Gaps between prime numbers and tensor rank of multiplication in finite fields

Hugues Randriam*

June 28, 2018

Abstract

We present effective upper bounds on the symmetric bilinear complexity of multiplication in extensions of a base finite field $\mathbb{F}_{p^2}$ of prime square order, obtained by combining estimates on gaps between prime numbers together with an optimal construction of auxiliary divisors for multiplication algorithms by evaluation-interpolation on curves. Most of this material dates back to a 2011 unpublished work of the author, but it still provides the best results on this topic at the present time.

Then a few updates are given in order to take recent developments into account, including comparison with a similar work of Ballet and Zykin, generalization to classical bilinear complexity over $\mathbb{F}_p$, and to short multiplication of polynomials, as well as a discussion of open questions on gaps between prime numbers or more generally values of certain arithmetic functions.

1 Introduction

Let F be a field and $\mathcal{A}$ a finite dimensional commutative F-algebra. Denote by $m_{\mathcal{A}} : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$ the multiplication map in $\mathcal{A}$, seen as a symmetric F-bilinear map, and by $T_{\mathcal{A}} \in \mathrm{Sym}^2(\mathcal{A}^\vee) \otimes_F \mathcal{A}$ the associated tensor, where $\mathcal{A}^\vee$ is the dual space of $\mathcal{A}$ over F and $\mathrm{Sym}^2(\mathcal{A}^\vee) \subset \mathcal{A}^\vee \otimes_F \mathcal{A}^\vee$ stands for the subspace of symmetric tensors.

By a symmetric bilinear multiplication algorithm for $\mathcal{A}$, of length n, we mean one of the following equivalent data (see e.g. [25] or [26, §5.1–5.3]):

- linear maps $\alpha : \mathcal{A} \longrightarrow F^n$ and $\omega : F^n \longrightarrow \mathcal{A}$ such that the following diagram commutes

$$\begin{array}{ccc} \mathcal{A} \times \mathcal{A} & \xrightarrow{m_{\mathcal{A}}} & \mathcal{A} \\ {\scriptstyle (\alpha,\alpha)}\downarrow & & \uparrow{\scriptstyle \omega} \\ F^n \times F^n & \xrightarrow{*} & F^n \end{array} \qquad (1)$$

  where $*$ denotes componentwise multiplication in F^n

*supported by ANR-14-CE25-0015 project Gardio and ANR-15-CE39-0013 project Manta

- linear forms $\alpha_1, \ldots, \alpha_n : \mathcal{A} \longrightarrow F$ and elements $w_1, \ldots, w_n \in \mathcal{A}$ such that, for all $x, y \in \mathcal{A}$, their product in $\mathcal{A}$ can be computed as

$$xy = \sum_{1 \leq i \leq n} \alpha_i(x)\alpha_i(y)w_i \tag{2}$$

- a decomposition

$$T_{\mathcal{A}} = \sum_{1 \leq i \leq n} \alpha_i^{\otimes 2} \otimes w_i \tag{3}$$

of $T_{\mathcal{A}}$ as a sum of n elementary symmetric tensors in $\mathrm{Sym}^2(\mathcal{A}^\vee) \otimes \mathcal{A}$.

We define the *symmetric bilinear complexity* of $\mathcal{A}$ over F

$$\mu_F^{\mathrm{sym}}(\mathcal{A}) \tag{4}$$

as the smallest length n for which such a symmetric bilinear multiplication algorithm exists. Equivalently, $\mu_F^{\mathrm{sym}}(\mathcal{A})$ is the *symmetric tensor rank* of $T_{\mathcal{A}}$.

Most of our interest will be when $F = \mathbb{F}_q$ is a finite field and $\mathcal{A} = \mathbb{F}_{q^k}$ is its (unique) degree k field extension. We then set

$$\mu_q^{\mathrm{sym}}(k) = \mu_{\mathbb{F}_q}^{\mathrm{sym}}(\mathbb{F}_{q^k}). \tag{5}$$

We will focus on upper bounds for this quantity or, which is essentially the same, on the construction of symmetric bilinear multiplication algorithms for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, especially when k is large. For this, a powerful method was introduced by Chudnovsky and Chudnovsky in 1987 with [12][13], using evaluation-interpolation on algebraic curves.

When looking at the literature, the reader should be wary that these authors, and those who followed them, actually expressed their results in terms of the classical (possibly asymmetric) bilinear complexity[1] $\mu_q(k)$, not in terms of the symmetric bilinear complexity $\mu_q^{\mathrm{sym}}(k)$. Indeed, this last notion was first introduced in this context only in 2012 with [25]. However, the original construction of [12][13] naturally produces symmetric algorithms. This allows us, in what follows, to restate the bounds derived by this method in terms of $\mu_q^{\mathrm{sym}}(k)$, even if the original statements were in terms of $\mu_q(k)$.

The first and probably the most spectacular achievement of this method is the proof that this quantity asymptotically grows linearly with k. Indeed, when recast in terms of symmetric complexity, the main result of [12][13] reads as:

$$\limsup_{k \to \infty} \frac{1}{k} \mu_q^{\mathrm{sym}}(k) \leq 2\left(1 + \frac{1}{\sqrt{q} - 3}\right) \qquad \text{for } q \geq 25 \text{ a square.} \tag{6}$$

Actually, parts of the proof given for this result were somehow sketchy, but all the missing details were later provided by Shparlinski, Tsfasman, and Vladut in 1991 with [29].

[1] Compared with (3), the (classical) bilinear complexity $\mu_F(\mathcal{A})$ of $\mathcal{A}$ over F is the (classical) tensor rank of $T_{\mathcal{A}}$, i.e. the minimal length n of a decomposition $T_{\mathcal{A}} = \sum_{1 \leq i \leq n} \alpha_i \otimes \beta_i \otimes w_i$ of $T_{\mathcal{A}}$ as a sum of n elementary tensors in $\mathcal{A}^\vee \otimes \mathcal{A}^\vee \otimes \mathcal{A}$, where now $\alpha_i, \beta_i \in \mathcal{A}^\vee$ are allowed to be different; equivalent definitions similiar to (1) or (2) can be given likewise.

At the same time they provided these missing details, these same authors also proposed the following improved bound:

$$\limsup_{k\to\infty} \frac{1}{k}\mu_q^{\mathrm{sym}}(k) \leq 2\left(1+\frac{1}{\sqrt{q}-2}\right) \qquad \text{for } q \geq 9 \text{ a square.} \tag{7}$$

Unfortunately, a fatal flaw was later found in their proof, as first observed in [9]. This error concerns the solution of what some authors now call "Riemann-Roch systems of equations" [10], a key ingredient in the Chudnovsky-Chudnovsky method, and it totally invalidates the proof given for (7).

Fortunately, an alternative method that allows to solve such Riemann-Roch systems was then discovered by the author around end of 2010, and published in 2013 with [23]. It readily allows to repair the proof of (7), with only one small downfall: the method only applies to sligthly larger q than originally needed.

It thus became desirable to try to fine tune the method of [23] in order to make it work for q as small as possible. This was the main goal of [24], and it allowed to repair the Shparlinski-Tsfasman-Vladut bound (7) as follows.

For any prime power q, define the *dense Ihara constant* [24, p. 23] as the smallest real number $A'(q)$ such that there exists a sequence of curves X_j over $\mathbb{F}_q$, of genus $g_j \to \infty$, with

- $\frac{|X_j(\mathbb{F}_q)|}{g_j} \to A'(q)$
- $\frac{g_{j+1}}{g_j} \to 1$

as $j \to \infty$. Then [24, Cor. 18] we have

$$\limsup_{k\to\infty} \frac{1}{k}\mu_q^{\mathrm{sym}}(k) \leq 2\left(1+\frac{1}{A'(q)-1}\right) \qquad \text{as soon as } A'(q) \geq 5-\tfrac{14q^2-4}{q^4+2q^2-1}, \tag{8}$$

and in particular we have

$$\limsup_{k\to\infty} \frac{1}{k}\mu_q^{\mathrm{sym}}(k) \leq 2\left(1+\frac{1}{\sqrt{q}-2}\right) \qquad \text{for } q \geq 49 \text{ a square.} \tag{9}$$

Actually, (9) does not requires the full strength of [24]. It can readily be derived from the original, simpler results of [23]. Thus, while (8) remains unpublished, (9) can be found in published form, with full proof, in [25, Th. 6.4]. Observe that it entirely repairs (7), but for $q \geq 49$ instead of $q \geq 9$, leaving only the cases $q = 9, 16, 25$ uncovered.

This far we discussed only works on *asymptotic* upper bounds. Parallel to these, some authors considered *effective* upper bounds on $\mu_q^{\mathrm{sym}}(k)$, that should apply to any (finite, explicit) value of k. This topic was treated by Ballet first in [2] and [3], and then improved in [4]. However it turned out this last work contained several errors, the most important of which being that it reproduced the flawed proof from [29] and based all its results on it.

Thus, in [24], while repairing the Shparlinski-Tsfasman-Vladut bound, the author also explained how his method could repair Ballet's results likewise. Actually, not only these results could be repaired, but they could also be improved. Indeed, part of Ballet's argument was based on Bertrand's postulate, proved by Chebyshev, that asserts that for any real $x > 1$, there is a prime between x and $2x$. It was clear that improved bounds on the bilinear complexity could be derived from finer estimates on the gaps between prime numbers (such as [1]).

This was presented in section 5 of [24], somehow as a digression (it is also discussed in [25], especially Rem. 5.3, 5.5, 5.8, but with a slightly different approach). Unfortunately, the fact that [24] remained unpublished, and the fact that this section 5 followed long and technical developments in a quite unrelated direction, did not help disseminate the ideas introduced there.

Ultimately, this method, which combines

(a) the author's optimal solution of Riemann-Roch systems for the Chudnovsky-Chudnovsky method

(b) fine estimates on the gaps between prime numbers,

and which still provides the best effective upper bounds on $\mu_q^{\mathrm{sym}}(k)$ when $q = p^2$ is a prime square, seemed to have been forgotten by the experts. As an illustration, very recently Ballet and Zykin [6] partially rediscovered this method (ingredient (b) only, not (a)), but a preliminary version of their work did not even mention [24] — fortunately this omission was quickly corrected.

Thus, almost seven years after it was first written, the author would like to take this opportunity to finally publish these results in the peer-reviewed literature. Hopefully this will provide a proper reference for future researchers. Accordingly, the next section is a translation into English of section 5 of [24], with essentially no significant change. Then in the last section we present some updates in order to take recent developments into account, and in particular we explain the links with [6]. We also discuss a few questions presented in [24]. This includes compatibilty with generalizations of the Chudnovsky-Chudnovsky method [25], leading to new effective and asymptotic bounds on the classical bilinear complexity $\mu_q(k)$ when $q = p$ is prime, and to similar results for short multiplication of polynomials; as well as open questions on gaps between prime numbers or more generally gaps in the set of values of certain arithmetic functions.

2 Main results as of 2011

As explained in the introduction, our aim here is to fix the proof of the main result claimed by Ballet in [4], and then to improve on it. This statement concerns effective upper bounds on $\mu_{p^2}^{\mathrm{sym}}(k)$, the symmetric bilinear multiplication complexity in extensions of a base field $\mathbb{F}_{p^2}$ of prime square order.

We first recall an instance of the basic construction of Chudnovsky and Chudnovsky [12][13]:

Proposition 1. *Let X be a curve of genus g over the finite field $\mathbb{F}_q$, equipped with a closed point Q of degree k, and with n points $P_1, \ldots, P_n$ of degree 1. Suppose that X also admits a $\mathbb{F}_q$-rational divisor D (w.l.o.g. of support disjoint from Q and the P_i) such that*

- *$D - Q$ is nonspecial*
  (so the evaluation map $L(D) \longrightarrow \mathbb{F}_q(Q) = \mathbb{F}_{q^k}$ is surjective)
- *$2D - (P_1 + \cdots + P_n)$ has no section*
  (so the evaluation map $L(2D) \longrightarrow \bigoplus_{i=1}^{n} \mathbb{F}_q(P_i) = \mathbb{F}_q^n$ is injective).

Then there is a symmetric bilinear multiplication algorithm of length n for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, i.e.

$$\mu_q^{\mathrm{sym}}(k) \leq n. \tag{10}$$

Observe that $D - Q$ nonspecial implies $\deg(D) - k \geq g - 1$, and $2D - (P_1 + \cdots + P_n)$ without section implies $2\deg(D) - n \leq g - 1$. So combining both, we see a necessary condition for the existence of such D, Q, and P_i is that X admits at least

$$|X(\mathbb{F}_q)| \geq n \geq 2k + g - 1 \tag{11}$$

points of degree 1.

We say a method for finding such data on X is *optimal* if it can work with equality attained in (11).

In the course of the proof of their main result in [12][13], Chudnovsky and Chudnovsky constructed such D, Q, and P_i, but only under the suboptimal condition

$$|X(\mathbb{F}_q)| \geq 2k + 2g - 1. \tag{12}$$

This was also stated more explicitely by Ballet as [2, Lemma 2.2]. Roughly speaking, the construction proceeds by first fixing Q and D, and then finding the P_i.

By contrast, in order to reach optimality, it is more natural to first fix Q and $G = P_1 + \cdots + P_n$, and then only look for D such that $D - Q$ is nonspecial and $2D - G$ has no section. Seen this way, the problem essentially reduces to a "Riemann-Roch system of equations" in the sense of [10].

In [29, pp. 161–162] a solution to this Riemann-Roch system is proposed under the optimal condition (11). Unfortunately, an error in the proof was detected by Cascudo in [9], which invalidates the argument. It turns out the very same result was later stated also by Ballet as [4, Prop. 2.1], with the same proof and the error it contains reproduced as well. Let us briefly explain this error: assuming $n = 2k + g - 1$, the core of the argument is to show that the number of divisor classes $[D]$ such that $2D - G$ has sections is not more than the number of effective divisors of degree $g - 1$; for this, to each such class, one assigns an effective divisor $E \sim 2D - G$, and one concludes with the claim that this map $[D] \mapsto E$ is injective; unfortunately this last claim is false in general: indeed, if the class group has some 2-torsion, it could happen that two divisors D and D' are not linearly equivalent, but $2D - G$ and $2D' - G$ are, and give the same E.

Fortunately, in [23] the author introduced a new construction that provides an optimal solution to certain Riemann-Roch systems. In [24] (and later in [25]) it was applied to the system associated with the Chudnovsky-Chudnovsky method, which allows to substitute Ballet's erroneous [4, Prop. 2.1] with the following [24, Cor. 20]:

Proposition 2. *Let X be a curve of genus g over a finite field $\mathbb{F}_q$, equipped with two $\mathbb{F}_q$-rational divisors Q and G. Set $k = \deg Q$ and $n = \deg G$, and assume*

$$|X(\mathbb{F}_q)| > 5g \tag{13}$$

and

$$n \geq 2k + g - 1. \tag{14}$$

Then there exists a $\mathbb{F}_q$-rational divisor D on X, with support in $X(\mathbb{F}_q)$, such that $D - Q$ is nonspecial of degree $g - 1$, and $2D - G$ has no section.

In particular, if $n = 2k + g - 1$, then both $D - Q$ and $2D - G$ are nonspecial of degree $g - 1$.

The only downfall is the new condition (13), but this does not cause any trouble unless q is very small. In particular it does not hinder optimality, so it will be sufficient for us in order to fix Ballet's result.

A proof of Proposition 2 is essentially included in that of [25, Th. 5.2]. We reproduce the argument for completeness.

Proof. Recall [23, Lemma 6] and [23, Lemma 9]:

(i) If A is a divisor on X with $\deg(A) \leq g - 2$ and $l(A) = 0$, then for all $P \in X(\mathbb{F}_q)$ except perhaps at most g of them, we also have $l(A + P) = 0$.

(ii) If A is a divisor on X with $\deg(A) \leq g - 3$ and $l(A) = 0$, then for all $P \in X(\mathbb{F}_q)$ except perhaps at most $4g$ of them, we also have $l(A+2P) = 0$.

We want a $\mathbb{F}_q$-rational divisor D of degree $\deg(D) = k + g - 1$ such that

$$l(D - Q) = l(2D - G) = 0. \tag{15}$$

Observe that D trivially satisfies (15) if $\deg(D)$ is small enough. Now, if some D with $\deg(D) < k + g - 1$ satisfies (15), then thanks to (13) and results (i)(ii) just recalled, we can find some $P \in X(\mathbb{F}_q)$ such that $D + P$ also satisfies (15). We can then continue by induction, replacing D with $D + P$, until we reach $\deg(D) = k + g - 1$. □

Actually, condition (13) could be slightly relaxed, using the machinery introduced in sections 1–2 of [24], which improves on the bound $4g$ in [23, Lemma 9] (recalled as (ii) in the proof above). Thus Proposition 2 is a simplified version, that follows directly from the original results of [23] without using the full strength of [24]. Anyway it will suffice for us here.

With this at hand, Ballet's [4, Th. 2.1(1)] is replaced with the following [24, Lemma 21]:

Lemma 3. *Let X be a curve of genus g over a finite field $\mathbb{F}_q$ with*

$$|X(\mathbb{F}_q)| > 5g. \tag{16}$$

Then for all integers k in the interval

$$\left\lceil 2\log_q \frac{2g+1}{\sqrt{q}-1} \right\rceil \;<\; k \;\leq\; \frac{|X(\mathbb{F}_q)|+1-g}{2} \tag{17}$$

we have

$$\mu_q^{\mathrm{sym}}(k) \leq 2k+g-1. \tag{18}$$

Proof. Following [24], this is a direct consequence of Proposition 1, together with [30, Cor. V.2.10.c] and Proposition 2 above.

Alternatively, it is also a special case of [25, Th. 5.2(c)] applied with $m=k$, $l=1$, $n_{1,1}=2k+g-1$, and $n_{d,u}=0$ for other values of d,u. □

For instance, taking $X=\mathbb{P}^1$, we find:

$$\mu_q^{\mathrm{sym}}(k) \leq 2k-1 \qquad \text{for } k \leq \frac{q}{2}+1, \tag{19}$$

an inequality that is in fact easily seen to be an equality [32].

Likewise, choosing for X a suitable elliptic curve, yields the following bound from [28]:

$$\mu_q^{\mathrm{sym}}(k) \leq 2k \qquad \text{for } k < \frac{q+e(q)+1}{2} \tag{20}$$

with $e(q) \lesssim 2\sqrt{q}$, and in particular $e(q)=2\sqrt{q}$ if q is a square.

One could continue in the same way with curves of genus 2, 3, etc.

Another equivalent point of view is the following. For any integer k, let $\mathcal{X}_{q,k}$ be the set of curves (up to isomorphism) X over $\mathbb{F}_q$, of genus $g=g(X)$, satisfying:

(a) $g \leq \frac{1}{2}(q^{(k-1)/2}(q^{1/2}-1)-1)$

(b) $|X(\mathbb{F}_q)| > 5g$

(c) $|X(\mathbb{F}_q)| \geq 2k+g-1$.

Then:

Lemma 4. *For any finite field $\mathbb{F}_q$, and for any integer k such that $\mathcal{X}_{q,k}$ is nonempty, we have*

$$\frac{1}{k}\mu_q^{\mathrm{sym}}(k) \leq 2 + \frac{\min_{X\in\mathcal{X}_{q,k}} g(X) - 1}{k}. \tag{21}$$

Proof. It is a reformulation of the previous lemma. □

Compared to similar results in the literature, our equivalent Lemma 3 and Lemma 4 impose less restriction between k, g, and the number of points on the curve. For instance, [2, Th. 1.1 and Cor. 2.1] reach the same conclusion, but only for $k \leq \frac{|X(\mathbb{F}_q)|+1-2g}{2}$ instead of the second inequality in (17), or equivalently, under the stronger condition $|X(\mathbb{F}_q)| \geq 2k+2g-1$ instead of (c) in the definition of $\mathcal{X}_{q,k}$. However, our method requires curves with "sufficiently many" points, as expressed by condition (b).

Now we can go on with the same arguments as in [4], and then improve on the result that is stated there.

Consider the Dedekind psi function, defined for any integer N by

$$\psi(N) = N \prod_{\substack{l|N \\ l \text{ prime}}} \left(1 + \frac{1}{l}\right). \tag{22}$$

Lemma 5. *Let p be a prime number, and N an integer prime to p. Then the modular curve $X_0(N)$ is smooth over $\mathbb{F}_p$, of genus*

$$g_0(N) \leq \frac{\psi(N)}{12}, \tag{23}$$

and it admits

$$|X_0(N)(\mathbb{F}_{p^2})| \geq (p-1)\frac{\psi(N)}{12} \tag{24}$$

points over $\mathbb{F}_{p^2}$.

Proof. See [31], § 4.1. □

Remark 6. Actually we can be slightly more precise in this lemma. Hurwitz's formula gives an exact expression

$$g_0(N) = \frac{\psi(N)}{12} + 1 - \frac{\nu_\infty(N)}{2} - \frac{\nu_3(N)}{3} - \frac{\nu_2(N)}{4} \tag{25}$$

where

- $\nu_\infty(N) = \sum_{d|N} \phi(\gcd(d, \frac{N}{d})) = \prod_{l^\nu || N} \begin{cases} 2l^{\frac{\nu-1}{2}} & \text{if } \nu \text{ odd} \\ (l+1)l^{\frac{\nu}{2}-1} & \text{if } \nu \text{ even} \end{cases}$
- $\nu_3(N) = \begin{cases} \prod_{l|N} \left(1 + \left(\frac{-3}{l}\right)\right) & \text{if } 9 \nmid N \\ 0 & \text{if } 9 \mid N \end{cases}$
- $\nu_2(N) = \begin{cases} \prod_{l|N} \left(1 + \left(\frac{-1}{l}\right)\right) & \text{if } 4 \nmid N \\ 0 & \text{if } 4 \mid N \end{cases}$

while the Eichler-Shimura relation gives

$$|X_0(N)(\mathbb{F}_{p^2})| = p^2 + 1 + pg_0(N) - \operatorname{tr} T_{p^2} \tag{26}$$

where the Hecke operator T_{p^2} acts on the space of cusp forms $S_2(\Gamma_0(N))$, and its trace can be computed explicitly, e.g. by the formula given in [21], Th. 6.8.4 and Rem. 6.8.1, pp. 263–264:

$$\operatorname{tr} T_{p^2} = \frac{\psi(N)}{12} + \delta(N, p^2) - \sum_t a(t) \sum_f b(t,f)c(t,f) \tag{27}$$

where $\delta(N, p^2) = p^2 + p + 1$ if $N > 1$. The terms $a(t)\sum_f b(t,f)c(t,f)$ are nonnegative, and their contribution to the sum has a simple expression for certain special values of t:

- $\frac{1}{2}\, p\, \nu_\infty(N)$ for $t = \pm 2p$
- $\frac{1}{3}\left(p + 1 - \left(\frac{-3}{p}\right)\right)\nu_3(N)$ for $t = \pm p$ (if $3 \nmid N$)
- $\frac{1}{4}\left(p + 1 - \left(\frac{-1}{p}\right)\right)\nu_2(N)$ for $t = 0$ (if $2 \nmid N$)

so that for $N > 1$ prime to $6p$:

$$|X_0(N)(\mathbb{F}_{p^2})| \geq (p-1)\frac{\psi(N)}{12} + \frac{1-\left(\frac{-3}{p}\right)}{3}\nu_3(N) + \frac{1-\left(\frac{-1}{p}\right)}{4}\nu_2(N) \tag{28}$$

Similar formulas can be derived for $2|N$ or $3|N$.

For any infinite subset $\mathcal{A}$ of $\mathbb{N}$ and for any real $x > 0$, let

$$\lceil x \rceil_{\mathcal{A}} = \min\, \mathcal{A} \cap [x, +\infty[\tag{29}$$

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

$$\epsilon_{\mathcal{A}}(x) = \sup_{y \geq x} \frac{\lceil y \rceil_{\mathcal{A}} - y}{y}, \tag{30}$$

so the function $\epsilon_{\mathcal{A}}$ is monotonously non-increasing, and for any $x > 0$, the interval $[x, (1 + \epsilon_{\mathcal{A}}(x))x]$ contains an element of $\mathcal{A}$.

For instance, if p is a prime number, then $\lceil x \rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})}$ is the smallest integer $n \geq x$ that can be written as $n = \psi(N)$ for an integer N prime to p, and:

Lemma 7. *With these notations, for $p \neq 2$ we have*

$$\lceil x \rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})} \leq 2x \quad \textit{for all } x \geq \frac{3}{2}, \tag{31}$$

or said otherwise:

$$\epsilon_{\psi(\mathbb{N}\setminus p\mathbb{N})}(3/2) \leq 1. \tag{32}$$

Proof. Indeed, for $j = \lfloor \frac{\log 2x/3}{\log 2} \rfloor$, we have $x < 3 \cdot 2^j = \psi(2^{j+1}) \leq 2x$. □

Proposition 8. *Let $p \geq 7$ be a prime number. Then for all $k > \frac{p^2+p+1}{2}$ we have*

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2 + \frac{\frac{1}{12}\left\lceil \frac{24k-12}{p-2} \right\rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})} - 1}{k}. \tag{33}$$

Proof. Choose N prime to p such that $\psi(N) = \left\lceil \frac{24k-12}{p-2} \right\rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})}$ and set $X = X_0(N)$. Then, by (23) and (24) we have $|X(\mathbb{F}_{p^2})| - g \geq (p-2)\frac{\psi(N)}{12}$, so condition (c) before Lemma 4 is satisfied.

Likewise we have $|X(\mathbb{F}_{p^2})| - 5g \geq (p-6)\frac{\psi(N)}{12}$, so for $p \geq 7$ condition (b) is satisfied too.

Last, by Lemma 7 we have $\psi(N) = \left\lceil \frac{24k-12}{p-2} \right\rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})} \leq \frac{48k-24}{p-2}$ so

$$g \leq \frac{\psi(N)}{12} \leq \frac{4k-2}{p-2}, \tag{34}$$

and for $p \geq 7$ and $k > \frac{p^2+p+1}{2}$, this last quantity is easily shown to be less than $\frac{1}{2}(p^{k-1}(p-1)-1)$. Thus condition (a) is satisfied, and we conclude with Lemma 4. □

Remark 9. Thanks to this proposition, any (effective) upper bound on the function $\lceil . \rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})}$, or on $\epsilon_{\psi(\mathbb{N}\setminus p\mathbb{N})}$, translates into an (effective) upper bound on the $\mu_{p^2}^{\mathrm{sym}}(k)$. Our task is then, for any given real $x > 0$, to find an integer N prime to p such that $\psi(N)$ is larger than or equal to x but as small as possible. A quick analysis suggests two natural approaches to this problem.

First, one can look for N among integers having only small prime factors. Indeed, let $\mathcal{B} = \{l_1, \ldots, l_B\}$ be a set of prime numbers, $p \notin \mathcal{B}$. Set $N_{\mathcal{B}} = \prod_{i=1}^{B} l_i$ and assume $\psi(N_{\mathcal{B}}) = \prod_{i=1}^{B}(l_i+1) < x$. Then if $N = N'N_{\mathcal{B}}$ where N' has all its prime factors in $\mathcal{B}$, we have $\psi(N) = N'\psi(N_{\mathcal{B}})$. Thus, if we can find an integer $N' \geq \frac{x}{\psi(N_{\mathcal{B}})}$ as small as possible with all its prime factors in $\mathcal{B}$, we deduce an upper bound on $\lceil x \rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})}$. For $\mathcal{B} = \{2\}$ this is precisely Lemma 7. It would be interesting to optimize the choice $\mathcal{B}$ (possibly depending on x) in order to get better estimates.

At the opposite, one can choose N among integers having only large prime factors. Indeed, if N has no prime factor smaller than $N^{1/u}$, then $\psi(N) \leq N\left(1 + \frac{1}{N^{1/u}}\right)^u$, and if we can produce such an $N \geq x$ as small as possible, then, for a convenient choice of u, one could hope to get a bound close enough to $\lceil x \rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})}$. The extreme case is $u = 1$, which means we look only at N prime. We then get the upper bound

$$\lceil x \rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})} \leq \lceil x-1 \rceil_{\mathcal{P}} + 1 \quad \text{for } x > p+1 \tag{35}$$

where $\mathcal{P}$ is the set of prime numbers (indeed, $N = \lceil x-1 \rceil_{\mathcal{P}}$ is a prime number larger than p, and $\psi(N) = N + 1 \geq x$). This allows to use all known results

on the function $\epsilon_{\mathcal{P}}$; for instance, Bertrand's postulate, proved by Chebyshev, gives $\epsilon_{\mathcal{P}}(1) = 1$, and combined with (35), it provides essentially the same bound as in Lemma 7. Several sharper bounds on $\epsilon_{\mathcal{P}}$ are known, and we list their consequences in the corollary below. However, here again, it would still be interesting to study whether a convenient choice of $u > 2$ (possibly depending on x), would give significantly better.

Corollary 10. *Let $p \geq 7$ be a prime number. Then*

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

$$\frac{1}{k}\mu^{\mathrm{sym}}_{p^2}(k) \leq 2\left(1 + \frac{1 + \epsilon_{\mathcal{P}}\left(\frac{24k}{p-2}\right)}{p-2}\right) \tag{36}$$

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

$$\frac{1}{k}\mu^{\mathrm{sym}}_{p^2}(k) \leq 2\left(1 + \frac{2}{p-2}\right) \tag{37}$$

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

$$\frac{1}{k}\mu^{\mathrm{sym}}_{p^2}(k) \leq 2\left(1 + \frac{1 + \frac{10}{139}}{p-2}\right) \tag{38}$$

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

$$\frac{1}{k}\mu^{\mathrm{sym}}_{p^2}(k) \leq 2\left(1 + \frac{1.000\,000\,005}{p-2}\right) \tag{39}$$

(v) for all $k \geq 16\,531\,(p-2)$,

$$\frac{1}{k}\mu^{\mathrm{sym}}_{p^2}(k) \leq 2\left(1 + \frac{1 + \frac{1}{25\log^2\frac{24k}{p-2}}}{p-2}\right) \tag{40}$$

(vi) for all k large enough,

$$\frac{1}{k}\mu^{\mathrm{sym}}_{p^2}(k) \leq 2\left(1 + \frac{1 + \frac{1}{\left(\frac{24k}{p-2}\right)^{0.475}}}{p-2}\right). \tag{41}$$

Proof. Item (i) follows from Proposition 8, from (35), and the obvious inequality $\left\lceil \frac{24k-12}{p-2} - 1 \right\rceil_{\mathcal{P}} \leq \left\lceil \frac{24k}{p-2} \right\rceil_{\mathcal{P}}$.

Item (ii) follows from (65), Proposition 8, and Lemma 7.

Noting that for $p \geq 7$ and $k > \frac{p^2+p+1}{2}$ we have $\frac{24k}{p-2} > 139$, item (iii) follows from (65), from (i), and from $\epsilon_{\mathcal{P}}(139) = 10/139$. To justify this last equality,

observe that if $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, ... is the sequence of prime numbers, then for all $n \leq n'$ we have

$$\epsilon_{\mathcal{P}}(p_n) = \max\left(\epsilon_{\mathcal{P}}(p_{n'}), \max_{n \leq j < n'} \frac{p_{j+1} - p_j}{p_j}\right). \tag{42}$$

Set $p_n = 139$, estimate $\epsilon_{\mathcal{P}}(p_{n'})$ for $p_{n'} = 2\,010\,881$ using [27] (or for $p_{n'} = 396\,833$ using [16]) and conclude by explicitly computing the (finitely many) remaining terms for $n \leq j < n'$.

Likewise, items (iv), (v) and (vi) follow from (i) and the estimates on $\epsilon_{\mathcal{P}}$ that are given in [22], [16] (preprint version only, beware that the published verion is different), and [1], respectively. □

3 More recent developments, and questions that remain open

3.1. New estimates on gaps between primes. Corollary 10(i) allows to systematically translate any estimate on gaps between primes into a bound on $\mu_{p^2}^{\mathrm{sym}}(k)$. In Corollary 10(iii)-(vi) we listed such bounds, based on the state of the literature in 2011, i.e. at the time when [24] was written.

Certainly many new results of this type have been published since then, and will be published in the future. One such result is Dudek's [15], that has been used by Ballet and Zykin [6] (see §3.5 below), and which asserts that for any real $x > e^{e^{33.3}}$ there is a prime between x and $x + 3x^{2/3}$, or with our notations, $\epsilon_{\mathcal{P}}(x) \leq 3x^{-1/3}$. Combined with Corollary 10(i), this gives at once:

Corollary 10 — continued. *(vii) For $p \geq 7$ and $k \geq \frac{p-2}{24} e^{e^{33.3}}$,*

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2\left(1 + \frac{1 + \frac{3}{\left(\frac{24k}{p-2}\right)^{1/3}}}{p-2}\right). \tag{43}$$

Actually, this Corollary 10(vii) is weaker than Corollary 10(vi) because the exponent $1/3$ is not as good as the exponent 0.475. But it is fully effective, in the sense that the range of k for which it holds is given explicitely from Dudek's work [15], while in [1] only the existence is proved (although the authors observe it could be made explicit with enough work).

How far could we hope to go with this method? It is known that, under the Riemann hypothesis, we should have $\epsilon_{\mathcal{P}}(x) = \widetilde{O}(x^{-1/2})$. Combined with Corollary 10(i), this gives:

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2\left(1 + \frac{1 + \widetilde{O}(k^{-1/2})}{p-2}\right). \tag{44}$$

Ultimately, it is conjectured $\epsilon_{\mathcal{P}}(x) = O(\log^2(x)/x)$ [14], which would give likewise:

$$\frac{1}{k}\mu_{p^2}^{\mathrm{sym}}(k) \leq 2\left(1 + \frac{1 + O(\log^2(k)/k)}{p-2}\right). \tag{45}$$

3.2. Gaps between prime numbers in a given residue class. (This is a translation of the paragraph at the bottom of [24, p. 31], and is also discussed in [25, Rem. 5.5].)

Our main results concerned a base field $\mathbb{F}_q$ where $q = p^2$ is a prime square, and used evaluation-interpolation on (classical) modular curves.

Using more general Shimura curves, as those from [29], one could get similar results for $q = p^{2m}$ with arbitrary m. This case is also mentioned in [4], however, we point out another error in the proof given there: Ballet applies Bertrand's postulate to the primes that correspond to the levels of these curves; but he forgets that, for these curves, he has to deal not with the set of all prime numbers, but only with those that split completely in a certain abelian extension L of $\mathbb{Q}$. This splitting condition translates into a certain congruence condition. So, in principle, this strategy of proof could work, but for this, instead of Bertrand's postulate, one should substitute an estimate, such as the one from [18], on the gaps between primes that live in some given residue class.

However, still other families of curves could be used, for instance Drinfeld modular curves. At this stage it is not clear which approach will produce the best effective bounds.

3.3. Gaps in the set of values of the Dedekind psi function. In Remark 9 we outlined two strategies that could lead to estimates on $\epsilon_{\psi(\mathbb{N}\setminus p\mathbb{N})}$, that is, on gaps in the set of values of the Dedekind psi function (at integers prime to p). However, quickly we restricted to values of ψ at prime numbers, so we only had to consider the more studied function $\epsilon_{\mathcal{P}}$.

Obviously, considering all values of ψ instead of only its values at primes, can only lead to smaller gaps, hence to better bounds on the complexity of multiplication. The question is: how much better can we get?

Initially, the author hoped to get significantly stronger bounds in this way, and this hope was one of the reasons for delaying the publication of this work (see also [25, Rem. 5.8]). A motivation for this was Corollary 10(ii), obtained very easily by considering the values of ψ at powers of 2: by comparison, it could also have been derived using values at prime numbers, but this requires Bertrand's postulate, whose proof, given by Chebyshev, is certainly not so trivial.

Unfortunately, the author is now much more pessimistic, for the following reason.

Very likely, a method that bounds gaps in the set of values of ψ, should apply to a larger class of arithmetic functions. To any map

$$a : \mathcal{P} \longrightarrow \mathbb{Z} \tag{46}$$

that takes only finitely many different values, associate an arithmetic function f_a by the formula

$$f_a(N) = N \prod_{\substack{l|N \\ l \text{ prime}}} \left(1 + \frac{a(l)}{l}\right) \tag{47}$$

and let

$$\mathcal{S}_a = f_a(\mathbb{N}_{>0}) \tag{48}$$

be the set of values of f_a. For instance:

- if $a(l) = 1$ for all l, then
$$\mathcal{S}_a = \psi(\mathbb{N}_{>0}) \tag{49}$$
is the set of all values of the Dedekind psi function
- if $a(p) = -p$ and $a(l) = 1$ for all $l \neq p$, then
$$\mathcal{S}_a = \{0\} \cup \psi(\mathbb{N} \setminus p\mathbb{N}) \tag{50}$$
is precisely the set appearing in our application to bilinear complexity
- if $a(l) = -1$ for all l, then
$$\mathcal{S}_a = \phi(\mathbb{N}_{>0}) \tag{51}$$
is the set of all values of the Euler totient function ϕ.

So we're interested in estimates on the gaps between elements of such a set $\mathcal{S}_a$, and more precisely, on upper bounds on the associated function $\epsilon_{\mathcal{S}_a}$. Specializing to values of f_a at primes readily gives

$$\epsilon_{\mathcal{S}_a}(x) \leq \epsilon_{\mathcal{P}}(x) + O(1/x) \tag{52}$$

but our hope would be to get a bound significantly sharper.

Now several authors already studied the distribution of the values of ϕ, and in particular, in [17, p. 70] it is asked: "Can it be shown, for example, that for x sufficiently large, there is a totient between x and $x + x^{1/2}$?"

That means that the inequality $\epsilon_{\phi(\mathbb{N}_{>0})}(x) \leq x^{-1/2}$ is still an open question. Or said otherwise, one does not know significantly better estimates on the gaps in the set of all values of ϕ, than what one could derive from its values at primes (namely, $\epsilon_{\mathcal{P}}(x) \leq x^{-0.475}$ by [1], and $\epsilon_{\mathcal{P}}(x) = O(x^{-1/2}\log^2 x)$ under RH).

Thus, contrary to the author's initial expectations, this now leaves very little hope for the similar question for ψ.

3.4. Generalizations of the basic Chudnovsky-Chudnovsky method. At the very end of [24, section 5], it is discussed how our optimal solution to Riemann-Roch systems could be combined with extensions of the Chudnovsky-Chudnovsky method such as [11], that use evaluation at points of higher degree and with multiplicities. This discussion was not reproduced here, because these

results are now superseded by [25, Th. 5.2(c)], which uses an even finer notion of generalized evaluation. Namely, the bounds from [25] involve the quantities

$$\mu_q^{\mathrm{sym}}(d,u) = \mu_{\mathbb{F}_q}^{\mathrm{sym}}(\mathbb{F}_{q^d}[t]/(t^u)) \tag{53}$$

which allow to take into account both higher degree d and multiplicity u at the same time and in the most accurate way.

Still there is a difficulty. Very often, generalized evaluation, and more precisely evaluation at points of higher degree, is used when dealing with curves that do not have that many points of degree 1. Thus, it becomes useful, for instance, if one works over a field $\mathbb{F}_p$ of prime order. However, our method, in Proposition 2 as well as in [25, Th. 5.2(c)], still requires curves with sufficiently many points of degree 1, as asked by condition (13). In practice, this makes our construction unsuitable for these specific applications, and instead, one has to revert to suboptimal methods. A possible solution would be to adapt Proposition 2 and make this optimal construction work, say, with curves having sufficiently many points of degree 2 (instead of degree 1), but this is still an open question.

However, there are two alternative directions where optimality can be reached.

3.4.1. Classical bilinear complexity. A first direction is if one is interested in the classical bilinear complexity $\mu_q(k)$, instead of the symmetric bilinear complexity $\mu_q^{\mathrm{sym}}(k)$. Note that the classical works [12][13] and [29] all dealt only with $\mu_q(k)$, as did also [4] and [24]. Indeed, the symmetric complexity $\mu_q^{\mathrm{sym}}(k)$ was first introduced in this context only in [25], together with the importance of the distinction between these two notions. In particular it is observed there that classical bilinear complexity allows asymmetric evaluation-interpolation algorithms, whose associated Riemann-Roch systems are easier to solve optimally. In this setting, instead of [25, Th. 5.2(c)], we can use [25, Th. 5.2(a)], which does not require a condition like (13) on the number of points of degree 1.

For instance, it specializes to the following:

Lemma 11. *Let X be a curve of genus g over the finite field $\mathbb{F}_q$. Suppose $q \geq 7$ and X admits*

- *a closed point Q of degree k*
- *n_1 closed points of degree 1*
- *n_2 closed points of degree 2*

with

$$n_1 + 2n_2 \geq 2k + g - 1. \tag{54}$$

Then we have

$$\mu_q(k) \leq n_1 + 3n_2. \tag{55}$$

Proof. Special case of [25, Th. 5.2(a)] applied with $m = k$, $l = 1$, $n_{1,1} = n_1$, $n_{2,1} = n_2$, and $n_{d,u} = 0$ for other values of d, u. □

This Lemma 11 repairs Ballet's [4, Th. 2.1(2)], in the same way Lemma 3 repaired Ballet's [4, Th. 2.1(1)].

We can then continue exactly as in Section 2, with the same modular curves $X_0(N)$, which we can now consider over the prime field $\mathbb{F}_p$. Lemma 5 gives $g_0(N) \leq \frac{\psi(N)}{12}$ and $2n_2 \geq (p-1)\frac{\psi(N)}{12}$, and with the very same computations we conclude:

Proposition 12. *Let $p \geq 7$ be a prime number. Then for all $k > \frac{p+1}{2}$, we have*

$$\frac{1}{k}\mu_p(k) \leq 3\left(1 + \frac{1 + \epsilon_{\mathcal{P}}\left(\frac{24k}{p-2}\right)}{p-2}\right). \tag{56}$$

Again this can be combined with any known upper bound on $\epsilon_{\mathcal{P}}$. For instance, from [15] we deduce

$$\frac{1}{k}\mu_p(k) \leq 3\left(1 + \frac{1 + \frac{3}{\left(\frac{24k}{p-2}\right)^{1/3}}}{p-2}\right) \tag{57}$$

for $k \geq \frac{p-2}{24}e^{e^{33.3}}$, and from [1] we deduce

$$\frac{1}{k}\mu_p(k) \leq 3\left(1 + \frac{1 + \frac{1}{\left(\frac{24k}{p-2}\right)^{0.475}}}{p-2}\right) \tag{58}$$

for k large enough. Observe also the following asymptotic consequence:

Corollary 13. *For $p \geq 7$ we have*

$$\limsup_{k\to\infty} \frac{1}{k}\mu_p(k) \leq 3\left(1 + \frac{1}{p-2}\right). \tag{59}$$

3.4.2. Short multiplication of polynomials. In a second direction, we observe that the obstruction discussed at the beginning of §3.4 applies to evaluation at points of higher degree, but not to evaluation with multiplicities (at points of degree 1). Moreover, a new feature introduced in [25] is that it does not only gives a bound *in terms* of the $\mu_q^{\mathrm{sym}}(d,u)$, it also gives a bound *on* them. In particular, set

$$\widehat{M}_q^{\mathrm{sym}}(l) = \mu_q^{\mathrm{sym}}(1,l) = \mu_{\mathbb{F}_q}^{\mathrm{sym}}(\mathbb{F}_q[t]/(t^l)). \tag{60}$$

Multiplication in the quotient algebra $\mathbb{F}_q[t]/(t^l)$ is sometimes called *short multiplication* of polynomials. Then:

Lemma 14. *Let X be a curve of genus g over a finite field $\mathbb{F}_q$ with*

$$|X(\mathbb{F}_q)| > 5g. \tag{61}$$

Then for all integers

$$l \leq \frac{|X(\mathbb{F}_q)| + 1 - g}{2} \tag{62}$$

we have

$$\widehat{M}_q^{\mathrm{sym}}(l) \leq 2l + g - 1. \tag{63}$$

Proof. Special case of [25, Th. 5.2(c)] applied with $m = 1$, $l = l$, $n_{1,1} = 2l+g-1$, and $n_{d,u} = 0$ for other values of d, u. □

Lemma 14 is the exact analogue of Lemma 3 for $\widehat{M}_q^{\mathrm{sym}}(l)$ instead of $\mu_q^{\mathrm{sym}}(k)$. Mutatis mutandis, we deduce

$$\widehat{M}_q^{\mathrm{sym}}(l) \leq 2l - 1 \qquad \text{for } l \leq \frac{q}{2} + 1, \tag{64}$$

$$\widehat{M}_q^{\mathrm{sym}}(l) \leq 2l \qquad \text{for } l < \frac{q + e(q) + 1}{2} \tag{65}$$

and $\widehat{M}_{p^2}^{\mathrm{sym}}(l)$ satisfy the same upper bounds as $\mu_{p^2}^{\mathrm{sym}}(k)$ in Proposition 8 and Corollary 10(i)-(vii). In particular:

Proposition 15. *For $p \geq 7$ prime, we have*

- *for $l > \frac{p^2+p+1}{2}$,*

$$\frac{1}{l}\widehat{M}_{p^2}^{\mathrm{sym}}(l) \leq 2 + \frac{\frac{1}{12}\left\lceil \frac{24l-12}{p-2} \right\rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})} - 1}{l} \tag{66}$$

- *for $l > \frac{p^2+p+1}{2}$,*

$$\frac{1}{l}\widehat{M}_{p^2}^{\mathrm{sym}}(l) \leq 2\left(1 + \frac{1 + \epsilon_{\mathcal{P}}\left(\frac{24l}{p-2}\right)}{p-2}\right). \tag{67}$$

Again this can be combined with all existing and future bounds on $\epsilon_{\mathcal{P}}$, leading for instance to

$$\frac{1}{l}\widehat{M}_{p^2}^{\mathrm{sym}}(l) \leq 2\left(1 + \frac{1 + \frac{3}{\left(\frac{24l}{p-2}\right)^{1/3}}}{p-2}\right) \tag{68}$$

for $l \geq \frac{p-2}{24}e^{e^{33.3}}$, or to

$$\frac{1}{l}\widehat{M}_{p^2}^{\mathrm{sym}}(l) \leq 2\left(1 + \frac{1 + \frac{1}{\left(\frac{24l}{p-2}\right)^{0.475}}}{p-2}\right) \tag{69}$$

for l large enough.

Asymptotically we also deduce the following, which was already observed (at least implicitely) in [25, Rem. 6.7]:

Corollary 16. *For $p \geq 7$ prime, we have*

$$\limsup_{l\to\infty} \frac{1}{l}\widehat{M}_{p^2}^{\mathrm{sym}}(l) \leq 2\left(1+\frac{1}{p-2}\right). \tag{70}$$

Moreover, as in §3.4.1, we can also get results over the prime field $\mathbb{F}_p$, provided we're interested in classical bilinear complexity instead of symmetric bilinear complexity. Setting $\widehat{M}_q(l) = \mu_q(1,l)$, the very same approach gives:

Proposition 17. *For $p \geq 7$ prime and $l > \frac{p+1}{2}$, we have*

$$\frac{1}{l}\widehat{M}_p(l) \leq 3\left(1+\frac{1+\epsilon_{\mathcal{P}}\left(\frac{24l}{p-2}\right)}{p-2}\right). \tag{71}$$

We leave it to the reader to derive as before the combination with any bound of his choice on $\epsilon_{\mathcal{P}}$.

Corollary 18. *For $p \geq 7$ prime, we have*

$$\limsup_{l\to\infty} \frac{1}{l}\widehat{M}_p(l) \leq 3\left(1+\frac{1}{p-2}\right). \tag{72}$$

3.5. Lower bounds. Our focus is on upper bounds only, but it is interesting to briefly mention some known lower bounds as a comparison.

Most such lower bounds use coding-theoretic arguments, originating in [7] and [20]. For instance, it is easily seen that if an *integral* algebra $\mathcal{A}$ of dimension k admits a bilinear algorithm of length n over F, then there exists a $[n,k,\geq k]$-code over F. From this, both finite and asymptotic upper bounds on codes readily translate into finite and asymptotic lower bounds on $\mu_q(k)$. It follows in particular

$$\liminf_{k\to\infty} \frac{1}{k}\mu_q(k) \geq 2+\frac{1}{q-1} \tag{73}$$

for any q. This result was first proved in [19] (it is also stated in [29, Cor 1.8] but with a mistake, later corrected in [9, pp. 172-173]).

A generalization was then proved in [8], getting rid of the integrality hypothesis, from which it follows similarly

$$\liminf_{l\to\infty} \frac{1}{l}\widehat{M}_q(l) \geq 2+\frac{1}{q-1}. \tag{74}$$

3.6. Recent work of Ballet and Zykin. Very recently Ballet and Zykin published the work [6], in which they independently rediscover part of the argument of [24, sect. 5], namely the use of fine estimates on gaps between primes such as the one of Baker-Harman-Pintz [1], as an improvement over Ballet's use of Bertrand's postulate in [4].

Actually, there are two parts in [6]. The first part, [6, Prop. 7], concerns a base field $\mathbb{F}_{p^2}$ of prime square order, so it can be compared directly with our results. Some differences are quite inessential:

- We first consider modular curves of arbitrary level N, and then specialize to N prime. On the other hand, Ballet and Zykin follow [29] and consider only level $11N$ (or $23N$). The curves produced in this way thus form a slightly less dense family.

- In passing from Proposition 8 to Corollary 10(i), we kept only the term proportional to k and we discarded the constant term. This gives a simpler expression, although slightly less precise. On the other hand, Ballet and Zykin kept track of this constant term.

- The strongest bounds in [24, Cor. 28] and in [6, Prop. 7] both are based on the estimate of Baker-Harman-Pintz [1]. Weaker but more explicit bounds are also proposed using alternative estimates. In particular Ballet and Zykin refer to Dudek's estimate [15], which did not exist at the time when [24] was written, but is now included for completeness as Corollary 10(vii), in §3.1 above. As explained there, any further progress on gaps between primes automatically translates into a bound on multiplication complexity.

All the details are essentially negligible. However there is another, much more important difference:

- Beside gaps between primes, a second ingredient in our work is our optimal solution to Riemann-Roch systems. Thanks to this, our uniform bounds match the best asymptotic bound (7). On the other hand, Ballet and Zykin use a suboptimal construction, which allow them only to match the weaker asymptotic bound (6), as they explicitly state in [6, Prop. 7(3)].

Because of this, all results in the first part of [6] are already covered by our stronger Corollary 10(i)-(vii). Only one very specific case of [6, Prop. 7] remains, namely the case $q = 25$.

On the other hand, the second part of [6] considers a base field of prime order. As discussed at the beginning of §3.4, our optimal method for solving Riemann-Roch systems does not work well for symmetric algorithms over prime fields. Instead, to prove [6, Prop. 10], Ballet and Zykin use a suboptimal method from [5], directly adapted from the original method of [12][13]. This is probably the best that could be done with the current state of knowledge, and [6, Prop. 10] is not covered at all by the present work.

Now it is interesting to compare the asymptotic bound they get this way for symmetric complexity [6, Prop. 10(3)]

$$\limsup_{k\to\infty} \frac{1}{k}\mu_p^{\mathrm{sym}}(k) \leq 3\left(1 + \frac{4/3}{p-3}\right) \tag{75}$$

with our Corollary 13 that holds for classical bilinear complexity. This suggests that, if one could solve the problem alluded to at the beginning of §3.4, this would lead to uniform bounds on the symmetric complexity matching the much

better, but still conjectural, asymptotic bound

$$\limsup_{k\to\infty} \frac{1}{k}\mu_p^{\mathrm{sym}}(k) \leq 3\left(1+\frac{1}{p-2}\right). \tag{76}$$

References

[1] R. C. Baker, G. Harman & J. Pintz, *The difference between consecutive primes, II*, Proc. London Math. Soc. **83** (2001) 532–562.

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

[3] S. Ballet, *Low increasing tower of algebraic function fields and bilinear complexity of multiplication in any extension of* $\mathbb{F}_q$, Finite Fields Appl. **9** (2003) 472–478.

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

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

[6] S. Ballet & A. Zykin, *Dense families of modular curves, prime numbers and uniform symmetric tensor rank of multiplication in certain finite fields*, preprint, June 2017 — `arxiv.org/abs/1706.09139`

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

[8] N. Bshouty, *A lower bound for the multiplication of polynomials modulo a polynomial*, Inform. Process. Letters **41** (1992) 321–326.

[9] I. Cascudo, *On asymptotically good strongly multiplicative linear secret sharing*, Ph.D. dissertation, University of Oviedo, 2010.

[10] I. Cascudo, R. Cramer & C. Xing, *Torsion limits and Riemann-Roch systems for function fields and applications*, IEEE Trans. Inform. Theory **60** (2014) 3871–3888.

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

[12] D. V. & G. V. Chudnovsky, *Algebraic complexities and algebraic curves over finite fields*, Proc. Nat. Acad. Sci. USA **84** (1987) 1739–1743.

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

[14] H. Cramer, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arith. **2** (1936) 23–46.

[15] A. Dudek, *An explicit result for primes between cubes*, Funct. Approx. Comment. Math. **55** (2016) 177–197.

[16] P. Dusart, *Estimates of some functions over primes without R.H.*, preprint, February 2010 — `arxiv.org/abs/1002.0442`

[17] K. Ford, *The Distribution of totients*, The Ramanujan J. **2** (1998) 67–151.

[18] H. Kadiri, *Short effective intervals containing primes in arithmetic progressions and the seven cubes problem*, Math. Comp. **77** (2008) 1733–1748.

[19] A. Lempel, G. Seroussi & S. Winograd, *On the complexity of multiplication in finite fields*, Theoret. Comput. Sci. **22** (1983) 285–296.

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

[21] T. Miyake, *Modular forms*, Springer-Verlag, 1989.

[22] O. Ramaré & Y. Saouter, *Short effective intervals containing primes*, J. Number Theory **98** (2003) 10–33.

[23] H. Randriambololona, $(2,1)$*-separating systems beyond the probabilistic bound*, Israel J. Math. **195** (2013) 171–186.

[24] H. Randriambololona, *Diviseurs de la forme* $2D - G$ *sans sections et rang de la multiplication dans les corps finis*, preprint, March 2011 — `arxiv.org/abs/1103.4335`

[25] H. Randriambololona, *Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method*, J. Complexity **28** (2012) 489–517.

[26] H. Randriambololona, "On products and powers of linear codes under componentwise multiplication", in: *Algorithmic arithmetic, geometry, and coding theory*, Contemp. Math. **637**, Amer. Math. Soc., 2015, pp. 3–78.

[27] L. Schoenfeld, *Sharper bounds for the Chebyshev functions* $\theta(x)$ *and* $\psi(x)$*, II*, Math. Comp. **30** (1976), 337–360.

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

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

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

[31] M. A. Tsfasman & S. G. Vladut, *Algebraic-geometric codes*, Kluwer Academic Publishers, 1991.

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