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

S. Ballet, J. Pieltant, M. Rambaud, H. Randriambololona, R. Rolland, and J. Chaumine

Abstract. In this paper, we give a survey of the known results concerning the tensor rank of multiplication in finite extensions of finite fields, enriched with some unpublished recent results, and we analyze these to enhance the qualitative understanding of the research area. In particular, we identify and clarify certain partially proved results and emphasise links with open problems in number theory, algebraic geometry, and coding theory.

Bibliography: 92 titles.

Keywords: finite field, tensor rank of multiplication, function field.

Contents

1. Introduction 30
   1.1. Tensor rank and multiplication algorithm 31
   1.2. Organization of the paper 34
2. Old classical results 34
3. The approach via algebraic curves 36
   3.1. The D.V. Chudnovsky and G.V. Chudnovsky multiplication algorithm (CCMA) 37
   3.2. The linearity of the bilinear complexity of multiplication 38
4. The approach via codes 40
   4.1. Connection with codes and asymptotic lower bounds 40
   4.2. Supercodes 41
5. Generalizations of the algorithm of D.V. Chudnovsky and G.V. Chudnovsky 42
   5.1. Motivation 42
   5.2. Evaluation at places of higher degree and with multiplicities 43
   5.3. Discussion on symmetry 45
   5.4. The current generalized CCMA 46
6. Choice of the curves 49
   6.1. Motivation and notation 49
   6.2. Explicit towers, densification and descent 51
   6.3. Modular and Shimura curves 52

AMS 2020 Mathematics Subject Classification. Primary 14H05; Secondary 12E20.

© 2021 Russian Academy of Sciences (DoM), London Mathematical Society, IOP Publishing Limited
1. Introduction

This article is a survey of results on the tensor rank of multiplication in finite fields. It is an update of the previous survey [25] published about fifteen years ago. The deep improvements achieved since then require a complete rewrite of the survey, highlighting the current state-of-the-art. In particular, we present the new techniques introduced in recent years. The growing importance of this topic has attracted many mathematicians and computer scientists, who developed new ideas and obtained new results. At the same time, we report a number of non-trivial errors and solutions, which testify to the vitality of the domain and the community concerned. Finite fields constitute an important area of mathematics. They arise in many applications, particularly in areas related to information theory. In particular, the complexity of multiplication in finite fields is a central problem. It is part of algebraic complexity theory, for which the best general reference is [35]. It turns out that studying this problem has raised many issues in number theory and algebraic geometry. Notably, it has revealed deep links between these different domains. So, one of the objectives of this article is also to make these links explicit and to present current related open problems. At the same time, we prove some as yet unpublished new results.

Let us describe the problem more precisely. Suppose that we have multiplication in a finite field \( \mathbb{F}_q \) and want to construct an algorithm of multiplication in the extension \( \mathbb{F}_{q^n} \) which is the least expensive in terms of the number of operations in \( \mathbb{F}_q \). Let us remark that, from this point of view, multiplication in \( \mathbb{F}_{q^n} \) is the multiplication of two polynomials of degree \(< n\) with coefficients in \( \mathbb{F}_q \). We then distinguish two types of operations in the algorithm, those which are linear with respect to the multiplied variables and those which are bilinear with respect to the two variables. More precisely, let \( \mathcal{B} = \{e_1, \ldots, e_n\} \) be a basis of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \).
If \( x = \sum_{i=1}^{n} x_i e_i \) and \( y = \sum_{i=1}^{n} y_i e_i \), then direct computation gives

\[
z = xy = \sum_{h=1}^{n} z_h e_h = \sum_{h=1}^{n} \left( \sum_{i,j=1}^{n} t_{ijh} x_i x_j \right) e_h, \tag{1}
\]

where

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

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

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

So, to obtain the product \( xy \) by direct computation, one needs to account for:

- \( n^3 - n \) additions,
- \( n^3 \) scalar multiplications,
- \( n^2 \) non-scalar or bilinear multiplications.

The bilinear complexity of the algorithm of multiplication is given by the number of bilinear multiplications used. Let us remark that the bilinear complexity is not the full complexity of the algorithm. The complexity of the linear part of the algorithm should also be taken into account. Nonetheless, there is a benefit in having low bilinear complexity. Indeed, it is more decisive for execution time than scalar complexity. Multiplication by a fixed known element can be treated in a special way and have faster execution time than that of general multiplication (for example, in the trivial cases when the constants are 0 or 1, or when using tables of precomputation). This is corroborated by specific situations in cryptography. It is known that the pairings calculation requires a lot of multiplications. For example, in his thesis (see [54], pp. 177–179), Estibals exhibits an algorithm, the implementation of which benefits from a significant improvement in computing time thanks to a multiplication formula obtained by Barbulescu, Detrey, Estibals, and Zimmermann in [28], the bilinear complexity of which is 11 instead of 12.

This bilinear complexity corresponds to the rank of the tensor of this multiplication algorithm in \( \mathbb{F}_{q^n} \) as a vector space over \( \mathbb{F}_q \), as will be explained in the next section.

Therefore, independently of the practical problem concerning the complexity of multiplication, there arises the theoretical mathematical problem of finding the rank of this tensor.

This paper is devoted to the study of this problem of the tensor rank of multiplication in finite fields. We state the results obtained in this part of algebraic complexity theory and number theory and discuss related issues.

### 1.1. Tensor rank and multiplication algorithm

Recall the notions of a multiplication algorithm and the associated bilinear complexity.
Definition 1.1. Let $K$ be a field and let $E_0, \ldots, E_s$ 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 (or indecomposable) 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 minimum length of a decomposition of $t$ as a sum of elementary tensors.

Definition 1.2. If $\alpha: E_1 \times \cdots \times E_s \to E_0$ is an $s$-linear map, the $s$-linear complexity of $\alpha$ is defined as the tensor rank of the element

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

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

Definition 1.3. Let $A$ be a finite-dimensional $K$-algebra. We denote by $\mu(A/K)$ the bilinear complexity of the multiplication map

$$m_A: A \times A \to A$$

considered as a $K$-bilinear map.

In particular, if $A = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$, we put

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

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

$$xy = \phi_1(x)\psi_1(y)w_1 + \cdots + \phi_n(x)\psi_n(y)w_n. \quad (2)$$

Indeed, such an expression is one and the same as a decomposition

$$t_M = \sum_{i=1}^n w_i \otimes \phi_i \otimes \psi_i \in A \otimes A^\vee \otimes A^\vee \quad (3)$$

for the multiplication tensor of $A$.

Definition 1.4. By a multiplication algorithm of length $n$ for $A/K$ we mean a collection of $\phi_i, \psi_i,$ and $w_i$ that satisfy (2) or, equivalently, a tensor decomposition

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

for the multiplication tensor of $A$. Such an algorithm is said to be symmetric if $\phi_i = \psi_i$ for all $i$ (this can happen only if $A$ is commutative).
Hence, when $A$ is commutative, it is interesting to study the minimum length of a symmetric multiplication algorithm.

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

$$
\mu_{\text{sym}}(A/K)
$$

is the minimum length of a symmetric multiplication algorithm.

In particular, if $A = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$, we put

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

Here are some basic properties of these quantities, taken from [74], Lemma 1.10.

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

$$
\mu(A_L/L) \leq \mu(A/K).
$$

Moreover, if $A$ is commutative, we also have

$$
\mu_{\text{sym}}(A_L/L) \leq \mu_{\text{sym}}(A/K).
$$

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

$$
\mu(A/K) \leq \mu(A/L)\mu(L/K).
$$

Moreover, if $A$ is commutative, we also have

$$
\mu_{\text{sym}}(A/K) \leq \mu_{\text{sym}}(A/L)\mu_{\text{sym}}(L/K).
$$

(c) If $A$ and $B$ are two finite-dimensional $K$-algebras, then

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

Moreover, if $A$ and $B$ are commutative, we also have

$$
\mu_{\text{sym}}(A \times B/K) \leq \mu_{\text{sym}}(A/K) + \mu_{\text{sym}}(B/K).
$$

(d) If $A$ and $B$ are two finite-dimensional $K$-algebras, then

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

Moreover, if $A$ and $B$ are commutative, we also have

$$
\mu_{\text{sym}}(A \otimes_K B/K) \leq \mu_{\text{sym}}(A/K)\mu_{\text{sym}}(B/K).
$$

In particular, the following lemma of Shparlinski, Tsfasman, and Vlăduţ (see [80], Lemma 1.2) is especially useful. Actually, the right-hand inequality was already stated in the original paper of D. V. Chudnovsky and G. V. Chudnovsky (see [43]), so the new contribution of Shparlinski, Tsfasman, and Vlăduţ is the left-hand inequality. This will be important when we consider asymptotic complexities in Lemma 8.1.
Lemma 1.7. For all $m, n$ we have

$$
\mu_q(n) \leq \mu_q(mn) \leq \mu_q(m)\mu_q^m(n).
$$

Actually, the same holds for symmetric complexity.

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

$$
\mu^\text{sym}_q(n) \leq \mu^\text{sym}_q(mn) \leq \mu^\text{sym}_q(m)\mu^\text{sym}_q(m^n).
$$

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

1.2. Organization of the paper. In §2 we present the classical results via the approach using multiplication by means of polynomial interpolation. In §3 we give a historical record of results obtained in the pioneering work of D.V. and G.V. Chudnovsky in [43], and later Shparlinski, Tsfasman, and Vlăduţ in [80]. In particular, we present the original algorithm. This modern approach uses interpolation over algebraic curves defined over finite fields. This approach, for which we recount the first success as well as the rocks on which the pioneers came to grief, enabled the first complete proof of the linearity of the bilinear complexity of multiplication by Ballet in [6]. In §4, we present the coding theory approach for bilinear complexity and explain the connection between the bilinear complexity of multiplication and so-called (exact) supercodes or, equivalently, multiplication friendly codes in the terminology of some authors. Then, in §5, we present various generalizations of the original D.V. and G.V. Chudnovsky algorithm, in particular, the currently most successful version of a of Chudnovsky–Chudnovsky type algorithm due to Randriambololona [74]. This part explains the links with algebraic geometry. In §6 we are interested in determining the families of algebraic curves adapted to the Chudnovsky–Chudnovsky algorithm (towers of algebraic function fields, families of Shimura curves as well as their densification and descent). We devote §7 to the problem of existence and determination of the divisors defining the Riemann–Roch spaces underlying the Chudnovsky–Chudnovsky algorithm (the problem of zero-dimensional divisors and 2-torsion). In §8 we recall the known results on the asymptotic bounds for symmetric and asymmetric bilinear complexity that have been established during the last 30 years. Then, in a similar manner, in §9, we give uniform bounds for symmetric and asymmetric bilinear complexity. Finally, in §10 we present methods for the effective construction of bilinear multiplication algorithms in finite fields.

2. Old classical results

Let

$$
P(u) = \sum_{i=0}^{n} a_i u^i
$$
be an irreducible monic polynomial of degree $n$ with coefficients in a field $F$. Let

$$R(u) = \sum_{i=0}^{n-1} x_i u^i \quad \text{and} \quad S(u) = \sum_{i=0}^{n-1} y_i u^i$$

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

Fiduccia and Zalcstein (cf. [55] and [35], p. 367, Proposition 14.47) studied the general problem of computing the coefficients of the product $R(u) \times S(u)$ and demonstrated that at least $2n - 1$ multiplications are needed. When the field $F$ is infinite, an algorithm reaching exactly this bound was given earlier by Toom in [82]. In [90] Winograd described all the algorithms reaching the bound $2n - 1$. Moreover, in [91] Winograd proved that, up to some transformations, every algorithm for computing the coefficients of $R(u) \times S(u) \mod P(u)$ which is of bilinear complexity $2n - 1$ necessarily computes the coefficients of $R(u) \times S(u)$ and, consequently, uses one of the algorithms described in [90]. These algorithms use interpolation techniques and cannot be performed if the cardinality of the field $F$ is $< 2n - 2$.

In conclusion, we have the following result.

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

Applying the results of Winograd and De Groote [46] and Theorem 2.1 to the multiplication in a finite extension $\mathbb{F}_{q^n}$ of a finite field $\mathbb{F}_q$, we obtain the following result.

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

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

with equality holding if and only if

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

This result provides no estimate of an upper bound for $\mu_q(n)$ when $n$ is large. In [64] Lempel, Seroussi, and Winograd proved that $\mu_q(n)$ has a quasi-linear upper bound. More precisely, the following result holds.

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

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

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

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

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

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

**Corollary 2.4.** Asymptotically,

$$f_q(n) < \log_q \log_q \ldots \log_q(n)$$

for any $k \geq 1$.

Furthermore, extending and using more efficiently the technique developed in [34], Bshouty and Kaninski showed that

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

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

### 3. The approach via algebraic curves

We have seen in the previous section that we cannot perform multiplication by the Winograd interpolation method if the number of points of the base field is too low. D.V. and G.V. Chudnovsky [43] designed an algorithm where interpolation is done on points of an algebraic curve over the base field with a sufficient number of rational points. Let us remark that the idea of using evaluations on the points of an algebraic curve is inspired by the theory of Goppa codes, introduced by Goppa in [59] and [60] and developed by Tsfasman in [83] and by Tsfasman, Vladuț, and Zink in [86]. We denote this Chudnovsky–Chudnovsky Multiplication Algorithm by CCMA. Using this algorithm, D.V. and G.V. Chudnovsky claimed that the bilinear complexity of multiplication in finite extensions of a finite field is asymptotically linear, but later Shparlinski, Tsfasman, and Vladuț [80] noted that they only proved that $m_q = \lim \inf_{k \to \infty} (\mu_q(k)/k)$ is bounded, which does not enable one to prove linearity. To prove linearity it is also necessary to show that $M_q = \lim \sup_{k \to \infty} (\mu_q(k)/k)$ is bounded, which was the main aim in [80]. However, Cascudo, Cramer, and Xing have recently detected a mistake in the proof of Shparlinski, Tsfasman, and Vladuț. Unfortunately, this mistake, which we explain in detail in this section, also had an effect on their improved estimates of $m_q$.

Following the above pioneering research, in [6] (cf. also [5]) Ballet obtained the first upper bounds for $\mu_q(n)$ uniform with respect to $q$. The CCMA being clearly symmetric, these first uniform bounds also apply to $\mu_q^{\text{sym}}(n)$. Moreover, being
unaffected by the same mistake, these bounds made it possible to prove at the same time the linearity of the bilinear complexity of multiplication in finite extensions of a finite field since it obviously follows that $M_q$ is finite. Critical improvements were subsequently introduced. In [5] and [6] Ballet introduced simple numerical conditions on algebraic curves of an arbitrary genus $g$, giving a sufficient condition for the application of the CCMA (the existence of places of certain degree and of non-special divisors of degree $g - 1$), which generalizes the result of Shokrollahi [79] for elliptic curves. Ballet introduced the use of towers of algebraic function fields in [5] and [6], and their densification in [8]. In [24] Ballet and Rolland introduced the use of places of higher degree, and they also introduced the descent over $\mathbb{F}_q$ of the definition field $\mathbb{F}_{q^2}$ of a densified tower defined over $\mathbb{F}_{q^2}$ for any finite field $\mathbb{F}_q$ with a characteristic $p = 2$. In [19], Ballet, Le Brigand, and Rolland generalized the method for any finite field. In [9] Ballet derived optimal criterions for a direct construction of the divisors satisfying the required conditions, and in [41] and [42] Chaumine proved that these criterions are always satisfied in the elliptic case, hence improving the result of Shokrollahi [79]. In [18], thanks to a theorem on the existence of non-special divisors of degree $g - 1$, Ballet and Le Brigand improved the sufficient conditions for the application of the CCMA for the extensions of arbitrary finite fields. In [1] Arnaud introduced the use of local expansion, called derivated evaluation. In [20] and [68] Ballet and Pieltant introduced the use of divisors of degree zero thanks to an existence result obtained in [23] by Ballet, Ritzenthaler, and Rolland, and they combined it with local expansion. Then Cenk and Özbudak [39] and Randriambololona [74] gave improvements by using local expansion and high degree places. These can be combined with other independent ingredients, also proposed in [74], namely allowing asymmetry in the interpolation procedure, which establishes the announced Shparlinski–Tsfasman–Vlăduţ estimates for $m_q$ and $M_q$, and using the best bilinear complexities recursively, an idea that was then also used in [15]. Finally, the following two ideas can be used in order to deal with symmetric complexities: bounds involving the 2-torsion [92], [72], [36], [37], and direct construction of the divisors satisfying the required conditions [75], [73], [74]. Ultimately, in the majority of cases, this allows one to obtain the Shparlinski–Tsfasman–Vlăduţ estimates also for $m_q^{\text{sym}}$ and $M_q^{\text{sym}}$, as well as other related estimates for symmetric complexity.

3.1. The D. V. Chudnovsky and G. V. Chudnovsky multiplication algorithm (CCMA). In this section we recall the brilliant idea of D. V. Chudnovsky and G. V. Chudnovsky and give their main result. First, we present the original CCMA, which was established in [43] in 1987.

**Theorem 3.1.** Let

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

Suppose that $Q, P_1, \ldots, P_N$ are not in the support of $\mathcal{D}$ and that
(a) the evaluation map

\[ \text{Ev}_Q : \mathcal{L}(D) \to \mathbb{F}_q^n \cong F_Q, \]
\[ f \mapsto f(Q) \]

is onto (where \(F_Q\) is the residue class field of \(Q\));
(b) the application

\[ \text{Ev}_{\mathcal{P}} : \mathcal{L}(2D) \to \mathbb{F}_q^N, \]
\[ f \mapsto (f(P_1), \ldots, f(P_N)) \]

is injective.

Then

\[ \mu_q(n) \leq N. \]

We present this result as it was formulated in [43], in terms of the bilinear complexity \(\mu_q(n)\). However, closer inspection of the method shows that it produces symmetric algorithms, so the conclusion also holds for symmetric bilinear complexity:

\[ \mu_q^{\text{sym}}(n) \leq N. \]

3.2. The linearity of the bilinear complexity of multiplication. As seen previously, Shparlinski, Tsfasman, and Vlăduţ [80] made many interesting observations on the CCMA and bilinear complexity. In particular, they considered asymptotic bounds\(^1\) for bilinear complexity in order to prove the linearity of this complexity from the CCMA. Following these authors, let us define

\[ M_q = \limsup_{k \to \infty} \frac{\mu_q(k)}{k} \quad \text{and} \quad m_q = \liminf_{k \to \infty} \frac{\mu_q(k)}{k}. \]

Moreover, we also have to consider the symmetric variants of these quantities, which were not considered by Shparlinski, Tsfasman, and Vlăduţ, but were first introduced by Randriambololona in [74], and have become equally important since then:

\[ M_q^{\text{sym}} = \limsup_{k \to \infty} \frac{\mu_q^{\text{sym}}(k)}{k} \quad \text{and} \quad m_q^{\text{sym}} = \liminf_{k \to \infty} \frac{\mu_q^{\text{sym}}(k)}{k}. \]

It is clear that

\[ M_q \leq M_q^{\text{sym}} \quad \text{and} \quad m_q \leq m_q^{\text{sym}}. \]

It is not obvious at all that any of these values are finite. Note that if \(M_q\) (\(M_q^{\text{sym}}\)) is finite, then the bilinear complexity (symmetric bilinear complexity) of multiplication is linear in the degree of extension, namely there exists a constant \(C_q \geq M_q\) (\(C_q^{\text{sym}} \geq M_q^{\text{sym}}\), respectively) such that, for any integer \(n > 1\),

\[ \mu_q(n) \leq C_q n \quad (\mu_q^{\text{sym}}(n) \leq C_q^{\text{sym}} n, \text{ respectively}). \]

\(^1\)The pioneers obtained only asymptotic bounds. Thus, in a private communication with Rolland, Tsfasman suggested that one should study the problem of finding uniform bounds.
From Theorem 3.1, D.V. Chudnovsky and G.V. Chudnovsky derived\footnote{This result was originally formulated for $\mu_q(n)$. At that time, although most of the authors did not distinguish in the notation between bilinear complexity and symmetric bilinear complexity, it was known that the CCMA naturally produces symmetric algorithms (cf. [80], the definition on p. 154 and Remark 2.2, and also more precisely [6], the proof of Theorem 1.1), so the estimate also holds for the symmetric bilinear complexity $\mu_q^{\text{sym}}(n)$.} Theorem 7.7 in [43]: for $q \geq 25$ a square, we have

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

as $n \to \infty$.

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

More precisely, relying on Ihara’s work [63], D.V. Chudnovsky and G.V. Chudnovsky considered Shimura modular curves having an asymptotically maximal number of points over $\mathbb{F}_q$, and in the final step of their argument they asserted that, for some given constant $C$ and for all integers $n$ large enough, they could choose curves of genus $g = Cn + o(n)$ in this family. Although it follows from [63] that this is possible for infinitely many $n$, D.V. Chudnovsky and G.V. Chudnovsky needed it to hold for all $n$, for which they did not give a justification. Because of this, Shparlinski, Tsfasman, and Vladuț explained that one should consider that, even though D.V. Chudnovsky and G.V. Chudnovsky stated an estimate for the limit superior $M_q$, their proof is valid only for the limit inferior $m_q$.

But then, with the claim in [80], p. 163, Shparlinski, Tsfasman, and Vladuț gave a precise description of a family of Shimura curves that satisfy the conditions needed by D.V. Chudnovsky and G.V. Chudnovsky, which essentially completed the proof of (4). Unfortunately, at the same time, Shparlinski, Tsfasman, and Vladuț also proposed to replace (4) with a sharper bound, and in doing so they introduced an unjustified argument in the proof. The gap in their proof was found by Cascudo, Cramer and Xing (cf. personal communication in 2009 and [37], § V). They present the gap as follows:

“...the mistake (in [80] from 1992) is in the proof of their Lemma 3.3, page 161, the paragraph following formulas about the degrees of the divisor. It reads: “Thus the number of linear equivalence classes of degree $a$ for which either Condition $\alpha$ or Condition $\beta$ fails is at most $D_{b'} + D_b$.” This is incorrect; $D_b$ should be multiplied by the torsion. Hence the proof of their asymptotic bound is incorrect.”

Note that a synthesis of the work enabling one to fill the gap left in the proof of D.V. and G.V. Chudnovsky with the approach of Shparlinski, Tsfasman, and Vladuț is possible but indirect. Anyway, by using the strategy of D.V. and G.V. Chudnovsky applied to the first tower\footnote{The advantage of this tower of algebraic function fields is that, firstly, the number of rational points and the genus for each step are known explicitly and, secondly, the ratio of rational points over the genus is very good.} of Garcia–Stichtenoth [57] attaining the Drinfeld–Vlăduț bound, together with a result concerning the existence of non-special divisors of degree $g - 1$, Ballet [6] gave independently the first complete proof of the linearity
of the bilinear complexity of multiplication. More precisely, it was done by determining directly the upper bounds for $C_{q}^{\text{sym}}$. Since then, diverse work has been done to improve the asymptotic bounds (cf. §8) and the uniform bounds (cf. §9).

4. The approach via codes

Initially, just after the pioneering work of D.V. and G.V. Chudnovsky [43], Shparlinski, Tsfasman, and Vlăduţ [80] specified the link between certain codes and multiplication tensors. Then they introduced the notion of exact supercodes, also called multiplication friendly codes.

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

Let us recall the following classical definition.

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

By [80], it is possible to construct a code using a decomposition of $t_M$ into a sum of rank one tensors. Indeed, if

$$t_M = \sum_{i=1}^{N} a_i \otimes b_i \otimes c_i,$$

where $a_i \in \mathbb{F}_q^n$, $b_i \in \mathbb{F}_q^n$, and $c_i \in \mathbb{F}_q^n$, then one can define an $\mathbb{F}_q$-linear map

$$\phi: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^N,$$

$$x \mapsto (a_1(x), \ldots, a_N(x)).$$

The following result is implied by [80].

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

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

Recall that there exists a continuous decreasing function $\alpha_q^{\text{lin}}(\delta)$ on the segment $[0, 1-1/q]$ which corresponds to the bound for the rate $R$ of the linear codes over $\mathbb{F}_q$ with relative minimum distance at least $\delta$ (cf. [85], §1.3.1). Hence the following result holds.

**Corollary 4.4.** One has

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

where $\delta_q$ is the unique solution of the equation $\alpha_q^{\text{lin}}(\delta) = \delta$.
Any upper bound for $\alpha_q^{\text{lin}}(\delta)$ gives an upper bound for $\delta_q$ and thus a lower bound for $m_q$. So it follows from this corollary that we can obtain lower bounds of the asymptotic quantity $m_q$ from asymptotic parameters of codes. Now, let us summarize the known lower bounds concerning this quantity, namely the lower bound on $m_2$ obtained by Brockett, Brown, and Dobkin in [31], [30] by using the bound of ‘four’; see [85], §1.3.2 for asymptotic parameters of binary codes, and the lower bound on $m_q$ for $q > 2$ given by Shparlinski, Tsfasman, and Vlăduţ in [80] by using the asymptotic Plotkin bound. Note that this last bound is a straightforward consequence of Proposition 4.3 established by D.V. and G.V. Chudnovsky in [43].

**Proposition 4.5.** One has

$$m_2 \geq 3.52$$

and

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

**4.2. Supercodes.** Let us recall the notion of supercode introduced by Shparlinski, Tsfasman, and Vlăduţ in [80]. First recall the idea leading to the emergence of this notion. By §4.1, any decomposition of the tensor $t_M$ into a sum of $N$ summands of rank one enables us to obtain an $[N, n, d]_q$-code. In fact, the notion of supercode follows from the converse question as to when it is possible to construct such a decomposition from a linear $[N, n, \geq n]_q$-code.

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

(a) the first projection

$$\pi_1 : \mathbb{F}_q^n \oplus \mathbb{F}_q^N \to \mathbb{F}_q^n$$

restricted to $S$ is surjective;

(b) let $S^2 = \{s_1s_2 | s_1, s_2 \in S\}$, where the multiplication is that in the $\mathbb{F}_q$-algebra $\mathbb{F}_q^n \oplus \mathbb{F}_q^N$, and let $\langle S^2 \rangle$ be the subspace in $\mathbb{F}_q^n \oplus \mathbb{F}_q^N$ spanned by $S^2$; then the second projection

$$\pi_2 : \mathbb{F}_q^n \oplus \mathbb{F}_q^N \to \mathbb{F}_q^N$$

restricted to $\langle S^2 \rangle$ is injective.

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

**Definition 4.7.** An $[N, n]_q$-supercode $S$ is said to be exact if $\pi_1$ is an isomorphism, that is, if $\dim S = n$.

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

1) $C$ is an $[N, \geq n, \geq n]_q$-code;
2) if $S$ is exact, then $C$ is an $[N, n, \geq n]_q$-code;
3) any supercode contains an exact sub-supercode.

In fact, the notion of exact supercode is equivalent to that of symmetric decomposition of $t_M$ into a sum of $N$ rank one tensors, up to the representation of $\mathbb{F}_q^n$, that is, modulo the following equivalence relation.
Definition 4.9. Let
\[ \sigma_1 = \sum_{i=1}^{N} u_i \otimes u_i \otimes w_i \quad \text{and} \quad \sigma_2 = \sum_{i=1}^{N} v_i \otimes v_i \otimes z_i \]
be two symmetric decompositions of \( t_M \). We call \( \sigma_1 \) and \( \sigma_2 \) equivalent if \( u_i = v_i \) for every \( i \).

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

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

Then, by [80], Proposition 1.11, and Corollary 1.13, we obtain the following corollary.

Corollary 4.11. 1) Any exact supercode \( S \subset \mathbb{F}_{q^n} \oplus \mathbb{F}_{q^N} \) yields a symmetric multiplication algorithm of bilinear complexity \( N \), and vice versa.

2) Any supercode \( S \subset \mathbb{F}_{q^n} \oplus \mathbb{F}_{q} \) yields a symmetric multiplication algorithm of bilinear complexity \( \leq N \).

Note that Shparlinski, Tsfasman, and Vlăduţ [80] gave an explicit construction of a symmetric tensor \( t_M \) of length \( N \) performing the multiplication in a finite field \( \mathbb{F}_{q^n} \) from an exact supercode \( S \subset \mathbb{F}_{q^n} \oplus \mathbb{F}_{q^N} \). Conversely, from an arbitrary symmetric decomposition, they obtained explicitly an exact supercode by Proposition 1.11 in [80].

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

Open problem 4.13. How to characterize those \([N, \geq k, \geq k]\)-codes which are projections of supercodes?

5. Generalizations of the algorithm of D. V. Chudnovsky and G. V. Chudnovsky

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

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

Concerning the first step (a generic statement of the CCMA), successive generalizations have been proposed by various authors, using several independent ingredients, among which we can list the following:

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

In this section we give more details on these improvements, with emphasis on the first two (in §§5.2 and 5.3), and we present the best finalized version of the CCMA (see [74], Theorem 3.5), which combines all of them. We then explain how the interim historical contributions can be retrieved as particular cases.

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

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

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

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

- First, Ballet and Rolland [24] generalized the algorithm by using places of degree 1 and 2.
- Then Arnaud [1] introduced, as in the Lagrange–Sylvester interpolation, the use of derivatives (evaluation with multiplicities) to improve the interpolation process.
- These ideas were combined and extended in the work of Cenk and Özbudak [39]. This generalization uses several coefficients in the local expansion at each place $P_i$ instead of just the first one. Due to the way it is obtained in [39], their bound for bilinear complexity involves the sum of local contributions, each of which is written as a product of two separate factors: one factor accounts for the degree of the place, and the other one for the multiplicity.
• Last, Randriambololona [74] refined this method by introducing a single quantity that combines both degree and multiplicity at the same time and leads to the sharpest bounds known to date.

Two versions of the quantity introduced in [74] can be defined, one for bilinear complexity and another one for symmetric bilinear complexity.

**Definition 5.1.** For any integers \( m, \ell \geq 1 \) we consider the \( \mathbb{F}_q \)-algebra \( \mathbb{F}_q^m \langle t \rangle / (t^\ell) \) of polynomials in one variable with coefficients in \( \mathbb{F}_q^m \), truncated at order \( \ell \), and we denote by
\[
\mu_q(m, \ell) = \mu((\mathbb{F}_q^m \langle t \rangle / (t^\ell))/\mathbb{F}_q)
\]
its bilinear complexity over \( \mathbb{F}_q \), and by
\[
\mu_q^{\text{sym}}(m, \ell) = \mu^{\text{sym}}((\mathbb{F}_q^m \langle t \rangle / (t^\ell))/\mathbb{F}_q)
\]
its symmetric bilinear complexity over \( \mathbb{F}_q \).

Note that for \( \ell = 1 \) we have
\[
\mu_q(m, 1) = \mu_q(m) \quad \text{and} \quad \mu_q^{\text{sym}}(m, 1) = \mu_q^{\text{sym}}(m).
\]

At the same time, we have \( \mu_q(1, \ell) = \widetilde{M}_q(\ell) \) for \( m = 1 \) as defined by Cenk and Özbudak in [39]. Namely, for a positive integer \( \ell \), let \( \widetilde{M}_q(\ell) \) denote the multiplicative complexity of computing the coefficients of the product of two \( \ell \)-term polynomials modulo \( x^\ell \) over \( \mathbb{F}_q \). In other words, \( \widetilde{M}_q(\ell) \) is the minimum number of multiplications in \( \mathbb{F}_q \) needed to obtain the first \( \ell \) coefficients of the product of two arbitrary \( \ell \)-term polynomials in \( \mathbb{F}_q[x] \) (likewise, we could put \( \mu_q^{\text{sym}}(1, \ell) = \widetilde{M}_q^{\text{sym}}(\ell) \), even though this quantity is not considered in [39]).

The generalized evaluation maps that appear in the generalized CCMA can be described either in the language of modern algebraic geometry, as in [74], or in the language of algebraic function fields, as in previous works. These two languages are in fact equivalent, so we can explain how to pass from one to the other.

Suppose we are given:

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

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

Now, for any divisor \( D \) on \( X \), we can define a generalized evaluation map that evaluates sections of \( D \) at \( P \) with multiplicity \( \ell \). In geometric terms, this is just the natural restriction map
\[
\varphi_{D, P, \ell} : \mathcal{L}(D) \to \mathcal{O}_X(D)|_{P^{[\ell]}}.
\]

After possibly replacing \( D \) by a linearly equivalent divisor, we will assume that \( P \) is not in the support of \( D \). We then have a natural identification \( \mathcal{O}_X(D)|_{P^{[\ell]}} = \mathcal{O}_{P^{[\ell]}} \).

Then, thanks to Lemma 3.4 in [74], we have an isomorphism of algebras
\[
\mathcal{O}_{P^{[\ell]}} \cong \mathbb{F}_q^m \langle t \rangle / (t^\ell),
\]
where \( t \) corresponds to a local parameter \( t_P \) at \( P \), and \( \mathbb{F}_{q^m} \) is identified with the residue field of \( P \). Last, in order to make everything explicit for computations, we can use the natural linear isomorphism \( \mathbb{F}_{q^m}[t]/(t^\ell) \cong (\mathbb{F}_{q^m})^\ell \) identifying a polynomial \( a_0 + a_1 t + \cdots + a_{\ell-1} t^{\ell-1} \) with its coefficients \( (a_0, a_1, \ldots, a_{\ell-1}) \). When all this is combined, the generalized evaluation map becomes

\[
\varphi_{D,P,\ell}: \mathcal{L}(D) \to (\mathbb{F}_{q^m})^\ell, \quad f \mapsto (f(P), f'(P), \ldots, f^{(\ell-1)}(P)),
\]

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

\[
f = f(P) + f'(P)t_P + f''(P)t_P^2 + \cdots + f^{(\ell)}(P)t_P^\ell + \cdots
\]
of \( f \) at \( P \) with respect to \( t_P \). Sometimes this is also called a derived evaluation map, although one should be careful because for \( k \geq 2 \) these \( f^{(k)}(P) \) are not precisely derivatives in the usual sense (at best they are ‘1/k! times the derivative’).

### 5.3. Discussion on symmetry

In the broader context of bilinear algorithms over finite fields, the distinction between (general) bilinear complexity and symmetric bilinear complexity, together with some of the mathematical issues related specifically to the construction of symmetric algorithms, were first discussed by Seroussi and Lempel [78] in 1984.

Now we focus on works based on the Chudnovsky–Chudnovsky method. It turns out that, until 2011, all results (including those in [43], [80], [25], [39], and [73]) had been stated in terms of \( \mu_q \) only (not \( \mu_{q',q} \)), although by construction the method always produced symmetric algorithms. Of course this does not mean that the authors were unaware of the distinction. Indeed, for instance, Shparlinski, Tsfasman, and Vladuț explicitly mentioned the issue when they observed (see [80], p. 154) that their notion of supercode corresponds only to symmetric algorithms.

However the situation became unsatisfactory when Cascudo, Cramer, and Xing discovered a gap in the construction of the divisor in [80], as already discussed in §3. Indeed, it turns out that the difficulty of this construction, which they analyze in terms of the 2-torsion in the divisor class group of the curve (see §7.1), is closely related to the symmetry requirement for the algorithm.

Finally, things were clarified by Randriambololona in [74]. Along with the contributions already discussed in §5.2, this work introduced two further improvements to the method:

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

As a consequence of these developments, whenever possible, two versions of the generalized CCMA should be stated, one for bilinear complexity and the other one for symmetric bilinear complexity. Likewise, two versions of the numerical bounds should accordingly be stated.
Besides the bilinear complexity $\mu_q$ and symmetric bilinear complexity $\mu_q^{\text{sym}}$, other refinements were introduced and studied in [78] and [76], Appendix A, namely the trisymmetric bilinear complexity $\mu_q^{\text{tri}}$ and normalized trisymmetric bilinear complexity $\mu_q^{\text{nrm}}$.

It should be noted that these quantities may not be well defined for some values of $q$ and $n$. More precisely, Proposition A.14 in [76] shows that $\mu_q^{\text{tri}}(n)$ is well defined for all values of $q$ and $n$, except for $q = 2$ and $n \geq 3$. Likewise, Proposition A.19 in [76] shows that $\mu_q^{\text{nrm}}(n)$ is well defined for all values of $q$ and $n$, except for $q = 2$, $n \geq 3$ and $q = 4$, $n \geq 2$.

In any case, when well defined, 
\[ \mu_q(n) \leq \mu_q^{\text{sym}}(n) \leq \mu_q^{\text{tri}}(n) \leq \mu_q^{\text{nrm}}(n). \]

Also, Theorem 2 in [78] gives 
\[ \mu_q^{\text{tri}}(n) \leq 4\mu_q^{\text{sym}}(n) \quad \text{for } q \neq 2 \text{ and } \text{char}(\mathbb{F}_q) \neq 3, \]
and Proposition A.19 in [76] gives 
\[ \mu_q^{\text{nrm}}(n) \leq 2\mu_q^{\text{tri}}(n) \quad \text{for } q \neq 7, \quad \text{and} \quad \mu_7^{\text{nrm}}(n) \leq 3\mu_7^{\text{tri}}(n). \]

Together with the linearity of $\mu_q^{\text{sym}}$, this gives the linearity of $\mu_q^{\text{nrm}}$ and $\mu_q^{\text{tri}}$ for most of the values of $q$.

But, apart from this, very little is known about these quantities.

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

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

(iii) Can one give better asymptotic bounds on them?

**5.4. The current generalized CCMA.** Now we can state Randriambololona’s result (see [74], Theorem 3.5), which provides the current most general CCMA. It makes use of the most elaborate form of derived evaluation, and gives bounds for both the asymmetric complexity and symmetric complexity.

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

**Theorem 5.3.** Let
- $q$ be a prime power,
- $F/\mathbb{F}_q$ be an algebraic function field,
- $Q$ be a place of $F/\mathbb{F}_q$ of degree $n = \deg Q$,
- $\ell$ be a positive integer,
- $D_1$ and $D_2$ be two divisors of $F/\mathbb{F}_q$,
- $\mathcal{P} = \{P_1, \ldots, P_N\}$ be a set of places of arbitrary degree $d_i = \deg P_i$,
- $u = \{u_1, \ldots, u_N\}$ be positive integers.

Suppose that neither $Q$ nor any of the places in $\mathcal{P}$ are in the support of $D_1$ and $D_2$, and that
(a) the maps

$$\varphi_{D_1,Q,\ell}: L(D_1) \rightarrow (F_q^n)^\ell \quad \text{and} \quad \varphi_{D_2,Q,\ell}: L(D_2) \rightarrow (F_q^n)^\ell$$

are onto,

(b) the map

$$\text{Ev}_{P,u}: L(D_1 + D_2) \rightarrow (F_q^{d_1})^{u_1} \times (F_q^{d_2})^{u_2} \times \cdots \times (F_q^{d_N})^{u_N},$$

$$f \mapsto (\varphi_1(f), \varphi_2(f), \ldots, \varphi_N(f))$$

is injective.

(Here $\varphi_{D_1,Q,\ell}$, $\varphi_{D_2,Q,\ell}$, and $\varphi_i = \varphi_{D_1+D_2,P_i,P_i}$ are the derived evaluation maps from (5).) Then

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

Moreover, if $D_1 = D_2$, the same holds for the symmetric bilinear complexity:

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

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

- a sufficient condition for the existence of $Q$ of degree $n$ is that
  $$2g + 1 \leq q^{(n-1)/2}(q^{1/2} - 1),$$

  where $g$ is the genus of $F$;

- a sufficient condition for (a) is that the divisors $D_1 - \ell Q$ and $D_2 - \ell Q$ are non-special:
  $$i(D_1 - \ell Q) = i(D_2 - \ell Q) = 0,$$

  where $i$ denotes the index of speciality;

- a necessary and sufficient condition for (b) is that the divisor $D_1 + D_2 - \mathcal{G}$ is zero-dimensional:
  $$\dim L(D_1 + D_2 - \mathcal{G}) = 0,$$

  where $\mathcal{G} = u_1 P_1 + \cdots + u_N P_N$.

The fact that $\mu_q(n, \ell)$ (respectively, $\mu^\text{sym}_q(n, \ell)$) appears on the left-hand side of the inequality allows one to apply the result recursively. For $n = 1$ it also provides bounds for the quantity $\tilde{M}_q(\ell)$ of Cenk and Özbudak (respectively, for $\tilde{M}^\text{sym}_q(\ell)$).

However, in the majority of applications we are interested mostly in the case $\ell = 1$. If we restate the result in this particular case and focus only on the symmetric part, this generalized version of the CCMA then specializes to the following statement (a special case of Theorem 3.5 in [74]), which suffices for most applications.
Corollary 5.4. Let
- $q$ be a prime power,
- $F/F_q$ be an algebraic function field,
- $Q$ be a place of $F/F_q$ of degree $n = \deg Q$ and with residue field $F_Q \cong F_q^n$,
- $D$ be a divisor of $F/F_q$,
- $\mathcal{P} = \{P_1, \ldots, P_N\}$ be a set of places of arbitrary degree $d_i = \deg P_i$,
- $u = \{u_1, \ldots, u_N\}$ be positive integers.

Suppose that neither $Q$ nor any of the places in $\mathcal{P}$ are in the support of $D$, and that
(a) the evaluation map
$$\varphi_{D,Q} : L(D) \to F_q^n,$$
$$f \mapsto f(Q)$$
is onto,
(b) the map
$$\text{Ev}_{\mathcal{P},u} : L(2D) \to (F_q^{d_1})^{u_1} \times (F_q^{d_2})^{u_2} \times \cdots \times (F_q^{d_N})^{u_N},$$
$$f \mapsto (\varphi_1(f), \varphi_2(f), \ldots, \varphi_N(f))$$
is injective, where $\varphi_i = \varphi_{2D,P_i,u_i}$ is the derived evaluation map from (5).

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

This can be specialized still further. Indeed, first observe that for all $d$ and $u$ we have the easy inequality
$$\mu_q^{\text{sym}}(d, u) \leq \mu_q^{\text{sym}}(d) \tilde{M}_q^{\text{sym}}(u).$$

This follows directly from Lemma 1.6, (b), applied with $A = F_q[t]/(t^u)$, $L = F_q^d$, and $K = F_q$. We deduce the following result.

Corollary 5.5. Under the same hypotheses as in Corollary 5.4, we have
$$\mu_q^{\text{sym}}(n) \leq \sum_{i=1}^{N} \mu_q^{\text{sym}}(d_i) \tilde{M}_q^{\text{sym}}(u_i).$$

Corollary 5.5 can be seen as a symmetric variant of the Cenk and Özbudak’s version of the CCMA [39]. It is weaker than Corollary 5.4 since the inequality $\mu_q^{\text{sym}}(d, u) \leq \mu_q^{\text{sym}}(d) \tilde{M}_q^{\text{sym}}(u)$ can be strict.

One should be careful to replace all bilinear complexities in the original statement of [39] (including the one for multiplicities) by symmetric bilinear complexities in order to get a valid symmetric reformulation.

Going further back in time, let us remark that the algorithm given in [43] by D. V. and G. V. Chudnovsky corresponds to the case $d_i = 1$ and $u_i = 1$ for $i = 1, \ldots, N$. The first generalization introduced by Ballet and Rolland in [24] concerns the case when $d_i$ is equal to 1 or 2 and $u_i = 1$ for $i = 1, \ldots, N$. Next, the generalization introduced by Arnaud in [1] concerns the case when $d_i$ is equal to 1 or 2 and $u_i$ is
equal to 1 or 2 for \( i = 1, \ldots, N \). In particular, as a corollary of Theorem 5.3, we have the following result obtained by Arnaud in [1] by gathering the places used with the same multiplicity; namely, he puts \( \ell_j := |\{ P_i | \deg P_i = j \text{ and } u_i = 2 \}| \) for \( j = 1, 2 \) and with \( \mathcal{D} = \mathcal{D}_1 = \mathcal{D}_2 \).

**Corollary 5.6.** Let

- \( q \) be a prime power,
- \( F/\mathbb{F}_q \) be an algebraic function field,
- \( Q \) be a degree \( n \) place of \( F/\mathbb{F}_q \),
- \( \mathcal{D} \) be a divisor of \( F/\mathbb{F}_q \),
- \( \mathcal{P} = \{ P_1, \ldots, P_{N_1}, P_{N_1+1}, \ldots, P_{N_1+N_2} \} \) be a set of \( N_1 \) places of degree one and \( N_2 \) places of degree two,
- \( 0 \leq \ell_1 \leq N_1 \) and \( 0 \leq \ell_2 \leq N_2 \) be two integers.

Suppose that neither \( Q \) nor any of the places in \( \mathcal{P} \) are in the support of \( \mathcal{D} \), and that

(a) the map

\[
\text{Ev}_Q : \mathcal{L}(\mathcal{D}) \rightarrow \mathbb{F}_{q^n} \cong F_Q
\]

is onto,

(b) the map

\[
\text{Ev}_{\mathcal{P}} : \mathcal{L}(2\mathcal{D}) \rightarrow \mathbb{F}_{q^N}^{\ell_1} \times \mathbb{F}_{q^N}^{\ell_1} \times \mathbb{F}_{q^2}^{\ell_2} \times \mathbb{F}_{q^2}^{\ell_2},
\]

\[
f \mapsto (f(P_1), \ldots, f(P_{N_1}), f'(P_1), \ldots, f'(P_{\ell_1}),
\]

\[
f(P_{N_1+1}), \ldots, f(P_{N_1+N_2}), f'(P_{N_1+1}), \ldots, f'(P_{N_1+\ell_2}))
\]

is injective.

Then

\[
\mu_{q, \text{sym}}^n(n) \leq N_1 + 2\ell_1 + 3N_2 + 6\ell_2.
\]

6. Choice of the curves

**6.1. Motivation and notation.** As seen in §§3 and 5, until now the best method to quantify the bilinear complexity of multiplication in finite fields is the CCMA based on interpolation over algebraic curves defined over a finite field. So, in this context, to get the best bounds on the upper-limit complexities \( M_q \) and \( M_q^\text{sym} \) or the upper bounds \( C_q \) and \( C_q^\text{sym} \) defined in §3.2, it is necessary to use sufficiently many different curves so as to deal with the worst cases. So let us give a name to the following requirement, formalized in [80], Claim on p. 163.

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

As introduced in the last section, multiplication algorithms based on interpolation on algebraic curves often require many points of higher degree \( r \geq 2 \). So let us study the best possible asymptotic ratios \( \beta_r \) of the number of places of degree \( r \) divided by the genus. The first definition is due to Tsfasman [84] (cf. also [26], Definitions 1.1, 1.2, and 1.3).
Definition 6.2. Let $\mathcal{X}/\mathbb{F}_q = (X_s/\mathbb{F}_q)$ be a sequence of curves $X_s/\mathbb{F}_q$ of genus $g_s = g(X_s/\mathbb{F}_q)$ defined over a finite field $\mathbb{F}_q$. Suppose that the sequence of genera $g_s$ is an increasing sequence growing to infinity. Then the sequence $\mathcal{X}/\mathbb{F}_q$ is said to be \textit{asymptotically exact} if for all $m \geq 1$ the limit $\beta_r(\mathcal{X}) = \lim_{s \to \infty} (B_r(X_s)/g_s)$ exists, where $B_r(X_s)$ denotes the number of closed points of degree $r$ of the curve $X_s$.

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

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

Then we put

$$A_r(q) = \sup_{\mathcal{X}} \beta_r(\mathcal{X}),$$

where $\mathcal{X}$ runs over all asymptotically exact sequences of curves, and

$$A'_r(q) = \sup_{\mathcal{X}} \beta_r(\mathcal{X}),$$

where $\mathcal{X}$ runs over all dense asymptotically exact sequences of curves.

Remark 6.4. Note that $A_1(q)$ is the classical Ihara constant $A(q)$ defined by Ihara in [63]. The order $r$ Ihara constants $A_r(q)$ were, in particular, defined in [26], Definition 1.3. Concerning the quantities $A'_r(q)$, note that the dense Ihara constant $A'_1(q)$ was first introduced (and denoted by $A'(q)$) by Randriambololona in [73] (cf. also [77]). The order $r$ dense Ihara constants $A'_r(q)$ were first introduced (and denoted by $A'_r(q)$) by Rambaud in [71].

The following result is possibly well known. It is essentially a consequence of Lemma IV.3 in [38], itself based on the generalized bound of Drinfeld and Vlăduț (cf. [84], Theorem 1, and also [26], Definitions 1.2 and 1.3).

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

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

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

As a corollary of Theorem 1 in [84], the following result holds.
Theorem 6.6.

\[ A'_r(q) \leq A_r(q) \leq \frac{\sqrt{q^r} - 1}{r}. \]  

6.2. Explicit towers, densification and descent. The pioneering papers [43] and [80], which aimed to prove the linearity (cf. §3.2) of bilinear complexity with respect to the extension degree, required the use of infinite families of curves with many rational points relative to the genus. However, the first families of curves (of modular and Shimura type) to have been found made it possible to obtain purely asymptotic bounds only. So, the objective of [5] (cf. also [6] and footnote 1 on p. 38) was to give the first uniform upper bounds with respect to \( q \). For this it was necessary to use more explicit families of curves. The first tower of algebraic function fields of Garcia–Stichtenoth [57] fulfilled the required conditions: the knowledge of fundamental invariants, namely the genus and the number of rational points of each step of the tower which attains the Drinfeld–Vlăduţ bound. From a general point of view, to obtain the best bounds by the CCMA, we need to use families of curves of genus increasing as slowly as possible (cf. §5.1 and Theorem 9.5 in §9.2). But a tower of algebraic function fields is composed of successive algebraic function fields whose genera increase with the extension degree between two consecutive steps according to the Hurwitz formula. For example, the first Garcia–Stichtenoth tower defined over \( \mathbb{F}_{q^2} \) is an Artin–Schreier tower for which the ratio of two consecutive genera is \( g_{i+1}/g_i > q \), where \( q \) is an arbitrary prime power.

In this case, an interesting strategy to improve the bounds obtained with this type of tower consisted in densifying this tower by adding intermediate steps (cf. [7]). It is easily possible in this case, even without knowing the recursive equation of intermediate steps, because the tower is a Galois tower. When the towers \( \mathcal{X}/\mathbb{F}_q \) used are such that the value of \( \beta_1(\mathcal{X}) \) is insufficiently large (which is the case when the finite fields of definition are small or when the best known lower bound of the Ihara constant \( A_r(q) \), associated with the definition field \( \mathbb{F}_q \) is insufficiently large), it is necessary to use places of degree > 1 because of the Drinfeld–Vlăduţ bound (cf. [24] and [20]). So, we need families of curves reaching the Drinfeld–Vlăduţ bound of order \( r > 1 \) (cf. [25] and assertion (ii) in Theorem 6.5). Until now, the only way to obtain such families has been the technique of descent of families of algebraic function fields defined over \( \mathbb{F}_{q^2} \) on the definition field \( \mathbb{F}_q \), which was introduced in [24]. Of course, the descent of the original tower of Garcia–Stichtenoth is always possible since the coefficients of the recursive equation lie in \( \mathbb{F}_q \). However, the problem arises as soon as we introduce intermediate steps. So, in [24], the descent was made explicit only for characteristic two and \( r = 2 \) because in this case the descended tower conserves the Galois property. Then, a generalization for any characteristic for \( r = 2 \) was realized in [19] by using two different techniques: theoretically by using the action of the Galois group of \( \mathbb{F}_{q^2}/\mathbb{F}_q \) on the intermediate steps of the tower defined on \( \mathbb{F}_{q^2} \), or by finding explicit equations of the intermediate steps. Then, with all the possibilities of the towers having been used, it became necessary to use families of algebraic function fields more dense than the towers. For this purpose, it was natural to go back to the study of families of modular and Shimura curves, which is the subject of the following section.
6.3. Modular and Shimura curves. The previous section motivates the search for dense families of curves becoming optimal after a base field extension of (low) degree $r$.

Firstly, given that the towers of Garcia–Stichtenoth [57], [58] are actually defined over their prime field $\mathbb{F}_p$, for any base extension degree $r$ there exist non-dense towers reaching the previous bound (see §6.2):

$$A_r(q) = \sqrt{q^r - 1}$$

as long as $q^r$ is a square. (8)

Now, in the particular case of quadratic extensions $r = 2$, the celebrated results of [63] and [86] (cf. also [80]) state that (see also the two original approaches of [48], Theorem IV.4.5), for all prime powers $q$ there exist dense families of Shimura modular curves over $\mathbb{F}_q$ that become optimal over $\mathbb{F}_{q^2}$; see also [88] for an introduction (in characteristic zero). Notice that classical modular curves over prime fields $\mathbb{F}_p$ are a particular case of Shimura curves.

Summing up, the Shimura curves mentioned above match the bound of Drinfeld and Vlăduţ over $\mathbb{F}_{q^2}$, which reads

$$A'_1(q^2) = q - 1.$$ (9)

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

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

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

- the canonical morphisms over $\mathbb{Q}$

$$X_0(l^2) \rightarrow X_0(l) \rightarrow X_0(1);$$

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

Remark 6.7. Actually, the first step is enough to deduce the whole tower recursively (see the historical notes and references in §6.3.3 below). Namely, one needs only the covering map $X_0(l) \rightarrow X_0(1)$ and the Atkin–Lehner involutions $w_i$ for $i = 0, 1$. Caution must be exercised since the fibre product of the first step $X_0(l)$ with its Atkin–Lehner twist, in addition to being highly singular, contains a second irreducible component on top of $X_0(l^2)$. This comes from degree considerations (or modular interpretation considerations, if one prefers); see [71], Chap. VI, §§2.3 and 3.2.
The genera in a single tower \( X_0(l^i)_\mathbb{F}_p \) for any \( p \) are tightly controlled by the prime powers \( l^i \):

\[
\frac{1}{12} l^i \left(1 + \frac{1}{l}\right) + o(g_i) \leq g_i \leq \frac{1}{12} l^i \left(1 + \frac{1}{l}\right)
\]  

(11)

(see [85], Chap. 4.1, or [47], Theorem 3.1.1 and p. 107). So, this single tower does not form a dense family.

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

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

for any \( i \) and \( j \). By doing so for each pair of indices \( i \) and \( j \), we obtain the family \( \{X_0(l^i l'^j)_\mathbb{Q}\}_{i,j} \). Let us call this family the ‘intertwining’ of the two recursive towers. This family has good reduction at any prime \( p \neq l, l' \) and is asymptotically optimal. The genera in this family are now closely controlled by the prime products \( l^i l'^j \), as follows from

\[
\frac{1}{12} l^i l'^j \left(1 + \frac{1}{l}\right) \left(1 + \frac{1}{l'}\right) + o(g_{i,j}) \leq g_{i,j} \leq \frac{1}{12} l^i l'^j \left(1 + \frac{1}{l}\right) \left(1 + \frac{1}{l'}\right).
\]  

(12)

The key observation is that the family of integers \( l^i l'^j \) is dense, that is, its growth rate tends to zero, so that the intertwined family \( \{X_0(l^i l'^j)_\mathbb{Q}\}_{i,j} \) is dense.

6.3.2. Problems of descent on Shimura curves and open questions. Let us turn to Shimura curves and consider three specific recursive towers \( X_0(p^i) \) defined over the same basis \( X_0(1) \) of genus zero. Let \( F = \mathbb{Q}[\cos(2\pi/7)] \) be a totally real number field of degree three, and let \( p_2 \) and \( p_3 \) be the prime ideals generated by the inert primes 2 and 3, and \( p_7 \) the prime ideal generated by the split prime 7. Let \( B \) be a quaternion algebra over \( F \), which is ramified exactly at two of the three real places and no finite place. The algebra \( B \) contains one unique conjugacy class of Eichler orders of given level. In particular, ‘the’ maximal order \( \mathcal{O} \) has its group of units \( \mathcal{O}^1 \), which embeds into \( \text{PSL}_2(\mathbb{R}) \) with the celebrated \((2,3,7)\) triangle group (it is the hyperbolic group of smallest covolume) as its image. The Shimura curve \( X_0(1)_{\mathbb{C}} \) uniformized by this group has a canonical model over \( F \) of genus zero with three rational points of order 2, 3, and 7, which arise precisely from the elliptic points. Above this base curve one has notably the three towers \( X_0(p^i) \), where \( p = p_2, p_3, \) and \( p_7 \), which have canonical models over \( F \). They have good reduction at every prime \( p' \) of \( F \) different from \( p_2, p_3, \) and \( p_7 \). If, furthermore, \( p' = (p) \) comes from an inert prime, then the reductions \( X_0(p^i)_{\mathbb{F}_p} \) modulo \( p \) have an asymptotically optimal number of points over \( \mathbb{F}_p^{6} \) (see Theorem IV.4.5 in [48], which has been established using two independent methods).

Now, intertwining the two towers \( X_0(p^j_2) \) and \( X_0(p^j_7) \) over \( X_0(1) \) gives a dense family \( \{X_0(p^i_2p^j_7)_{\mathbb{F}}\}_{i,j} \) over \( F \), with genera tightly controlled by the products \( 8^i \cdot 7^j \):

\[
g_{i,j} = 7^{j-2} \left(\frac{8^{i-1} \cdot 6}{7} + \frac{1}{7}\right) \quad \text{for } i \geq 1 \text{ and } j \geq 2
\]  

(13)

(and similar formulae for smaller \( i \) or \( j \); see [71], Chap. IV, Corollary 2.12). In particular, it has good reduction modulo \( p_3 = (3) \) and yields an asymptotically
optimal dense family $X_0(p_2^j p_7^j)_{F_{3^3}}$ over $F_{3^3}$ with many points in $F_{3^6}$. Now, an interesting problem for bilinear multiplication over $F_3$ is this: *Can we descend this family over $F_3$?* Much of the work towards this result has been done since it was proved in [71], Chap. VI, §5.2, that the first two steps of the reductions modulo $p' = p_3$ of the two towers descend over $F_3$. But recall that, over $F$, these first two steps are sufficient to build the whole family. So, the problem of descent of the family over $F_3$ comes down to the following general question.

**Open problem 6.8.** Are good reductions of towers of Shimura curves recursive?

**Conjecture 6.8.1.** *The answer to Open problem 6.8 is positive.*

We are confident that this point comes down to the modular interpretation of integral models of Shimura curves (and not only models over number fields such as $F$), which should also be well known to experts.

Additional evidence supports the descent question we are concerned with since it was also established in [71], Chap. V, Theorem 5.14, that the family \{ $X_0(p_2^i p_7^j)_{F}$ \}$_{i,j}$ descends over $\mathbb{Q}$, and strong numerical evidence (the number of points) suggests that the canonical reduction of the third steps ($i = 3$ and/or $j = 3$) over $F_{3^3}$ also descends over $F_3$ (see [71], Chap. VI, §5.2).

Recapitulating: Descent of the previous family, as would be implied, for example, by Conjecture 6.8.1, would provide a dense family over $F_3$ with many points of degree 6, which would thus establish that

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

which was (prematurely) claimed as Theorem B in [71].

Likewise, intertwining the two towers $X_0(p_3^i)$ and $X_0(p_7^j)$ over $X_0(1)$ gives a dense family \{ $X_0(p_2^i p_7^j)_{F}$ \}$_{i,j}$ over $F$, with genera tightly controlled by the products $27^i \cdot 7^j$, good reduction modulo $p_2 = (2)$ over $F_{2^3}$, and asymptotically many points in $F_{2^6}$.

**Open problem 6.9.** Similarly, we are concerned with the descent of this dense family over $F_2$, which if true would thus yield the value $A'_6(2) = (2^3 - 1)/6$. Assume that the previous Conjecture 6.8.1 is true. Then this would already imply that the tower $X_0(p_7^j)$ descends over $F_2$. So, we would then be left to show that the first two steps of the tower $X_0(p_3^i)$ also descend. More precisely, we state the next conjecture.

**Conjecture 6.9.1.** *The following morphisms descend over $F_2$: the canonical branched cover $X_0(p_2^i p_7^j)_{F_{2^3}} \to X_0(p_3^i)_{F_{2^3}}$ and the Atkin–Lehner involution on $X_0(p_3^i)_{F_{2^3}}$.*

Finally, notice that the first step of this tower $X_0(p_3)_{\mathbb{Q}} \to X_0(1)_{\mathbb{Q}}$ was explicitly computed over $\mathbb{Q}$ in [53]: a Belyi map of degree 27. So, if it were true that good reduction of towers of Shimura curves is also recursive from the first step (see Remark 6.7), then one would be left with the easier problem of finding a good reduction modulo (3) of this Belyi map of degree 27.

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

**Conjecture 6.10.1.** Let \( p \) be a prime number and \( 2t \geq 4 \) an even integer. Then

\[
A'(q) = \frac{p^{t} - 1}{2t}.
\]  

(15)

In other words: There exists a family \( \{X_s/\mathbb{F}_p^{2t}\}_{s \geq 1} \) of curves over \( \mathbb{F}_p \) with (increasing) genera \( g_s \) tending to infinity such that

(i) \( X_s \) is, actually, defined over the prime field \( \mathbb{F}_p \);

(ii) \( \lim_{s \to \infty} (g_{s+1}/g_s) = 1 \) (maximal density condition);

(iii) \( \lim_{s \to \infty} (|X_s(\mathbb{F}_p^{2t})|/g_s) = p^t - 1 \) (Ihara constant over \( \mathbb{F}_p^{2t} \)).

**Open problem 6.11.** The following conjecture was proposed in [72], to which we add a density requirement.

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

Its consequence would be the asymptotic vanishing of 2-torsion in classical modular curves.

**Proposition 6.11.2.** Under Conjecture 6.11.1, there exists a dense family of (classical modular) curves \( \{X_0(N_s)/\mathbb{F}_p\}_{s \geq 1} \) such that

\[
(\text{Cl}_0(X_0(N_s)))(\mathbb{F}_p^{2})[2] = \{0\}
\]

(that is, curves that have no 2-torsion in their class group).

This proposition is stated as Conjecture 2.8 in [71], Chap. I. A detailed proof that it results from Conjecture 6.11.1 is given there; see the discussion above Conjecture 2.8 in [71], Chap. I, §2.2 (for the key formula (2.6)) and also [71], Chap. II, §5 (for the proof of the key formula (2.6)). The following practical consequence will be proved in the Appendix (§11).

**Proposition 6.11.3.** Let \( p \) be a prime number such that Conjecture 6.11.1 holds for \( p \), and let \( r \) be an integer such that \( \{q = p \text{ and } r = 2\} \) or \( \{q = p^2 \text{ and } r = 1\} \). Then formula (a) in Theorem 8.21 also holds.

6.3.3. References and historical notes for §6. Recursive modular towers. The recursivity of towers of classical modular curves was pointed out in the seminal paper of Elkies [50], where more details and a proof over \( \mathbb{C} \) can be found. The proof carries over to the canonical models over \( \mathbb{Q} \) since the moduli interpretation in terms of elliptic curves is the same. Elkies also claims (and uses it) that towers of Shimura curves are recursive. The proof of this fact is formally analogous; see [48], Proposition IV.5.1. But, actually, extra care must be taken with the irreducibility of the tensor products involved (see [71], Chap. VI, §§2.3 and 3.2) because the moduli interpretation is much more complicated.
Intertwining two towers over the same basis: This construction was already mentioned in [50]. The crucial observation that the resulting family is dense was pointed out to us by Elkies in August 2015.

Recursivity from the first step. The fact that the first step of modular towers is actually enough to construct them recursively was already pointed out in [50], footnote 4, and in [52], and brought to our attention by Elkies in 2017.

About Conjecture 6.10.1. This conjecture was essentially stated as Lemma IV.4 in [38]. For the proof, the authors claim that some specific Shimura curves with Galois invariant parameters descend over the rationals. This claim is unfortunately false. In [22], §3, we exhibited counterexamples to this claim, which evidence that, more generally, Shimura curves do not descend over their field of moduli. Consequences of Conjecture 6.10.1 on upper-limit asymptotic complexities are given by Rambaud in [71], Table 2.2, lines ‘Conj Y’. Notice that they are a slight improvement on those claimed in [38], displayed in footnote 11 on p. 67.

More on explicit computations. Following the seminal works of [86] and [63] on Shimura curves with many points, many equations of curves of genus zero and one were computed in [51], [61], and [81]. Further examples of recursive towers of Shimura curves can be found in [48], Chap. IV, Example 5.3, [62], and [71], Chap. VI, §3 (defined over a totally real field of narrow class number two, with a record number of points over $F_{5^4}$ in genus 5). The (non-explicit) list of Shimura curves of genus less than two can be found in [89]. From this data and the recent tools for Belyi maps developed in [67], one could obtain a dozen of recursive towers whose first step is the covering map of $\mathbb{P}^1$ of degree $\leq 9$ ramified above three points. Finally, in the case when the first step is over a genus one curve, the first example was computed in Levrat’s master’s thesis [65].

7. Obtaining a divisor of optimal degree for symmetric algorithms

Using the numerical criteria at the end of Theorem 5.3, in the symmetric case $\mathcal{D}_1 = \mathcal{D}_2$ we come across the following problem. Given

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

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

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

and

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

are both satisfied?

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

$$N \geq 2n + g - 1 \quad (18)$$

is a necessary condition for the existence of a solution.
Observe that, in order to get the algorithm with best complexity for a given \( n \), we need \( N \) to be as small as possible.

In their original paper [43], D. V. Chudnovsky and G. V. Chudnovsky introduced a simple cardinality and degree argument, later made more explicit by Ballet in [6]. This proved the existence of a solution under the suboptimal condition

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

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

In order to repair their proof, two approaches have been devised:

- choose curves with 2-torsion as small as possible;
- directly construct \( D \) under condition (18).

### 7.1. Bounding 2-torsion

Bounds on torsion in the class group were first introduced by Xing [92] in a very similar context, namely that of frameproof codes (also called linear intersecting codes). Indeed, in order to obtain an \( s \)-frameproof code of high rate, given a divisor \( G \), one needs to prove the existence of a divisor \( D \) of high degree such that

\[
\dim L(sD - G) = 0. \tag{20}
\]

Xing proved the existence of such a \( D \) using a cardinality argument similar to that of D. V. and G. V. Chudnovsky, and of Shparlinski, Tsfasman, and Vlăduţ, while correctly recognizing the difficulty with \( s \)-torsion. His result on the rate of \( s \)-frameproof codes thus includes a term accounting for the size of the \( s \)-torsion subgroup. Actually, Xing used the well-known upper bound \( s^{2g} \) for the size of the \( s \)-torsion subgroup in the Jacobian of a curve of genus \( g \).

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

- by Randriambololona, through the quantity \( \delta_s^-(q) \) in [72],
- and by Cascudo, Cramer, and Xing, through the torsion-limit \( J_r(q, a) \) in [36] and [37].

One of the questions asked by Randriambololona in [72] is the following: For given \( q \) and \( s \), can one find an infinite sequence of curves having many rational points (ideally, matching the Ihara constant \( A(q) \)), but whose class group has low \( s \)-torsion?

How asymptotically small this \( s \)-torsion can be is measured by the following quantity.

**Definition 7.1.** Let \( \delta_s^-(q) \) be the smallest real number such that there exists a sequence \( (X_k)_{k \geq 1} \) of curves over \( \mathbb{F}_q \) of increasing genus \( g_k = g(X_k) \) with the asymptotic number of rational points

\[
\lim_{k \to \infty} \frac{|X_k(\mathbb{F}_q)|}{g_k} = A(q)
\]
and such that the cardinal number of the $s$-torsion subgroup $J_k(\mathbb{F}_q)[s]$ of the group of rational points over $\mathbb{F}_q$ of the Jacobian $J_k = J(X_k)$ satisfies
\[
\lim_{k \to \infty} \frac{\log_s |J_k(\mathbb{F}_q)[s]|}{g_k} = \delta_s^{-}(q).
\]

**Open problem 7.2.** Estimating $\delta_s^{-}(q)$ for an infinite sequence of curves attaining the Drinfeld–Vlăduţ bound. Randriambololona conjectured that $\delta_s^{-}(q) = 0$ for all $s$ and $q$, that is, there exist curves that have an asymptotically maximal number of points over $\mathbb{F}_q$ and whose class groups have asymptotically negligible $s$-torsion. Of special importance for us is the case $s = 2$, that is, the case of 2-torsion. In [72] Randriambololona focused on classical modular curves, which have an asymptotically maximal number of points over $\mathbb{F}_{p^2}$ (for a prime number $p$). The size of the class group of such a curve is given by the determinant of a Hecke operator. This leads to deep number theoretic questions on the parity of these determinants, which remain conjectural at this time.

In [37] Cascudo, Cramer, and Xing generalized conditions like (16) and (17) or like (20) into what they name Riemann–Roch systems of equations. They adapted the cardinality argument of [43], [80], and [92] in this more general framework. First, for a function field $F/\mathbb{F}_q$, let $J_F$ be its zero divisor class group. Then let $J_F[r]$ be its $r$-torsion subgroup of cardinality $J_F[r] = |J_F[r]|$. Their main result (see [37], Theorem 3.2) is as follows.

**Proposition 7.3.** Let
- $q$ be a prime power,
- $F/\mathbb{F}_q$ be a function field,
- $h$ be the class number of $F$,
- $A_m$ be the number of effective divisors of degree $m$ in the group of divisors $\text{Div}(F)$ for $m > 0$,
- $u \geq 1$ be an integer,
- $\mathcal{Y}_1, \ldots, \mathcal{Y}_u$ be divisors of $F$,
- $m_1, \ldots, m_u$ be non-zero integers.

Suppose that for some integer $s \in \mathbb{Z}$ the inequality
\[
h > \sum_{i=1}^{u} A_{r_i(s)} J_F[m_i]
\]
holds, where $r_i(s) = m_i s + \deg \mathcal{Y}_i$. Then the system of conditions
\[
\dim \mathcal{L}(m_1 \mathcal{D} + \mathcal{Y}_1) = \cdots = \dim \mathcal{L}(m_u \mathcal{D} + \mathcal{Y}_u) = 0
\]
is satisfied by some divisor $\mathcal{D}$ of degree $s$.

In order to measure the size of the torsion subgroups, in [37] the authors introduce the notion of torsion-limit.

**Definition 7.4.** For each family $\mathcal{F} = \{F/\mathbb{F}_q\}$ of function fields with increasing genus $g(F)$, we define the asymptotic limit
\[
J_r(\mathcal{F}) = \liminf_{F \in \mathcal{F}} \frac{\log_q J_F[r]}{g(F)}.
\]
For a prime power $q$, an integer $r > 1$, and a real number $a \leq A(q)$, let $\Upsilon$ be a set of families $\{\mathcal{F}\}$ of function fields over $\mathbb{F}_q$ such that the genus in each family tends to $\infty$ and the Ihara limit satisfies $A(\mathcal{F}) \geq a$ for every $\mathcal{F} \in \Upsilon$. Then the asymptotic quantity $J_r(q,a)$ is defined by

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

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

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

This torsion-limit can be introduced as a correcting term in the denominator of the bound claimed by Shparlinski, Tsfasman, and Vladut, as we shall see in §8.2. However, another approach is possible, namely, a direct construction.

### 7.2. Direct construction.

The direct construction consists in finding the best divisors $D$ to apply the CCMA, that is, divisors $D$ satisfying conditions (16) and (17) for given $q$ and $n$. The idea was explicitly introduced by Ballet in [9], Theorem 2.2, as we shall see more precisely in §9.2. Then Chaumine proved in [41] (cf. also [42]) that the direct construction is optimal in the elliptic case, hence improving the result of Shokrollahi [79], as we shall see in §9.1. Then, Randriambololona introduced new ideas, which originated in his work [75], for the construction of intersecting codes. The technique was then extended in [73] in order to solve more general Riemann–Roch systems of equations. In the case of the Riemann–Roch system associated with a CCMA, it facilitates an effective construction of a solution, in most cases up to the optimal degree.

The key point is the following result (see [75], Lemma 9), which can be seen as a numerical variant of a generalized Plücker formula.

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

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

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

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

In [73] it was shown how the bound $4g$ can be slightly improved when $K$ is a finite field. However, the original Lemma 7.5 suffices to prove the following result (see [73], Corollary 20).

**Proposition 7.6.** Let

- $q$ be a prime power,
- $F/\mathbb{F}_q$ be a function field of genus $g$,
- $Q$ be a divisor of $F/\mathbb{F}_q$ of degree $n = \deg Q$,
- $G$ be a divisor of $F/\mathbb{F}_q$ of degree $N = \deg G$.
Assume that the number of degree 1 places of $F$ satisfies

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

Then, provided that

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

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

- $\deg D = n + g - 1$,
- $\dim L(D - Q) = i(D - Q) = 0$,
- $\dim L(2D - G) = 0$.

Observe that for a divisor of degree $g - 1$, the properties of being non-special and zero-dimensional are equivalent, so here $i(D - Q) = 0$ and $\dim L(D - Q) = 0$ are equivalent.

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

Besides [73], the proof of this Proposition 7.6 can also be found inside that of Theorem 5.2, (c), in [74].

8. Asymptotic upper bounds

The asymptotic study of the bilinear complexity of multiplication consists in evaluating the quantities $m_q$, $M_q$, $m_q^{\text{sym}}$, and $M_q^{\text{sym}}$. The importance of this study comes from the fact that, generally, we have better estimates of these quantities than of the constants $C_q$ and $C_q^{\text{sym}}$. Indeed, the best known families of curves suitable to the application of the D.V. and G.V. Chudnovsky algorithm are known asymptotically, in particular, the families of Shimura curves used by Shparlinski, Tsfasman, and Vlăduț in [80]. The latter authors established the following general result, which we can view as a direct consequence of Lemma 1.7 (or Lemma 1.2 in [80])

$^4$

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

$$m_q \leq m_q^n \cdot \mu_q(n)n^{-1} \quad (22)$$

and

$$M_q \leq M_q^n \cdot \mu_q(n). \quad (23)$$

Actually, inequality (22) for $m_q$ is already implicit in the original paper of D.V. Chudnovsky and G.V. Chudnovsky (equation (6.2) in [43]). So, here, the important new contribution of Shparlinski, Tsfasman, and Vlăduț is inequality (23) for $M_q$. Note that these inequalities are also true in the symmetric case, as a consequence of Lemma 1.8.

$^4$Their main motivation to introduce this lemma was to deduce the finiteness of $M_q$ for all $q$ from the finiteness of $M_q$ for $q$ a square.
Lemma 8.2.

\[ m_{q}^{\text{sym}} \leq m_{q^n}^{\text{sym}} \cdot \mu_{q}^{\text{sym}}(n)n^{-1} \] (24)

and

\[ M_{q}^{\text{sym}} \leq M_{q^n}^{\text{sym}} \cdot \mu_{q}^{\text{sym}}(n). \] (25)

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

Corollary 8.3. For every prime power \( q \),

\[ m_{q} \leq \frac{3}{2} m_{q^2}, \quad m_{q}^{\text{sym}} \leq \frac{3}{2} m_{q^2}^{\text{sym}}, \quad M_{q} \leq 3 M_{q^2}, \quad \text{and} \quad M_{q}^{\text{sym}} \leq 3 M_{q^2}^{\text{sym}}. \]

If \( q \geq 4 \), then

\[ m_{q} \leq \frac{5}{3} m_{q^3}, \quad m_{q}^{\text{sym}} \leq \frac{5}{3} m_{q^3}^{\text{sym}}, \quad M_{q} \leq 5 M_{q^3}, \quad \text{and} \quad M_{q}^{\text{sym}} \leq 5 M_{q^3}^{\text{sym}}. \]

Recall that \( A(q) \) denotes the Ihara limit defined by

\[ A(q) := \limsup_{g \to \infty} \frac{N_{q}(g)}{g}, \]

where \( N_{q}(g) \) is the maximum number of rational places over all the algebraic function fields over \( \mathbb{F}_q \) of genus \( g \) (cf. also Definition 7.1).

8.1. Upper bounds for \( m_{q} \) and \( M_{q} \). Thanks to the asymmetric interpolation allowed by the generalized CCMA (cf. §5.3), Randriambololona (see [74], Theorems 6.3 and 6.4) obtained bounds for \( m_{q} \) and \( M_{q} \).

For \( m_{q} \) the bound is as follows.

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

\[ m_{q} \leq 2 \left( 1 + \frac{1}{A(q) - 1} \right). \] (26)

For \( M_{q} \) we have the following bound.

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

\[ M_{q} \leq 2 \left( 1 + \frac{1}{\sqrt{q} - 2} \right). \] (27)

Combined with Lemma 8.1 and \( \mu_{q}(2) = 3 \), this implies at once the following result.

**Corollary 8.6.** Let \( q \geq 3 \) be a prime or a non-square prime power. Then

\[ m_{q} \leq 3 \left( 1 + \frac{1}{q - 2} \right) \] (28)

and

\[ M_{q} \leq 6 \left( 1 + \frac{1}{q - 2} \right). \] (29)
Moreover, from Theorem 9.18, Pieltant and Randriambololona deduced the following asymptotic bounds in the general case.

**Theorem 8.7.**

\[ M_3 \leq 6, \quad M_4 \leq \frac{87}{19} \approx 4.579, \quad M_5 \leq 4.5, \quad M_{11} \leq 3.6, \quad \text{and} \quad M_{13} \leq 3.5. \]

These bounds are the best published current asymptotic bounds in the general case. They are deduced from the best known uniform bounds. Indeed, the purely asymptotic bounds given in [69], Theorem 5.3, Corollaries 5.4 and 5.5, are unproved as established in [22].

In addition, as a corollary of the uniform bounds in Proposition 9.19 (cf. §9.3), Randriambololona has recently obtained the following result.

**Theorem 8.8.** For \( p \geq 7 \) we have

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

Finally, in [71] Rambaud obtained the current best general upper-limit asymptotic bound, stated in the following theorem.

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

\[ M_q \leq 2 \mu_q(r, l) \left( 1 + \frac{1}{rlA_r'(q) - 1} \right). \]

In particular, this result enables one to obtain the following value (with \((r, l) = (4, 1), \mu_q(r, l) \leq \mu_q^{\text{sym}}(r, l) = 9\) by Table 1 in §9.1, and \( A_r'(2) = 3/4 \) by formula (7)).

**Corollary 8.10.**

\[ M_2 \leq 7. \]

### 8.2. Upper bounds for \( m_q^{\text{sym}} \) and \( M_q^{\text{sym}} \)

Initially, by using the original D.V. Chudnovsky and G.V. Chudnovsky results, Shparlinski, Tsfasman, and Vlăduț [80] obtained upper bounds\(^6\) for \( M_q^{\text{sym}} \) and \( m_q^{\text{sym}} \) for any \( q \), which were incompletely proved because of the gap mentioned in §3.2. In [74], Theorems 6.3 and 6.4, Randriambololona obtained the following results, which prove the bounds of Shparlinski, Tsfasman and Vlăduț with a slight restriction on the range of the values for \( A(q) \) and \( q \). For \( m_q^{\text{sym}} \) the bound is as follows.

\(^5\)These unproved bounds are

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

for \( q \) a prime power and \( t \geq 1 \) an integer such that \( q^t \geq 9 \) is a square, and

\[ M_2 \leq \frac{35}{6}, \quad M_3 \leq \frac{36}{7}, \quad M_4 \leq \frac{30}{7}, \quad M_7 \leq 3.6, \quad \text{and} \quad M_8 \leq 3.5. \]

\(^6\)These are the following bounds:

\[ m_q^{\text{sym}} \leq 2 \left( 1 + \frac{1}{A(q) - 1} \right), \quad \text{where} \quad A(q) > 1 \quad \text{is defined in Proposition 8.14}; \]

\[ m_q^{\text{sym}} \leq 2 \left( 1 + \frac{1}{\sqrt{q} - 2} \right), \quad \text{where} \quad q \geq 9 \quad \text{is a perfect square}; \]
Theorem 8.11. Let \( q \) be a prime power such that \( A(q) > 5 \). Then
\[
m_q^{\text{sym}} \leq 2 \left( 1 + \frac{1}{A(q) - 1} \right). \tag{30}
\]

For \( M_q^{\text{sym}} \) we have the following bound.

Theorem 8.12. Let \( q = p^{2r} \geq 49 \) be a square prime power. Then
\[
M_q^{\text{sym}} \leq 2 \left( 1 + \frac{1}{\sqrt{q} - 2} \right). \tag{31}
\]

Combined with Lemma 8.2 and \( m_q^{\text{sym}}(2) = 3 \), this implies at once the following result.

Corollary 8.13. Let \( q \geq 7 \) be a prime or a non-square prime power. Then
\[
m_q^{\text{sym}} \leq 3 \left( 1 + \frac{1}{q - 2} \right) \tag{32}
\]
and
\[
M_q^{\text{sym}} \leq 6 \left( 1 + \frac{1}{q - 2} \right). \tag{33}
\]

In [17] Ballet, Chaumine, and Pieltant obtained slightly less accurate bounds than the above ones, but for slightly larger ranges of values for \( A(q) \) and \( q \). They gave the following propositions.

Proposition 8.14. Let \( q \) be a prime power such that \( A(q) > 2 \). Then
\[
m_q^{\text{sym}} \leq 2 \left( 1 + \frac{1}{A(q) - 2} \right).
\]

Corollary 8.15. Let \( q = p^{2m} \) be a square prime power such that \( q \geq 16 \). Then
\[
m_q^{\text{sym}} \leq 2 \left( 1 + \frac{1}{\sqrt{q} - 3} \right).
\]
\[
m_q^{\text{sym}} \leq 2 \left( 1 + \frac{1}{c \log_2 q - 1} \right), \quad \text{where } q \geq 2^{1/c} \text{ with } c \text{ a positive constant;}
\]
\[
m_q^{\text{sym}} \leq 2 \left( 1 + \frac{q^{1/3} + 2}{2q^{2/3} - q^{1/3} - 4} \right); \quad m_2^{\text{sym}} \leq \frac{35}{6};
\]
\[
m_q^{\text{sym}} \leq 3 \left( 1 + \frac{1}{q - 2} \right), \quad \text{where } q > 2;
\]
\[
M_q^{\text{sym}} \leq 2 \left( 1 + \frac{1}{\sqrt{q} - 2} \right), \quad \text{where } q \geq 9 \text{ is a perfect square;}
\]
\[
M_q^{\text{sym}} \leq 6 \left( 1 + \frac{1}{q - 2} \right), \quad \text{where } q > 2; \quad M_2^{\text{sym}} \leq 27.
\]

These bounds were given, respectively, in [80], Theorem 3.1, [80], Corollary 3.4, [80], Corollary 3.5, [80], Remark 3.6, [80], Corollary 3.7, [80], Corollary 3.8, [80], Theorem 3.9, and [80], Corollary 3.10, for the last two bounds. Note that these bounds were originally formulated with notation \( m_q \) and \( M_q \), but for the same reasons as those mentioned in footnote 2 of §3.2, these bounds concern the quantities \( M_q^{\text{sym}} \) and \( m_q^{\text{sym}} \). Note that there exist proved bounds exceeding the last one (cf. Proposition 8.23).
Note that this corollary slightly improves the range of the bound (4) proved by D.V. and G.V. Chudnovsky. The following assertion was obtained in [17] in the case of an arbitrary $q$.

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

\[ m_q^{\text{sym}} \leq 3 \left( 1 + \frac{1}{q - 3} \right). \]

Moreover, for $M_q^{\text{sym}}$, in [17] the authors obtained the same value for the same range as those for $m_q^{\text{sym}}$.

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

\[ M_q^{\text{sym}} \leq 2 \left( 1 + \frac{1}{\sqrt{q} - 3} \right). \]  
(34)

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

\[ M_q^{\text{sym}} \leq 3 \left( 1 + \frac{2}{q - 3} \right). \]  
(35)

**Remark 8.19.** For $q$ a square, the bound (34) is better than (35), except for $q = 16$.

When $q$ is a prime number, the uniform bounds of Proposition 9.14 obtained in [27], Proposition 10, by Ballet and Zykin lead to the asymptotic symmetric complexity given in the following proposition.

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

\[ M_p^{\text{sym}} \leq 3 \left( 1 + \frac{4/3}{p - 3} \right). \]  
(36)

The following theorem due to Rambaud in [71] generalizes essentially all the known formulae, providing the current best symmetric upper-limit asymptotic bounds.

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

(a) if $r = 1$ and $q$ is such that $A'_1(q) > 5$, then

\[ M_q^{\text{sym}} \leq \frac{2\mu_q^{\text{sym}}(r, l)}{rl} \left( 1 + \frac{1}{rlA'_r(q) - 1} \right); \]

(b) \[ M_q^{\text{sym}} \leq \frac{2\mu_q^{\text{sym}}(r, l)}{rl} \left( 1 + \frac{2}{rlA'_r(q) - 2} \right); \]

(c) if $2 \mid q$, then

\[ M_q^{\text{sym}} \leq \frac{2\mu_q^{\text{sym}}(r, l)}{rl} \left( 1 + \frac{1 + \log_q 2}{rlA'_r(q) - 1 - \log_q 2} \right); \]

(d) if $2 \nmid q$, then

\[ M_q^{\text{sym}} \leq \frac{2\mu_q^{\text{sym}}(r, l)}{rl} \left( 1 + \frac{1 + 2\log_q 2}{rlA'_r(q) - 1 - 2\log_q 2} \right). \]
Remark 8.22. The following can be concluded by comparison with the other known results.

- Bound (a) encompasses the upper-limit bounds of Theorem 8.4 and Corollary 8.6, where it adds multiplicities of evaluation. This additional tool was introduced in [1] and improved in [39], followed by Lemma 3.4 in [74].
- Bound (b) allows evaluation on points of arbitrary degree compared to Proposition 11 in [17].
- Bounds (c) and (d) allow evaluation on points of odd degree in Theorem 5.18 in [37], and adds multiplicities of evaluation. Also, instead of the formula $A'_r(q) = (\sqrt{q^r} - 1)/r$ in loc. cit., which is unproven in the general case, these bounds use $A'_r(q)$. Notice that bounds (b) and (c) give strictly better numerical values than Proposition 8.18 for all values of $q$ for which Proposition 8.18 holds. Indeed, it suffices to take $r = 2$ (and $l = 1$) and to use the known value (10) of $A'_2(q)$ in §6.

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

We present in detail how the upper bounds of $\mu_{q}^{\text{sym}}(r, l)$ are inferred because many of them have not been published explicitly. Because they are interesting, these bounds will be summarized in §9.2. To obtain these upper bounds we often use formula (58) in [74], Lemma 3.2, given by inequality (6) in §5.4:

$$\mu_{q}^{\text{sym}}(r, l) \leq \mu_{q}^{\text{sym}}(1, l)\mu_{q}^{\text{sym}}(r);$$

in particular

$$\mu_{q}^{\text{sym}}(2, 2) \leq \mu_{q}^{\text{sym}}(1, 2)\mu_{q}^{\text{sym}}(2) \leq 3 \cdot 3 = 9$$

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

The strongest emphasis must be placed on the upper bound

$$\mu_{q}^{\text{sym}}(2, 5) \leq 30,$$

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

$$\mu_{q}^{\text{sym}}(1, 5) \leq 10,$$

only published in [70], Table 2, in the justification of entry (1,10). It is regrettable that this record bound was not emphasized more in [70]. This was remedied in [71], Appendix §2.3, where an explicit formula attaining this bound was given. Even more regrettably, the entry for (1,10) in [70], Tables 1 and 2, is grossly false. One should not take it to be $\mu_{q}^{\text{sym}}(1, 10) \leq 30$, but instead $\mu_{q}^{\text{sym}}(2, 5) \leq 30$, as can be deduced from formula (37) above. This was corrected in [71], Table 3.1. The error in [70], Tables 1 and 2, comes from a massively wrong application of formula (37).

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

---

7Proposition 8.18 is presented because of its simplicity.
For $q = 2$: from (b) with $(r, l) = (2, 5)$ and $\mu_q^{\text{sym}}(2, 5) \leq 30$ as emphasized above. For $q = 3$: from (b) with $(r, l) = (2, 3)$ and

$$
\mu_3(2, 3) \leq 5 \mu_3^{\text{sym}}(1, 3) \mu_3^{\text{sym}}(2, 1) \leq \mu_3^{\text{sym}}(1, 3) \mu_3^{\text{sym}}(2, 1) \leq 5 \cdot 3 = 15,
$$

where the latter value, 3, is given by the Karatsuba algorithm and the former one, 5, comes from [40], Table 1, column (2.4). (Note that 5 is actually equal to the asymmetric complexity by [28], Table 3.)

For $q = 4$: from (c) with $(r, l) = (2, 2)$ and $\mu_4(2, 2) \leq 8$ from [74], (88). (Which, as a side remark, we even claim to be an equality, as follows from an unpublished exhaustive search performed while working on [70], §1.)

For $q = 5$: from (d) with $(r, l) = (2, 2)$ and $\mu_5(2, 2) \leq 8$ (see [74], (88)).

For $q = 7$: from (d) with $(r, l) = (2, 1)$.\(^8\)

For $q = 8$: from (c) with $(r, l) = (2, 1)$.

For $q = 9$: from (d) with $(r, l) = (2, 1)$.

For $q = 11$: from (d) with $(r, l) = (2, 1)$.

For $q = 25$: apply Proposition 8.23 obtained in [17], Proposition 2.\(^9\)

**Proposition 8.23.**

$$
M^{\text{sym}}_2 \leq 10, \quad M^{\text{sym}}_3 \leq 7.5, \quad M^{\text{sym}}_4 \leq 5.33, \quad M^{\text{sym}}_5 \leq 5.21, \quad M^{\text{sym}}_7 \leq 4.08, \quad M^{\text{sym}}_8 \leq 3.71, \quad M^{\text{sym}}_9 \leq 3.77, \quad M^{\text{sym}}_{11} \leq 3.56, \quad \text{and} \quad M^{\text{sym}}_{25} \leq 3.
$$

These asymptotic bounds are the current best published numerical ones in the symmetric case.\(^10\)

Now, if equation (14) did hold, that is, if $A'_q(3) = (3^3 - 1)/6 = 13/3$, as would be implied, for example, by Conjecture 6.8.1, then applying criterion (b) to (6,1) and using $\mu_3^{\text{sym}}(6, 1) \leq 15$ from [39], Table 1, would yield $M^{\text{sym}}_3 \leq 65/12 \approx 5.41$, and likewise for the other two bounds mentioned in [71], Table 2.2, in the two lines named ‘Adding theorem B’. Similarly, Conjectures 6.9.1, 6.10.1, and 6.11.1 would imply the bounds in the corresponding lines of Table 2.2 in [71].

Then, using the general quantities linked to the 2-torsion (cf. §7.1), Cascudo, Cramer, and Xing obtained the following general result in [37], Theorem 6.27 (cf. also [36]).

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

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

\(^8\)Recall that $\mu_q(2, 1) = \mu_q(2) = 3$.

\(^9\)Notice that the authors did not apply their bound to $q = 25$ because it gives a higher value than the one from [37]. At the time they did not know that the latter bound had not actually been proved. Note also that this bound is obtained by using criterion 1) in Theorem 9.5 with $a = 0$, obtained in [6], Theorem 1.1.

\(^10\)These bounds improve the bounds $M^{\text{sym}}_2 \leq 1035/68 \approx 15.23$ and $M^{\text{sym}}_3 \leq 1933/250 \approx 7.74$ obtained for $q = 2$ and $q = 3$ in [21], Theorem 4.9, and the bound $M^{\text{sym}}_4 \leq 237/39 \approx 6.08$ obtained for $q = 4$ in [22], Theorem 1.6, (i), which was already an improvement of the following old results: $M^{\text{sym}}_2 \leq 477/26 \approx 18.35$ obtained in [20], Theorem 4.1, and $M^{\text{sym}}_3 \leq 27$ obtained from the remark to Corollary 3.1 in [8].
In particular, if $A(q) \geq 1 - J_2(a, A(q))$, then

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

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

In order to be useful, this result should be combined with upper bounds on the torsion-limit. Some upper bounds of this sort can easily be deduced from Weil’s classical results on the torsion in Abelian varieties. However, Cascudo, Cramer, and Xing obtained a spectacular improvement using the Deuring–Shafarevich theorem. This allowed them to give an upper-bound on the 2-torsion-limit of certain explicit towers (such as the Garcia–Stichtenoth tower), as well as the following general result (see [37], Theorem 2.3, (iii)).

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

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

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

Note that all the upper bounds for $M^\text{sym}_q$ obtained by Cascudo et al. in [38] and [37] are unproved because the proofs are based on Lemma IV in [38], which is not entirely correct, as was shown in [22], §3 (cf. also [71]). However, the bounds are correct under Conjecture 6.10.1.\(^\text{11}\)

\(^{11}\)The following results rely on the above unproven assumption: Theorems IV.6 and IV.7 and the list of specific bounds in Corollary IV.8 of [38], and also Theorem V.18 and the list of bounds in Corollary V.19 of [37]. More precisely, here are the unproved bounds:

- The symmetric bounds in Theorems IV.6 and IV.7 and the list of specific bounds in Corollary IV.8 of [38], namely the following:

$$M^\text{sym}_q \leq \mu^\text{sym}_q (2t) \frac{q^t - 1}{t(q^t - 5)}$$

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

$$M^\text{sym}_q \leq \mu^\text{sym}_q (t) \frac{q^{t/2} - 1}{t(q^{t/2} - 5)}$$

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

| $q$  | 2   | 3   | 4   | 5   | 7   | 8   | 9   | 11  | 13  |
|------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| $M^\text{sym}_q$ | 7.47 | 5.49 | 4.98 | 4.8 | 3.82 | 3.74 | 3.68 | 3.62 | 3.59 |

- The symmetric bounds in Theorem V.18 and the list of bounds in Corollary V.19 of [37], namely:

$$M^\text{sym}_q \leq \begin{cases} \mu^\text{sym}_q (2t) \frac{q^t - 1}{t(q^t - 2 - \log_2 q)} & \text{if } 2 \mid q, \\ \mu^\text{sym}_q (2t) \frac{q^t - 1}{t(q^t - 2 - 2 \log_2 q)} & \text{otherwise,} \end{cases}$$
9. Uniform bounds

9.1. Some exact values for $\mu_q^{\text{sym}}(n)$. Recall that, by Theorem 2.2, we have $\mu_q^{\text{sym}}(n) = \mu_q(n) = 2n - 1$ if and only if $n \leq q/2 + 1$. By applying the CCMA with well fitted elliptic curves, Shokrollahi [79] (for the strict inequality) and Chau-mine [42] showed the following result.

**Theorem 9.1.** If

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

where $\epsilon$ is the function defined by

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

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

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

**Open problem 9.2.** We still do not know if the converse is true. More precisely, the question is this: Suppose that $\mu_q(n) = 2n$. Are inequalities (39) true?

Moreover, for the values of $n$ not considered in Theorems 2.2 and 9.1, very few particular exact values are known, and all of them were obtained in [43]; see Table 1.

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

**Remark 9.3.** The bilinear complexity $\mu_2(4) = 9$ was obtained in [43], Example 6.1, with the aid of a personal computer program. It is easy to check that this value can be obtained by means of a symmetric tensor corresponding to the iteration of the Karatsuba algorithm. Then

$$\mu_2(4) = \mu_2^{\text{sym}}(4) = 9.$$ 

The bilinear complexity $\mu_2(6) = 15$ was obtained in [43], Example 6.2, thanks to inequality (22) of Lemma 8.1 and a lower bound for the length of binary codes of dimension 6 equal to the minimal distance.

**Open problem 9.4.** Find the exact values for $\mu_q^{\text{sym}}(n)$ and $\mu_q(n)$. Find examples where $\mu_q(n) < \mu_q^{\text{sym}}(n)$.

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

| $q$ | $2$ | $3$ | $4$ | $5$ |
|-----|-----|-----|-----|-----|
| $M_q^{\text{sym}}$ | 7.23 | 5.45 | 4.44 | 4.34 |
9.2. Upper bounds for \( \mu_q^{\text{sym}}(n) \) and \( \mu_q^{\text{sym}}(l, r) \). From the results of [6] and the algorithm of Corollary 5.6 with \( \ell_1 = \ell_2 = 0 \), we obtain the following result (cf. [6] and [24]).

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

1) If \( N_1 + a > 2n + 2g - 2 \) for some integer \( a \geq 0 \), then
   \[
   \mu_q^{\text{sym}}(n) \leq 2n + g - 1 + a.
   \]

2) If there exists a non-special divisor of degree \( g - 1 \) (which is always the case if \( q \geq 4 \)) and \( N_1 + a_1 + 2(N_2 + a_2) > 2n + 2g - 2 \) for some integers \( a_1 \geq 0 \) and \( a_2 \geq 0 \), then
   \[
   \mu_q^{\text{sym}}(n) \leq 3n + 2g + \frac{a_1}{2} + 3a_2 - 1.
   \]

3) If \( N_1 + 2N_2 > 2n + 4g - 2 \), then
   \[
   \mu_q^{\text{sym}}(n) \leq 3n + 6g.
   \]

**Remark 9.6.** The last theorem makes it possible to obtain general bounds on the bilinear complexity of multiplication in \( \mathbb{F}_q^n \) over \( \mathbb{F}_q \) from infinite families of algebraic function fields defined over \( \mathbb{F}_q \). But for a fixed finite field \( \mathbb{F}_q^n \), if we want to obtain the best possible bound, we can search for the best algebraic function field defined over \( \mathbb{F}_q \) (that is, with the smallest possible genus) satisfying the conditions of this theorem.

Finally, from good towers of algebraic function fields satisfying Theorem 9.5, various improvements of the bounds for symmetric bilinear complexity were successively obtained in [6], [8], [24], [19], [9], [16], [1], [21], and [22].

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

\[
\mu_q^{\text{sym}}(n) \leq C_q^{\text{sym}} n.
\]

The best current values of the constants \( C_q^{\text{sym}} \) are as follows:

1) If \( q = 2 \), then
   \[
   C_2^{\text{sym}} = 15.4575
   \]
   (see [21], Corollary 29);

2) If \( q = 3 \), then
   \[
   C_3^{\text{sym}} = \frac{1933}{250} \approx 7.732
   \]
   (see [21]);
3) if \( q = p \geq 7 \), then

\[
C_q^{\text{sym}} = 3\left(1 + \frac{8}{3p - 5}\right)
\]

(see [22], Theorem 1.6, (ii));

4) if \( q = p^2 \geq 25 \), then

\[
C_q^{\text{sym}} = 2\left(1 + \frac{2}{p - 33/16}\right)
\]

(see [22], Theorem 1.7, (ii));

5) if \( q = p^{2k} \geq 64 \) with \( k \geq 2 \), then

\[
C_q^{\text{sym}} = 2\left(1 + \frac{p}{\sqrt{q} - 3 + (p - 1)\sqrt{q}/(\sqrt{q} + 1)}\right)
\]

(see [1] and [22], Theorem 1.7, (i));

6) if \( q \geq 4 \), then

\[
C_q^{\text{sym}} = 3\left(1 + \frac{4p/3}{q - 3 + 2(p - 1)q/(q + 1)}\right)
\]

(see [22], Theorem 1.6, (i)).

**Remark 9.8.** Note that, from Corollary 5.6 applied to a Garcia–Stichtenoth tower, the bound 5) of Theorem 9.7 was obtained by Arnaud in [1] (which is unpublished). In [22] the authors gave a detailed proof of bound 5). The two revised bounds 3) and 4) for \( \mu_{p^2}(n) \) and \( \mu_p(n) \) were also proved in [22].

Note also that the upper bounds\(^\dagger\) obtained successively in [11] and [10] were established by using the mistaken statements of Shparlinski, Tsfasman, and Vlăduţ [80] mentioned above in §3.2.

Moreover, for certain finite fields (in particular, the cases of \( \mathbb{F}_2, \mathbb{F}_3, \) and \( \mathbb{F}_4 \)), we have some refined bounds for certain extensions obtained in [39], Table 1. Let us recall this in Table 2.

---

\(^\dagger\)In [1] Arnaud gives the following two bounds with no detailed calculations:

(3’) If \( p \geq 5 \) is a prime, then \( \mu_{p^2}^{\text{sym}}(n) \leq 3(1 + 4/(p - 1))n \); (4’) If \( p \geq 5 \) is a prime, then \( \mu_{p^2}^{\text{sym}}(n) \leq 2(1 + 2/(p - 2))n \).

In fact, one can check that the denominators \( p - 1 \) and \( p - 2 \) are slightly overestimated under Arnaud’s hypotheses.

\(^\dagger\)In [11] and [10] Ballet gives the following unproved bounds:

(1) If \( q \geq 3 \) is a prime power, then \( \mu_{q^2}^{\text{sym}}(n) \leq 2(1 + 2/(q - 2))n \);
(2) If \( q \geq 5 \) is a prime power, then \( \mu_{q^2}^{\text{sym}}(n) \leq 6(1 + 2/(q - 2))n \);
(3) If \( q = p^r > 3 \) is a prime power, then \( \mu_{q^2}^{\text{sym}}(n) \leq 3(1 + 2/(p - 2))n \);
(4) If \( p > 5 \) is a prime, then \( \mu_{p^2}^{\text{sym}}(n) \leq 3(1 + 2/(p - 2))n \).
Table 2. Best known bounds on complexities for small fields.

|   | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|
| $\mu_{2}^{\text{sym}}(n) \leq$ | 3 | 6 | 9 | 13 | 15 | 22 | 24 | 30 | 33 | 39 | 42 | 48 | 51 | 54 | 60 | 67 | 69 |
| $\mu_{3}^{\text{sym}}(n) \leq$ | 3 | 6 | 9 | 11 | 15 | 19 | 21 | 26 | 27 | 34 | 36 | 42 | 45 | 50 | 54 | 58 | 62 |
| $\mu_{4}^{\text{sym}}(n) \leq$ | 3 | 6 | 8 | 11 | 14 | 17 | 20 | 23 | 27 | 30 | 33 | 37 | 39 | 45 | 45 | 53 | 51 |

Moreover, in [15], Tables 3 and 4, bounds were given for certain particular extensions, improving the results obtained in [39] and [74], Example 4.7:

|   | 163 | 233 | 283 | 409 | 571 |
|---|-----|-----|-----|-----|-----|
| $\mu_{2}^{\text{sym}}(n)$ | 906 | 1340 | 1668 | 2495 | 3566 |

|   | 57 | 97 | 150 | 200 | 400 |
|---|----|----|-----|-----|-----|
| $\mu_{3}^{\text{sym}}(n)$ | 234 | 410 | 643 | 878 | 1879 |

The bounds presented in the above tables are the current best published bounds for $\mu_{q}^{\text{sym}}(n)$. For $\mu_{q}(r, l)$ with $l > 1$, different values were given by Rambaud in [71]; these are explained in §8.2. We summarize these values for $q = 2$ (including the case $l = 1$) in Table 3.

Table 3. Upper bounds on the complexities $\mu_{2}^{\text{sym}}(r, l)$.

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

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

For other values of $q$, let us summarize the known results, obtained in §8.2:

$\mu_{q}^{\text{sym}}(2, 2) \leq 9$, $\mu_{q}^{\text{sym}}(2, 5) \leq 30$; $\mu_{q}^{\text{sym}}(1, 5) \leq 10$.

In [27] Ballet and Zykin have recently improved all the known uniform upper bounds for $\mu_{p}^{\text{sym}}(n)$ and $\mu_{p}^{\text{sym}}(n)$ for any prime $p \geq 5$. Their approach consists in using dense families of modular curves, which are not obtained asymptotically but thanks to prime number density theorems of Hoheisel type, in particular, a result due to Dudek [49]. Note that one of the main ideas used in [27] was introduced by Ballet [11] thanks to the use of the Chebyshev theorem (also called the Bertrand Postulate) to bound the gaps between prime numbers in order to construct families of modular curves which are as dense as possible. Later, motivated by [11], the approach based on using such bounds on gaps between prime numbers (for instance, Baker–Harman–Pintz [4]) was also used by Randriambololona in the preprint [73].
in order to improve the upper bounds of $\mu^{\text{sym}}_{p^2}(n)$, where $p$ is a prime number. In summary, let us present the new uniform bounds given there (and recalled in [77]).

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

$$[x]_{\mathcal{A}} = \min \mathcal{A} \cap [x, +\infty[ $$

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

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

Now, we have the following proposition.

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

1) for all $k \geq (p^2 + p + 1)/2$,

$$\frac{1}{k} \mu^{\text{sym}}_{p^2}(k) \leq 2 \left( 1 + \frac{1 + \epsilon_{\mathcal{P}}(24k/(p - 2))}{p - 2} \right),$$

where $\mathcal{P}$ is the set of prime numbers;

2) for all $k \geq 1$,

$$\frac{1}{k} \mu^{\text{sym}}_{p^2}(k) \leq 2 \left( 1 + \frac{1 + 10/139}{p - 2} \right);$$

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

$$\frac{1}{k} \mu^{\text{sym}}_{p^2}(k) \leq 2 \left( 1 + \frac{1.000000005}{p - 2} \right);$$

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

$$\frac{1}{k} \mu^{\text{sym}}_{p^2}(k) \leq 2 \left( 1 + \frac{1}{p - 2} \left( 1 + \left( \frac{24k}{p - 2} \right)^{-1} \right) \right);$$

5) for any $k$ large enough,

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

By combining his results of [73] with the result of Dudek [49] as in [27], Randriambololona [77] has recently improved almost all these bounds, except for the case $q = p^2 = 25$ obtained in [27]. In summary, let us state the new uniform bound for symmetric bilinear complexity given, respectively, in [77], Corollary 10, and [27], Proposition 7.

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

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

$$\frac{1}{k} \mu^{\text{sym}}_{p^2}(k) \leq 2 \left( 1 + \frac{1}{p - 2} \left( 1 + 3 \left( \frac{24k}{p - 2} \right)^{-1/3} \right) \right).$$
Proposition 9.11. Let $x_{\alpha}$ be the constant defined in [27], Theorem 6 (recalled in Theorem 9.12). For any integer $n \geq x_{\alpha} + 3$ we have

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

Let us recall the following key result as a direct consequence of the results of Baker, Harman, and Pintz [4] and Dudek [49], on which assertion 5) in Proposition 9.9 as well as Propositions 9.10 and 9.11 are essentially based. Their results concern explicit prime number density theorems, usually called theorems of Hoheisel type. In particular, the following theorem (see [27], Theorem 6) can be deduced directly from a result of Baker, Harman, and Pintz (see [4], Theorem 1) established in 2001 and a recent result established by Dudek (see [49], Theorem 1.1) in 2016.

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

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

for any prime $l_k \geq x_{\alpha}$.

In particular, one can take $\alpha = 2/3$ with $x_{\alpha} = \exp(\exp(33.217))$. Moreover, one can take $\alpha = 21/40$ with a value of $x_{\alpha}$ that can, in principle, be determined effectively.

Open problem 9.13. A highly non-trivial problem consists in determining effectively the value of $x_{\alpha}$ for $\alpha = 21/40$. This is a typical problem of analytic number theory, a problem of Hoheisel type.

Then, the following Proposition 9.14 concerns the case of prime fields. The optimal method used by Randriambololona [77] for solving Riemann–Roch systems (cf. §7.1) does not work well for symmetric algorithms over prime fields. Instead, to prove Proposition 10 in [27] Ballet and Zykin used a suboptimal method from [26] associated to descent techniques (cf. §6.2) and obtained the following result.

Proposition 9.14. Let $p \geq 5$ be a prime number and let $x_{\alpha}$ be defined as in Theorem 9.12.

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

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

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

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

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

where $\epsilon_p(n) = (2n/(p-3))^{\alpha - 1}$. 
9.3. Upper bounds for $\mu_q(n)$ and $\mu_q(l, r)$. By using the asymmetric part of Theorem 5.3, Pieltant and Randriambololona [69] obtained results concerning non-necessarily symmetric bilinear complexity. In particular, they obtained the best bounds in the extensions of $\mathbb{F}_2$, $\mathbb{F}_p$, and $\mathbb{F}_{p^2}$ for all $p \geq 3$, as well as $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ for all $q \geq 4$.

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

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

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

Then

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

where

$$\gamma_{q,d} = \max_{i\mid d} \frac{\mu_q(i, 2)}{i} - \frac{2\mu_q^\text{sym}(d)}{d} \quad \text{and} \quad \kappa_{q,d} \leq \frac{\mu_q^\text{sym}(d)}{d}(\alpha_q + d - 1).$$

By choosing $d = 1, 2,$ or $4$, they obtained the following two corollaries.

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

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

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

Then

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

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

and, for $q > 5$,

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

or, in the particular case when $N_2 = \ell_2 = 0$,

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

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

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

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

Then

$$\mu_2(n) \leq \frac{9}{2} \left(n + \frac{g}{2}\right) + \frac{3}{2} \sum_{i\mid 4} i\ell_i + 18.$$
Then, they established new asymmetric uniform bounds.

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

1) if $q = 2$, then
   \[ \mu_2(n) \leq \frac{189}{22} n + 18; \]

2) if $q = 3$, then
   \[ \mu_3(n) \leq 6n; \]

3) if $q = 4$, then
   \[ \mu_4(n) \leq \frac{87}{19} n; \]

4) if $q = 5$, then
   \[ \mu_5(n) \leq \frac{9}{2} n; \]

5) if $q \geq 4$, then
   \[ \mu_{q^2}(n) \leq 2 \left( 1 + \frac{p}{q - 2 + (p - 1)q/(q + 1)} \right) n - 1; \]

6) if $p \geq 3$, then
   \[ \mu_{p^2}(n) \leq 2 \left( 1 + \frac{2}{p - 1} \right) n - 1; \]

7) if $q > 5$, then
   \[ \mu_q(n) \leq 3 \left( 1 + \frac{p}{q - 2 + (p - 1)q/(q + 1)} \right) n; \]

8) if $p > 5$, then
   \[ \mu_p(n) \leq 3 \left( 1 + \frac{2}{p - 1} \right) n. \]

By using the same dense families of modular curves defined over $\mathbb{F}_p$ as those used to get Proposition 9.9 in §9.2, Randriambololona has recently obtained the following result.

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

1) for all $k > (p + 1)/2$,
   \[ \frac{1}{k} \mu_p(k) \leq 3 \left( 1 + \frac{1 + \epsilon \mathcal{P}(24k/(p - 2))}{p - 2} \right), \]
   where $\mathcal{P}$ is the set of prime numbers;

2) for all $k \geq (p - 2)e^{e^{33.217}}/24$,
   \[ \frac{1}{k} \mu_p(k) \leq 3 \left( 1 + \frac{1}{p - 2} \left( 1 + 3 \left( \frac{24k}{p - 2} \right)^{-1/3} \right) \right); \]

3) for any $k$ large enough,
   \[ \frac{1}{k} \mu_p(k) \leq 3 \left( 1 + \frac{1}{p - 2} \left( 1 + \left( \frac{24k}{p - 2} \right)^{-0.475} \right) \right). \]
Remark 9.20. Note that the difficulty of solving the Riemann–Roch systems (cf. §7.2) in the context of symmetric algorithms using curves with insufficiently many rational points is avoided here since the above result is obtained by using the asymmetric version of a Chudnovsky–Chudnovsky type algorithm (cf. §§5.3 and 5.4) applied over places of degree two.

Now, let us recall some particular values for $\mu_q(l, r)$ obtained in §8.2:

$$
\mu_3(2, 3) \leq 15, \quad \mu_4(2, 2) \leq 8, \quad \text{and} \quad \mu_5(2, 2) \leq 8.
$$

10. Effective construction of bilinear multiplication algorithms

In this section we are interested in the study of the effective construction of bilinear multiplication algorithms in finite fields. Very little work has been done on the effective construction of Chudnovsky–Chudnovsky type algorithms. Such algorithms are mainly contained in [29], [7], [39], [15], [2], and [3].

10.1. Non-asymptotic construction.

10.1.1. Classical multiplication algorithms.

(a) Example of an effective symmetric construction using an elliptic curve. This example, developed by Baum and Shokrollahi in [29], is the first effective construction of a bilinear algorithm of multiplication which implements the CCMA. It concerns a multiplication algorithm in the finite field $\mathbb{F}_{256}$ over $\mathbb{F}_4$, with $q = 4$ and $n = 4$, using the maximal Fermat elliptic curve $y^2 + y = x^3 + 1$. The bilinear complexity $\mu_{\text{sym}}(U)$ of this symmetric algorithm $U$ is optimal and such that

$$
\mu_{\text{sym}}(U) = \mu_{q \text{sym}}(n) = \mu_q(n) = 2n = 8.
$$

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

$$
\mu_{\text{sym}}(U) = 2n + 1,
$$

which proves that $2n \leq \mu_q(n) \leq \mu_{q \text{sym}}(n) \leq 2n + 1$.

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

(c) Example of an effective symmetric construction using higher degree places and derived evaluations at rational places on elliptic curves. This example, developed by Cenk and Özbudak in [39], is the first effective construction of a bilinear algorithm of multiplication which implements a combination of the generalizations of the CCMA introduced in [24] using places of degree one and two and in [1] using derived evaluations. Note that in this example derived evaluations are only used at
rational places of order one. More precisely, it concerns a multiplication algorithm in the finite field \( \mathbb{F}_{3^9} \) over \( \mathbb{F}_3 \) using the non-optimal elliptic curve \( y^2 = x^3 + x + 2 \). In this case, in [39] the authors use the evaluation at four rational places with derived evaluation at two of them as well as the evaluation at six places of degree two. The bilinear complexity of this symmetric algorithm \( \mathcal{U} \) is such that

\[
\mu^{\text{sym}}(\mathcal{U}) = 4 + 2 \cdot 2 + 6 \cdot 3 = 26.
\]

(d) Example of effective asymmetric construction using higher degree places on algebraic curves. This example, developed by Ballet, Baudru, Bonnecaze, and Tukumuli in [12] (announced in [13]) and by Tukumuli in [87], is the first effective construction of bilinear algorithms of multiplication which implements the asymmetric generalization of the CCMA introduced in [74]. Note that these examples use two distinct Riemann–Roch spaces \( \mathcal{L}(D_1) \) and \( \mathcal{L}(D_2) \) without derived evaluations. More precisely, three algorithms were constructed in [12]. The first example concerns a multiplication algorithm in the finite field \( \mathbb{F}_{16^{13}} \) over \( \mathbb{F}_{16} \) using the maximal hyperelliptic curve \( y^2 + y = x^5 \) and only rational places on it. The second example concerns a multiplication algorithm in the finite field \( \mathbb{F}_{4^4} \) over \( \mathbb{F}_4 \) using the optimal curve \( y^2 + y = \frac{x}{x^3 + x + 1} \) over \( \mathbb{F}_4 \). The third example concerns a multiplication algorithm in the finite field \( \mathbb{F}_{2^5} \) over \( \mathbb{F}_2 \) using the optimal curve \( y^2 + y = \frac{x}{x^3 + x + 1} \) over \( \mathbb{F}_4 \).

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

In 2009 Couveignes and Lercier constructed in [45], Theorem 4, two families of bases (called elliptic and normal elliptic) for finite field extensions, from which they obtained a model \( \Xi \) defined as follows. With every couple \( (q,n) \), they associated a model \( \Xi(q,n) \) of the degree \( n \) extension of \( \mathbb{F}_q \) for which there is a positive constant \( K \) such that the following statements are true:
elements in $\mathbb{F}_{q^n}$ are represented by vectors for which the number of components in $\mathbb{F}_q$ is upper bounded by $Kn(\log n)^2 \log(\log n)^2$;

- there exists an algorithm that multiplies two elements at the expense of

$$Kn(\log n)^4 \log \log n|^3$$

multiplications in $\mathbb{F}_q$;

- exponentiation by $q$ consists of a circular shift of the coordinates.

Therefore, for each extension of a finite field, they showed that there exists a model which allows both fast multiplication and fast application of the Frobenius automorphism. Their model has the advantage of existing for all extensions. However, the bilinear complexity of their algorithm is not competitive compared with the best known methods, as pointed out in [45], §4.3.4. Indeed, it is clear that such a model requires at least $Kn(\log n)^2(\log \log n)^2$ bilinear multiplications.

The authors of [3] proposed another model with the following characteristics.

(a) The model is based on the CCMA, thus the multiplication algorithm has bilinear complexity in $O(n)$, which is optimal.

(b) The model is tailored to parallel computation. Hence the computation time used to perform a multiplication or any exponentiation can easily be reduced with an adequate number of processors. Since the method has bilinear complexity of multiplication of order $O(n)$, it can be parallelized to obtain constant time complexity using $O(n)$ processors. The aforementioned earlier works ([56] and [45]) do not give any parallel algorithm (such an algorithm is more difficult to conceive than a serial one).

(c) Exponentiation by $q$ is a circular shift of the coordinates and can be considered free. Thus, efficient parallelization can be done when doing exponentiation.

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

(e) The model uses the Coppersmith–Winograd [44] method (denoted CW) or any variants thereof to improve matrix products and to reduce the number of scalar operations.

**Open problem 10.2.** The structure of the matrices involved in the CCMA should be examined more closely but, unfortunately, at the present time there are no theoretical means or criteria to build the best matrices because they depend on the geometry of the curves, the field of definition of these curves, as well as the Riemann–Roch spaces involved. A study of suitable optimization strategies for the CCMA from this point of view can be found in [14]. In particular, the CCMA using an elliptic curve for multiplication in $\mathbb{F}_{256}/\mathbb{F}_4$ constructed by Baum and Shokrollahi [29] has been improved. The remaining open question is how to choose the geometrical objects in order to minimise the number of zeroes in a matrix of the evaluation map at the rational points of a curve.
10.2. Asymptotic construction. In [43] D.V. and G.V. Chudnovsky claimed that one can construct in polynomial time a bilinear multiplication algorithm realizing bilinear complexity for which the upper bound for $m_q$ is attained. Then, Shparlinski, Tsfasman, and Vlăduţ noted in [80] that the argument of D.V. and G.V. Chudnovsky is insufficient. Indeed, the construction of such algorithms involves some random choice of divisors having prescribed properties over an exponentially large set of divisors.

Shparlinski, Tsfasman, and Vlăduţ obtained a partial result concerning this polynomial construction in the following way. Let $q = p^{2m} \geq 49$ and let $X_i = X_0(11l_i)$ be the reduction of the classical modular curve, $l_i$ being the $i$th prime (for $q = p^2$), or $X_i = X_0(p_i)$, where $p_i$ is an irreducible polynomial over $\mathbb{F}_q$ of odd degree coprime with $q - 1$ (for $q = p^{2m}$). Here, $X_0(p_i)$ is the reduction of the Drinfeld modular curve. Note that $\{X_i\}$ is a family of absolutely irreducible smooth curves of genus $g = g_i$ with $\lim_{g \to \infty} \frac{|X(F_q)|}{g} = \sqrt{q} - 1$. Then, in [80] they proved the following result.

Proposition 10.3. Suppose that, for a family of modular curves as described above, for any $X \in \{X_i\}$ an explicit point $Q$ of $X$ of some degree $n$ is given such that
\[
\frac{1}{2} g_i \left( \sqrt{q} - 5 \right) - o(g) \leq n \leq \frac{1}{2} g_i \left( \sqrt{q} - 5 \right).
\]
Let $Q$ be defined by its coordinates in some projective embeddings. Then one can polynomially construct a sequence $\mathcal{U} = \mathcal{U}_i$ of bilinear multiplication algorithms in finite fields $\mathbb{F}_{q^n}$ for the given sequence of $n \to \infty$ such that
\[
\lim_{g \to \infty} \frac{\mu_{\text{sym}}(\mathcal{U})}{n} = 2 \left( 1 + \frac{4}{\sqrt{q} - 5} \right).
\]

This proposition means that to get a polynomially constructible algorithm with linear complexity one needs to construct explicitly (that is, polynomially) points of corresponding degrees on modular curves (or on other curves with many points). Unfortunately, at present it is unknown how to produce such points.

In [74], Remark 6.6, Randriambololona improved this result under the same hypothesis concerning the construction of a point of degree $n$. More precisely, up to this existence result, he obtained a polynomial time (in $n$) construction of a multiplication algorithm (a symmetric multiplication algorithm) in $\mathbb{F}_{q^n}/\mathbb{F}_q$ of length $2n(1 + 1/\sqrt{q} - 2) + o(n)$ for $q \geq 9$ ($q \geq 49$, respectively).

In [15] Ballet, Bonnecaze, and Tukumuli obtained a polynomial construction of a symmetric multiplication algorithm of elliptic Chudnovsky–Chudnovsky type (that is, with the Chudnovsky–Chudnovsky interpolation method on an elliptic curve) in time
\[
O \left( n \left( \frac{2q}{K} \right)^{\log^*(n)} \right),
\]
where
\[
\log^*(n) = \begin{cases} 
0 & \text{if } n \leq 1, \\
1 + \log^* \log(n) & \text{otherwise},
\end{cases}
\]
with $K = 2/3$ if the characteristic of $\mathbb{F}_q$ is 2 or 3, and $K = 5/8$ otherwise. Note that the length is only quasi-linear in $n$. However, this construction is without the
restriction linked to the construction of a point of degree \( n \). Moreover, this asymptotic construction is realized not from an infinite family of suitable curves as the above results, but thanks to the use of a sequence \( \mathcal{A}_{q,n} \) of symmetric bilinear multiplication algorithms constructed from an arbitrary elliptic curve defined over \( \mathbb{F}_q \) and using high degree points of this curve.

In [32] Bshouty gave a deterministic polynomial time construction of a tester of type \( (\mathcal{H}_{\mathcal{L}}\mathcal{F}(\mathbb{F}_q, n, d), \mathbb{F}_q^n, \mathbb{F}_q)) \) and of size \( \mu = O(d^{\tau(d,q)} n) \), where

\[
\tau(d, q) = \begin{cases} 
3 & \text{if } q \geq c d^2, \ c > 1 \text{ is a constant, and } q \text{ is a perfect square}, \\
4 & \text{if } q \geq c d \text{ and } c > 1 \text{ is a constant}, \\
5 & \text{if } q \geq d + 1, \\
6 & \text{if } q = d. 
\end{cases}
\]

In [33], Corollary 2, Bshouty used [32] to give the first polynomial time construction of a multilinear multiplication algorithm with linear multiplicative complexity in \( O(d^{\tau(d,q)} n) \) for the multiplication of \( d \) elements in any extension of the finite field \( \mathbb{F}_q^n \). This solves the open problem of deterministic polynomial time construction of a bilinear algorithm (that is, with \( d = 2 \)) with linear bilinear complexity for the multiplication of two elements in finite fields [43], [80], [9]. However, it does not solve the problem of deterministic polynomial time construction of a bilinear algorithm of Chudnovsky–Chudnovsky type. Indeed, the method of Bshouty is only based upon the equivalence between the optimal tester size and multilinear complexity. More precisely, the minimal size of a tester for \( \mathcal{H}_{\mathcal{L}}\mathcal{F}(\mathbb{F}_q, n, d) \) turns out to be equivalent to the rank of the tensor of multiplication of \( d \) elements in \( \mathbb{F}_q^n \) over \( \mathbb{F}_q \). The minimal size of a tester for \( \mathcal{H}_{\mathcal{P}}(\mathbb{F}_q, n, d) \) is equivalent to the symmetric rank of the tensor of multiplication of \( d \) elements.

11. Appendix: Proofs of Theorems 8.21, 8.9, and Proposition 6.11.3

Here we present a compressed version of the proof in [71], Chap. II, §§1.2, 1.3.

11.1. Repairing (and extending) the criterion of Cascudo et al. The following theorem facilitates control of 2-torsion in the worst case. It is a direct generalization of Theorem 5.18 in [37]. The parameters will be specified in the next paragraph to derive criterions for asymptotic bounds.

**Theorem 11.1.** Let \( X \) be a curve of genus \( g \) over \( \mathbb{F}_q \), where \( q \geq 2 \) is any prime power, and let \( m \geq 1 \) be an integer. Suppose that \( X \) admits a closed point \( Q \) of degree \( \deg Q = m \) (a sufficient condition for this is \( 2g + 1 \leq q^{(m-1)/2}(q^{1/2} - 1) \)).

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

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

where \( B_d(X) \) denotes the number of closed points of \( X \) of degree \( d \).
Let $R$ the smallest integer such that

$$R \geq g(1 + \log_q 2) + 2m + 3 \log_q \frac{3qg}{(\sqrt{q} - 1)^2} + 2 \quad \text{if } 2 \mid q$$

(43)

and

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

(44)

Then, provided that

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

(45)

we have

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

(46)

The following proposition gathers together the upper bounds used in the proof. The first two follow from [66], Chap. II, Question 1 (or Chap. II, §6), whereas the third one is borrowed from Proposition 3.4 in [37].

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

1) If $q$ is odd, then $J(\mathbb{F}_q)[2] \leq 2^{2g}$.

2) If $q$ is even, then $J(\mathbb{F}_q)[2] \leq 2^g$.

3) Let $h$ be the class number of $X$ and, for any integer $i$ with $0 \leq i \leq g - 1$, let $A_i$ be the number of $\mathbb{F}_q$-rational effective divisors of degree $r$. Then

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

Let us now follow the original proof of the theorem of Cascudo et al. (only in the case of even $q$, the odd case being identical modulo using the corresponding upper-bound in Proposition 11.2). Adding the terms $-\log_q (3qg/(\sqrt{q} - 1)^2)$ and $2g(1 - \log_q 2)$ to both sides of inequality (43), we get

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

Thus, there exists an even integer $2d$ between the two sides of the last inequality. Raising $q$ to the power on either side of each of the inequalities

LHS $\leq 2d$ and $2d \leq$ RHS
gives, respectively,
\[
g \frac{g}{q^{g-(2g-d+m)-1}(\sqrt{q} - 1)^2} \leq \frac{1}{3} \tag{47}
\]
and
\[
g \cdot 2^g \frac{g}{q^{g-(2d-R)-1}(\sqrt{q} - 1)^2} \leq \frac{1}{3}. \tag{48}
\]

Using upper bound 3) of Proposition 11.2, and combining the two inequalities (47) and (48) with upper bound 2) yields
\[
h > \frac{2}{3} h \geq A_{2g-d+m} + J(\mathbb{F}_q)[2]A_{2d-R}. \tag{49}
\]

Now let us choose a collection of pairwise distinct thickened points \(\{P\}\) on the curve \(X\) such that, for each \((d, u)\), there are exactly \(n_{d,u}\) points among them of degree \(d\) and multiplicity \(u\) (this is possible by assumption). Let \(G\) be their divisorial sum and \(Q\) a closed point of degree \(m\) as in the assumption. Since \(G\) is of degree greater than \(R\) by assumption (45), the general criterion of [36], §4, Theorem 6, along with the inequality (49) imply the existence of a divisor \(D = X\) of degree \(d\) that satisfies the following system of vanishing conditions for Riemann–Roch spaces (with \(K\) being the canonical divisor of \(X\)):
\[
l(K - X + Q) = 0, \tag{50}
l(2X - G) = 0. \tag{51}
\]

Thus, criterions (i’) and (ii’) of Theorem 3.5 in [74] are satisfied for \(G\) and \(D\).

11.2. Deriving the bounds in Theorem 8.21. Let \((X_s)_s\) be a dense sequence of curves over \(\mathbb{F}_q\) with genera \(g_s\) growing to infinity and the ratio of points of degree \(r\) matching \(A'_r(q)\). Noting that \(A'_r = A'_r(q)\), we have
\[
g_s \xrightarrow{s \to \infty} \infty, \tag{52}
B_r(X_s) = A'_r g_s + o(g_s), \tag{53}
g_s = g_{s-1} + o(g_s). \tag{54}
\]

First we prove bound (b) in Theorem 8.21, which generalizes Proposition 3 in [17], but the arguments of which were already introduced in Theorem 3.2 in [20]. Given an integer \(n\), let \(s(n)\) be the smallest integer such that
\[
rlB_r(X_{s(n)}) - 2g_{s(n)} \geq 2n + 3. \tag{55}
\]

Formula (53) makes it clear (or in any case it will become clear in the following equivalences) that such an integer \(s(n)\) exists as soon as the denominator in criterion (b) of Theorem 8.21 is strictly positive.

Moreover, for a large enough \(g\), Proposition 4.3 and Remark 4.4 in [23] state, in general, the existence of a zero-dimensional divisor of degree \(g - 5\) on \(X_{s(n)}\), hence the existence of a non-special divisor \(R\) of degree (lower than) \(g + 3\).
Therefore, the Corollary to Proposition 5.1 in [74] applies to (55). Taking all \(n_{d,u}\) null, except for \(n_{r,l}\) equal to \(B_r(X_{s(n)})\), we have

\[
\mu_q^{sym}(n) \leq \mu_q^{sym}(r,l)B_r(X_{s(n)}).
\] (56)

Let us now tie together the asymptotic behavior of \(g_{s(n)}\) and \(B_r(X_{s(n)})\). The minimality of \(s(n)\) satisfying (55) implies that

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

Dividing the two inequalities by \(g_{s(n)}-1\), and applying the asymptotic equivalences (53) and (54) (and (52)) yields

\[
rlA_r' - 2 + o(n) \geq \frac{2n}{g_{s(n)}} + o(1) > rlA_r' - 2 + o(n).
\]

Hence the asymptotic equivalence

\[
2n + o(n) = (rlA_r' - 2)g_{s(n)} + o(g_{s(n)})
\]

(which implies, in particular, that \(o(n) = o(g_{s(n)})\)). One can now divide both sides of the upper bound (56) by the previous equality:

\[
\frac{\mu_q^{sym}(n)}{n} \leq \mu_q^{sym}(r,l) : 2 \left( \frac{A_r'g_{s(n)} + o(n)}{(rlA_r' - 2)g_{s(n)} + o(n)} \right).
\]

Multiplying and dividing the RHS parenthesis by \(rl\), then subtracting and adding \(2g_{s(n)}\) in the numerator on the RHS, we obtain the result by letting \(n\) tend to infinity.

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

\[
rlB_r(X_{s(n)}) - g_{s(n)} \geq 2n + 5, \quad \text{then apply Proposition 5.7 in [74] for Theorem 8.9};
\]
\[
rlB_r(X_{s(n)}) - g_{s(n)} \geq 2n + 1, \quad \text{then apply Proposition 5.2,c), in [74] for Theorem 8.21,(a)};
\]
\[
rlB_r(X_{s(n)}) - g_{s(n)} \geq 2n + 1 \quad \text{(the same \(s(n)\)) this time for Proposition 6.11.3 (justification for the latter: due to Proposition 6.11.2, simply put \(Cl_0(X)(\mathbb{F}_q)[2] = 0\) in the proof of Theorem 11.1)};
\]
\[
rlB_r(X_{s(n)}) - (1 + \log_q 2)g_{s(n)} \geq 2n + 3 \log_q \left( \frac{3qg_{s(n)}}{(\sqrt{q} - 1)^2} \right) + 3 \quad \text{for Theorem 8.21,(c)};
\]
\[
rlB_r(X_{s(n)}) - (1 + 2\log_q 2)g_{s(n)} \geq 2n + 3 \log_q \left( \frac{3qg_{s(n)}}{(\sqrt{q} - 1)^2} \right) + 3 \quad \text{for Theorem 8.21,(d)}.
\]
Bibliography

[1] N. Arnaud, *Evaluation dérivée, multiplication dans les corps finis et codes correcteurs*, PhD thesis, Univ. de la Méditerranée, Inst. Math. de Luminy 2006.

[2] K. Atighehchi, S. Ballet, A. Bonnecaze, and R. Rolland, “Effective arithmetic in finite fields based on Chudnovsky’s multiplication algorithm”, *C. R. Math. Acad. Sci. Paris* 354:2 (2016), 137–141.

[3] K. Atighehchi, S. Ballet, A. Bonnecaze, and R. Rolland, “Arithmetic in finite fields based on the Chudnovsky–Chudnovsky multiplication algorithm”, *Math. Comp.* 86:308 (2017), 2975–3000.

[4] R. C. Baker, G. Harman, and J. Pintz, “The difference between consecutive primes. II”, *Proc. London Math. Soc.* (3) 83:3 (2001), 532–562.

[5] S. Ballet, *Complexité bilinéaire de la multiplication dans les corps finis par interpolation sur des courbes algébriques*, PhD thesis, Univ. de la Méditerranée, Inst. Math. de Luminy 1998.

[6] S. Ballet, “Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$”, *Finite Fields Appl.* 5:4 (1999), 364–377.

[7] S. Ballet, “Quasi-optimal algorithms for multiplication in the extensions of $\mathbb{F}_{16}$ of degree 13, 14 and 15”, *J. Pure Appl. Algebra* 171:2-3 (2002), 149–164.

[8] S. Ballet, “Low increasing tower of algebraic function fields and bilinear complexity of multiplication in any extension of $\mathbb{F}_{q^2}$”, *Finite Fields Appl.* 9:4 (2003), 472–478.

[9] S. Ballet, “An improvement of the construction of the D. V. and G. V. Chudnovsky algorithm for multiplication in finite fields”, *Theoret. Comput. Sci.* 352:1-3 (2006), 293–305.

[10] S. Ballet, “A note on the tensor rank of the multiplication in certain finite fields”, *Algebraic geometry and its applications*, SAGA (Papeete 2007), Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ 2008, pp. 332–342.

[11] S. Ballet, “On the tensor rank of the multiplication in the finite fields”, *J. Number Theory* 128:6 (2008), 1795–1806.

[12] S. Ballet, N. Baudru, A. Bonnecaze, and M. Tukumuli, *On the effective construction of asymmetric Chudnovsky multiplication algorithms in finite fields without derivated evaluation*, 2016, 23 pp., arXiv:1611.02883.

[13] S. Ballet, N. Baudru, A. Bonnecaze, and M. Tukumuli, “On the construction of the asymmetric Chudnovsky multiplication algorithm in finite fields without derivated evaluation”, *C. R. Math. Acad. Sci. Paris*, 2017, no. 7, 729–733.

[14] S. Ballet, A. Bonnecaze, and Thanh-Hung Dang, “On the scalar complexity of Chudnovsky multiplication algorithm in finite fields”, *Algebraic informatics*, CAI 2019 (Niš 2019), Lecture Notes in Comput. Sci., vol. 11545, Springer, Cham 2019, pp. 64–75.

[15] S. Ballet, A. Bonnecaze, and M. Tukumuli, “On the construction of elliptic Chudnovsky-type algorithms for multiplication in large extensions of finite fields”, *J. Algebra Appl.* 15:1 (2016), 1650005, 26 pp.

[16] S. Ballet and J. Chaumine, “On the bounds of the bilinear complexity of multiplication in some finite fields”, *Appl. Algebra Engrg. Comm. Comput.* 15:3-4 (2004), 205–211.

[17] S. Ballet, J. Chaumine, and J. Pieltant, “Shimura modular curves and asymptotic symmetric tensor rank of multiplication in any finite field”, *CAI’13: Algebraic informatics*, Lecture Notes in Comput. Sci., vol. 8080, Springer, Heidelberg 2013, pp. 160–172.
[18] S. Ballet and 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**:2 (2006), 293–310.

[19] S. Ballet, D. Le Brigand, and R. Rolland, “On an application of the definition field descent of a tower of function fields”, *Arithmetics, geometry, and coding theory*, AGCT 2005 (Marseilles 2005), Sémin. Congr., vol. 21, Soc. Math. France, Paris 2010, pp. 187–203.

[20] S. Ballet and J. Pieltant, “On the tensor rank of multiplication in any extension of \( \mathbb{F}_2 \)”, *J. Complexity* **27**:2 (2011), 230–245.

[21] S. Ballet, D. Le Brigand, and R. Rolland, “On an application of the definition field descent of a tower of function fields”, *Arithmetics, geometry, and coding theory*, AGCT 2005 (Marseilles 2005), Sémin. Congr., vol. 21, Soc. Math. France, Paris 2010, pp. 187–203.

[22] S. Ballet, J. Pieltant, M. Rambaud, and J. Sijsling, “On some bounds for symmetric tensor rank of multiplication in finite fields”, *Arithmetic, geometry, cryptography and coding theory*, Contemp. Math., vol. 686, Amer. Math. Soc., Providence, RI 2017, pp. 93–121.

[23] S. Ballet, C. Ritzenthaler, and R. Rolland, “On the existence of dimension zero divisors in algebraic function fields defined over \( \mathbb{F}_q \)”, *Acta Arith.* **143**:4 (2010), 377–392.

[24] S. Ballet and R. Rolland, “Multiplication algorithm in a finite field and tensor rank of the multiplication”, *J. Algebra* **272**:1 (2004), 173–185.

[25] S. Ballet and R. Rolland, “On the bilinear complexity of the multiplication in finite fields”, *Arithmetic, geometry and coding theory*, AGCT 2003 (Luminy 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris 2005, pp. 179–188.

[26] S. Ballet and R. Rolland, “Families of curves over any finite field attaining the generalized Drinfeld–Vladut bound”, *Publ. Math. Besançon Algèbre Théorie Nr.* **2011** (2011), 5–18.

[27] S. Ballet and A. Zykin, “Dense families of modular curves, prime numbers and uniform symmetric tensor rank of multiplication in certain finite fields”, *Des. Codes Cryptogr.* **87**:2-3 (2019), 517–525.

[28] R. Barbulescu, J. Detrey, N. Estibals, and P. Zimmermann, “Finding optimal formulae for bilinear maps”, *Arithmetic of finite fields*, Lecture Notes in Comput. Sci., vol. 7369, Springer, Heidelberg 2012, pp. 168–186.

[29] U. Baum and M. A. Shokrollahi, “An optimal algorithm for multiplication in \( \mathbb{F}_{256}/\mathbb{F}_4 \)”, *Appl. Algebra Engrg. Comm. Comput.* **2**:1 (1991), 15–20.

[30] R. W. Brockett and D. Dobkin, “On the optimal evaluation of a set of bilinear forms”, *Linear Algebra Appl.* **19**:3 (1978), 207–235.

[31] M. R. Brown and D. P. Dobkin, “An improved lower bound on polynomial multiplication”, *IEEE Trans. Comput.* **C-29**:5 (1980), 337–340.

[32] N. Bshouty, “Testers and their applications”, *Electronic Colloquium on Computational Complexity (ECCC)*, 2012, TR12-011, 108 pp., https://eccc.weizmann.ac.il/report/2012/011/.

[33] N. Bshouty, “Multilinear complexity is equivalent to optimal tester size”, *Electronic Colloquium on Computational Complexity (ECCC)*, 2013, TR13-011, 39 pp., https://eccc.weizmann.ac.il/report/2013/011/.

[34] N. H. Bshouty and M. Kaminski, “Multiplication of polynomials over finite fields”, *SIAM J. Comput.* **19**:3 (1990), 452–456.

[35] P. Bürgisser, M. Clausen, and M. A. Shokrollahi, *Algebraic complexity theory*, Grundlehren Math. Wiss., vol. 315, Springer-Verlag, Berlin 1997, xxiv+618 pp.
[36] I. Cascudo, R. Cramer, and Chaoping Xing, “The torsion-limit for algebraic function fields and its application to arithmetic secret sharing”, *Advances in cryptology – CRYPTO* 2011 (Santa Barbara, CA 2011), Lecture Notes in Comput. Sci., vol. 6841, Springer, Heidelberg 2011, pp. 685–705.

[37] I. Cascudo, R. Cramer, and Chaoping Xing, “Torsion limits and Riemann–Roch systems for function fields and applications”, *IEEE Trans. Inform. Theory* 60:7 (2014), 3871–3888.

[38] I. Cascudo, R. Cramer, Chaoping Xing, and An Yang, “Asymptotic bound for multiplication complexity in the extensions of small finite fields”, *IEEE Trans. Inform. Theory* 58:7 (2012), 4930–4935.

[39] M. Cenk and F. Özbudak, “On multiplication in finite fields”, *J. Complexity* 26:2 (2010), 172–186.

[40] M. Cenk and F. Özbudak, “Multiplication of polynomials modulo $x^n$”, *Theoret. Comput. Sci.* 412:29 (2011), 3451–3462.

[41] J. Chaumine, *Corps de fonctions algébriques et algorithme de D. V. et G. V. Chudnovsky pour la multiplication dans les corps finis*, PhD thesis, Univ. de la Polynésie Française 2005, 93 pp.

[42] J. Chaumine, “Complexité bilinéaire de la multiplication dans des petits corps finis”, *C. R. Math. Acad. Sci. Paris* 343:4 (2006), 265–266.

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

[44] D. Coppersmith and S. Winograd, “Matrix multiplication via arithmetic progressions”, *STOC’ 87 Proceedings of the nineteenth annual ACM symposium on theory of computing*, ACM, New York, NY 1987, pp. 1–6.

[45] J.-M. Couveignes and R. Lercier, “Elliptic periods for finite fields”, *Finite Fields Appl.* 15:1 (2009), 1–22.

[46] H.F. de Groote, “Characterization of division algebras of minimal rank and the structure of their algorithm varieties”, *SIAM J. Comput.* 12:1 (1983), 101–117.

[47] F. Diamond and J. Shurman, *A first course in modular forms*, Grad. Texts in Math., vol. 288, Springer-Verlag, New York 2005, xvi+436 pp.

[48] V. Ducet, *Construction of algebraic curves with many rational points over finite fields*, PhD thesis, Univ. d’Aix-Marseille, Inst. Math. de Luminy 2013, 100 pp., http://iml.univ-mrs.fr/~kohel/phd/thesis_ducet.pdf.

[49] A.W. Dudek, “An explicit result for primes between cubes”, *Funct. Approx. Comment. Math.* 55:2 (2016), 177–197.

[50] N.D. Elkies, “Explicit modular towers”, *Proceedings of the thirty-fifth annual Allerton conference on communication, control and computing* (Allerton House, Monticello, IL 1997), Univ. of Illinois, Urbana-Champaign 1997, pp. 23–32.

[51] N.D. Elkies, “Shimura curve computations”, *Algorithmic number theory*, ANTS-III (Portland, OR 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin 1998, pp. 1–47.

[52] N.D. Elkies, “Explicit towers of Drinfeld modular curves”, *European Congress of Mathematics*, vol. 2 (Barcelona 2000), Progr. Math., vol. 202, Birkhäuser, Basel 2001, pp. 189–198.

[53] N.D. Elkies, “Shimura curves for level-3 subgroups of the (2,3,7) triangle group, and some other examples”, *Algorithmic number theory*, ANTS-VII (Berlin 2006), Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin 2006, pp. 302–316.

[54] N. Estibals, *Algorithmes et arithmétique pour l’implémentation de couplages cryptographiques*, PhD thesis, Univ. de Lorraine, Nancy 2013, 219 pp., https://tel.archives-ouvertes.fr/tel-00924743.
On the tensor rank of multiplication in finite extensions of finite fields

[55] C. M. Fiduccia and Y. Zalcstein, “Algebras having linear multiplicative complexities”, J. Assoc. Comput. Mach. 24:2 (1977), 311–331.

[56] S. Gao, J. von zur Gathen, D. Panario, and V. Shoup, “Algorithms for exponentiation in finite fields”, J. Symb. Comput. 29:6 (2000), 879–889.

[57] A. Garcia and H. Stichtenoth, “A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound”, Invent. Math. 121:1 (1995), 211–222.

[58] A. Garcia, H. Stichtenoth, and H.-G. Rück, “On tame towers over finite fields”, J. Reine Angew. Math. 2003:557 (2003), 53–80.

[59] V. D. Goppa, “Codes on algebraic curves”, Dokl. Akad. Nauk SSSR 259:6 (1981), 1289–1290; English transl. in Soviet Math. Dokl. 24 (1981), 170–172.

[60] V. D. Goppa, “Algebraico-geometric codes”, Izv. Akad. Nauk SSSR Serw. Mat. 46:4 (1982), 762–781; English transl. in Math. USSR-Izv. 21:1 (1983), 75–91.

[61] E. Hallouin, “Computation of a cover of Shimura curves using a Hurwitz space”, J. Algebra 321:2 (2009), 558–566.

[62] T. Hasegawa, An explicit Shimura tower of function fields over a number field: an application of Takeuchi’s list, 2017, 8 pp., arXiv:1701.07551.

[63] Y. Ihara, “Some remarks on the number of rational points of algebraic curves over finite fields”, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28:3 (1981), 721–724.

[64] A. Lempel, G. Seroussi, and S. Winograd, “On the complexity of multiplication in finite fields”, Theoret. Comput. Sci. 22:3 (1983), 285–296.

[65] C. Levrat, Tours de courbes de Shimura, Master’s thesis, Univ. Paris-Saclay, Univ. de Versailles Saint-Quentin, Paris 2018, 37 pp., https://perso.telecom-paristech.fr/rambaud/teaching/.

[66] D. Mumford, Abelian varieties, Tata Inst. Fund. Res. Stud. Math., vol. 5, Oxford Univ. Press, London 1970, viii+242 pp.

[67] M. Musty, S. Schiavone, J. Sijsling, and J. Voight, “A database of Belyi maps”, Proceedings of the thirteenth algorithmic number theory symposium, ANTS XIII (Univ. of Wisconsin-Madison, WI 2018), Open Book Ser., vol. 2, Math. Sci. Publ., Berkeley, CA 2019, pp. 375–392.

[68] J. Pieltant, Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis, PhD thesis, Univ. d’Aix-Marseille, Inst. Math. de Luminy 2012, 96 pp., http://iml.univ-mrs.fr/theses/files/pieltant-these.pdf.

[69] J. Pieltant and H. Randriam, “New uniform and asymptotic upper bounds on the tensor rank of multiplication in extensions of finite fields”, Math. Comp. 84:294 (2015), 2023–2045.

[70] M. Rambaud, “Finding optimal Chudnovsky–Chudnovsky multiplication algorithms”, Arithmetic of finite fields, WAIFI 2014 (Gebze 2014), Lecture Notes in Comput. Sci., vol. 9061, Springer, Cham 2015, pp. 45–60.

[71] M. Rambaud, Shimura curves and bilinear multiplication algorithms in finite fields, PhD thesis, Télécom ParisTech 2017.

[72] H. Randriam, “Hecke operators with odd determinant and binary frameproof codes beyond the probabilistic bound?”, Proceedings of the IEEE information theory workshop, ITW’10 (Dublin 2010), IEEE, Piscataway, NJ 2010, pp. 1–5.

[73] H. Randriam, Diviseurs de la forme 2D-G sans sections et rang de la multiplication dans les corps finis, 2011, 35 pp., arXiv: 1103.4335.

[74] H. Randriambololona, “Bilinear complexity of algebras and the Chudnovsky–Chudnovsky interpolation method”, J. Complexity 28:4 (2012), 489–517.

[75] H. Randriambololona, “(2,1)-separating systems beyond the probabilistic bound”, Israel J. Math. 195:1 (2013), 171–186.
[76] H. Randriambololona, “On products and powers of linear codes under componentwise multiplication”, *Algorithmic arithmetic, geometry, and coding theory*, AGCT 2013 (CIRM, Marseille 2013), Contemp. Math., vol. 637, Amer. Math. Soc., Providence, RI 2015, pp. 3–78.

[77] H. Randriam, “Gaps between prime numbers and tensor rank of multiplication in finite fields”, *Des. Codes Cryptogr.* **87**:2–3 (2019), 627–645.

[78] G. Seroussi and A. Lempel, “On symmetric algorithms for bilinear forms over finite fields”, *J. Algorithms* **5**:3 (1984), 327–344.

[79] M.A. Shokrollahi, “Optimal algorithms for multiplication in certain finite fields using elliptic curves”, *SIAM J. Comput.* **21**:6 (1992), 1193–1198.

[80] I.E. Shparlinski, M.A. Tsfasman, and S.G. Vladut, “Curves with many points and multiplication in finite fields”, *Coding theory and algebraic geometry*, AGCT-3 (Luminy 1991), Lectures Notes in Math., vol. 1518, Springer, Berlin 1992, pp. 145–169.

[81] J. Sijsling, “Canonical models of arithmetic (1; e)-curves”, *Math. Z.* **273**:1-2 (2013), 173–210.

[82] A.L. Toom, “The complexity of a scheme of functional elements realizing the multiplication of integers”, *Dokl. Akad. Nauk SSSR* **150**:3 (1963), 496–498; English transl. in *Soviet Math. Dokl.* **4** (1963), 714–716.

[83] M.A. Tsfasman, “Goppa codes that are better than the Varshamov–Gilbert bound”, *Probl. Peredachi Informatsii* **18**:3 (1982), 3–6; English transl. in *Problems Inform. Transmission* **18**:3 (1982), 163–166.

[84] M.A. Tsfasman, “Some remarks on the asymptotic number of points”, *Coding theory and algebraic geometry*, AGCT-3 (Luminy 1991), Lecture Notes in Math., vol. 1518, Springer, Berlin 1992, pp. 178–192.

[85] M.A. Tsfasman and S.G. Vlăduţ, *Algebraic-geometric codes*, Math. Appl. (Soviet Ser.), vol. 58, Kluwer Acad. Publ., Dordrecht 1991, xxiv+667 pp.

[86] M. Tukumuli, *Étude de la construction effective des algorithmes de type Chudnovsky pour la multiplication dans les corps finis*, PhD thesis, Univ. d'Aix-Marseille, Inst. Math. de Luminy 2013, 95 pp.

[87] J. Voight, *Three lectures on Shimura curves*, 2006, 15 pp., https://www.maths.usyd.edu.au/u/NumTheorySeminar/notes/shimura-magma-survey.pdf.

[88] J. Voight, “Shimura curves of genus at most two”, *Math. Comp.* **78**:266 (2009), 1155–1172.

[89] S. Winograd, “Some bilinear forms whose multiplicative complexity depends on the field of constants”, *Math. Systems Theory* **10**:2 (1976), 169–180.

[90] S. Winograd, “On multiplication in algebraic extension fields”, *Theoret. Comput. Sci.* **8**:3 (1979), 359–377.
[92] Chaoping Xing, “Asymptotic bounds on frameproof codes”, IEEE Trans. Inform. Theory 48:11 (2002), 2991–2995.