Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method

Hugues Randriambololona

March 22, 2012

Abstract

We give new improvements to the Chudnovsky-Chudnovsky method that provides upper bounds on the bilinear complexity of multiplication in extensions of finite fields through interpolation on algebraic curves. Our approach features three independent key ingredients:

- We allow asymmetry in the interpolation procedure. This allows to prove, via the usual cardinality argument, the existence of auxiliary divisors needed for the bounds, up to optimal degree.
- We give an alternative proof for the existence of these auxiliary divisors, which is constructive, and works also in the symmetric case, although it requires the curves to have sufficiently many points.
- We allow the method to deal not only with extensions of finite fields, but more generally with monogenous algebras over finite fields. This leads to sharper bounds, and is designed also to combine well with base field descent arguments in case the curves do not have sufficiently many points.

As a main application of these techniques, we fix errors in, improve, and generalize, previous works of Shparlinski-Tsfasman-Vladut, Ballet, and Cenk-Özbudak. Besides, generalities on interpolation systems, as well as on symmetric and asymmetric bilinear complexity, are also discussed.

Contents

Introduction

The bilinear complexity $\mu(\mathcal{A}/K)$ of a finite-dimensional algebra $\mathcal{A}$ over a field K measures the essential minimal number of two-variable multiplications in K needed to perform a multiplication in $\mathcal{A}$, and considering other operations, such as multiplication by a constant, as having no cost. More intrinsically, it can be defined as the rank of the tensor in

$$\mathcal{A} \otimes \mathcal{A}^\vee \otimes \mathcal{A}^\vee \tag{1}$$

naturally deduced from the multiplication map in $\mathcal{A}$.

The study of $\mu(\mathcal{A}/K)$, and the effective derivation of multiplication algorithms, are of both theoretical and practical importance. Pioneering works in this field are Karatsuba's algorithm [23] for integer and polynomial multiplication, and Strassen's algorithm [33] for matrix multiplication.

There are (at least) two ways in which these questions could be addressed from an algebraic geometry point of view. These two approaches are seemingly unrelated, although, to the author's knowledge, possible links between the two have never been seriously studied (nor will they be here). The first one is to consider tensors of rank 1 as defining points of a certain Segre variety, and tensors of higher rank, points of its successive secant varieties. This leads to deep and beautiful problems [35, 24], but we will not be interested in this approach here. The second one is through the theory of interpolation. Karatsuba's algorithm may be interpreted as follows: evaluate the polynomials at the points $0, 1, \infty$ of the projective line, multiply these values locally, and interpolate the results to reconstruct the product polynomial. Replacing the line with algebraic curves of higher genus allowed Chudnovsky and Chudnovsky in [17] to first prove that the bilinear complexity of multiplication in certain extensions of finite fields grows at most linearly with the degree. For example, letting $\mu_q(n) = \mu(\mathbb{F}_{q^n}/\mathbb{F}_q)$, their result implies

$$\liminf_{n\to\infty} \frac{1}{n}\mu_q(n) \leq 2\left(1 + \frac{1}{\sqrt{q}-3}\right) \tag{2}$$

for $q \geq 25$ a square.

Several improvements and variants of the Chudnovsky-Chudnovsky algorithm were then proposed by various authors in order to give sharper or more general asymptotic, as well as non-asymptotic, upper bounds. Roughly speaking, they all rely on the following three ingredients:

a) A "generic" interpolation process which explains how to derive these upper bounds from the existence, postulated a priori, of certain geometric objects. These objects are:

b) Algebraic curves having "good" parameters, meaning, most of the time, that they have sufficiently many points of various degrees, and controlled genus.

c) Divisors on these curves, such that certain evaluation maps associated to them are injective or surjective. Often this can be reformulated as requiring

the existence of systems of simultaneously zero-dimensional or non-special divisors of a certain form and appropriate degree.

These three points are important. However remark that a well-designed algorithm in a) should make the existence of the objects b) and c) it needs easier to check. In this paper we will give new contributions to a), and also to c), and then proceed to some direct, but hopefully already significant, applications (further applications could be given, but they require combination with quite different methods, so they will be treated elsewhere).

Our main technical results are Theorems 3.5 and 5.2 below.

Theorem 3.5 is our main contribution to a). There we present a generalization of the Chudnovsky-Chudnovsky algorithm that has two new features:

- We allow interpolation at arbitrary closed subschemes of the curve in a uniform way. The original method of Chudnovsky-Chudnovsky used only points of degree 1, with multiplicity 1. Variants introduced by Ballet-Rolland and Arnaud allowed interpolation at points of higher degree, or with higher multiplicity. These improvements were combined and further generalized by Cenk-Özbudak in [14]. However, somehow, Cenk-Özbudak still deal with degree m and multiplicity l separately since they use two parameters, $\mu_q(m)$ and $\widehat{M}_q(l)$, for them. Here we introduce a new quantity,

$$\mu_q(m,l), \tag{3}$$

  the bilinear complexity of the algebra $\mathbb{F}_{q^m}[t]/(t^l)$ over $\mathbb{F}_q$, to deal with both at the same time. This leads ultimately to improved bounds and is especially useful when combined, for example, with descent arguments, such as the ones used in [7, 4, 5]. Another indication of the naturality of our approach is that these $\mu_q(m,l)$ can be made to appear on both sides of our inequalities. This means, not only do we have upper bounds *in terms* of these $\mu_q(m,l)$, but at the same time we can also derive upper bounds *on* them.

- We allow asymmetry when lifting the elements to be multiplied, even if the multiplication law is commutative (as is permitted by the very definition of bilinear complexity). This has dramatic consequences for applications since it makes the existence of the divisors mentioned in c) above much easier to prove. Technically speaking, classical "symmetric" variants of the Chudnovsy-Chudnovsky algorithm (starting from the original) suppose given two effective divisors G and G' and ask for the existence of an auxiliary divisor D such that:

  - $D - G'$ is non-special
  - $2D - G$ is zero-dimensional. (4)

  In our asymmetric version, we ask for *two* divisors D_1, D_2 such that:

  - $D_1 - G'$ and $D_2 - G'$ are non-special
  - $D_1 + D_2 - G$ is zero-dimensional. (5)

As explained below, this small change allows us at once to fill a gap in the proof of bounds claimed by Shparlinski-Tsfasman-Vladut [31] and Ballet [1, 2].

Then Theorem 5.2 combines Theorem 3.5 with general existence results for divisors as asked above, leading to bounds that depend only on the number of points of the curve, in a somehow optimal way. To be more precise, while all divisors of negative degree are zero-dimensional (and likewise all divisors of degree more than $2g-1$ are non-special), for the bounds on the complexity to be as sharp as possible, one needs the divisors involved to be of degree as near to $g-1$ as possible.

Shparlinski-Tsfasman-Vladut, and later also Ballet, claimed they were able to solve system (4) up to degree $g-1$ (or at least, asymptotically in [31], while exactly in [1]). For this they use a cardinality argument. They consider the map that sends the linear equivalence class $[D]$ to the class $[2D-G]$, and from this, deduce that the number of linear equivalence classes of D such that $2D-G$ is not zero-dimensional is not more than the number of effective divisors of the corresponding degree. However this inference is incorrect, because the map $[D] \mapsto [2D-G]$ is not injective. Taking this non-injectivity into account multiplies their bound by the 2-torsion order of the class group, which ruins the argument.

This error was first mentioned in a preprint of Cascudo-Cramer-Xing, although this discussion was removed from the final version of their paper. However it can still be found in Cascudo's PhD dissertation [11], Chap. 12.

On the other hand, our new asymmetric system (5) is much easier to solve. Indeed, the divisors D_1 and D_2 can then be constructed one at a time, there is no multiplication-by-2 map in the class group involved, and the cardinality argument works smoothly. This allows us, under very mild assumptions, to solve system (5) up to degree exactly $g-1$, which is optimal, and ultimately, to complete the proof of the bounds claimed in [1, 2, 31] (except for one, where there is another error, discussed in the text). These repaired bounds now form our Corollary 5.4 and Theorems 6.3 and 6.4. For example, (2) can now be replaced safely with the new estimate (first claimed in [31])

$$\limsup_{n\to\infty} \frac{1}{n}\mu_q(n) \leq 2\left(1+\frac{1}{\sqrt{q}-2}\right) \tag{6}$$

for $q \geq 9$ a square.

A small drawback of this cardinality argument, already mentioned in [31], is its non-constructiveness. Also, for some applications, it might appear unsatisfactory to get only asymmetric multiplication algorithms for an algebra in which the multiplication law is commutative. So we propose an alternative method, more constructive, that solves system (5), as well as the original symmetric system (4), also up to degree exactly $g-1$, although only under more restrictive assumptions. This alternative construction, that relies on the theory of Weierstrass gap and order sequences, is a straightforward adaptation of a

method previously developed by the author in another context [28]. In doing so we are also led to stress the distinction between the usual bilinear complexity, and a more restricted notion of *symmetric* bilinear complexity. For example, our symmetric variant of (6) yields

$$\limsup_{n\to\infty} \frac{1}{n}\mu_q^{\mathrm{sym}}(n) \leq 2\left(1+\frac{1}{\sqrt{q}-2}\right) \tag{7}$$

for $q \geq 49$ a square (note the stronger restriction on q).

Besides these two main Theorems 3.5 and 5.2 and their applications in Corollary 5.4 and Theorems 6.3 and 6.4, other topics of possible interest discussed in this paper include a fairly general presentation of interpolation systems in Section 2, as well as a study of low degree (or low genus) examples in Section 4 that clarifies and improves statements of [14].

Before we finish this Introduction, we would like to mention the very close links that exist between this domain and other areas of mathematics and theoretical computer science. One first such area is coding theory, and more precisely the theory of *intersecting codes*. The link between multiplication algorithms and intersecting codes was first stressed in [9] and [25]. More important, in [38], Xing studied intersecting codes arising from algebraic curves, and he gave a criterion for their existence, that reduces essentially to the second part of system (4). Hence here also the 2-torsion in the class group is an obstruction to get optimal parameters (see [27] for elaborations on this). This problem was essentially solved, or more properly, bypassed by the author in [28] with the method discussed above (although the analog problem for t-torsion, $t \geq 3$, is still open).

Another such area is cryptography with the theory of *linear secret sharing systems with multiplication property*, in particular within the framework of *secure multi-party computation* [18]. In one direction, to optimize the parameters of these systems, multiplication algorithms with low bilinear complexity are sometimes required. In the other direction, secure multi-party computation schemes based on algebraic curves were introduced by Chen and Cramer in [16], and the design of these schemes also involves a system similar to (4). And again, the 2-torsion in the class group is an obstruction to get optimal parameters [11, 13]. It would be interesting to check how the tools introduced in the present work could be put to use in this context.

Conventions. In this text we make free use of the language of modern algebraic geometry: schemes, sheaves, and cohomology. Admittedly, the only place where this is necessary is at the end of Section 2, while designing interpolation systems from higher dimensional algebraic varieties, and this point is quite secondary in our presentation. From Section 3 on, we deal only with curves, and everything could be equally well expressed in the language of function fields in one indeterminate. We made the choice to stick to the geometric point of view, but, keeping in mind that application oriented readers might be more familiar

with the function field terminology, we tried to keep the level of exposition accessible so that translation from one language to the other would remain easy. As standard references for these subjects we advise [22] for the general geometric language and [32] for the function field approach in the case of curves.

1 Tensor rank and 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

$$\alpha : E_1 \times \cdots \times E_s \longrightarrow E_0 \tag{8}$$

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

$$\widetilde{\alpha} \in E_0 \otimes E_1^\vee \otimes \cdots \otimes E_s^\vee \tag{9}$$

naturally deduced from α.

For $s = 1$, these notions are very well understood (they reduce essentially to the rank of a matrix). However, starting from $s = 2$, they can be surprisingly difficult to handle.

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

$$\mu(\mathcal{A}/K) \tag{10}$$

the bilinear complexity of the multiplication map

$$m_{\mathcal{A}} : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A} \tag{11}$$

considered as a K-bilinear map.

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

$$xy = \phi_1(x)\psi_1(y)w_1 \ + \ \cdots \ + \ \phi_n(x)\psi_n(y)w_n. \tag{12}$$

Indeed, such an expression is the same thing as a decomposition

$$\widetilde{m}_{\mathcal{A}} = \sum_{i=1}^{n} w_i \otimes \phi_i \otimes \psi_i \ \in \ \mathcal{A} \otimes \mathcal{A}^\vee \otimes \mathcal{A}^\vee \tag{13}$$

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

Remark that here, the notion of algebra is taken in its broadest sense. However, in Proposition 2.4, and then from Section 3 on, we will only consider algebras that are associative, commutative, and with unity.

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

The study of $\mu(\mathcal{A}/K)$, and the effective derivation of multiplication algorithms, are of both theoretical and practical importance. Pioneering works in this field are Karatsuba's algorithm [23] for integer and polynomial multiplication, and Strassen's algorithm [33] for matrix multiplication.

In practical terms, focusing on the bilinear complexity of the multiplication in $\mathcal{A}$ means according importance only to the number of two-variable multiplications in K needed to perform a multiplication in $\mathcal{A}$, and considering other operations, such as multiplication by a constant, as having no cost. This is a reasonable assumption although its relevance clearly depends on the computation model.

When $\mathcal{A}$ is commutative, it is sometimes convenient to favour the study of symmetric multiplication algorithms. Thus, as $\mu(\mathcal{A}/K)$ is defined as the minimal length of a (possibly asymmetric) multiplication algorithm for $\mathcal{A}/K$, we also introduce the following:

Definition 1.5. If $\mathcal{A}$ is a finite-dimensional commutative K-algebra, we define its *symmetric bilinear complexity*

$$\mu^{\mathrm{sym}}(\mathcal{A}/K) \tag{14}$$

as the minimal length of a symmetric multiplication algorithm for $\mathcal{A}/K$.

Equivalently, it is the minimal length of a decomposition of the multiplication tensor $\widetilde{m}_{\mathcal{A}}$ as a sum of symmetric elementary tensors, that is, of tensors of the form $w \otimes \phi \otimes \phi \in \mathcal{A} \otimes \mathcal{A}^\vee \otimes \mathcal{A}^\vee$.

Here we gather a few elementary properties of these notions. Lemma 1.6 shows that symmetric bilinear complexity is well defined, and compares it with its non-symmetric counterpart. Lemma 1.9 gives basic lower bounds for $\mu(\mathcal{A}/K)$, and Lemma 1.10 deals with some functorial properties. Certainly most things here are already classical and can be found from other sources. The reader is especially refered to the foundational work [34] (and to the additional material in [9, 19, 25, 37]), or to textbooks such as [10, 21], for historical details and further results of this type.

Lemma 1.6. *Let $\mathcal{A}$ be a finite-dimensional commutative K-algebra. Then $\mathcal{A}$ admits a symmetric multiplication algorithm, hence $\mu^{sym}(\mathcal{A}/K) < \infty$ is well defined. More precisely, it satisfies*

$$\mu^{sym}(\mathcal{A}/K) \leq \frac{d(d+1)}{2} \tag{15}$$

where $d = \dim \mathcal{A}$. If $\operatorname{char} K \neq 2$, then also

$$\mu^{sym}(\mathcal{A}/K) \leq 2\mu(\mathcal{A}/K). \tag{16}$$

In the other direction, we always have

$$\mu(\mathcal{A}/K) \leq \mu^{sym}(\mathcal{A}/K). \tag{17}$$

Proof. Let $e_1, \dots, e_d$ be a basis of $\mathcal{A}$, and let $e_1^\vee, \dots, e_d^\vee$ be the dual basis. First remark that the multiplication tensor of $\mathcal{A}$ can always be decomposed as $\widetilde{m}_{\mathcal{A}} = \sum_{i,j}(e_i e_j) \otimes e_i^\vee \otimes e_j^\vee$, and since $\mathcal{A}$ is commutative this can be rearranged as:

$$\widetilde{m}_{\mathcal{A}} = \sum_{1 \le i \le d} (e_i^2) \otimes e_i^\vee \otimes e_i^\vee + \sum_{1 \le i < j \le d} (e_i e_j) \otimes (e_i^\vee \otimes e_j^\vee + e_j^\vee \otimes e_i^\vee). \tag{18}$$

The first sum is already composed of symmetric tensors, and the second sum can also be put in such a form since

$$e_i^\vee \otimes e_j^\vee + e_j^\vee \otimes e_i^\vee = (e_i^\vee + e_j^\vee) \otimes (e_i^\vee + e_j^\vee) - e_i^\vee \otimes e_i^\vee - e_j^\vee \otimes e_j^\vee. \tag{19}$$

We plug this into the previous equality and then regroup the similar terms to find:

$$\widetilde{m}_{\mathcal{A}} = \sum_{1 \le i \le d} (2e_i^2 - e_i s) \otimes e_i^\vee \otimes e_i^\vee + \sum_{1 \le i < j \le d} (e_i e_j) \otimes (e_i^\vee + e_j^\vee) \otimes (e_i^\vee + e_j^\vee) \tag{20}$$

where $s = \sum_{j=1}^n e_j$. This gives (15).

Now suppose $\operatorname{char} K \neq 2$, and let w_i, ϕ_i, ψ_i define a multiplication algorithm of length $n = \mu(\mathcal{A}/K)$ for $\mathcal{A}$. We can then write

$$\begin{aligned} \widetilde{m}_{\mathcal{A}} &= \sum_{i=1}^n w_i \otimes \phi_i \otimes \psi_i = \sum_{i=1}^n w_i \otimes \psi_i \otimes \phi_i \\ &= \frac{1}{2} \sum_{i=1}^n w_i \otimes (\phi_i \otimes \psi_i + \psi_i \otimes \phi_i) \\ &= \frac{1}{4} \sum_{i=1}^n w_i \otimes (\phi_i + \psi_i) \otimes (\phi_i + \psi_i) \; - \; w_i \otimes (\phi_i - \psi_i) \otimes (\phi_i - \psi_i), \end{aligned} \tag{21}$$

hence (16).

Last, (17) is trivial. □

Remark 1.7. Let $K = \mathbb{F}_2$. We can interpret (19) as giving a decomposition of the rank *two* symmetric matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ as a sum of *three* rank 1 symmetric matrices:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{22}$$

For $K = \mathbb{F}_2$ it is easily seen that this decomposition is *minimal*.

As a consequence, if $\mathcal{A}$ is the 2-dimensional commutative (but non-associative and without unity) $\mathbb{F}_2$-algebra with basis e_1, e_2 and multiplication defined by $e_1 e_2 = e_2 e_1 = e_1$ and $e_1^2 = e_2^2 = 0$, then

$$\mu(\mathcal{A}/K) = 2 \; < \; \mu^{\mathrm{sym}}(\mathcal{A}/K) = 3. \tag{23}$$

This gives an example of strict inequality in (17).

Definition 1.8. Given a multiplication algorithm as in (12), one associates to it two linear codes C_ϕ and $C_\psi \subset K^n$, namely the images of the evaluation maps

$$\begin{array}{rccc} \phi: & \mathcal{A} & \longrightarrow & K^n \\ & x & \mapsto & (\phi_1(x), \ldots, \phi_n(x)) \end{array} \quad \text{and} \quad \begin{array}{rccc} \psi: & \mathcal{A} & \longrightarrow & K^n \\ & y & \mapsto & (\psi_1(y), \ldots, \psi_n(y)) \end{array} \tag{24}$$

respectively.

Lemma 1.9. *Let $\mathcal{A}$ be a finite-dimensional K-algebra.*

a) If $\mathcal{A}$ admits a unit element,

$$\mu(\mathcal{A}/K) \geq \dim_K \mathcal{A}. \tag{25}$$

b) If $\mathcal{A}$ has no zero-divisor,

$$\mu(\mathcal{A}/K) \geq 2\dim_K \mathcal{A} - 1. \tag{26}$$

Proof. Consider a multiplication algorithm as in (12). If $\mathcal{A}$ admits a unit element, then $w_1, \ldots, w_n$ span $\mathcal{A}$, hence the first inequality. For the second inequality, remark that if $\mathcal{A}$ has no zero-divisor, then:

- the maps ϕ and ψ must be injective, hence the codes C_ϕ and C_ψ have dimension $k = \dim_K \mathcal{A}$,
- these two codes must be *mutually intersecting*, that is, any non-zero $c \in C_\phi$ and $c' \in C_\psi$ must have non-disjoint supports.

By the first point, if $k > \lceil n/2 \rceil$, one could find a non-zero $c \in C_\phi$ vanishing on the first $\lceil n/2 \rceil$ coordinates, and a non-zero $c' \in C_\psi$ vanishing on the last $\lceil n/2 \rceil$. These c, c' would then contradict the second point. Hence $k \leq \lceil n/2 \rceil$, which gives precisely (26). □

The link between multiplication algorithms and intersecting codes was first stressed in [9] and [25]. For more on this last topic, see for example [28] and the references therein. Another coding-theoretical view on some bilinear complexity problems has also been proposed, through the notion of *supercode*, in [31].

Lemma 1.10. *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*

$$\mu(\mathcal{A}_L/L) \leq \mu(\mathcal{A}/K). \tag{27}$$

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

$$\mu(\mathcal{A}/K) \leq \mu(\mathcal{A}/L)\mu(L/K). \tag{28}$$

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

$$\mu(\mathcal{A} \times \mathcal{B}/K) \leq \mu(\mathcal{A}/K) + \mu(\mathcal{B}/K). \tag{29}$$

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

$$\mu(\mathcal{A} \otimes_K \mathcal{B}/K) \leq \mu(\mathcal{A}/K)\mu(\mathcal{B}/K). \tag{30}$$

Moreover, when the algebras are commutative, then (27)(28)(29)(30) *also hold with μ^{sym} in place of μ.*

Proof. To prove a), remark that if linear forms $\phi_1, \ldots, \phi_n$ and $\psi_1, \ldots, \psi_n : \mathcal{A} \longrightarrow K$ and elements $w_1, \ldots, w_n \in \mathcal{A}$ define a multiplication algorithm for $\mathcal{A}/K$, then the ϕ_i and ψ_i lift to linear forms $\mathcal{A}_L \longrightarrow L$, and the w_i can be seen as elements of $\mathcal{A}_L$, and as such they define a multiplication algorithm for $\mathcal{A}_L/L$ of the same length n.

To prove b) we use an analogue of the concatenation procedure in coding theory. Formally, suppose we are given:

- a multiplication algorithm of length m for L/K, defined by linear forms $\alpha_1 \ldots, \alpha_m$ and $\beta_1 \ldots, \beta_m : L \longrightarrow K$ and elements $l_1, \ldots, l_m \in L$,
- a multiplication algorithm of length n for $\mathcal{A}/L$, defined by linear forms $\lambda_1 \ldots, \lambda_n$ and $\rho_1 \ldots, \rho_n : \mathcal{A} \longrightarrow L$ and elements $a_1, \ldots, a_n \in \mathcal{A}$.

Then, letting $N = mn$, the two collections of N linear forms $\phi_{i,j} = \alpha_i \circ \lambda_j$ and $\psi_{i,j} = \beta_i \circ \rho_j : \mathcal{A} \longrightarrow K$, and the N elements $w_{i,j} = l_i a_j \in \mathcal{A}$, for $1 \leq i \leq m$ and $1 \leq j \leq n$, define a multiplication algorithm of length N for $\mathcal{A}/K$. Indeed, for all $x, y \in \mathcal{A}$,

$$xy = \sum_{1 \leq j \leq n} \lambda_j(x)\rho_j(y)a_j = \sum_{1 \leq j \leq n} \left(\sum_{1 \leq i \leq m} \alpha_i(\lambda_j(x))\beta_i(\rho_j(y))l_i \right) a_j. \tag{31}$$

To make the connection with concatenation in coding theory clearer, remark that C_ϕ is then the concatenated code $C_\alpha \circ C_\lambda$, and likewise $C_\psi = C_\beta \circ C_\rho$.

The proof of c) proceeds analogously using the notion of direct sum of multiplication algorithms. Suppose we are given:

- a multiplication algorithm of length m for $\mathcal{A}/K$, defined by linear forms $\phi_1 \ldots, \phi_m$ and $\psi_1 \ldots, \psi_m : \mathcal{A} \longrightarrow K$ and elements $a_1, \ldots, a_m \in \mathcal{A}$,
- a multiplication algorithm of length n for $\mathcal{B}/K$, defined by linear forms $\lambda_1 \ldots, \lambda_n$ and $\rho_1 \ldots, \rho_n : \mathcal{B} \longrightarrow K$ and elements $b_1, \ldots, b_n \in \mathcal{B}$.

Identify $\mathcal{A}$ with the subspace $\mathcal{A} \times \{0\}$ and $\mathcal{B}$ with the subspace $\{0\} \times \mathcal{B}$ in $\mathcal{A} \times \mathcal{B}$. Then for any $x = (r, s)$ and $y = (u, v)$ in $\mathcal{A} \times \mathcal{B}$ we have

$$xy = ru + sv = \sum_{1 \leq i \leq m} \phi_i(r)\psi_i(u)a_i + \sum_{1 \leq j \leq n} \lambda_j(s)\rho_j(v)b_j \tag{32}$$

hence this defines a multiplication algorithm of length $m+n$ for $\mathcal{A}\times\mathcal{B}$.

For d) we skip the details since everything works the same: suppose given ϕ_i, ψ_i, a_i and λ_j, ρ_j, b_j as in the proof of c), then the $\phi_i\otimes\lambda_j, \psi_i\otimes\rho_j, a_i\otimes b_j$ give a multiplication algorithm of length $N=mn$ for $\mathcal{A}\otimes\mathcal{B}$.

For the last assertion, remark that if we start with symmetric algorithms, then the constructions given above lead also to symmetric algorithms. □

Question 1.11. It would be interesting to have criteria for equality in this Lemma 1.10. For the inequalities in parts a) and b) (and hence also for part d), there are non-trivial examples in which equality holds, and others in which the inequality is strict (see below, or [37]). A general rule does not seem obvious. Turning to c), the author does not know any example were the inequality is strict. In fact, the now folklore *direct sum conjecture* (see [19, 34, 37]) suggests there should always be equality:

$$\mu(\mathcal{A}\times\mathcal{B}/K) \stackrel{?}{=} \mu(\mathcal{A}/K)+\mu(\mathcal{B}/K). \tag{33}$$

Proofs are known only for some very specific classes of algebras. The general case is still open.

Remark 1.12. We would like to indicate a few possible generalizations of the notions developed so forth.

First, we worked over a field, but it is also possible to work over a ring, or even over a more general base. This could be of interest, for instance, if one is given a family of tensors that vary with some parameters, and one requests elementary decompositions for them that vary accordingly.

In another direction, one could also extend the notion of symmetry. Given a group G acting on some tensor space, we can ask whether every G-invariant tensor admits a decomposition as a sum of G-invariant elementary tensors (and if so, what is the minimal length of such a decomposition). For $G=\mathfrak{S}_2$ the symmetric group of order 2 acting on $\mathcal{A}\otimes\mathcal{A}^\vee\otimes\mathcal{A}^\vee$ by permuting the last two factors, we saw in Lemma 1.6 that this is true (although the minimal symmetric decomposition might be longer than the non-symmetric one). However for more general group actions this is not always possible. The elegant counterexample that follows is due to Cascudo [12]:

Consider the trilinear map

$$\begin{array}{ccc} \mathbb{F}_4\times\mathbb{F}_4\times\mathbb{F}_4 & \longrightarrow & \mathbb{F}_4 \\ (x,y,z) & \mapsto & xyz \end{array} \tag{34}$$

over $\mathbb{F}_2$. It defines a tensor in $\mathbb{F}_4\otimes\mathbb{F}_4^\vee\otimes\mathbb{F}_4^\vee\otimes\mathbb{F}_4^\vee$, and since $\mathbb{F}_4$ is commutative, this tensor is $\mathfrak{S}_3$-invariant, where $\mathfrak{S}_3$ acts by permuting the last three factors. Suppose this tensor admits an $\mathfrak{S}_3$-invariant elementary decomposition. This means one can find elements $w_1,\ldots,w_n\in\mathbb{F}_4$, and linear forms $\phi_1,\ldots,\phi_n : \mathbb{F}_4\to\mathbb{F}_2$, such that for all $x,y,z\in\mathbb{F}_4$, one has $xyz=\sum_{i=1}^n \phi_i(x)\phi_i(y)\phi_i(z)w_i$.

But then for all $x, y \in \mathbb{F}_4$ one finds

$$\begin{aligned} x^2 y &= \sum_{i=1}^{n} \phi_i(x)^2 \phi_i(y) w_i \\ xy^2 &= \sum_{i=1}^{n} \phi_i(x) \phi_i(y)^2 w_i \end{aligned} \tag{35}$$

and the two quantities on the right are equal because all $\alpha \in \mathbb{F}_2$ satisfy $\alpha^2 = \alpha$. This is a contradiction since there are $x, y \in \mathbb{F}_4$ with $x^2 y \neq xy^2$.

2 Interpolation systems

If $\mathcal{B}$ is a K-algebra and if $E_1, E_2 \subset \mathcal{B}$ are two linear subspaces, we denote by $E_1 E_2$ the *linear span* of the products $e_1 e_2$ in $\mathcal{B}$, for $e_1 \in E_1$ and $e_2 \in E_2$.

Definition 2.1. Let $\mathcal{A}$ and $\mathcal{A}'$ be two finite-dimensional K-algebras. By an *interpolation system* for $\mathcal{A}'$ by $\mathcal{A}$ we mean the following data:

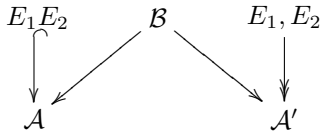
- a K-algebra $\mathcal{B}$ (of possibly infinite dimension) equipped with two K-algebra morphisms $f : \mathcal{B} \longrightarrow \mathcal{A}$ and $f' : \mathcal{B} \longrightarrow \mathcal{A}'$
- two linear subspaces $E_1, E_2 \subset \mathcal{B}$

satisfying the following conditions:

(i) the restriction $f|_{E_1 E_2} : E_1 E_2 \longrightarrow \mathcal{A}$ is injective

(ii) the restrictions $f'|_{E_1} : E_1 \longrightarrow \mathcal{A}'$ and $f'|_{E_2} : E_2 \longrightarrow \mathcal{A}'$ are surjective.

This can be summarized with the following diagram:



Such an interpolation system is said *symmetric* if $E_1 = E_2$.

Proposition 2.2. *Let $\mathcal{A}$ and $\mathcal{A}'$ be two finite-dimensional K-algebras. Suppose there exists an interpolation system for $\mathcal{A}'$ by $\mathcal{A}$. Then*

$$\mu(\mathcal{A}'/K) \leq \mu(\mathcal{A}/K). \tag{36}$$

Moreover, if $\mathcal{A}$ and $\mathcal{A}'$ are commutative and the interpolation system is symmetric, then also $\mu^{sym}(\mathcal{A}'/K) \leq \mu^{sym}(\mathcal{A}/K)$.

Proof. Let $\phi_1, \ldots, \phi_n$, $\psi_1, \ldots, \psi_n : \mathcal{A} \longrightarrow K$, and $w_1, \ldots, w_n \in \mathcal{A}$ define a multiplication algorithm for $\mathcal{A}/K$, where $n = \mu(\mathcal{A}/K)$.

Suppose we are given an interpolation system for $\mathcal{A}'$ by $\mathcal{A}$. Thanks to properties *(i)* and *(ii)* above, we can choose:

- a retraction $\rho : \mathcal{A} \longrightarrow E_1E_2$ of $f|_{E_1E_2}$
- sections $\sigma_1 : \mathcal{A}' \longrightarrow E_1$ of $f'|_{E_1}$ and $\sigma_2 : \mathcal{A}' \longrightarrow E_2$ of $f'|_{E_2}$.

Then, for $1 \leq i \leq n$, we let:

- $\phi'_i = \phi_i \circ f|_{E_1} \circ \sigma_1 : \mathcal{A}' \longrightarrow K$
- $\psi'_i = \psi_i \circ f|_{E_2} \circ \sigma_2 : \mathcal{A}' \longrightarrow K$
- $w'_i = f'(\rho(w_i)) \in \mathcal{A}'$.

Then $\phi'_1, \ldots, \phi'_n$, $\psi'_1, \ldots, \psi'_n$, and $w'_1, \ldots, w'_n$ define a multiplication algorithm for $\mathcal{A}'/K$. Indeed, for any $x', y' \in \mathcal{A}'$, if we let $x = f(\sigma_1(x'))$ and $y = f(\sigma_2(y'))$, then:

$$\begin{aligned}
\sum \phi'_i(x')\psi'_i(y')w'_i &= \sum \phi_i(x)\psi_i(y)f'(\rho(w_i)) \\
&= f'(\rho(\sum \phi_i(x)\psi_i(y)w_i)) \\
&= f'(\rho(xy)) \\
&= f'(\rho(f(\sigma_1(x'))f(\sigma_2(y')))) \\
&= f'(\rho(f(\sigma_1(x')\sigma_2(y')))) \\
&= f'(\sigma_1(x')\sigma_2(y')) \\
&= f'(\sigma_1(x'))f'(\sigma_2(y')) \\
&= x'y'.
\end{aligned} \tag{37}$$

Thus $\mu(\mathcal{A}'/K) \leq n$, as claimed.

For the last assertion, supposing $E_1 = E_2$, remark that if we start with a symmetric algorithm for $\mathcal{A}/K$ and if we choose $\sigma_1 = \sigma_2$, then the construction gives a symmetric algorithm for $\mathcal{A}'/K$. □

Corollary 2.3. *If $\mathcal{A}$ is a finite-dimensional K-algebra, and if $\mathcal{A}'$ is a subalgebra of $\mathcal{A}$, or a quotient algebra of $\mathcal{A}$, then*

$$\mu(\mathcal{A}'/K) \leq \mu(\mathcal{A}/K). \tag{38}$$

If $\mathcal{A}$ is commutative, then also $\mu^{sym}(\mathcal{A}'/K) \leq \mu^{sym}(\mathcal{A}/K)$.

Proof. If $\mathcal{A}'$ is a subalgebra of $\mathcal{A}$, define an interpolation system by taking $E_1 = E_2 = \mathcal{B} = \mathcal{A}'$, f the natural inclusion, and $f' = \mathrm{id}_{\mathcal{A}'}$.

If $\mathcal{A}'$ is a quotient algebra of $\mathcal{A}$, take $E_1 = E_2 = \mathcal{B} = \mathcal{A}$, $f = \mathrm{id}_{\mathcal{A}}$, and f' the natural projection. □

The preceding corollary makes a rather trivial use of the notion of interpolation system. We will see more interesting examples, arising from algebraic geometry (for which we refer to standard textbooks such as [22]), as follows.

Proposition 2.4. *Let X be an algebraic variety, or more generally an arbitrary scheme over K, and let Σ and Σ' be two closed subschemes of X that are finite over K. Suppose there are two invertible sheaves $\mathcal{L}_1$ and $\mathcal{L}_2$ on X such that:*

(i) the natural restriction map

$$\Gamma(X, \mathcal{L}_1 \otimes \mathcal{L}_2) \longrightarrow \Gamma(\Sigma, \mathcal{L}_1 \otimes \mathcal{L}_2) \tag{39}$$

is injective

(ii) the natural restriction maps

$$\Gamma(X, \mathcal{L}_1) \longrightarrow \Gamma(\Sigma', \mathcal{L}_1) \qquad \Gamma(X, \mathcal{L}_2) \longrightarrow \Gamma(\Sigma', \mathcal{L}_2) \tag{40}$$

are surjective.

Consider the rings $\mathcal{A} = \Gamma(\Sigma, \mathcal{O}_\Sigma)$ *and* $\mathcal{A}' = \Gamma(\Sigma', \mathcal{O}_{\Sigma'})$. *Then*

$$\mu(\mathcal{A}'/K) \leq \mu(\mathcal{A}/K). \tag{41}$$

Moreover, if $\mathcal{L}_1 = \mathcal{L}_2$, *then also* $\mu^{sym}(\mathcal{A}'/K) \leq \mu^{sym}(\mathcal{A}/K)$.

A sufficient criterion for the conditions (i) and (ii) above to hold, hence also for the conclusion (41), *can be expressed in terms of vanishing of certain cohomology groups as follows:*

(i') $h^0(X, \mathcal{I}(\mathcal{L}_1 \otimes \mathcal{L}_2)) = 0$

(ii') $h^1(X, \mathcal{I}'\mathcal{L}_1) = h^1(X, \mathcal{I}'\mathcal{L}_2) = 0$

where $\mathcal{I}$ *and* $\mathcal{I}'$ *are the sheaves of ideals on* X *defining* Σ *and* Σ', *respectively. In fact, (i) and (i') are equivalent, while (ii') only implies (ii) a priori.*

Proof. Remark first that Σ and Σ' are finite over K, hence affine, and the rings $\mathcal{A}$ and $\mathcal{A}'$ are Artinian, and as such they can be written as a finite direct product of local rings. Thus any invertible module over $\mathcal{A}$ or $\mathcal{A}'$, or equivalently any invertible sheaf over Σ or Σ', is free. In particular, we can choose trivializations

$$\Gamma(\Sigma, \mathcal{L}_1) \simeq \Gamma(\Sigma, \mathcal{L}_2) \simeq \mathcal{A} \qquad \Gamma(\Sigma', \mathcal{L}_1) \simeq \Gamma(\Sigma', \mathcal{L}_2) \simeq \mathcal{A}' \tag{42}$$

and from these, deduce, for any integers i_1, i_2, trivializations

$$\Gamma(\Sigma, \mathcal{L}_1^{\otimes i_1} \otimes \mathcal{L}_2^{\otimes i_2}) = \Gamma(\Sigma, \mathcal{L}_1)^{\otimes i_1} \otimes \Gamma(\Sigma, \mathcal{L}_2)^{\otimes i_2} \simeq \mathcal{A} \tag{43}$$

$$\Gamma(\Sigma', \mathcal{L}_1^{\otimes i_1} \otimes \mathcal{L}_2^{\otimes i_2}) = \Gamma(\Sigma', \mathcal{L}_1)^{\otimes i_1} \otimes \Gamma(\Sigma', \mathcal{L}_2)^{\otimes i_2} \simeq \mathcal{A}'. \tag{44}$$

Consider now the bigraded algebra

$$\mathcal{B} = \bigoplus_{i_1, i_2 \geq 0} \Gamma(X, \mathcal{L}_1^{\otimes i_1} \otimes \mathcal{L}_2^{\otimes i_2}). \tag{45}$$

It comes equipped with two morphisms of bigraded algebras

$$\mathcal{B} \longrightarrow \bigoplus_{i_1, i_2 \geq 0} \Gamma(\Sigma, \mathcal{L}_1^{\otimes i_1} \otimes \mathcal{L}_2^{\otimes i_2}) \qquad \mathcal{B} \longrightarrow \bigoplus_{i_1, i_2 \geq 0} \Gamma(\Sigma', \mathcal{L}_1^{\otimes i_1} \otimes \mathcal{L}_2^{\otimes i_2}) \tag{46}$$

defined by the natural restriction maps, and composing with (43) and (44), and then taking the sum, we get

$$f : \mathcal{B} \longrightarrow \mathcal{A} \qquad\qquad f' : \mathcal{B} \longrightarrow \mathcal{A}'. \tag{47}$$

Since (43) and (44) were defined in a compatible way from (42) as i_1, i_2 vary, we see that f and f' are not merely morphisms of vector spaces, they are in fact morphisms of algebras. Now we take

$$E_1 = \mathcal{B}_{1,0} = \Gamma(X, \mathcal{L}_1) \qquad\qquad E_2 = \mathcal{B}_{0,1} = \Gamma(X, \mathcal{L}_2) \tag{48}$$

so

$$E_1 E_2 \subset \mathcal{B}_{1,1} = \Gamma(X, \mathcal{L}_1 \otimes \mathcal{L}_2) \tag{49}$$

and conditions *(i)* and *(ii)* in our hypotheses imply conditions *(i)* and *(ii)* in the definition of interpolation systems. We can now conclude thanks to Proposition 2.2.

To show that *(i)* and *(i')* are equivalent, and that *(ii')* implies *(ii)*, use the long exact sequence in cohomology associated with the short exact sequence

$$0 \longrightarrow \mathcal{J}\mathcal{L} \longrightarrow \mathcal{L} \longrightarrow \mathcal{L}|_{V(\mathcal{J})} \longrightarrow 0 \tag{50}$$

with $\mathcal{J} = \mathcal{I}$ or $\mathcal{I}'$, and $\mathcal{L} = \mathcal{L}_1$, $\mathcal{L}_2$, or $\mathcal{L}_1 \otimes \mathcal{L}_2$. □

Remark that conditions *(i)* and *(ii)*, or *(i')* and *(ii')*, in Proposition 2.4, are very similar to conditions used to estimate the parameters (dimension, distance) of AG codes. Thus, borrowing techniques from this field, one could hope to get good interpolation systems from classes of varieties on which one knows how to construct good codes, for example, algebraic surfaces, or toric varieties.

However up to now, the geometric objects that are best understood from this point of view, especially regarding asymptotic properties, are algebraic curves. Thus interpolation systems constructed from algebraic curves will be studied in the next section.

But before doing that, we give an example of use of the general Proposition 2.4.

Example 2.5. It is well known that $\mathbb{F}_8$ admits a symmetric multiplication algorithm of length 6 over $\mathbb{F}_2$. This is best shown by giving an explicit ad hoc description of this algorithm. It turns out that this construction admits a nice interpretation in terms of interpolation on the projective plane $\mathbb{P}^2$ over $\mathbb{F}_2$.

So let $X = \mathbb{P}^2$, and $\mathcal{L}_1 = \mathcal{L}_2 = \mathcal{O}(1)$ the universal line bundle on it. Let x, y, z be the standard basis of $\Gamma(\mathbb{P}^2, \mathcal{O}(1))$, that is, x, y, z are the usual projective coordinate functions on $\mathbb{P}^2$.

Write $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ with $\alpha^3 = \alpha + 1$, and let Σ' be (the schematic image of) the point with homogeneous coordinates $(1 : \alpha : \alpha^2)$. Hence evaluation at Σ' maps the function $\lambda x + \mu y + \nu z \in \Gamma(\mathbb{P}^2, \mathcal{O}(1))$ to the element $\lambda + \mu\alpha + \nu\alpha^2 \in \mathbb{F}_8$, so the surjectivity condition *(ii)* in Proposition 2.4 is satisfied (with, in fact, bijectivity).

For Σ we choose the union of the six points $(1:0:0)$ $(0:1:0)$ $(0:0:1)$ $(1:1:0)$ $(1:0:1)$ $(0:1:1)$, and remark that evaluation of the basis functions $x^2, y^2, z^2, xy, xz, yz$ of $\Gamma(\mathbb{P}^2, \mathcal{O}(2))$ at these six points gives a triangular unipotent matrix, so the injectivity condition *(i)* is also satisfied (with, in fact, bijectivity).

This is enough to conclude the existence of the algorithm, but in fact, since all proofs are constructive, we can describe it explicitly. Write down the four evaluation maps

$$\begin{array}{lccc} f: & \Gamma(\mathbb{P}^2, \mathcal{O}(1)) =< x, y, z > & \longrightarrow & \Gamma(\Sigma, \mathcal{O}(1)) \simeq (\mathbb{F}_2)^6 \\ f': & \Gamma(\mathbb{P}^2, \mathcal{O}(1)) =< x, y, z > & \longrightarrow & \Gamma(\Sigma', \mathcal{O}(1)) \simeq \mathbb{F}_8 \\ F: & \Gamma(\mathbb{P}^2, \mathcal{O}(2)) =< x^2, y^2, z^2, xy, xz, yz > & \longrightarrow & \Gamma(\Sigma, \mathcal{O}(2)) \simeq (\mathbb{F}_2)^6 \\ F': & \Gamma(\mathbb{P}^2, \mathcal{O}(2)) =< x^2, y^2, z^2, xy, xz, yz > & \longrightarrow & \Gamma(\Sigma', \mathcal{O}(2)) \simeq \mathbb{F}_8 \end{array}$$

where we have just seen that f' and F are bijective. Now the proof of Proposition 2.2 shows that multiplication in $\mathbb{F}_8$ decomposes as

$$\begin{array}{ccc} \mathbb{F}_8 \times \mathbb{F}_8 & \xrightarrow{m_{\mathbb{F}_8}} & \mathbb{F}_8 \\ {\scriptstyle \phi\times\phi}\downarrow & & \uparrow{\scriptstyle w} \\ (\mathbb{F}_2)^6 \times (\mathbb{F}_2)^6 & \xrightarrow{m_{(\mathbb{F}_2)^6}} & (\mathbb{F}_2)^6 \end{array} \tag{51}$$

where $m_{(\mathbb{F}_2)^6}$ is coordinatewise multiplication, and $\phi = f \circ (f')^{-1}$ and $w = F' \circ F^{-1}$ are given in matrix form by

$$\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad w = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{52}$$

relative to the basis $1, \alpha, \alpha^2$ of $\mathbb{F}_8$ and the canonical basis of $(\mathbb{F}_2)^6$, with column vector convention.

Of course there are other ways to interpret this construction, for example, as interpolation on the affine space $\mathbb{A}^3$. However remark that this would not have been possible working with *curves* only (or at least, not in a natural way), because curves over $\mathbb{F}_2$ of sufficiently small genus do not admit enough points for the interpolation to be possible.

Another situation in which Proposition 2.4 could be useful is if one is interested in the bilinear complexity of a local algebra $\mathcal{A}'$ that cannot be written as a quotient of a polynomial algebra in only one variable. Indeed such an algebra cannot be "embedded" in a curve (see the discussion on monogenous local algebras below), hence requires higher-dimensional objects for interpolation.

3 The extended Chudnovsky-Chudnovsky algorithm

From now on, K will be a finite field, say $K = \mathbb{F}_q$. We will only consider algebras that are associative, commutative, and with unity.

In fact we will be particularly interested in the following family of $\mathbb{F}_q$-algebras, and their bilinear complexities:

Definition 3.1. For any integers $m, l \geq 1$ we consider the $\mathbb{F}_q$-algebra of polynomials in one indeterminate with coefficients in $\mathbb{F}_{q^m}$, truncated at order l:

$$\mathcal{A}_q(m,l) = \mathbb{F}_{q^m}[t]/(t^l) \tag{53}$$

of dimension

$$\dim_{\mathbb{F}_q} \mathcal{A}_q(m,l) = ml, \tag{54}$$

and we denote by

$$\mu_q(m,l) = \mu(\mathcal{A}_q(m,l)/\mathbb{F}_q) \tag{55}$$

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

Of special significance are the following two cases: when $l = 1$,

$$\mu_q(m,1) = \mu_q(m) \tag{56}$$

is the bilinear complexity of multiplication in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$; and when $m = 1$,

$$\mu_q(1,l) = \widehat{M}_q(l) \tag{57}$$

is the quantity used in the estimates of [14].

Lemma 3.2. *With the notations above,*

$$\mu_q(m,l) \leq \mu_q(m)\widehat{M}_{q^m}(l). \tag{58}$$

Proof. Direct consequence of Lemma 1.10.b). □

Remark 3.3. As will be shown later, there are examples where this inequality is strict.

We now introduce another class of $\mathbb{F}_q$-algebras, before studying how they relate to the $\mathcal{A}_q(m,l)$:

- We say that a finite-dimensional $\mathbb{F}_q$-algebra A is *monogenous* if it can be written as a quotient of the ring of polynomials in one indeterminate over $\mathbb{F}_q$, say: $A \simeq \mathbb{F}_q[t]/(P(t))$. These are precisely the algebras whose bilinear complexity was first studied in [19, 37].

  Moreover we say that A is *local* if it has only one maximal ideal. Thus, by the Chinese remainder theorem, a monogenous local $\mathbb{F}_q$-algebra is necessarily of the form

  $$A \simeq \mathbb{F}_q[t]/(Q(t)^l) \tag{59}$$

  for some *irreducible* polynomial Q over $\mathbb{F}_q$ and some integer $l \geq 1$.

- More generally, let X be an algebraic curve over $\mathbb{F}_q$ (the situation discussed just above corresponds to the case $X = \mathbb{P}^1$). By a *thickened point* in X we mean any closed subscheme of X supported on a closed point (of arbitrary degree). For example, if Q is a closed point in X, we denote by $\mathcal{I}_Q$ the sheaf of ideals defining it, and for any integer $l \geq 1$ we let $Q^{[l]}$ be the closed subscheme of X defined by the sheaf of ideals $(\mathcal{I}_Q)^l$. Then $Q^{[l]}$ is a thickened point supported on Q. Conversely, any thickened point in X is of this form. Indeed, by convention a curve X is always supposed smooth, hence the local ring $\mathcal{O}_{X,Q}$ of X at Q is principal, and every ideal in this ring is of the form (t_Q^l), where t_Q is a local parameter at Q.

  We remark that such a thickened point is necessarily affine, and we let

$$\mathcal{A}_{Q^{[l]}} = \Gamma(Q^{[l]}, \mathcal{O}_{Q^{[l]}}) = \Gamma(X, \mathcal{O}_X/(\mathcal{I}_Q)^l) = \mathcal{O}_{X,Q}/(t_Q^l) \tag{60}$$

  be its ring of regular functions.

Lemma 3.4. *Any monogenous local $\mathbb{F}_q$-algebra, and more generally the ring of functions of any thickened point on a curve over $\mathbb{F}_q$, is isomorphic to some $\mathcal{A}_q(m,l)$. More precisely:*

- *Let Q be an irreducible polynomial over $\mathbb{F}_q$, of degree $\deg Q = m$, and let $l \geq 1$ be an integer. Then, as $\mathbb{F}_q$-algebras,*

$$\mathbb{F}_q[t]/(Q(t)^l) \simeq \mathcal{A}_q(m,l). \tag{61}$$

- *More generally, let X be a curve over $\mathbb{F}_q$ and Q a closed point in X, of degree $\deg Q = m$, and let $l \geq 1$ be an integer. Then, as $\mathbb{F}_q$-algebras,*

$$\mathcal{A}_{Q^{[l]}} \simeq \mathcal{A}_q(m,l). \tag{62}$$

As a consequence, all these algebras have the same bilinear complexity $\mu_q(m,l)$.

Proof. This is a special case of Cohen's structure theorem for complete local rings in equal characteristic (see e.g. [8] AC IX.30, §3, Th. 2). But for ease of the reader we recall how this works concretely in our specific situation.

Write $\mathcal{A}_{Q^{[l]}} = \mathcal{O}_{X,Q}/(t_Q^l)$, where $\mathcal{O}_{X,Q}$ is the local ring of X at Q, and t_Q a local parameter. We will construct an isomorphism

$$(\mathcal{O}_{X,Q}/t_Q)[t]/(t^l) \xrightarrow{\sim} \mathcal{O}_{X,Q}/(t_Q^l) \tag{63}$$

hence proving the lemma, since $\mathcal{O}_{X,Q}/(t_Q) \simeq \mathbb{F}_{q^m}$.

To do so, first choose any α generating $\mathcal{O}_{X,Q}/(t_Q)$ over $\mathbb{F}_q$, with minimal polynomial F_α, and invoke Hensel's lemma to lift α to $\widetilde{\alpha}$ root of F_α in $\mathcal{O}_{X,Q}/(t_Q^l)$. Sending α to $\widetilde{\alpha}$ then defines a morphism of $\mathbb{F}_q$-algebras

$$\mathcal{O}_{X,Q}/(t_Q) \longrightarrow \mathcal{O}_{X,Q}/(t_Q^l) \tag{64}$$

section of the natural projection $\mathcal{O}_{X,Q}/(t_Q^l) \longrightarrow \mathcal{O}_{X,Q}/(t_Q)$, and to conclude, we extend (64) to (63) by sending t to t_Q. □

If X is an algebraic curve over $\mathbb{F}_q$, and D a divisor on X, we denote by

$$L(D) = \Gamma(X, \mathcal{O}_X(D)) \tag{65}$$

its Riemann-Roch space, and by

$$l(D) = \dim L(D) \tag{66}$$

the dimension (over $\mathbb{F}_q$) of the latter. We also choose a canonical divisor K_X on X and we let

$$i(D) = l(K_X - D) \tag{67}$$

be the *index of specialty* of D. Recall that the Riemann-Roch theorem can then be stated as

$$l(D) - i(D) = \deg D + 1 - g \tag{68}$$

where g is the genus of X.

Theorem 3.5. *Let X be a curve of genus g over $\mathbb{F}_q$, and let $m, l \geq 1$ be two integers. Suppose that X admits a closed point Q of degree $\deg Q = m$. Let G be an effective divisor on X, and write*

$$G = u_1 P_1 + \cdots + u_n P_n \tag{69}$$

where the P_i are pairwise distinct closed points, of degree $\deg P_i = d_i$. Suppose there exist two divisors D_1, D_2 on X such that:

(i) The natural evaluation map

$$L(D_1 + D_2) \longrightarrow \prod_{i=1}^{n} \mathcal{O}_X(D_1 + D_2)|_{P_i^{[u_i]}} \tag{70}$$

is injective.

(ii) The natural evaluation maps

$$L(D_1) \longrightarrow \mathcal{O}_X(D_1)|_{Q^{[l]}} \qquad L(D_2) \longrightarrow \mathcal{O}_X(D_2)|_{Q^{[l]}} \tag{71}$$

are surjective.

Then

$$\mu_q(m, l) \leq \sum_{i=1}^{n} \mu_q(d_i, u_i). \tag{72}$$

In fact we also have $\mu_q(m, l) \leq \mu(\prod_{i=1}^{n} \mathcal{A}_q(d_i, u_i)/\mathbb{F}_q)$. Moreover, if $D_1 = D_2$, all these inequalities also hold for the symmetric bilinear complexity μ^{sym}.

Sufficient numerical criteria for the hypotheses above to hold can be given as follows. A sufficient condition for the existence of Q of degree m on X is that $2g + 1 \leq q^{(m-1)/2}(q^{1/2} - 1)$, while sufficient conditions for (i) and (ii) are:

(i') *The divisor $D_1 + D_2 - G$ is zero-dimensional:*

$$l(D_1 + D_2 - G) = 0. \tag{73}$$

(ii') *The divisors $D_1 - lQ$ and $D_2 - lQ$ are non-special:*

$$i(D_1 - lQ) = i(D_2 - lQ) = 0. \tag{74}$$

More precisely, (i) and (i') are equivalent, while (ii') only implies (ii) a priori.

Proof. Use Proposition 2.4 with $\Sigma = P_1^{[u_1]} \cup \cdots \cup P_n^{[u_n]}$, $\Sigma' = Q^{[l]}$, and $\mathcal{L}_1 = \mathcal{O}_X(D_1)$ and $\mathcal{L}_2 = \mathcal{O}_X(D_2)$. Combined with Lemma 3.4 this gives

$$\mu_q(m,l) \leq \mu(\prod_{i=1}^{n} \mathcal{A}_q(d_i,u_i)/\mathbb{F}_q) \tag{75}$$

as claimed. One can then apply Lemma 1.10.c) to get (72) (whether we lose in passing from (75) to (72) depends on the direct sum conjecture (33)).

As for the numerical sufficient condition stated here for the existence of Q, it can be found in [32], Cor. V.2.10.(c). □

Remark 3.6. For applications it might be useful to make things more explicit, so we describe in more concrete terms how the various geometric data in Theorem 3.5 lead to an interpolation system as in Definition 2.1. The key point is to describe the evaluation maps, which can be done in relatively elementary terms when X is a curve. For example we describe the composite map

$$L(D_1) \longrightarrow \mathcal{O}_X(D_1)|_{Q^{[l]}} \xrightarrow{\sim} \mathcal{A}_q(m,l). \tag{76}$$

As a first step, we choose a local parameter t_Q at Q. Then $t_Q^{v_Q(D_1)}$ is a local generator for $\mathcal{O}_X(D_1)$ at Q, and we use this local generator to define a trivialization $\mathcal{O}_X(D_1)|_{Q^{[l]}} \simeq \mathcal{O}_X|_{Q^{[l]}} = \mathcal{O}_{X,Q}/(t_Q^l)$ as asked in (42). Thus we get a map

$$\begin{array}{ccc} L(D_1) & \longrightarrow & \mathcal{O}_{X,Q}/(t_Q^{\,l}) \\ f & \mapsto & t_Q^{-v_Q(D_1)} f \mod (t_Q^{\,l}) \end{array} \tag{77}$$

and we compose this with the isomorphism $\mathcal{O}_{X,Q}/(t_Q^l) \xrightarrow{\sim} (\mathcal{O}_{X,Q}/(t_Q))[t]/(t^l) \simeq \mathcal{A}_q(m,l)$ given in Lemma 3.4 (and explicited in its proof) to conclude.

The other maps $L(D_2) \longrightarrow \mathcal{A}_q(m,l)$ and $L(D_1 + D_2) \longrightarrow \prod_{i=1}^n \mathcal{A}_q(d_i,u_i)$ are described in the same way.

A nice property of these evaluation maps, as is best seen from (77), is that they do not need the points at which we evaluate to be disjoint from the support of the divisor (although this is not a crucial point of the construction, since this situation can also be avoided thanks to the strong approximation theorem).

Remark 3.7. This Theorem 3.5 encompasses essentially all presently known variants of the Chudnovsky-Chudnovsky interpolation method as special cases. For example, restricting to $l = 1$ and $D_1 = D_2$, and using Lemma 3.2, gives Th. 3.1 of [14] (if one further restricts to all $d_i = u_i = 1$, this gives the original version of Chudnovsky-Chudnovsky [17]). Thus one can say that Theorem 3.5 improves the method of [14] in at least two points:

- Allowing asymmetry ($D_1 \neq D_2$) makes conditions *(i)* and *(ii)*, or *(i')* and *(ii')*, easier to satisfy than their counterparts in [14]; in turn this allows more flexibility in the choice of the curve X and the divisor G.
- The use of $\mu_q(d,u)$ in the right-hand side of (72), instead of $\mu_q(d)\widehat{M}_{q^d}(u)$ as in [14], leads to stronger estimates. Of course, for this to be useful, one needs upper bounds on these $\mu_q(d,u)$ that are better than the one given in Lemma 3.2. But a nice feature of (72) is that this same quantity $\mu_q(m,l)$ also appears in the left-hand side, so we can try to get these upper bounds from Theorem 3.5 itself, in a sort of recursive procedure.

These points will be illustrated in the following three sections.

4 Genus 0 or 1

The main motivation for this section is the following:

Question 4.1. What is the actual value of $\mu_q(m,l)$ for small q, m, l? Or at least, find upper bounds that are better than the one given in Lemma 3.2.

Answering this question can lead to improved bounds also for high values of the parameters. For example, suppose that in Theorem 3.5 we take $l = 1$ and the divisor G consists of:

- N_1 points of degree 1, of which l_1 with multiplicity 2 and the remaining $N_1 - l_1$ with multiplicity 1
- N_2 points of degree 2, of which l_2 with multiplicity 2 and the remaining $N_2 - l_2$ with multiplicity 1
- N_4 points of degree 4, of which l_4 with multiplicity 2 and the remaining $N_4 - l_4$ with multiplicity 1.

Then (72) gives

$$\mu_q(m) \leq N_1 + 2l_1 + 3N_2 + (\mu_q(2,2) - 3)l_2 + \mu_q(4)N_4 + (\mu_q(4,2) - \mu_q(4))l_4. \quad (78)$$

Provided $\mu_q(2,2) < 9$ or $\mu_q(4,2) < 3\mu_q(4)$, this improves the bound in Prop. 3.1 of [5]. Such bounds on $\mu_q(2,2)$ or $\mu_q(4,2)$ will be given in Examples 4.4 and 4.5 and Lemma 4.6 below.

Proposition 4.2. *Let $m, l \geq 1$ be two integers with*

$$ml \leq \frac{q}{2} + 1. \tag{79}$$

Then

$$\mu_q(m,l) \leq \mu_q^{sym}(m,l) \leq 2ml - 1. \tag{80}$$

More generally let G be an effective divisor on $\mathbb{P}^1$, and write

$$G = u_1 P_1 + \cdots + u_n P_n \tag{81}$$

where the P_i are pairwise distinct closed points, of degree $\deg P_i = d_i$. Suppose

$$\deg G = \sum_{i=1}^{n} d_i u_i \geq 2ml - 1. \tag{82}$$

Then

$$\mu_q(m,l) \leq \sum_{i=1}^{n} \mu_q(d_i, u_i) \tag{83}$$

and likewise $\mu_q^{sym}(m,l) \leq \sum_{i=1}^{n} \mu_q^{sym}(d_i, u_i)$.

Proof. Remark that the first assertion is a particular case of the second, because if $n = 2ml - 1 \leq q + 1$, we can find n distinct points of degree 1 on $\mathbb{P}^1$ and let G be their sum. Recall also that $\mathbb{P}^1$ admits points of any degree, and that any divisor of degree -1 on $\mathbb{P}^1$ is both zero-dimensional and non-special. So, to conclude, let D be any divisor of degree $ml - 1$ on $\mathbb{P}^1$, and apply Theorem 3.5 with $D_1 = D_2 = D$. □

Recall that an elliptic curve over $\mathbb{F}_q$ is a curve X of genus 1 with a chosen point $P_\infty \in X(\mathbb{F}_q)$. This set $X(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of X, or equivalently, of closed points of degree 1, then admits a structure of abelian group with identity element P_∞. Also, given such an elliptic curve, there is a map

$$\sigma : \mathrm{Div}(X) \longrightarrow X(\mathbb{F}_q) \tag{84}$$

uniquely defined by the condition that each divisor D of degree d is linearly equivalent to the divisor $\sigma(D) + (d-1)P_\infty$. This map σ is a group morphism, it passes to linear equivalence, and induces an isomorphism of the degree 0 class group $\mathrm{Cl}^0(X)$ with $X(\mathbb{F}_q)$. We now generalize a result of Shokrollahi [30] and Chaumine [15]:

Proposition 4.3. *Let X be an elliptic curve over $\mathbb{F}_q$, with all notations as above. Let $m, l \geq 1$ be two integers. Suppose that X admits a closed point Q of degree $\deg Q = m$. Let G be an effective divisor on X, and write*

$$G = u_1 P_1 + \cdots + u_n P_n \tag{85}$$

where the P_i are pairwise distinct closed points, of degree $\deg P_i = d_i$*, so* $\deg G = \sum_{i=1}^n d_i u_i$*. Then*

$$\mu_q(m,l) \leq \sum_{i=1}^{n} \mu_q(d_i, u_i) \tag{86}$$

provided one of the following conditions is satisfied:

a) $\deg G = 2ml$ *and* $|X(\mathbb{F}_q)| \geq 3$

b) $\deg G = 2ml$ *and* $|X(\mathbb{F}_q)| \geq 2$*, and either* $\sigma(G) \neq P_\infty$ *or* $X(\mathbb{F}_q)$ *is not entirely of 2-torsion (or both)*

c) $\deg G \geq 2ml + 1$ *and* $|X(\mathbb{F}_q)| \geq 2$

d) $\deg G \geq 2ml + 3$.

Moreover in cases b), c), or d), one also has $\mu_q^{sym}(m,l) \leq \sum_{i=1}^n \mu_q^{sym}(d_i, u_i)$.

Proof. Recall that a divisor of degree 0 on X is both zero-dimensional and non-special, unless it is linearly equivalent to zero.

Suppose first we're in case a), so $X(\mathbb{F}_q) \simeq \mathrm{Cl}^0(X)$ has order at least 3. This implies that there are two divisors Z and Z' of degree 0 on X that are not linearly equivalent nor linearly equivalent to zero. Let then $D_1 = lQ + Z$, and let $D_2 = lQ+Z$ or $lQ+Z'$, depending on whether $D_1+D_2-G = 2lQ+2Z-G$ or $2lQ + Z + Z' - G$ is not linearly equivalent to zero. With this choice, conditions *(i')* and *(ii')* in Theorem 3.5 are satisfied, and the conclusion follows.

Suppose now we're in case b). Suppose first that $X(\mathbb{F}_q) \simeq \mathrm{Cl}^0(X)$ is not entirely of 2-torsion. Then there are two divisors Z and Z' of degree 0 not linearly equivalent to zero, and such that $2Z$ and $2Z'$ are not linearly equivalent. Let then $D_1 = D_2 = lQ + Z$ or $D_1 = D_2 = lQ + Z'$, depending on whether $D_1 + D_2 - G = 2lQ + 2Z - G$ or $2lQ + 2Z' - G$ is not linearly equivalent to zero. With this choice, conditions *(i')* and *(ii')* are satisfied again. On the other hand, suppose $X(\mathbb{F}_q) \simeq \mathrm{Cl}^0(X)$ is entirely of 2-torsion, so that $\sigma(G) \neq P_\infty$ by our hypothesis. Let Z be a divisor of degree 0 not linearly equivalent to zero (it exists since $|X(\mathbb{F}_q)| \geq 2$) and take $D_1 = D_2 = lQ + Z$, so condition *(ii')* is satisfied. Then $\sigma(D_1+D_2-G) = \sigma(G) \neq P_\infty$ and condition *(i')* is also satisfied.

Case c) works likewise: let Z be a divisor of degree 0 not linearly equivalent to zero and take $D_1 = D_2 = lQ+Z$, so condition *(ii')* is satisfied, while condition *(i')* is also satisfied for degree reasons.

In case d), we take $D_1 = D_2 = (ml + 1)P_\infty$. Then conditions *(i')* and *(ii')* are satisfied for degree reasons.

Last, remark that except perhaps in case a), we always took $D_1 = D_2$ in the proof, so that the estimates then also work for the symmetric bilinear complexity μ^{sym}. □

Example 4.4. Proposition 4.2 gives

$$\mu_q(2,2) \leq 7 \qquad \text{for } q \geq 7 \tag{87}$$

and Proposition 4.3 gives

$$\mu_q(2,2) \leq 8 \qquad \text{for } q = 4 \text{ or } 5. \tag{88}$$

Indeed, recall that the number of points of degree 1 on an elliptic curve X over $\mathbb{F}_q$ can be written as $|X(\mathbb{F}_q)| = q + 1 - t$ for some integer t, the *trace* of X, satisfying $|t| \leq 2\sqrt{q}$. Conversely, Honda-Tate theory gives additional sufficient and necessary conditions on t for a curve having this number of points to exist ([36], Th. 4.1). The trace t then also determines the number of points on X of any degree. For example, we have $|X(\mathbb{F}_{q^2})| = (q+1)^2 - t^2$, hence X has $\frac{1}{2}(|X(\mathbb{F}_{q^2})| - |X(\mathbb{F}_q)|) = \frac{(q+1-t)(q+t)}{2}$ points of degree 2 (and likewise, $\frac{((q+1)^2-t^2)(q^2-2q+t^2)}{4}$ points of degree 4, we will use it in the next example).

Using this machinery, we see that for $q = 4$ or 5 there exists an elliptic curve over $\mathbb{F}_q$ with eight points of degree 1 (and at least one point of degree 2), so in Proposition 4.3 we can take as G all these points of degree 1, each with multiplicity 1.

Unfortunately it seems difficult to improve the bound $\mu_q(2,2) \leq 9$ for $q = 2$ or 3, at least with this generic method. Whether this is the exact value is yet unsettled.

Example 4.5. Proposition 4.2 gives

$$\mu_q(4,2) \leq 15 \qquad \text{for } q \geq 16 \tag{89}$$

and Proposition 4.3 gives

$$\mu_q(4,2) \leq 16 \qquad \text{for } q = 9,\ 11,\ \text{or } 13 \tag{90}$$

$$\mu_8(4,2) \leq 17 \qquad \mu_7(4,2) \leq 18 \qquad \mu_5(4,2) \leq 19 \tag{91}$$

$$\mu_4(4,2) \leq 20 \qquad \mu_3(4,2) \leq 23 \qquad \mu_2(4,2) \leq 26. \tag{92}$$

The proof of these bounds follows the same lines as in the previous example.

For $q = 9$, 11, or 13, there is an elliptic curve over $\mathbb{F}_q$ with 16 points of degree 1 (and at least one point of degree 4), so in Proposition 4.3 we can take as G all these points of degree 1, each with multiplicity 1.

For $q = 8$ we can choose the trace $t = -5$, and G consists of 14 points of degree 1 and 1 point of degree 2, all with multiplicity 1.

For $q = 7$ we choose $t = -5$, and G consists of 12 points of degree 1 and 2 points of degree 2, all with multiplicity 1.

For $q = 5$ we choose $t = -4$, and G consists of 10 points of degree 1 and 3 points of degree 2, all with multiplicity 1.

For $q = 4$ we choose $t = -3$, and G consists of 8 points of degree 1 and 4 points of degree 2, all with multiplicity 1.

For $q = 3$ we choose $t = -2$, and G consists of 2 points of degree 1 with multiplicity 1, 4 points of degree 1 with multiplicity 2, and 3 points of degree 2 with multiplicity 1.

For $q = 2$ we choose $t = -1$, and G consists of 4 points of degree 1 with multiplicity 3, and 2 points of degree 2 with multiplicity 1.

Remark that all these bounds already improve the one given by Lemma 3.2 (at least given the best upper bounds on $\mu_q(4)$ known up to now). However, for small q it is possible to do even better as follows.

Lemma 4.6. *Suppose m is not prime, and write $m = de$ for some integers $d, e \geq 2$. Then*

$$\mu_q(m, l) \leq \mu_q(d)\mu_{q^d}(e, l) \tag{93}$$

(and likewise $\mu_q^{sym}(m, l) \leq \mu_q^{sym}(d)\mu_{q^d}^{sym}(e, l)$). In particular:

$$\mu_3(4, 2) \leq \mu_3(2)\mu_9(2, 2) \leq 21, \qquad \mu_2(4, 2) \leq \mu_2(2)\mu_4(2, 2) \leq 24. \tag{94}$$

Proof. Direct consequence of Lemma 1.10.b), noting that $\mathcal{A}_q(m, l)$ can be considered as an algebra over $\mathbb{F}_{q^d}$, and as such can be identified with $\mathcal{A}_{q^d}(e, l)$. □

We do not claim these new upper bounds to be optimal. Any further improvement (as well as lower bounds, on the other side) would be of interest.

Example 4.7. In [14], section 5, Cenk and Özbudak give upper bounds on $\mu_2(163)$ and $\mu_3(97)$. However there is an error in their proof of the first, and the second would need a slight extra justification.

The origin of the error is in their Th. 3.6, which, as stated, is false. Condition (1) in this Th. 3.6 asks for the existence of a non-special divisor of degree $n + g - 1$ (instead of $g - 1$ as in their Th. 3.2 or Cor. 3.5) in order for their evaluation map Ev_Q to be surjective. However this condition is not sufficient, as illustrated as follows.

To give an upper bound on $\mu_2(163)$, the authors of [14] introduce the elliptic curve $y^2 + y = x^3 + x + 1$ over $\mathbb{F}_2$, which has only one point of degree 1, which means that its class group Cl^0 is trivial. They take a point Q of degree 163 on this curve, and a non-special divisor D of degree 163 disjoint from Q. They need their map $Ev_Q : L(D) \longrightarrow \mathcal{O}_Q/Q$ to be surjective (which the proof of their Th. 3.6 claims). However, this map fits in the long exact sequence

$$0 \longrightarrow L(D - Q) \longrightarrow L(D) \longrightarrow \mathcal{O}_Q/Q \longrightarrow \ldots \tag{95}$$

and since $D - Q$ has degree 0, and the curve has trivial class group, we have $D - Q \sim 0$ and $l(D - Q) = 1$. This means that Ev_Q is non-injective, and since $L(D)$ and $\mathcal{O}_Q/Q$ have the same dimension (namely 163), Ev_Q is non-surjective as well.

To fix this error, we can use our Proposition 4.3 instead. We use the same curve as in [14], but since this curve has only one point of degree 1, we need case d) of the proposition, and the divisor G has to be modified accordingly: we take the only point of degree 1 with multiplicity 5, and then we take all 2 points of degree 2, all 4 points of degree 3, all 5 points of degree 4, all 8 points of

degree 5, all 8 points of degree 6, all 25 points of degree 8, all with multiplicity 1. Then G has degree

$$\deg G = 1\cdot 5 + 2\cdot 2 + 4\cdot 3 + 5\cdot 4 + 8\cdot 5 + 8\cdot 6 + 25\cdot 8 = 329 = 2\cdot 163 + 3 \quad (96)$$

and Proposition 4.3.d) gives

$$\begin{aligned}\mu_2(163) \leq \mu_2(1,5) + 2\mu_2(2) + 4\mu_2(3) + 5\mu_2(4) + \\ + 8\mu_2(5) + 8\mu_2(6) + 25\mu_2(8) \leq 910.\end{aligned} \quad (97)$$

See [14], Table 1, for the numerical details. Remark they give the upper bound $\mu_2(7) \leq 22$, with the quotient $22/7$ being the highest among similar estimates up to degree 8. This is why we didn't use points of degree 7 in our G, and explains why our upper bound 910 is better than the upper bound 916 in [14], despite our G having higher degree. This said, perhaps further optimizations of this sort are possible.

Concerning the upper bound $\mu_3(97) \leq 426$, Cenk and Özbudak use the curve $y^2 = x^3 + x^2 + 2x + 1$ over $\mathbb{F}_3$. This curve has 3 points of degree 1, hence its Cl^0 is non-trivial, so the error in Condition (1) of their Th. 3.6 is not harmful. However for their upper bound to be fully justified they also need to explain why their application ϕ is injective, which they do not. But here again we can use Proposition 4.3 (case a) instead, with the same curve and the same divisor G as theirs. This gives the same bound $\mu_3(97) \leq 426$, without needing any extra justification.

5 Fixing some bounds of Ballet

For any curve X over $\mathbb{F}_q$, we denote by $B_d(X/\mathbb{F}_q)$ the number of closed points of degree d on X, so that, for all n,

$$|X(\mathbb{F}_{q^n})| = \sum_{d|n} dB_d(X/\mathbb{F}_q). \quad (98)$$

We now want to apply Theorem 3.5 with curves of higher genus, as well as give easy verifiable criteria for the existence of divisors D_1, D_2 satisfying conditions *(i)* and *(ii)*, or *(i')* and *(ii')*, in this theorem. For example, we can do so as these conditions be satisfied for degree reasons:

Proposition 5.1. *Let X be a curve of genus g over $\mathbb{F}_q$, and let $m, l \geq 1$ be two integers.*

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

Suppose also that X admits a non-special divisor S, of degree $g + e - 1$, for an integer e as small as possible (hence $e \leq g$ by the Riemann-Roch theorem).

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,

$$n_d = \sum_u n_{d,u} \leq B_d(X/\mathbb{F}_q). \quad (99)$$

Then, provided

$$\sum_{d,u} n_{d,u} du \geq 2ml + 2e + 2g - 1 \tag{100}$$

we have

$$\mu_q(m,l) \leq \sum_{d,u} n_{d,u} \mu_q(d,u) \tag{101}$$

and likewise

$$\mu_q^{sym}(m,l) \leq \sum_{d,u} n_{d,u} \mu_q^{sym}(d,u). \tag{102}$$

Proof. For $1 \leq j \leq n_{d,u}$ choose a point $P_{d,u,j}$ of degree d in X, such that $P_{d,u,j} \neq P_{d,u',j'}$ if $(u,j) \neq (u',j')$. This is possible by (99). Let then $G = \sum_{d,u} \sum_{1 \leq j \leq n_{d,u}} u P_{d,u,j}$, so that $\deg G = \sum_{d,u} n_{d,u} du$. Let also $D = D_1 = D_2 = S + lQ$, so $D - lQ$ is non-special, and $2D - G$ has negative degree by (100). Hence conditions *(i')* and *(ii')* in Theorem 3.5 are satisfied and we can conclude. □

In order to use this proposition one needs good upper bounds on e. For results of this type, see for example [3] or [6]. In many cases it is possible to take $e = 0$. However under some mild hypothesis on q or X, it is possible to do substantially better, namely we can gain an additional constant g in (100). For this to be possible, one needs to replace the degree argument in the proof with a finer method ensuring that conditions *(i')* and *(ii')* are still satisfied for some divisors D_1, D_2 of appropriate degree. Having allowed asymmetry in our interpolation system will make this easier. In fact we will give two different methods achieving this. The first one will show the existence of D_1, D_2 using a cardinality argument. The second one will be more constructive, and works also in a symmetric setting, although only under more restrictive conditions.

Theorem 5.2. *Let X be a curve of genus g over $\mathbb{F}_q$, and let $m, l \geq 1$ be two integers.*

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,

$$n_d = \sum_u n_{d,u} \leq B_d(X/\mathbb{F}_q). \tag{103}$$

Suppose also

$$\sum_{d,u} n_{d,u} du \geq 2ml + g - 1. \tag{104}$$

Then:

a) If $q > 5$, we have

$$\mu_q(m,l) \leq \sum_{d,u} n_{d,u} \mu_q(d,u). \tag{105}$$

b) If $|X(\mathbb{F}_q)| > 2g$, we have

$$\mu_q(m,l) \leq \sum_{d,u} n_{d,u}\mu_q(d,u). \tag{106}$$

Moreover, suppose X and Q are given explicitly, that $2g+1$ points of degree 1 on X are given explicitly, and, for any d, that n_d points of degree d on X are given explicitly. Suppose also that for each d,u such that $n_{d,u} > 0$, we are given explicitly a multiplication algorithm of length $l_{d,u}$ for $\mathcal{A}_q(d,u)$. Then, after at most $3g^2$ computations of Riemann-Roch spaces on X, we can construct explicitly a multiplication algorithm of length $\sum_{d,u} n_{d,u}l_{d,u}$ for $\mathcal{A}_q(m,l)$.

c) If $|X(\mathbb{F}_q)| > 5g$, we have

$$\mu_q^{sym}(m,l) \leq \sum_{d,u} n_{d,u}\mu_q^{sym}(d,u). \tag{107}$$

Moreover, suppose X and Q are given explicitly, that $5g+1$ points of degree 1 on X are given explicitly, and, for any d, that n_d points of degree d on X are given explicitly. Suppose also that for each d,u such that $n_{d,u} > 0$, we are given explicitly a symmetric multiplication algorithm of length $l_{d,u}$ for $\mathcal{A}_q(d,u)$. Then, after at most $5g^2$ computations of Riemann-Roch spaces on X, we can construct explicitly a symmetric multiplication algorithm of length $\sum_{d,u} n_{d,u}l_{d,u}$ for $\mathcal{A}_q(m,l)$.

Proof. For $1 \leq j \leq n_{d,u}$ choose a point $P_{d,u,j}$ of degree d in X, such that $P_{d,u,j} \neq P_{d,u',j'}$ if $(u,j) \neq (u',j')$. This is possible by (99) (moreover, in cases b) and c), these $P_{d,u,j}$ are chosen among the n_d points of degree d given explicitly). Let then $G = \sum_{d,u}\sum_{1\leq j\leq n_{d,u}} uP_{d,u,j}$, so that $\deg G = \sum_{d,u} n_{d,u}du$.

Proof of case a). We suppose $q > 5$, and we can also suppose $g \geq 2$, otherwise the conclusion follows from the results of the previous section. Let $h = |\operatorname{Cl}^0(X)|$ be the class number of X. Then we also have $h = |\operatorname{Cl}^i(X)|$ for any integer i, where $\operatorname{Cl}^i(X)$ is the set of linear equivalence classes of divisors of degree i on X. Let also

$$\operatorname{Cl}^i_{\text{eff}}(X) \subset \operatorname{Cl}^i(X) \tag{108}$$

be the set of linear equivalence classes of effective divisors of degree i on X, or equivalently, the set of linear equivalence classes of divisors D of degree i on X such that $l(D) > 0$. We then recall from [26], eq. (6), that if A_i is the number of effective divisors on X, then

$$A_{g-1} + 2\sum_{i=0}^{g-2} q^{(g-i-1)/2}A_i \leq \frac{h}{(q^{1/2}-1)^2} \tag{109}$$

hence for any $i \leq g-1$

$$|\operatorname{Cl}^i_{\text{eff}}(X)| \leq A_i \leq \frac{h}{(q^{1/2}-1)^2} < \frac{h}{2} \tag{110}$$

(see also [1], Lemma 2.1, and [6], Th. 3.3). We now let

$$t = ml + g - 1 \tag{111}$$

and we claim that we can find divisors D_1, D_2 of degree t such that:

(i') $D_1 + D_2 - G$ is zero-dimensional

(ii'_1) $D_1 - lQ$ is non-special

(ii'_2) $D_2 - lQ$ is non-special.

Indeed, (ii'_1) means that the linear equivalence class $[D_1 - lQ]$ is not in $\mathrm{Cl}^{g-1}_{\mathrm{eff}}(X)$, or equivalently,

$$[D_1] \notin \mathrm{Cl}^{g-1}_{\mathrm{eff}}(X) + [lQ]. \tag{112}$$

But since translation by $[lQ]$ puts $\mathrm{Cl}^{g-1}(X)$ in bijection with $\mathrm{Cl}^t(X)$, applying (110) shows the translate $\mathrm{Cl}^{g-1}_{\mathrm{eff}}(X) + [lQ]$ cannot cover all $\mathrm{Cl}^t(X)$, hence we can find D_1 as wished. Now, this D_1 being fixed, (i') and (ii'_2) together mean

$$[D_2] \ \notin \ (\mathrm{Cl}^{2t-\deg G}_{\mathrm{eff}}(X) + [G - D_1]) \cup (\mathrm{Cl}^{g-1}_{\mathrm{eff}}(X) + [lQ]), \tag{113}$$

where $2t - \deg G \leq g-1$ by (104). But again (110) shows that the union of these translates has cardinality less than $h/2 + h/2$, and we can find D_2 as wished. All this done we can now apply Theorem 3.5 and conclude.

Proof of case b). Suppose we are given a set $\mathcal{S} = \{P_0, P_1, \ldots, P_{2g}\}$ of $2g+1$ points of degree 1 on X. As in case a), all we need is to construct divisors D_1, D_2 of degree t satisfying (i'), (ii'_1), (ii'_2), and apply Theorem 3.5 to conclude. From [28], Lemma 6, we recall the following:

If A is a divisor on X with $\deg A \leq g-2$ and $l(A) = 0$, there are at most g points $P \in X(\mathbb{F}_q)$ such that $l(A+P) > 0$. (114)

For $-1 \leq i \leq g-1$ we construct a divisor Y_i on X of degree $ml + i$ such that $l(Y_i - lQ) = 0$ iteratively as follows:

- Start with $Y_{-1} = (ml-1)P_0$, so $l(Y_{-1} - lQ) = 0$ for degree reasons.
- Suppose up to some $i < g-1$ we have found Y_i such that $l(Y_i - lQ) = 0$ as wished. Then by (114) there exists $P \in \mathcal{S}$ such that $l(Y_i + P - lQ) = 0$. We put $Y_{i+1} = Y_i + P$.
- This ends when $i = g-1$.

We can then put $D_1 = Y_{g-1}$, so that (ii'_1) is satisfied.

Now for $-1 \leq i \leq g-1$ we construct a divisor Z_i on X of degree $ml+i$ such that $l(Z_i - lQ) = 0$ and $l(D_1 + Z_i - G) = 0$ iteratively as follows:

- Start with $Z_{-1} = (ml-1)P_0$, so $l(Z_{-1} - lQ) = 0$ and $l(D_1 + Z_{-1} - G) = 0$ for degree reasons (via hypothesis (104) for the second).

- Suppose up to some $i < g-1$ we have found Z_i such that $l(Z_i - lQ) = 0$ and $l(D_1 + Z_i - G) = 0$ as wished. We claim there is a point $P \in \mathcal{S}$ such that $l(Z_i + P - lQ) = 0$ and $l(D_1 + Z_i + P - G) = 0$. Indeed by (114) the first can fail at most g times, and likewise the second can fail at most g times. We then put $Z_{i+1} = Z_i + P$.

- This ends when $i = g-1$.

We can then put $D_2 = Z_{g-1}$, so that (i') and (ii'_2) are satisfied, and we're done.

Proof of case c). Suppose we are given a set $\mathcal{T} = \{P_0, P_1, \ldots, P_{5g}\}$ of $5g+1$ points of degree 1 on X. From [28], Lemma 9, we recall the following:

If A is a divisor on X with $\deg A \leq g-3$ and $l(A) = 0$, there are at most $4g$ points $P \in X(\mathbb{F}_q)$ such that $l(A + 2P) > 0$. (115)

Then for $-1 \leq i \leq g-1$ we construct a divisor T_i on X of degree $ml + i$ such that $l(T_i - lQ) = 0$ and $l(2T_i - G) = 0$ iteratively as follows:

- Start with $T_{-1} = (ml-1)P_0$, so $l(T_{-1} - lQ) = 0$ and $l(2T_{-1} - G) = 0$ for degree reasons (via hypothesis (104) for the second).

- Suppose up to some $i < g-1$ we have found T_i such that $l(T_i - lQ) = 0$ and $l(2T_i - G) = 0$ as wished. We claim there is a point $P \in \mathcal{T}$ such that $l(T_i + P - lQ) = 0$ and $l(2T_i + 2P - G) = 0$. Indeed by (114) the first can fail at most g times, and by (115) the second can fail at most $4g$ times. We then put $T_{i+1} = T_i + P$.

- This ends when $i = g-1$.

We can then put $D_1 = D_2 = T_{g-1}$ and conclude by Theorem 3.5 again. □

Remark 5.3. As explained in the Introduction, this Theorem 5.2 fixes an error in an article of Ballet. More precisely, if we take $l = 1$, and we choose all $n_{d,u}$ equal to zero except for $n_{1,1}$, then case a) of Theorem 5.2 gives statement (1) in Th. 2.1 of [1] as a special case; and likewise if we choose all $n_{d,u}$ equal to zero except for $n_{1,1}$ and $n_{2,1}$, we get its statement (2).

Remark that our proof of case a) is structurally the same as Ballet's. The only difference is that we allowed the asymmetry $D_1 \neq D_2$, so D_1 and D_2 could be constructed one at a time, and in establishing (112) and (113) we only had to consider translations $[D] \mapsto [D] - [A]$ which put $\mathrm{Cl}^*(X)$ in bijection with $\mathrm{Cl}^{*-\deg A}(X)$. On the other hand Ballet had to consider a map of the form $[D] \mapsto 2[D] - [G]$ which might be non-injective. The error in Ballet's [1], Prop. 2.1, is that he did not take the possible kernel of this multiplication-by-2 map (that is, the 2-torsion in the class group) into account. As explained in the Introduction, this error was in fact borrowed from [31], and was first spotted by Cascudo-Cramer-Xing (see [11], Chapter 12).

Remark also that case c) of Theorem 5.2 gives another way of fixing this error, while keeping symmetry. A drawback is that the condition $X(\mathbb{F}_q) > 5g$

in case c) imposes serious restrictions on the curves to be used, hence for some values of q, it does not lead to interesting bounds.

So, for applications, case a) is often more suitable, and indeed it allows us to fix the proof of further bounds of Ballet that were jeopardized by the error in his Th. 2.1:

Corollary 5.4. *Let p be a prime number and $q = p^r$ a power of p, with $q > 5$. Then for all integer $n \geq 1$ we have*

$$\frac{1}{n}\mu_q(n) \leq \begin{cases} 3\left(1+\frac{2}{p-2}\right) & \text{if } r = 1 \\ 2\left(1+\frac{2}{\sqrt{q}-2}\right) & \text{if } r = 2 \\ 3\left(1+\frac{p}{q-2}\right) & \text{if } r \geq 3 \text{ odd.} \end{cases} \tag{116}$$

Proof. Use Theorem 5.2 instead of Th. 2.1 of [1], in the proof of the corresponding cases of Th. 3.1 of [1] and Th. 2.1 and 2.2 of [2].

More precisely, Theorem 5.2 with $l = 1$, $m = n$, $n_{1,1} = B_1(X/\mathbb{F}_q)$, and the other $n_{d,u} = 0$, replaces Th. 2.1.(1) of [1]. While Theorem 5.2 with $l = 1$, $m = n$, $n_{1,1} = B_1(X/\mathbb{F}_q)$, $n_{2,1} = B_2(X/\mathbb{F}_q)$, and the other $n_{d,u} = 0$, replaces Th. 2.1.(2) of [1]. □

Remark 5.5. There is a case of Th. 3.1 of [1] that we didn't include in our Corollary. Namely, Th. 3.1 of [1] claims that the bound $\frac{1}{n}\mu_q(n) \leq 2\left(1+\frac{2}{\sqrt{q}-2}\right)$ holds for all r even, not only for $r = 2$. The reason for this omission is that there is another error in the proof of this Th. 3.1 of Ballet, apart from the oversight of the 2-torsion already mentioned.

Indeed in his proof Ballet considers two consecutive prime numbers l_1 and l_2 determined by n and he claims that he can apply his Prop. 3.1.(2) to this l_2. However this Prop. 3.1.(2) only states that *there exists* a prime number l for which its conclusion holds, not that it holds *for all* prime numbers. Looking more closely at the proof, we see it works for primes l for which certain points split completely in a certain morphism of curves, which in turn can be translated as the primes l lying in a certain arithmetic progression. However there is no reason that l_2 should be in this arithmetic progression, except in the case $r = 2$ where it is trivial.

On the other hand, it is easy to see that this bound, and even a slightly stronger one, holds at least asymptotically (if not for all n), as will be seen with our fix of the Shparlinski-Tsfasman-Vladut bound below.

To end this section, we want to show how the condition $q > 5$ in Theorem 5.2.a) can be relaxed, at the cost of only weakening condition (104) by a small absolute constant, independent of g. For this we will use a generalization of (110), that might also be seen as a variant of [6], Th. 3.3 and Cor. 3.4.

Lemma 5.6. *Let X be a curve of genus $g \geq 2$ over $\mathbb{F}_q$, of class number h, and for any integer i let A_i be the number of effective divisors of degree i on X.*

Define an integer e_q as follows:

$$e_q = \begin{cases} 2 & \text{if } q = 2 \\ 1 & \text{if } q = 3, 4, 5 \\ 0 & \text{if } q > 5. \end{cases} \tag{117}$$

Then there is an integer e with $0 \leq e \leq e_q$ such that

$$A_{g-e-1} + A_j < h \tag{118}$$

for all $j \leq g + 2e - 3e_q - 1$.

Proof. We first consider the case $q = 2$. If $g = 2$, take $e = e_q = 2$, so (118) is satisfied since $A_j = 0$ for $j < 0$. Now suppose $g \geq 3$, and write (109) in the form

$$A_{g-1} + 2\sqrt{2}A_{g-2} + 4A_{g-3} + \cdots + 2(\sqrt{2})^{g-1}A_0 \leq (3 + 2\sqrt{2})h. \tag{119}$$

We proceed by contradiction and suppose that the lemma is false. This means that the following three inequalities hold:

$$A_{g-3} + A_j \geq h \qquad \text{for some } j \leq g - 3 \tag{120}$$

$$A_{g-2} + A_{j'} \geq h \qquad \text{for some } j' \leq g - 5 \tag{121}$$

$$A_{g-1} + A_{j''} \geq h \qquad \text{for some } j'' \leq g - 7. \tag{122}$$

We multiply (120) by 2, (121) by $2\sqrt{2}$, and sum with (122), to get:

$$A_{g-1} + 2\sqrt{2}A_{g-2} + 2A_{g-3} + 2A_j + 2\sqrt{2}A_{j'} + A_{j''} \geq (3 + 2\sqrt{2})h. \tag{123}$$

Comparing coefficients (and discussing whether $j = g - 3$ or $j \leq g - 4$, and whether j, j', j'' are all distinct or some of them are equal) we see that the left-hand side of (123) is less than or equal to the left-hand side of (119). To get a contradiction, it suffices to prove that the inequality is strict.

If $g \geq 4$, the coefficient of $A_0 = 1$ in (123) is strictly less than in (119), so the inequality is strict indeed.

Last, if $g = 3$, the only way to have equality is to have $j = g - 3 = 0$, with equality also in (120), (121), and (122). But from this and $A_0 = 1$ we deduce $h = 2 = A_1 = A_2$. However $A_1 = 2$ means there are two points P_1, P_2 of degree 1 on X, and considering the divisors $2P_1, 2P_2, P_1 + P_2$, we find $A_2 \geq 3$, a contradiction.

The case $q = 3$ works the same. Write (109) as

$$A_{g-1} + 2\sqrt{3}A_{g-2} + 6A_{g-3} + \cdots + 2(\sqrt{3})^{g-1}A_0 \leq (1 + \sqrt{3}/2)h < 2h. \tag{124}$$

If the lemma were false, one could find $j \leq g - 2$ with $A_{g-2} + A_j \geq h$, and $j' \leq g - 4$ with $A_{g-1} + A_{j'} \geq h$. Summing these two inequalities would then contradict (124).

To finish the proof, for $q = 4$ or 5, remark that (109) implies $A_i < h/2$ for $i \leq g - 2$, so we can take $e = e_q = 1$. And for $q > 5$ we find $A_i < h/2$ for $i \leq g - 1$, so $e = e_q = 0$ works, as claimed. □

Proposition 5.7. *Let X be a curve of genus $g \geq 2$ over $\mathbb{F}_q$, where $q \geq 2$ is any prime power, and let $m, l \geq 1$ be two integers.*

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

Let e_q be defined as in the previous lemma (remark $e_q \leq 2$ in any case).

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,

$$n_d = \sum_u n_{d,u} \leq B_d(X/\mathbb{F}_q). \tag{125}$$

Then, provided

$$\sum_{d,u} n_{d,u} du \geq 2ml + 3e_q + g - 1, \tag{126}$$

we have

$$\mu_q(m,l) \leq \sum_{d,u} n_{d,u} \mu_q(d,u). \tag{127}$$

Proof. We argue essentially as in the proof of Theorem 5.2.a) with only a few minor changes. From the collection of integers $n_{d,u}$ we first construct a divisor G, of degree $\deg G = \sum_{d,u} n_{d,u} du$, as before. For any integer i we let

$$\mathrm{Cl}^i_{\mathrm{sp}}(X) \subset \mathrm{Cl}^i(X) \tag{128}$$

be the set of linear equivalence classes of special divisors on X, hence by the Riemann-Roch theorem $\mathrm{Cl}^i_{\mathrm{sp}}(X) = [K_X] - \mathrm{Cl}^{2g-2-i}_{\mathrm{eff}}(X)$, so

$$|\,\mathrm{Cl}^i_{\mathrm{sp}}(X)| = |\,\mathrm{Cl}^{2g-2-i}_{\mathrm{eff}}(X)| \leq A_{2g-2-i}, \tag{129}$$

and by Lemma 5.6 there is an e with $0 \leq e \leq e_q$ and

$$|\,\mathrm{Cl}^{g+e-1}_{\mathrm{sp}}(X)| \leq |\,\mathrm{Cl}^j_{\mathrm{eff}}(X)| + |\,\mathrm{Cl}^{g+e-1}_{\mathrm{sp}}(X)| \leq A_j + A_{g-e-1} < h \tag{130}$$

for all $j \leq g + 2e - 3e_q - 1$.

Then letting

$$t = ml + e + g - 1 \tag{131}$$

and using (130) instead of (110), we can first find a divisor D_1 of degree t such that

$$[D_1] \notin \mathrm{Cl}^{g+e-1}_{\mathrm{sp}}(X) + [lQ], \tag{132}$$

ensuring (ii'_1) as in the proof of Theorem 5.2.a), and then, a divisor D_2 of degree t such that

$$[D_2] \notin (\mathrm{Cl}^{2t-\deg G}_{\mathrm{eff}}(X) + [G - D_1]) \cup (\mathrm{Cl}^{g+e-1}_{\mathrm{sp}}(X) + [lQ]), \tag{133}$$

(remark $2t - \deg G \leq g + 2e - 3e_q - 1$ by (126)), ensuring (i') and (ii'_2), and we conclude as before. □

Remark 5.8. Many results in this part, concerning "uniform" upper bounds, can still be improved or generalized, in various directions, for example:

- Following Ballet's proof, the case $r = 2$ in Corollary 5.4 uses modular curves of *prime* genus, and then relies on Bertrand's postulate (proved by Chebyshev) for these primes. It is possible to refine both parts of this argument (allow non-prime values for the genus, and get a finer control on the gaps between these values), leading to sharper bounds in this case.
- Theorem 5.2 (and Proposition 5.7) can also be combined with descent arguments, such as those used in [5], to derive better bounds than the ones in Corollary 5.4 when q is not a square.

All these improvements or generalizations require quite long technical discussions and are somehow independent of the main ideas presented in this paper, so they will be treated elsewhere.

6 Fixing the Shparlinski-Tsfasman-Vladut asymptotic upper bound

The Shparlinski-Tsfasman-Vladut upper bound [31] concerns the asymptotic quantities defined below. As explained earlier in the text, there was a gap in their proof, which our methods allow to fill (with two independent arguments).

Definition 6.1. If q is a prime power, we let

$$\begin{aligned} m_q &= \liminf_{n\to\infty} \frac{1}{n}\mu_q(n) \\ M_q &= \limsup_{n\to\infty} \frac{1}{n}\mu_q(n) \end{aligned} \tag{134}$$

and their symmetric counterparts m_q^{sym} and M_q^{sym} are defined likewise.

Definition 6.2. We let $A(q)$ be the largest real number such that there exists a family of curves X_s over $\mathbb{F}_q$, of genus g_s going to infinity, with

$$\lim_{s\to\infty} \frac{|X_s(\mathbb{F}_q)|}{g_s} = A(q). \tag{135}$$

Theorem 6.3. *If $A(q) > 1$, then*

$$m_q \leq 2\left(1 + \frac{1}{A(q)-1}\right). \tag{136}$$

Moreover, if $A(q) > 5$, then also $m_q^{sym} \leq 2\left(1 + \frac{1}{A(q)-1}\right)$.

Proof. Consider a family of curves X_s over $\mathbb{F}_q$, of genus g_s going to infinity, with

$$\lim_{s\to\infty} \frac{|X_s(\mathbb{F}_q)|}{g_s} = A(q). \tag{137}$$

Given an integer s, let

$$n(s) = \left\lfloor \frac{1}{2}(|X_s(\mathbb{F}_q)| - g_s - 5) \right\rfloor, \tag{138}$$

hence by (137)

$$\lim_{s\to\infty} \frac{n(s)}{g_s} = \frac{A(q)-1}{2}. \tag{139}$$

Then for s large enough we have $2g_s + 1 \leq q^{(n(s)-1)/2}(q^{1/2} - 1)$ and we can apply Proposition 5.7 with $l = 1$ and $m = n(s)$, and with all $n_{d,u}$ zero except $n_{1,1} = 2n(s) + g_s + 5$, to get

$$\mu_q(n(s)) \leq 2n(s) + g_s + 5, \tag{140}$$

which allows to conclude.

If $A(q) > 5$, then $|X_s(\mathbb{F}_q)| > 5g_s$ for s large enough, and we can use Theorem 5.2.c) to conclude likewise. □

Theorem 6.4. *If $q = p^{2r} \geq 9$ is a square, then*

$$M_q \leq 2\left(1 + \frac{1}{\sqrt{q}-2}\right). \tag{141}$$

Moreover, if $q = p^{2r} \geq 49$, then also $M_q^{sym} \leq 2\left(1 + \frac{1}{\sqrt{q}-2}\right)$.

Proof. Consider the Shimura curves described in [31], pp. 163–166. They form a family of curves X_s over $\mathbb{F}_q$, of genus g_s going to infinity, with

$$\lim_{s\to\infty} \frac{|X_s(\mathbb{F}_q)|}{g_s} = \sqrt{q} - 1 \tag{142}$$

and

$$\lim_{s\to\infty} \frac{g_{s+1}}{g_s} = 1. \tag{143}$$

Given an integer n, let $s(n)$ be the smallest integer such that

$$|X_{s(n)}(\mathbb{F}_q)| \geq 2n + g_{s(n)} - 1, \tag{144}$$

hence by (142) and (143),

$$g_{s(n)} = \frac{2n}{\sqrt{q}-2} + o(n). \tag{145}$$

This then gives $2g_{s(n)} + 1 \leq q^{(n-1)/2}(q^{1/2} - 1)$ for n large enough, and we can apply Theorem 5.2.a) with $l = 1$ and $m = n$, and with all $n_{d,u}$ zero except $n_{1,1} = 2n + g_{s(n)} - 1$, to get

$$\mu_q(n) \leq 2n + g_{s(n)} - 1. \tag{146}$$

This holds for all n large enough, hence dividing by n and using (145) again allows to conclude.

If $q \geq 49$, then we can use Theorem 5.2.c) instead, and conclude likewise. □

Remark 6.5. As noted in [2], we also immediately get from Corollary 5.4 the bounds $M_p \leq 3\left(1 + \frac{2}{p-2}\right)$ for p prime, and $M_q \leq 3\left(1 + \frac{p}{q-2}\right)$ for $q = p^r$, $r \geq 3$ odd.

Remark 6.6. Prop. 4.1 of [31] also discusses some constructiveness issues, which we can improve here. Suppose that $q \geq 9$ is a square, and that for some increasing sequence of integers n, we are given explicitly a curve X_n of genus

$$g_n = \frac{2n}{\sqrt{q} - 2} + o(n), \tag{147}$$

together with a point Q of degree n on X_n, and a set S of points of degree 1 on X_n, such that

$$|S| \geq 2n + g_n - 1 \tag{148}$$

(this is possible, for example, with the curves in [20]). Then in the preceding proof we can use Theorem 5.2.b) instead of Theorem 5.2.a), which leads to a *polynomial time* (in n) construction of a multiplication algorithm for $\mathbb{F}_{q^n}/\mathbb{F}_q$, of length $2n\left(1 + \frac{1}{\sqrt{q}-2}\right) + o(n)$ (moreover if $q \geq 49$, we can use Theorem 5.2.c) to make the algorithm symmetric). This is better than Prop. 4.1 of [31] which, under the same hypothesis, gives an algorithm of length $2n\left(1 + \frac{4}{\sqrt{q}-5}\right) + o(n)$.

Remark 6.7. Here we studied the asymptotics of $\mu_q(n) = \mu_q(n, 1)$. We could do the same thing for $\widehat{M}_q(n) = \mu_q(1, n)$, or more generally for $\mu_q(m, l)$ when both m and l vary.

Note that the parameters m and l appear at two places in Theorem 5.2 (or likewise in Proposition 5.7):

- First, m appears alone when one asks that the curve X should admit a point Q of degree m.
- Then m and l appear together through the product $ml = \dim \mathcal{A}_q(m, l)$ in condition (104).

Since the curves in the proofs of Theorems 6.3 and 6.4 all admit at least one point of degree 1, we see that the asymptotic estimates given there for $\mu_q(n)$ also hold for $\widehat{M}_q(n)$:

$$\liminf_{n\to\infty} \frac{1}{n}\widehat{M}_q(n) \leq 2\left(1 + \frac{1}{A(q) - 1}\right) \qquad \text{for } A(q) > 1 \tag{149}$$

$$\limsup_{n\to\infty} \frac{1}{n}\widehat{M}_q(n) \le 2\left(1+\frac{1}{\sqrt{q}-2}\right) \qquad \text{for } q \ge 9 \text{ a square} \qquad (150)$$

(and likewise for their symmetric counterparts).

The same techniques also give asymptotic upper bounds for

$$\frac{1}{ml}\mu_q(m,l). \qquad (151)$$

However in order to ensure that the curves admit a point of degree m, we will rely on the sufficient condition $2g+1 \le q^{(m-1)/2}(q^{1/2}-1)$, and since in the proofs we will have curves of genus g growing linearly with $n = ml$ (see (139) or (145)), these upper bounds will be valid only in a domain in which m grows at least logarithmically with ml.

Question 6.8. The condition $A(q) > 5$ in the last statement of Theorem 6.3 (and likewise $q \ge 49$ in Theorem 6.4) might appear strange. A natural question is whether the estimate should be valid under the condition $A(q) > 1$ also in the symmetric case. In fact this condition $A(q) > 5$ can be relaxed very slightly, as shown in [29]. However, to relax it further to $A(q) > 1$ would require much deeper results, such as the conjectures proposed in [27] on the existence of curves having many points but few 2-torsion in their class group.

This also leads to the following question: do $m_q^{\mathrm{sym}} = m_q$, or $M_q^{\mathrm{sym}} = M_q$, or more generally $\mu_q^{\mathrm{sym}}(m,l) = \mu_q(m,l)$ for all q, m, l? Of course this should be put in contrast with the example in Remark 1.7.

References

[1] S. Ballet, *On the tensor rank of the multiplication in the finite fields*, J. Number Theory **128** (2008) 1795–1806.

[2] S. Ballet, "A note on the tensor rank of the multiplication in certain finite fields", in: J. Chaumine, J. Hirschfeld & R. Rolland (eds.), *Algebraic geometry and its applications, Proceedings of the first SAGA conference (Papeete, France, 7-11 May 2007)*, Ser. Number Theory Appl. **5**, World Sci. Publ., 2008, pp. 332–342.

[3] S. Ballet & D. Le Brigand, *On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$*, J. Number Theory **116** (2006) 293–310.

[4] S. Ballet, D. Le Brigand & R. Rolland, "On an application of the definition field descent of a tower of function fields", in: F. Rodier & S. Vladut (eds.), *Proceedings of the Conference "Arithmetic, Geometry and Coding Theory" (AGCT 2005)*, Séminaires et Congrès **21**, Société Mathématique de France, 2010, pp. 187–203.

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

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

[7] S. Ballet & R. Rolland, *Multiplication algorithm in a finite field and tensor rank of the multiplication*, J. Algebra **272** (2004) 173–185.

[8] N. Bourbaki, *Éléments de mathématique, Algèbre commutative, Chapitres 8 et 9*, Masson, 1983. Reprint: Springer-Verlag, 2006.

[9] R. W. Brocket & D. Dobkin, *On the optimal evaluation of a set of bilinear forms*, Lin. Alg. Appl. **19** (1978) 624–628.

[10] P. Bürgisser, M. Clausen & A. Shokrollahi, *Algebraic complexity theory*, Grundlehren der Math. Wissenschaften **315**, Springer-Verlag, 1997.

[11] I. Cascudo Pueyo, *On asymptotically good strongly multiplicative linear secret sharing*, Tesis doctoral, Universidad de Oviedo, 2010.

[12] I. Cascudo Pueyo, personal communication.

[13] I. Cascudo, R. Cramer & C. Xing, *The torsion-limit for algebraic functions fields and its application to arithmetic secret sharing*, in: Ph. Rogaway (ed.) *Advances in cryptology – CRYPTO 2011*, Lecture Notes in Comp. Science **6841**, Springer-Verlag, 2011, pp. 685–705.

[14] M. Cenk & F. Özbudak, *On multiplication in finite fields*, J. Complexity **26** (2010) 172–186.

[15] J. Chaumine, "Multiplication in small finite fields using elliptic curves", in: J. Chaumine, J. Hirschfeld & R. Rolland (eds.), *Algebraic geometry and its applications, Proceedings of the first SAGA conference (Papeete, France, 7-11 May 2007)*, Ser. Number Theory Appl. **5**, World Sci. Publ., 2008, pp. 343–350.

[16] H. Chen & R. Cramer, "Algebraic geometric secret sharing schemes and secure multi-party computations over small fields", in: C. Dwork (ed.), *Advances in cryptology – CRYPTO 2006*, Lecture Notes in Comp. Science **4117**, Springer-Verlag, 2006, pp. 521–536.

[17] D. V. & G. V. Chudnovsky, *Algebraic complexities and algebraic curves over finite fields*, J. Complexity **4** (1988) 285–316.

[18] R. Cramer, I. Damgård & U. Maurer, "Efficient general secure multi-party computation from any linear secret-sharing scheme", in: B. Prenel (ed.) *Advances in cryptology – EUROCRYPT 2000*, Lecture Notes in Comp. Science **1807**, Springer-Verlag, 2000, pp. 316–334.

[19] C. Fiduccia & Y. Zalcstein, *Algebras having linear multiplicative complexities*, J. Assoc. Comput. Mach. **24** (1977) 311–331.

[20] A. Garcia & H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995) 211–222.

[21] H. F. de Groote, *Lectures on the complexity of bilinear problems*, Lecture Notes in Comp. Science **245**, Springer-Verlag, 1987.

[22] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer-Verlag, 1977.

[23] А. Карацуба & Ю. Офман, *Умножение многозначных чисел на автоматах*, Доклады Акад. Наук СССР **145** (1962) 293–294. English translation: A. Karatsuba & Yu. Ofman, *Multiplication of multi-digit numbers on automata*, Soviet Physics Doklady **7** (1963) 595–596.

[24] J. M. Landsberg, *Geometry and the complexity of matrix multiplication*, Bull. Amer. Math. Soc. **45** (2008) 247–284.

[25] A. Lempel & S. Winograd, *A new approach to error-correcting codes*, IEEE Trans. Inform. Theory **23** (1977) 503–508.

[26] H. Niederreiter & C. Xing, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl **2** (1996) 241–273.

[27] H. Randriam, "Hecke operators with odd determinant and binary frame-proof codes beyond the probabilistic bound?", in *Proc. of ITW 2010 Dublin – IEEE Information Theory Workshop, Dublin, Ireland, 2010.*

[28] H. Randriambololona, $(2,1)$*-separating systems beyond the probabilistic bound*, to appear in Israel J. Math. — `http://arxiv.org/abs/1010.5764`

[29] H. Randriambololona, *Diviseurs de la forme* $2D - G$ *sans sections et rang de la multiplication dans les corps finis*, preprint. — `http://arxiv.org/abs/1103.4335`

[30] M. A. Shokrollahi, *Optimal algorithms for multiplication in certain finite fields using elliptic curves*, SIAM J. Comput. **21** (1992) 1193–1198.

[31] I. Shparlinski, M. Tsfasman & S. Vladut, "Curves with many points and multiplication in finite fields", in: H. Stichtenoth & M. A. Tsfasman (eds.), *Coding theory and algebraic geometry (Luminy, 1991)*, Lecture Notes in Math. **1518**, Springer-Verlag, 1992, pp. 145–169.

[32] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, 1993.

[33] V. Strassen, *Gaussian elimination is not optimal*, Numer. Math. **13** (1969) 354–356.

[34] V. Strassen, *Vermeidung von Divisionen*, J. Reine Angew. Math. **264** (1973) 184–202.

[35] V. Strassen, *Rank and optimal computation of generic tensors*, Linear Algebra Appl. **52/53** (1983) 645–685.

[36] W. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. **2** (1969) 521–560.

[37] S. Winograd, *Some bilinear forms whose multiplicative complexity depends on the field of constants*, Math. Systems Theory **10** (1977) 169–180.

[38] C. Xing, *Asymptotic bounds on frameproof codes*, IEEE Trans. Inform. Theory **48** (2002) 2991–2995.