_q$ be an algebraic function field of genus g and N_k a number of places of degree k in $F/\mathbb{F}_q$. If $F/\mathbb{F}_q$ is such that there exists a place of degree n(which is always the case if $2g+1 \leq q^{\frac{n-1}{2}}(q^{\frac{1}{2}}-1)$) then:*

1) if $N_1 + a > 2n + 2g - 2$ for some integer $a \geq 0$, then

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

2) if there exists a non-special divisor of degree $g-1$ (which is always the case if $q \geq 4$) and $N_1 + a_1 + 2(N_2 + a_2) > 2n + 2g - 2$ for some integers $a_1 \geq 0$ and $a_2 \geq 0$, then

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + 2g + \frac{a_1}{2} + 3a_2 - 1,$$

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

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

Remark 9.6. *The previous theorem enables to obtain general bounds on the bilinear complexity of the multiplication in $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ from infinite families of algebraic function fields defined over $\mathbb{F}_q$. But a fixed finite field $\mathbb{F}_q^n$, if we want to obtain the best possible bound, we can search the best algebraic function field defined over $\mathbb{F}_q$ (i.e with the possible smallest genus) satisfying the conditions of this theorem.*

Finally, from good towers of algebraic functions fields satisfying Theorem 9.5, different improvements of the bounds of the symmetric bilinear complexity were successively obtained in [6], [8], [25], [19], [9], [16], [1], [22], and [23]:

Theorem 9.7. *Let $q = p^r$ be a power of the prime p and let n be an integer > 1. Then the symmetric bilinear complexity of multiplication in any finite field $\mathbb{F}_{q^n}$ is linear with respect to the extension degree n; more precisely, there exists a constant C_q^{sym} such that for any $n > 1$:*

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

The best current values of the constants C_q^{sym} are :

$$C_q^{sym} = \begin{cases} \text{if } q = 2, & \text{then (1)} \quad 15.4575 \\ & \text{see [22, Corollary 29]} \\ \text{else if } q = 3, & \text{then (2)} \quad \dfrac{1933}{250} \simeq 7.732 \\ & \text{see [22]} \\ \text{else if } q = p \geq 7, & \text{then (3)} \quad 3\left(1 + \frac{8}{3p-5}\right) \\ & \text{see [23, Theorem 1.6 (ii)]} \\ \text{else if } q = p^2 \geq 25, & \text{then (4)} \quad 2\left(1 + \frac{2}{p-\frac{33}{16}}\right) \\ & \text{see [23, Theorem 1.7 (ii)]} \\ \text{else if } q = p^{2k} \geq 64 \quad (k \geq 2), & \text{then (5)} \quad 2\left(1 + \frac{p}{\sqrt{q}-3+(p-1)\frac{\sqrt{q}}{\sqrt{q}+1}}\right) \\ & \text{see [1] and [23, Theorem 1.7 (i)]} \\ \text{else if } q \geq 4, & \text{then (6)} \quad 3\left(1 + \frac{\frac{4}{3}p}{q-3+2(p-1)\frac{q}{q+1}}\right) \\ & \text{see [23, Theorem 1.6 (i)]} \end{cases}$$

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
$\mu_4^{\mathrm{sym}}(n) \leq$	3	6	8	11	14	17	20	23	27	30	33	37	39	45	45	53	51

TABLE 2. Best known bounds on complexities for small fields

Remark 9.8. *Note that, from Corollary 5.6 applied on a Garcia-Stichtenoth tower, N. Arnaud obtained in* [1] *which is not published the bound (5) of Theorem 9.7. In* [23]*, the authors give a detailed proof of Bound (5). In* [23]*, it is also proved the two revised bounds (3) and (4) for* $\mu_{p^2}(n)$ *and* $\mu_p(n)$[12].

Note also that the upper bounds[13] obtained successively in [11] and [10] are obtained by using the mistaken statements of I. Shparlinski, M. Tsfasman and S. Vladut [78] mentioned in the above section 3.2.

Moreover, for certain finite fields (in particular the cases of $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$), we have certain refined bounds for certain extensions obtained in [40, Table 1]. Let us recall this table:

Moreover, in [15, Tables 3 and 4], improving results obtained in [40] and [72, Example 4.7], bounds are given for certain particular extensions:

n	163	233	283	409	571
$\mu_2^{\mathrm{sym}}(n)$	906	1340	1668	2495	3566

n	57	97	150	200	400
$\mu_3^{\mathrm{sym}}(n)$	234	410	643	878	1879

The bounds presented in the previous tables are the best published current bounds for $\mu_q(n)$. For the quantity $\mu_q(r,l)$, with $l > 1$, different values have been

[12]In [1], N. Arnaud gives the two following bounds with no detailed calculation:

(3') If $p \geq 5$ is a prime, then $\mu_p^{\mathrm{sym}}(n) \leq 3\left(1 + \frac{4}{p-1}\right) n$.

(4') If $p \geq 5$ is a prime, then $\mu_{p^2}^{\mathrm{sym}}(n) \leq 2\left(1 + \frac{2}{p-2}\right) n$.

In fact, one can check that the denominators $p-1$ and $p-2$ are slightly overestimated under Arnaud's hypotheses.

[13]In [11] and [10], S. Ballet gives the unproved following bounds:

(1) If $q \geq 3$ is a prime power, then $\mu_{q^2}^{\mathrm{sym}}(n) \leq 2\left(1 + \frac{2}{q-2}\right) n$,

(2) If $q \geq 5$ is a prime power, then $\mu_q^{\mathrm{sym}}(n) \leq 6\left(1 + \frac{2}{q-2}\right) n$,

(3) If $q = p^r > 3$ is a prime power, then $\mu_q^{\mathrm{sym}}(n) \leq 3\left(1 + \frac{2}{p-2}\right) n$,

(4) If $p > 5$ is a prime, then $\mu_q^{\mathrm{sym}}(n) \leq 3\left(1 + \frac{2}{p-2}\right) n$.

given by M. Rambaud in [69] and explained in Section 8.2. Let us summarize for $q = 2$ these values (including the case l=1) in the following table 3.

$l\backslash r$	1	2	3	4
1	1	3	6	9
2	3	9	16	24
3	5	15	30	
4	8	21		
5	11	30		

$l\backslash r$	1	2	3	4
6	14			
7	18			
8	22			
9	27			
10	31			

TABLE 3. Upper bounds on the complexities $\mu_2^{\mathrm{sym}}(r, l)$.

For other values of q let us summarize the known results, obtained in Section 8.2.

$$\mu_q^{\mathrm{sym}}(2, 2) \leq 9,\ \mu_q^{\mathrm{sym}}(2, 5) \leq 30.$$

$$\mu_4^{\mathrm{sym}}(1, 5) \leq 10.$$

Recently in [28], S. Ballet and A. Zykin would improve all the known uniform upper bounds for $\mu_{p^2}^{\mathrm{sym}}(n)$ and $\mu_p^{\mathrm{sym}}(n)$ for a prime $p \geq 5$. Their approach consists on using dense families of modular curves which are not obtained asymptotically thanks to prime number density theorems of type Hoheisel, in particular a result due to Dudek [50]. Note that one of main ideas used in [28] was introduced in [11] by S. Ballet thanks to the use of the Chebyshev Theorem (or also called the Bertrand Postulat) to bound the gaps between prime numbers in order to construct families of modular curves as dense as possible. Later, motivated by [11], the approach of using such bounds on gaps between prime numbers (e.g. Baker-Harman-Pintz [4]) was also used by H. Randriambololona in the preprint [71] in order to improve the upper bounds of $\mu_{p^2}^{\mathrm{sym}}(n)$ where p is a prime number. In summary, let us give the new uniform bounds given there (and recalled in [75]).

In order to present these bounds, let us recall the following notation. For any infinite subset $\mathcal{A}$ of $\mathbb{N}$ and for any real $x > 0$, let

$$\lceil x \rceil_{\mathcal{A}} = \min \mathcal{A} \cap [x, +\infty[$$

be the smallest element of $\mathcal{A}$ larger than or equal to x. Also set:

$$\epsilon_{\mathcal{A}}(x) = \sup_{y \geq x} \frac{\lceil y \rceil_{\mathcal{A}} - y}{y}.$$

Now, we have:

Proposition 9.9. *Let $p \geq 7$ be a prime number. Then:*

(1) for all $k \geq \frac{p^2+p+1}{2}$,

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2\left(1 + \frac{1 + \epsilon_{\mathcal{P}}(\frac{24k}{p-2})}{p-2}\right).$$

(2) for all $k \geq 1$,

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2\left(1 + \frac{2}{p-2}\right).$$

(3) for all $k \geq 1$,

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2\left(1+\frac{1+\frac{10}{139}}{p-2}\right)$$

(4) for all $k \geq e^{50}p$,

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2\left(1+\frac{1.000000005}{p-2}\right)$$

(5) for all $k \geq 16531(p-2)$,

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2\left(1+\frac{1+\frac{1}{25\log^2(\frac{24k}{p-2})}}{p-2}\right)$$

(6) for k *large enough,*

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2\left(1+\frac{1+\frac{1}{(\frac{24k}{p-2})^{0.475}}}{p-2}\right).$$

Recently, combining his results of [71] with the result of A. Dudek [50] as in [28], H. Randriambolona improves in [75] almost all these bounds except for the case $q = p^2 = 25$ obtained in [28]. In summary, let us give the new uniform bound of the symmetric bilinear complexity given respectively in [75, Corollary 10] and [28, Proposition 7].

Proposition 9.10. *Let* $p \geq 7$ *be a prime number. Then:*

(7) for all $k \geq \frac{p-2}{24}e^{e^{33.217}}$,

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2\left(1+\frac{1+\frac{3}{(\frac{24k}{p-2})^{\frac{1}{3}}}}{p-2}\right).$$

Proposition 9.11. *Let* x_α *be the constant defined in* [28, Theorem 6] *(recalled in Theorem 9.12). For any integer* $n \geq x_\alpha + 3$ *we have*

$$\mu_{25}^{\mathrm{sym}}(n) \leq 2\left(1+\frac{1+n^{\alpha-1})}{2}\right)n - 3n^{\alpha-1} - 4.$$

Let us recall the following key result as direct consequence of the results of Baker, Harman, and Pintz [4] and A. Dudek [50] on which Assertion (vi) in Proposition 9.9, Proposition 9.10 as well as Proposition 9.11 are essentially based on.

Their results concern explicit prime number density theorems, usually called theorems of type Hoheisel. In particular, by a result of Baker, Harman and Pintz [4, Theorem 1] established in 2001 and by a recent result established by Dudek [50, Theorem 1.1] in 2016, we directly deduce the following result [28, Theorem 6]:

Theorem 9.12. *Let* l_k *be the* k*-th prime number. Then there exist real numbers* $\alpha < 1$ *and* x_α *such that the difference between two consecutive prime numbers* l_k *and* l_{k+1} *satisfies*

$$l_{k+1} - l_k \leq l_k^\alpha$$

for any prime $l_k \geq x_\alpha$*. In particular, one can take* $\alpha = \frac{2}{3}$ *with* $x_\alpha = \exp(\exp(33.217))$*. Moreover, one could take* $\alpha = \frac{21}{40}$ *with a value of* x_α *that could in principle be determined effectively.*

Open problems 9.13. A problem which is highly not trivial consists on determining effectively a value of x_α for $\alpha = \frac{21}{40}$. This problem is a typical problem of analytic number theory, said problem of type Hoheisel.

Then, the second result concerns the case of prime fields. The optimal method used by H. Randriambolona [75] for solving Riemann-Roch systems (cf. Section 7.1) does not work well for symmetric algorithms over prime fields. Instead, to prove [28, Proposition 10] Ballet and Zykin use a suboptimal method from [27] associated to descent technics (cf. Section 6.2) and obtain:

Proposition 9.14. *Let $p \geq 5$ be a prime number, let x_α be defined as in Theorem 9.12.*

(1) If $p \neq 11$, then for any integer $n \geq \frac{p-3}{2} x_\alpha + \frac{p+1}{2}$ we have

$$\mu_p^{\mathrm{sym}}(n) \leq 3\left(1 + \frac{\frac{4}{3}(1+\epsilon_p(n))}{p-3}\right) n - \frac{2(1+\epsilon_p(n))(p+1)}{p-3},$$

where $\epsilon_p(n) = \left(\frac{2n}{p-3}\right)^{\alpha-1}$.

(2) For $p = 11$ and $n \geq (p-3)x_\alpha + p - 1 = 8x_\alpha + 10$ we have

$$\mu_p^{\mathrm{sym}}(n) \leq 3\left(1 + \frac{\frac{4}{3}(1+\epsilon_p(n))}{p-3}\right) n - \frac{4(1+\epsilon_p(n))(p-1)}{p-3} + 1,$$

where $\epsilon_p(n) = \left(\frac{2n}{p-3}\right)^{\alpha-1}$.

9.3. **Upper bounds for $\mu_q(n)$ and $\mu_q(l,r)$.** By using the asymmetric part of Theorem 5.3, J. Pieltant and H. Randriambolololona obtained in [67] results about bilinear complexity not necessarily symmetric. In particular, they obtain the best bounds in the extensions of $\mathbb{F}_2$, $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ for all $p \geq 3$ and $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ for all $q \geq 4$.

Proposition 9.15. *Let q be a prime power and d be an positive integer for which all proper divisors verify $j < \frac{1}{2}(q+1+\epsilon(q))$ if $q \geq 4$, or $j \leq \frac{1}{2}q + 1$ if $q \in \{2,3\}$. Let $F/\mathbb{F}_q$ be an algebraic function field of genus $g \geq 2$ with N_i places of degree i and let ℓ_i be integers such that $0 \leq \ell_i \leq N_i$, for all $i|d$. Suppose that:*

(i) there exists a place of degree n in $F/\mathbb{F}_q$,

(ii) $\sum_{i|d} i(N_i + \ell_i) \geq 2n + g + \alpha_q$, where $\alpha_2 = 5, \alpha_3 = \alpha_4 = \alpha_5 = 2$ and $\alpha_q = -1$ for $q > 5$.

Then

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

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

By choosing $d = 1, 2$ or 4, they obtain the two following corollaries:

Corollary 9.16. *Let $q \geq 3$ be a prime power and $F/\mathbb{F}_q$ be an algebraic function field of genus $q \geq 2$ with N_i places of degree i. Let ℓ_i be integers such that $0 \leq \ell_i \leq N_i$. Suppose that:*

(i) there is a place of degree n in $F/\mathbb{F}_q$,

(ii) $N_1 + \ell_1 + 2(N_2 + \ell_2) \geq 2n + g + \alpha_q$, *where* $\alpha_3 = \alpha_4 = \alpha_5 = 2$ *and* $\alpha_q = -1$ *for* $q > 5$.

Then

$$\mu_3(n) \leq 3n + \frac{3}{2}g + \frac{3}{2}(\ell_1 + 2\ell_2) + \frac{9}{2},$$

$$\mu_q(n) \leq 3n + \frac{3}{2}g + \ell_1 + 2\ell_2 + \frac{9}{2}, \text{ for } q = 4 \text{ or } 5,$$

and for $q > 5$,

$$\mu_q(n) \leq 3n + \frac{3}{2}g + \frac{1}{2}(\ell_1 + 2\ell_2),$$

or in the particular case where $N_2 = \ell_2 = 0$

$$\mu_q(n) \leq 2n + g + \ell_1 - 1.$$

Corollary 9.17. *Let* $F/\mathbb{F}_2$ *be an algebraic function field of genus* $g \geq 2$ *with* N_i *places of degree* i *and let* ℓ_i *be integers such that* $0 \leq \ell_i \leq N_i$. *Suppose that:*

(i) there is a place of degree n *in* $F/\mathbb{F}_2$,

(ii) $\sum_{i|4} i(N_i + \ell_i) \geq 2n + g + 5$,

then

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

Then, they establish new asymmetrical uniform bounds:

Theorem 9.18. *For* $n \geq 2$,

(i) if $q = 2$, *then*

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

(ii) if $q = 3$, *then*

$$\mu_3(n) \leq 6n,$$

(iii) if $q = 4$, *then*

$$\mu_4(n) \leq \frac{87}{19}n,$$

(iv) if $q = 5$, *then*

$$\mu_5(n) \leq \frac{9}{2}n,$$

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

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

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

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

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

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

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

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

Recently, by using the same dense families of modular curves defined over $\mathbb{F}_p$ than the one used to get Theorem 9.9 in Section 9.2, H. Randriambololona obtains the following result.

Proposition 9.19. *Let $p \geq 7$ be a prime number. Then:*

(1) for all $k > \frac{p+1}{2}$,

$$\frac{1}{k}\mu_p(k) \leq 3\left(1 + \frac{1 + \epsilon_{\mathcal{P}}(\frac{24k}{p-2})}{p-2}\right),$$

(2) for all $k \geq \frac{p-2}{24}e^{e^{33.217}}$,

$$\frac{1}{k}\mu_p(k) \leq 3\left(1 + \frac{1 + \frac{3}{(\frac{24k}{p-2})^{\frac{1}{3}}}}{p-2}\right),$$

(3) for k large enough,

$$\frac{1}{k}\mu_p(k) \leq 3\left(1 + \frac{1 + \frac{1}{(\frac{24k}{p-2})^{0.475}}}{p-2}\right).$$

Remark 9.20. *Note that the difficulty of solving the Riemann-Roch systems (cf. 7.2) in the context of symmetric algorithms using curves having not sufficiently rational points is avoided here, since the previous result is obtained by using the asymmetric version of type Chudnovsky algorithm (cf. Section Section 5.3 and Section 5.4) applied over places of degree two.*

Now, let us recall some particular values of the quantities $\mu_q(l, r)$, obtained in Section 8.2:

$$\mu_3(2,3) \leq 15,\ \mu_4(2,2) \leq 8,\ \mu_5(2,2) \leq 8.$$

10. Effective construction of bilinear multiplication algorithms

In this section, we are interested by the study of the effective construction of bilinear multiplication algorithms in finite fields. Little few work has been done on the effective construction of the algorithms of type Chudnovky. They are mainly contained in the following articles: [30], [7], [40], [15], [2] and [3].

10.1. **Non-asymptotic construction.**

10.1.1. *Classical multiplication algorithms.*

a) Example of an effective symmetric construction using an elliptic curve.

This example developped by U. Baum and A. Shokrollahi in [30] is the first effective construction of an bilinear algorithm of multiplication which implements CCMA. It concerns a multiplication algorithm in the finite field $\mathbb{F}_{256}$ over $\mathbb{F}_4$, namely $q = 4$ and $n = 4$, using the maximal Fermat elliptic curve $y^2 + y = x^3 + 1$. The bilinear complexity $\mu^{\mathrm{sym}}(\mathcal{U})$of this symmetric algorithm $\mathcal{U}$ is optimal and such that

$$\mu^{\mathrm{sym}}(\mathcal{U}) = \mu_q^{\mathrm{sym}}(n) = \mu_q(n) = 2n = 8.$$

b) Example of effective symmetric constructions using an hyperelliptic curve.

This example developped by S. Ballet in [7] is the first effective construction of an bilinear algorithm of multiplication which implements CCMA for an algebraic curve of genus $g > 1$. It concerns a multiplication algorithm in the finite field $\mathbb{F}_{16^n}$ over $\mathbb{F}_{16}$, more precisely $q = 16$ and $n = 13, 14, 15$, using the maximal hyperelliptic curve $y^2 + y = x^5$. The bilinear complexity of this symmetric algorithm $\mathcal{U}$ is quasi-optimal and such that

$$\mu^{\mathrm{sym}}(\mathcal{U}) = 2n + 1,$$

which proves that $2n \leq \mu_q(n) \leq \mu_q^{\mathrm{sym}}(n) \leq 2n + 1$.

Open problems 10.1. Find the exact bilinear complexity in these finite fields $\mathbb{F}_{16^n}$ over $\mathbb{F}_{16}$ with $n = 13, 14, 15$, knowing that this complexity is $2n$ or $2n + 1$. Optimize the scalar complexity of these constructions.

c) Example of an effective symmetric construction using higher degree places and derivated evaluations on rational places on elliptic curves.

This example developped by M. Cenk and F. Özbudak in [40] is the first effective construction of an bilinear algorithm of multiplication which implements the combination of the generalizations of CCMA introduced in [25] using places of degree one and two and in [1] using derivated evaluations. Note that in this example, the derivated evaluations are only used on rational places at the order one. More precisely, it concerns a multiplication algorithm in the finite field $\mathbb{F}_{3^9}$ over $\mathbb{F}_3$ using the non-optimal elliptic curve $y^2 = x^3 + x + 2$. In this case, the authors use the evaluation on four rational places with derivated evaluation on two among them as well as the evaluation on six places of degree two. The bilinear complexity of this symmetric algorithm $\mathcal{U}$ is such that

$$\mu^{\mathrm{sym}}(\mathcal{U}) = 4 + 2 \times 2 + 6 \times 3 = 26.$$

d) Example of effective asymmetric construction using higher degree places on algebraic curves.

This example developped by S. Ballet, N. Baudru, A. Bonnecaze and M. Tukumuli in [12] (announced in [13]) and by Tukumuli in [84] is the first effective construction of bilinear algorithms of multiplication which implements the asymetric generalization of CCMA introduced in [72]. Note that these examples use two distinct Riemann-Roch spaces $\mathcal{L}(D_1)$ and $\mathcal{L}(D_2)$ without derivated evaluations. More precisely, in [12], three algorithms are constructed. The first example concerns a multiplication algorithm in the finite field $\mathbb{F}_{16^{13}}$ over $\mathbb{F}_{16}$ using the maximal hyperelliptic curve $y^2 + y = x^5$ and only rational places on it. The second example concerns a multiplication algorithm in the finite field $\mathbb{F}_{4^4}$ over $\mathbb{F}_4$ using the optimal curve $y^2 + y = \frac{x}{x^3+x+1}$ over $\mathbb{F}_4$. The third example concerns a multiplication algorithm in the finite field $\mathbb{F}_{2^5}$ over $\mathbb{F}_2$ using the optimal curve $y^2 + y = \frac{x}{x^3+x+1}$ over $\mathbb{F}_4$.

10.1.2. *Parallel algorithms designed for multiplication and exponentiation.* In [2] and [3], thanks to a new construction of CCMA, K. Atighechi, S. Ballet, A. Bonnecaze, and R. Rolland design efficient algorithms for both the exponentiation and the multiplication in finite fields. They are tailored to hardware implementation and they allow computations to be parallelized while maintaining a low number of bilinear multiplications. Notice that so far, practical implementations of multiplication algorithms over finite fields have failed to simultaneously optimize the number of scalar multiplications, additions and bilinear multiplications. Regarding exponentiation algorithms, the use of a normal basis is of interest because the q^{th} power of an element is just a cyclic shift of its coordinates. A remaining question is, how to implement multiplication efficiently in order to have simultaneously fast multiplication and fast exponentiation. In 2000, S. Gao et al. [56] show that fast multiplication methods can beadapted to normal bases constructed with Gauss periods. They show that if $\mathbb{F}_{q^n}$ is represented by a normal basis over $\mathbb{F}_q$ generated by a Gauss period of type (n, k), the multiplication in $\mathbb{F}_{q^n}$ can be computed with $\mathrm{O}\big(nk \log nk \log\log nk\big)$ and the exponentiation with $\mathrm{O}\big(n^2 k \log k \log\log nk\big)$ operations in $\mathbb{F}_q$ (q being small). This result is valuable when k is bounded. However, in the general case k is upper-bounded by $\mathrm{O}\big(n^3 \log^2 nq\big)$.

In 2009, J.-M. Couveignes and R. Lercier construct in [46, Theorem 4] two families of basis (called elliptic and normal elliptic) for finite field extensions from which they obtain a model Ξ defined as follows. To every couple (q, n), they associate a model, $\Xi(q, n)$, of the degree n extension of $\mathbb{F}_q$ such that the following holds: there is a positive constant K such that the following are true:

- Elements in $\mathbb{F}_{q^n}$ are represented by vectors for which the number of components in $\mathbb{F}_q$ is upper bounded by $Kn(\log n)^2 \log(\log n)^2$.
- There exists an algorithm that multiplies two elements at the expense of $Kn(\log n)^4 |\log(\log n)|^3$ multiplications in $\mathbb{F}_q$.
- Exponentiation by q consists in a circular shift of the coordinates.

Therefore, for each extension of finite field, they show that there exists a model which allows both fast multiplication and fast application of the Frobenius automorphism. Their model has the advantage of existing for all extensions. However, the bilinear complexity of their algorithm is not competitive compared with the best known methods, as pointed out in [46, Section 4.3.4]. Indeed, it is clear that such a model requires at least $Kn(\log n)^2(\log(\log n))^2$ bilinear multiplications.

The authors of [3] propose another model with the following characteristics:

- The model is based on CCMA, thus the multiplication algorithm has a bilinear complexity in $O(n)$, which is optimal.
- The model is tailored to parallel computation. Hence, the computation time used to perform a multiplication or any exponentiation can easily be reduced with an adequate number of processors. Since the method has a bilinear complexity of multiplication in $O(n)$, it can be parallelized to obtain a constant time complexity using $\mathrm{O}\big(n\big)$ processors. The previous aforementioned works ([56] and [46]) do not give any parallel algorithm (such an algorithm is more difficult to conceive than a serial one).
- Exponentiation by q is a circular shift of the coordinates and can be considered free. Thus, efficient parallelization can be done when doing exponentiation.

- The scalar complexity of their exponentiation algorithm is reduced, compare to a basic exponentiation using CCMA, thanks to a suitable basis representation of the Riemann-Roch space $\mathcal{L}(2D)$ in the second evaluation map. More precisely, the normal basis representation of the residue class field is carried in the associated Riemann-roch space $\mathcal{L}(D)$, and the exponentiation by q consists in a circular shift of the n first coordinates of the vectors lying in the Riemann-Roch space $\mathcal{L}(2D)$.

- The model uses Coppersmith-Winograd [45] method (denoted CW) or any variants thereof to improve matrix products and to diminish the number of scalar operations.

Open problems 10.2. The structure of the involved matrices in the algorithm CCMA should be looked at more closely but unfortunately, there are no theoretical means or criteria today to build the best matrices because they depend on the geometry of the curves, the field of definition of these curves, as well as the Riemann-Roch spaces involved. A study of suitable optimisation strategies of CCMA from this point of view can be found in [14]. In particular, the algorithm CCMA using an elliptic curve for multiplication in $\mathbb{F}_{256}/\mathbb{F}_4$ constructed by U. Baum and A. Shokrollahi [30] is improved. The remaining open question is how to choose the geometrical objects in order to minimise the number of zeroes in a matrix of the evaluation map on the rational points of a curve.

10.2. **Asymptotic construction.** D. V. and G.V. Chudnovsky claim in [44] that one can construct in polynomial time bilinear multiplication algorithm realizing a a bilinear complexity attaining the upper bound for m_q. Then, I. Shparlinsky, M. Tsfasman and S. Vladut in [78] note that the argument of D. V. and G.V. Chudnovsky is insufficient. Indeed, the construction of such algorithms involves some random choice of divisors having prescribed properties over an exponentially large set of divisors.

I. Shparlinsky, M. Tsfasman and S. Vladut obtain a partial result concerning this polynomial construction by the following way. Let $q = p^{2m} \geq 49$ and let $X_i = X_0(11l_i)$ be the reduction of the classical modular curve, l_i being the i-th prime (for $q = p^2$), or $X_i = X_0(p_i)$ where p_i is an irreducible polynomial over $\mathbb{F}_q$ of odd degree coprime with $q-1$ (for $q = p^{2m}$). Here, $X_0(p_i)$ is the reduction of the Drinfeld modular curve. Note that $\{X_i\}$ is a family of absolutely irreducible smooth curves of genus $g = g_i$ with $\lim_{g\to\infty} \frac{|X(\mathbb{F}_q)|}{g} = \sqrt{q} - 1$. Then, they prove the following result:

Proposition 10.3. *Suppose that for a family of modular curves described above for any $X \in \{X_i\}$ there is given an explicit point Q of X of some degree n such that*

$$g.\left(\sqrt{q}-5\right)/2 - o(g) \leq n \leq g.\left(\sqrt{q}-5\right)/2.$$

Let Q be defined by its coordinates in some projective embeddings. Then one can polynomially construct a sequence $\mathcal{U} = \mathcal{U}_i$ of bilinear multiplication algorithms in finite fields $\mathbb{F}_{q^n}$ for the given sequence of $n \to \infty$ such that

$$\lim_{g\to\infty} \mu^{sym}(\mathcal{U})/n = 2\left(1 + \frac{4}{\sqrt{q}-5}\right).$$

This proposition means that to get a polynomially constructable algorithm with linear complexity, one needs to construct explicitly (i.e polynomially) points of

corresponding degrees on modular curves (or on other curves with many points). Unfortunately, so far it is unknown how to produce such points.

In [72, Remark 6.6], H. Randriambololona improves this result under the same hypothesis concerning the construction of a point of degree n. More precisely, up to this existence, he obtains a polynomial time (in n) construction of a multiplication algorithm (respect. a symmetric multiplication algorithm) in $\mathbb{F}_{q^n}/\mathbb{F}_q$ of length $2n(1+\frac{1}{\sqrt{q}-2})+o(n)$ for $q \geq 9$ (resp. $q \geq 49$).

In [15], S. Ballet, A. Bonnecaze and M. Tukumuli obtain a polynomial construction of a symmetric multiplication algorithm of type elliptic Chudnovsky–Chudnovsky (i.e with the Chudnovsky-Chudnovky interpolation method on an elliptic curve) of length in $O(n(2q/K)^{\log^\star(n)})$ where

$$\log^\star(n) = \begin{cases} 0 & \text{if } n \leq 1, \\ 1+\log^\star(\log n) & \text{otherwise,} \end{cases} \tag{40}$$

$K = 2/3$ if the characteristic of $\mathbb{F}_q$ is 2 or 3 and $K = 5/8$ otherwise. Note that the length is only quasi-linear in n. However, this construction is without the restriction linked to the construction of a point of degree n. Moreover, this asymptotical construction is not realized from an infinite family of suitable curves as the above results but thanks to the use of a sequence $\mathcal{A}_{q,n}$ of symmetric bilinear multiplication algorithms constructed from an arbitrary elliptic curve defined over $\mathbb{F}_q$ and using high degree points of this curve.

In [33], N. Bshouty gives a deterministic polynomial time construction of a tester of type $(\mathcal{HLF}(\mathbb{F}_q, n, d), \mathbb{F}_{q^n}, \mathbb{F}_q))$ and of size $\mu = O(d^{\tau(d,q)}n)$ where

$$\tau(d,q) = \begin{cases} 3 \quad \text{if} \quad q \geq cd^2, & c>1 \text{ constant, } q \text{ perfect square,} \\ 4 \quad \text{if} \quad q \geq cd, & c>1 \text{ constant,} \\ 5 \quad \text{if} \quad q \geq d+1, & \\ 6 \quad \text{if} \quad q = d. & \end{cases} \tag{41}$$

From [33], in [34, Corollary 2], N. Bshouty gives the first polynomial time construction of a multilinear multiplication algorithm with linear multiplicative complexity in $O(d^{\tau(d,q)}n)$ for the multiplication of d elements in any extension finite field $\mathbb{F}_{q^n}$. This solves the open problem of deterministic polynomial time constructing a bilinear algorithm (i.e with $d=2$) with linear bilinear complexity for the multiplication of two elements in finite fields [44][78][9]. However, it does not solve the problem of deterministic polynomial time constructing a bilinear algorithm of type Chudnovsky–Chudnovsky. Indeed, the method of N. Bshouty is only based upon the equivalence between an optimal tester size and multilinear complexity. More precisely, the minimal size of a tester for $\mathcal{HLF}(\mathbb{F}_q, n, d)$ turns out to be equivalent to the rank of the tensor of the multiplication of d elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The minimal size of a tester for $\mathcal{HP}(\mathbb{F}_q, n, d)$ is equivalent to the symmetric rank of the tensor of multiplication of d elements.

11. Appendix: proof of Theorem 8.21, Theorem 8.9 and Proposition 6.11.2

We compress here the proof in [69, II §1.2-3].

11.1. **Repairing (and extending) the criterion of Cascudo & al.** The following theorem does control for 2-torsion in the worst case. It is a straight generalization of [38, Theorem 5.18]. The parameters will be later specified in the next paragraph to derive criterions for asymptotic bounds.

Theorem 11.1. *Let X be a curve of genus g over $\mathbb{F}_q$, where $q \geq 2$ is any prime power, and let $m \geq 1$ be an integer.*

Suppose that X admits a closed point Q of degree $\deg Q = m$ (a sufficient condition for this is $2g+1 \leq q^{(m-1)/2}(q^{1/2}-1)$).

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

$$n_d = \sum_u n_{d,u} \leq B_d(X), \tag{42}$$

where $B_d(X)$ denotes the number of closed points of X of degree d.

Let R the smallest integer *such that*

$$R \geq g(1+\log_q(2)) + 2m + 3log_q\left(\frac{3qg}{(\sqrt{q}-1)^2}\right) + 2 \text{ (if } 2|q) \tag{43}$$

$$R \geq g(1+2\log_q(2)) + 2m + 3log_q\left(\frac{3qg}{(\sqrt{q}-1)^2}\right) + 2 \text{ (otherwise).} \tag{44}$$

Then, provided

$$\sum_{d,u} n_{d,u} du \geq R$$

we have

$$\mu_q(m) \leq \sum_{d,u} n_{d,u}\mu_q(d,u). \tag{45}$$

The following proposition gathers the upper-bounding made in the proof. The first two follow from [65, p. 39 (or p. 64)] whereas the third one is borrowed from [38, Proposition 3.4].

Proposition 11.2. *Let $\mathbb{F}_q$ be a finite field and X a curve over $\mathbb{F}_q$ of genus $g \geq 1$. Let J be the Jacobian of X and $J(\mathbb{F}_q)$ the rational class group.*

1. *If q is odd, then $J(\mathbb{F}_q)[2] \leq 2^{2g}$*
2. *If q is even, then $J(\mathbb{F}_q)[2] \leq 2^g$*
3. *Let h be the class number of X and, for any integer i with $0 \leq i \leq g-1$, A_i the number of $\mathbb{F}_q$-rational effective divisors of degree r. Then*

$$\frac{A_i}{h} \leq \frac{g}{q^{g-i-1}(\sqrt{q}-1)^2}$$

Let us now follow the original proof of the theorem of Cascudo & al [only in the case q even, the odd case being identic modulo using the corresponding upper-bound in Proposition 11.2]. Adding the terms $-\log_q\left(\frac{3qg}{(\sqrt{q}-1)^2}\right)$ and $2g(1-\log_q(2))$ to both sides of the inequality (43) reads :

$$2g + 2m + 2\log_q\left(\frac{3qg}{(\sqrt{q}-1)^2}\right) \leq g(1-\log_q(2)) + R - \log_q\left(\frac{3qg}{\sqrt{q}-1)^2}\right) - 2$$

Thus there exists an even integer $2d$ between the two sides of the previous inequality. Raising q to the inequalities $LHS \leq 2d$ and $2d \leq RHS$ respectively gives:

$$\frac{g}{q^{g-(2g-d+m)-1}(\sqrt{q}-1)^2} \leq \frac{1}{3} \tag{46}$$

$$\frac{g2^g}{q^{g-(2d-R)-1}(\sqrt{q}-1)^2} \leq \frac{1}{3} \tag{47}$$

Using the upper-bound (3) of Proposition 11.2, and combining the two inequalities (46) and (47) above with the upper-bound 11.2, yields

$$h > \frac{2}{3}h \geq A_{2g-d+m} + J(\mathbb{F}_q)[2]A_{2d-R}$$

Now let us choose a collection of pairwise distinct thickened points $\{P\}$ on the curve X such that, for each (d,u), there are exactly $n_{d,u}$ points among them of degree d and multiplicity u (this is possible by assumption). Let G be their divisorial sum and Q a closed point of degree m as in the assumption. G being of degree greater than R by assumption (11.1), the general criterion of [37, §4 Theorem 6] along with the inequality (11.1) imply the existence of a divisor $D = X$ of degree d that satisfies the following system of Riemann-Roch spaces vanishing conditions (with K being the canonical divisor of X):

$$l(K - X + Q) = 0 \tag{48}$$

$$l(2X - G) = 0 \tag{49}$$

Thus criterions (i') and (ii') of Theorem [72, Theorem 3.5] are satisfied with the divisors G and D.

11.2. **Deriving the bounds from the previous theorem and other criterions from the litterature.** Let $(X_s)_s$ be a dense sequence of curves over $\mathbb{F}_q$ with genera g_s growing to infinity, and a ratio of points of degree r matching $A'_r(q)$. Noting $A'_r = A'_r(q)$, this reads :

$$g_s \xrightarrow[s\to\infty]{} \infty \tag{d1}$$

$$B_r(X_s) = A'_r g_s + o(g_s) \tag{d2}$$

$$g_s = g_{s-1} + o(g_s) \tag{d3}$$

Let us prove first the bound (b) in 8.21, which generalizes [17, Proposition 3], but whose arguments were already introduced in [20, Theorem 3.2]. Given an integer n, let $s(n)$ be the smallest integer such that

$$rlB_r(X_{s(n)}) - 2g_{s(n)} \geq 2n + 3.$$

(d2) makes clear (or anyway it will be in the following equivalences), that such an integer $s(n)$ exists as soon as the denominator in the criterion (b) of Theorem 8.21 is strictly positive.

Moreover g being large enough, [24, Proposition 4.3 and Remark 4.4] state in general the existence of a zero-dimensional divisor of degree $g-5$ on $X_{s(n)}$. Thus the existence of a non-special divisor R of degree (lower than) $g+3$.

Therefore, Corollary [72, Proposition 5.1] applies to (11.2). Taking all $n_{d,u}$ null except $n_{r,l}$ equal to $B_r(X_{s(n)})$, this reads :

$$\mu_q^{\mathrm{sym}}(n) \leq \mu_q^{\mathrm{sym}}(r,l)B_r(X_{s(n)}).$$

Let us now tie the asymptotics behaviors of $g_{s(n)}$ and $B_r(X_{s(n)})$. The minimality of $s(n)$ satisfying (11.2) implies :

$$rlB_r(X_{s(n)}) - 2g_{s(n)} \geq 2n + 3 > rlB_r(X_{s(n)-1}) - 2g_{s(n)-1}$$

Dividing the two inequalities by $g_{s(n)-1}$, and applying the asymptotic equivalences (d2) and (d3) (and (d1)) yields :

$$rlA'_r - 2 + o(n) \geq \frac{2n}{g_{s(n)}} + o(1) > rlA'_r - 2 + o(n)$$

hence the asymptotic equivalence :

$$2n + o(n) = (rlA'_r - 2)g_{s(n)} + o(g_{s(n)}) \tag{50}$$

(which implies in particular that $o(n) = o(g_{s(n)})$). One can now divide both sides of the upper-bound (11.2) by the previous equality :

$$\frac{\mu_q^{\mathrm{sym}}(n)}{n} \leq \mu_q^{\mathrm{sym}}(r,l).2\left(\frac{A'_r g_{s(n)} + o(n)}{(rlA'_r - 2)g_{s(n)} + o(n)}\right)$$

Multiplying and dividing the RHS parenthesis by rl, then subtracting and adding $2g_{s(n)}$ to the numerator of the RHS, gives the result by letting n tend to infinity.

The other bounds are derived similarly. Namely, given an integer n, consider $s(n)$ be the smallest integer such that the following inequalities hold, then apply the respective criterions with all the $n_{d,u}$ null excepted $n_{r,l} = B_r(X_{s(n)})$:

(51)
$rlB_r(X_{s(n)}) - g_{s(n)} \geq 2n + 5$ then apply [72, Proposition 5.7] for Theorem 8.9

(52)
$rlB_r(X_{s(n)}) - g_{s(n)} \geq 2n + 1$ then apply [72, Proposition 5.2 c)] for Theorem 8.21 (a)

(53)
$rlB_r(X_{s(n)}) - g_{s(n)} \geq 2n + 1$ (same $s(n)$) this time for Proposition 6.11.2

[Justification for the latter: simply set $\mathrm{Cl}_0(X)(\mathbb{F}_q)[2] = 0$ in the proof of Theorem 11.1, thanks to Proposition 6.11.1]

(54)
$$rlB_r(X_{s(n)}) - (1 + \log_q 2)g_{s(n)} \geq 2n + 3log_q\left(\frac{3qg_{s(n)}}{(\sqrt{q}-1)^2}\right) + 3 \text{ if } 2|q \text{ for Theorem 8.21 (c)}$$

(55)
$$rlB_r(X_{s(n)}) - (1 + 2\log_q 2)g_{s(n)} \geq 2n + 3log_q\left(\frac{3qg_{s(n)}}{(\sqrt{q}-1)^2}\right) + 3 \text{ otherwise for Theorem 8.21 (d).}$$

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] Kevin Atighehchi, Stéphane Ballet, Alexis Bonnecaze, and Robert Rolland. Effective arithmetic in finite fields based on Chudnovsky's multiplication algorithm. *Comptes Rendus Mathematique*, 354(2):137–141, February 2016.

[3] Kevin Atighehchi, Stéphane Ballet, Alexis Bonnecaze, and Robert Rolland. Arithmetic in Finite Fields based on Chudnovsky's multiplication algorithm. *Mathematics of Computation*, 86(308):297–3000, 2017.

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

[5] Séphane Ballet. *Complexité bilinéaire de la multiplication dans les corps finis par interpolation sur des courbes algébriques*. PhD thesis, Université de la Méditerranée, Institut de Mathématiques de Luminy, 1998.

[6] 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.

[7] Stéphane Ballet. Quasi-optimal Algorithms for Multiplication in the Extensions of $\mathbb{F}_{16}$ of degree 13, 14, and 15. *Journal of Pure and Applied Algebra*, 171:149–164, 2002.

[8] 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.

[9] Stéphane Ballet. An improvement of the construction of the D.V. and G.V. Chudnovsky algorithm for multiplication in finite fields. *Theoretical Computer Science*, 352:293–305, 2006.

[10] Stéphane Ballet. A note on the tensor rank of the multiplication in certain finite fields. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 332–342. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

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

[12] Stéphane Ballet, Nicolas Baudru, Alexis Bonnecaze, and Mila Tukumuli. On the Effective Construction of Asymmetric Chudnovsky Multiplication Algorithms in Finite Fields Without Derivated Evaluation. *ArXiv e-prints*.

[13] Stéphane Ballet, Nicolas Baudru, Alexis Bonnecaze, and Mila Tukumuli. On the Construction of the Asymmetric Chudnovsky Multiplication Algorithm in Finite Fields Without Derivated Evaluation. *Comptes Rendus de l'Académie des Sciences, Série I*, (355):729–733, 2017.

[14] Stéphane Ballet, Alexis Bonnecaze, and Hung Dang. On the scalar complexity of chudnovsky^2 multiplication algorithm in finite fields. In *CAI'19*, Lecture Notes in Computer Science, page To appear. Springer, 2019.

[15] Stéphane Ballet, Alexis Bonnecaze, and Mila Tukumuli. On the construction of elliptic Chudnovsky-type algorithms for multiplication in large extensions of finite fields. *Journal of Algebra and Its Applications*, 15(1):26 pages, 2016.

[16] 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.

[17] Stéphane Ballet, Jean Chaumine, and Julia Pieltant. Shimura modular curves and asymptotic symmetric tensor rank of multiplication in any finite field. In *CAI'13*, pages 160–172. Springer, 2013.

[18] 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 of Number Theory*, 116:293–310, 2006.

[19] 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.

[20] Stéphane Ballet and Julia Pieltant. On the tensor rank of multiplication in any extension of $\mathbb{F}_2$. *Journal of Complexity*, 27:230–245, 2011.

[21] Stéphane Ballet and Julia Pieltant. Tower of algebraic function fields with maximal Hasse-Witt invariant and tensor rank of multiplication in any extension of $\mathbb{F}_2$ and $\mathbb{F}_3$. *ArXiv e-prints*, Sep 2014.

[22] Stéphane Ballet and Julia Pieltant. Tower of algebraic function fields with maximal Hasse-Witt invariant and tensor rank of multiplication in any extension of $\mathbb{F}_2$ and $\mathbb{F}_3$. *Journal of Pure and Applied Algebra*, 222(5):1069–1086, 2018.

[23] Stéphane Ballet, Julia Pieltant, Matthieu Rambaud, and Jeroen Sijsling. On some bounds for symmetric tensor rank of multiplication in finite fields. *Contemporary Mathematics, Amer. Math. Soc., Providence, RI*, (686):93–121, 2017.

[24] Stéphane Ballet, Christophe Ritzenthaler, and Robert Rolland. On the existence of dimension zero divisors in algebraic function fields defined over $\mathbb{F}_q$. *Acta Arithmetica*, 143(4):377–392, 2010.

[25] 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.

[26] Stéphane Ballet and Robert Rolland. On the bilinear complexity of the multiplication in finite fields. In *Proceedings of the Conference Arithmetic, Geometry and Coding Theory (AGCT 2003)*, volume 11, pages 179–188. Société Mathématique de France, sér. Séminaires et Congrès, 2005.

[27] Stéphane Ballet and Robert Rolland. Families of curves over any finite field attaining the generalized Drinfeld-Vlăduţ bound. *Publications Mathématiques de Besançon, Algèbre et Théorie des Nombres*, pages 5–18, 2011.

[28] Stéphane Ballet and Alexey Zykin. Dense families of modular curves, prime numbers and uniform symmetric tensor rank of multiplication in certain finite fields. *Design, Codes and Cryptography*, 87(2–3):517–525, 2019.

[29] Razvan Barbulescu, Jérémie Detrey, Nicolas Estibals, and Paul Zimmermann. Finding Optimal Formulae for Bilinear Maps. In Ferruh Özbudak and Francisco Rodriguez-Henriquez, editors, *Arithmetic of Finite Fields*, volume 7369 of *Lecture Notes in Computer Science*, pages 168–186. Springer Berlin Heidelberg, 2012.

[30] 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.

[31] Roger Brockett and David Dobkin. On the optimal evaluation of a set of bilinear forms. *Linear Algebra and Its Applications*, 19:207–235, 1978.

[32] Mark Brown and David Dobkin. An improved lower bound on polynomial multiplication. *Computers IEEE Transactions on*, C-29(5):337–340, 1980.

[33] Nader Bshouty. Tester and their applications. *Electronic Colloquium on Computational Complexity (ECCC)*, 19(11), 2012.

[34] Nader Bshouty. Multilinear Complexity is Equivalent to Optimal Tester Size. *Electronic Colloquium on Computational Complexity (ECCC)*, Tr13(11), 2013.

[35] Nader Bshouty and Michaël Kaminski. Multiplication of polynomials over finite fields. *SIAM Journal on Computing*, 19(3):452–456, 1990.

[36] Peter Bürgisser, Michael Clausen, and Amin Shokrollahi. *Algebraic Complexity Theory*. Springer, 1997.

[37] 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. Springer, 2011.

[38] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. Torsion limits and Riemann-Roch Systems for Function Fields and Applications. *IEEE Transactions on Information Theory*, 60(7):3871–3888, 2014.

[39] 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.

[40] Murat Cenk and Ferruh Özbudak. On multiplication in finite fields. *Journal of Complexity*, pages 172–186, 2010.

[41] Murat Cenk and Ferruh Özbudak. Multiplication of polynomials modulo x^n. *Theoretical Computer Science*, pages 3451–3462, 2011.

[42] Jean Chaumine. *Corps de fonctions algébriques et algorithme de D.V. et G.V. Chudnovsky pour la multiplication dans les corps finis*. PhD thesis, Université de la Polynésie Française, 2005.

[43] Jean Chaumine. On the bilinear complexity of multiplication in small finite fields. *Comptes Rendus de l'Académie des Sciences, Série I*, 343:265–266, 2006.

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

[45] Don Coppersmith and Shmuel Winograd. Matrix Multiplication via Arithmetic Progressions. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, pages 1–6, New York, NY, USA, 1987. ACM.

[46] Jean-Marc Couveignes and Reynald Lercier. Elliptic periods for finite fields. *Finite Fields and Their Applications*, 15(1):1–22, 2009.

[47] Hans 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.

[48] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Springer Berlin Heidelberg, 2004.
[49] Virgile Ducet. *Construction of algebraic curves with many rational points over finite fields*. PhD thesis, Université d'Aix-Marseille, Institut de Mathématiques de Marseille, 2013.
[50] Adrian W. Dudek. An explicit result for primes between cubes. *Functiones and Approximatio Commmentarii Mathematici*, 55(2):177–197, 2016.
[51] Noam Elkies. Explicit modular towers. In *In Tamer Basar and Alexander Vardy, editors, Proceedings of the Thirty-fifth annual Allerton conference on communication, control and computing*, Progress in Mathematics. Birkhäuser, 1997.
[52] Noam Elkies. Shimura curves computations. In *Proceedings of ANTS*, 1998.
[53] Noam Elkies. Explicit towers of Drinfeld modular curves. In *European Congress of Mathematics*, volume 202 of *Progress in Mathematics*, pages 189–198. Birkhäuser, 2001. Proceedings of the 3rd European Congress of Mathematics, Barcelona, July 10-14, 2000.
[54] Noam Elkies. Shimura curves arising from the (2,3,7) triangle group. In *Proceedings of ANTS*, 2006.
[55] Charles Fiduccia and Yechezkel Zalcstein. Algebras having linear multiplicative complexities. *Journal of the ACM*, 24:311–331, 1977.
[56] Shuhong Gao. *Normal Bases over Finite Fields*. PhD thesis, University of Waterloo, 1993.
[57] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. *Inventiones Mathematicae*, 121:211–222, 1995.
[58] Arnaldo Garcia, Henning Stichtenoth, and Hans-Georg Ruck. On tame towers over finite fields. *Journal für die reine und angewandte Mathematik*, 557:53–80, 2003.
[59] Emmanuel Hallouin. Computation of a cover of shimura curves using a hurwitz space. *J. Algebra*, 2009.
[60] Takehiro Hasegawa. An explicit shimura tower of function fields over a number field: An application of takeuchi's list. *preprint https://arxiv.org/abs/1701.07551*, 2017.
[61] 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*, 28:721–724, 1981.
[62] Abraham Lempel, Gadiel Seroussi, and Shmuel Winograd. On the complexity of multiplication in finite fields. *Theoretical Computer Science*, 22:285–296, 1983.
[63] Christophe Levrat. Tours de courbes de shimura. Master's thesis, Université Paris-Saclay et Université de Versailles Saint-Quentin, https://perso.telecom-paristech.fr/rambaud/teaching/20182018.
[64] Jeroen Sijsling Michael Musty, Sam Schiavone and John Voight. A database of belyi maps. In *Proceedings of ANTS*, 2018.
[65] David Mumford. *Abelian varieties*. Oxford University Press, 1970.
[66] 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.
[67] Julia Pieltant and Hugues Randriambololona. New uniform and asymptotic upper bounds on the tensor rank of multiplication in extensions of finite fields. *Mathematics of Computation*, 84:2023–2045, 2015.
[68] Matthieu Rambaud. Optimal chudnovsky-chudnovsky multiplication algorithms. In *WAIFI*, 2014.
[69] Matthieu Rambaud. *Courbes de Shimura et algorithmes bilinéaires de multiplication dans les corps finis*. PhD thesis, Telecom ParisTech, 2017. written in English.
[70] Hugues Randriambololona. Hecke operators with odd determinant and binary frameproof codes beyond the probabilistic bound? In *2010 IEEE Information Theory Workshop (ITW 2010 Dublin)*, 2010.
[71] Hugues Randriambololona. Divisors of the form $2D - G$ without sections and bilinear complexity of multiplication in finite fields (in French). *ArXiv e-prints*, 2011.
[72] Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *Journal of Complexity*, 28(4):489–517, 2012.
[73] Hugues Randriambololona. $(2, 1)$-separating systems beyond the probabilistic bound. *Israel J. Math.*, 195(1):171–186, 2013.
[74] Hugues Randriambololona. On products and powers of linear codes under componentwise multiplication. In *Algorithmic arithmetic, geometry, and coding theory*, volume 637 of *Contemp. Math.*, pages 3–78. Amer. Math. Soc., Providence, RI, 2015.

[75] Hugues Randriambololona. Gaps between prime numbers and tensor rank of multiplication in finite fields. *Design, Codes and Cryptography*, 87(2–3):627–645, 2019.
[76] G. Seroussi and A. Lempel. On symmetric algorithms for bilinear forms over finite fields. *J. Algorithms*, 5(3):327–344, 1984.
[77] Amin Shokhrollahi. Optimal algorithms for multiplication in certain finite fields using algebraic curves. *SIAM Journal on Computing*, 21(6):1193–1198, 1992.
[78] 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.
[79] Jeroen Sijsling. Canonical models of arithmetic $(1; e)$-curves. *Math. Z.*, 2013.
[80] André Toom. The complexity of schemes of functional elements realizing the multiplication of integers. *Soviet Mathematics (Translations of Doklady Akademie Nauk S.S.S.R.)*, 4:714–716, 1963.
[81] Michael Tsfasman. Some remarks on the asymptotic number of points. In H. Stichtenoth and M.A. Tsfasman, editors, *Coding Theory and Algebraic Geometry*, volume 1518 of *Lecture Notes in Mathematics*, pages 178–192, Berlin, 1992. Springer-Verlag. Proceedings of AGCT-3 conference, June 17-21, 1991, Luminy.
[82] Michael Tsfasman and Serguei Vlăduţ. *Algebraic-Geometric Codes*. Kluwer Academic Publishers, Dordrecht/Boston/London, 1991.
[83] Michael Tsfasman, Serguei Vlăduţ, and Thomas Zink. *Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound*, volume 109 of *Math. Nachr.* 1982.
[84] Mila Tukumuli. *Étude de la construction effective des algorithmes de type Chudnovsky pour la multiplication dans les corps finis*. PhD thesis, Université d'Aix-Marseille, Institut de Mathématiques de Luminy, 2013.
[85] John Voight. Three lectures on shimura curves. 2006.
[86] John Voight. Shimura curves of genus at most two. *Math. Comp.*, 2009.
[87] Shmuel Winograd. Some bilinear forms whose multiplicative complexity depends on the field of constants. *Mathematical Systems Theory*, 10:169–180, 1977.
[88] Shmuel Winograd. On Multiplication in Algebraic Extension Fields. *Theoretical Computer Science*, 8:359–377, 1979.
[89] Chaoping Xing. Asymptotic bounds on frameproof codes. *IEEE Trans. Inform. Theory*, 48(11):2991–2995, 2002.

Aix-Marseille Université, CNRS, Centrale Marseille, Institut de Mathématiques de Marseille, case 907, 163 avenue de Luminy, F13288 Marseille cedex 9, France
E-mail address: stephane.ballet@univ-amu.fr

Laboratoire Géométrie Algébrique et Applications à la Théorie de l'Information, Université de la Polynésie Française, B.P. 6570, 98702 Faa'a, Tahiti, France
E-mail address: jean.chaumine@upf.pf

Conservatoire National des Arts et Métiers, Équipe en émergence Sécurité-Défense, EPN 15 STRATÉGIES, Pôle Sécurité Défense - Chaire de Criminologie, 40 rue des Jeûneurs, F75002 Paris, France
E-mail address: julia.pieltant@lecnam.net

CNRS LCTI, Télécom ParisTech, 46 rue Barrault, F-75634 Paris cedex 13, France
E-mail address: rambaud@enst.fr

CNRS LCTI, Télécom ParisTech, 46 rue Barrault, F-75634 Paris cedex 13, France
E-mail address: randriambololona@enst.fr

Aix-Marseille Université, CNRS, Centrale Marseille, Institut de Mathématiques de Marseille, case 907, 163 avenue de Luminy, F13288 Marseille cedex 9, France
E-mail address: robert.rolland@acrypta.fr