Dense families of modular curves, prime numbers and uniform symmetric tensor rank of multiplication in certain finite fields

Stéphane Ballet$^{1,2}$ · Alexey Zykin$^{3,4,5}$

Received: 24 November 2017 / Revised: 27 June 2018 / Accepted: 20 September 2018 / Published online: 1 October 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract
We obtain new uniform bounds for the symmetric tensor rank of multiplication in finite extensions of any finite field $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ where $p$ denotes a prime number $\geq 5$. In this aim, we use the symmetric Chudnovsky-type generalized algorithm applied on sufficiently dense families of modular curves defined over $\mathbb{F}_{p^2}$ attaining the Drinfeld–Vladuts bound and on the descent of these families to the definition field $\mathbb{F}_p$. These families are obtained thanks to prime number density theorems of type Hoheisel, in particular a result due to Dudek (Funct Approx Commentarii Math, 55(2):177–197, 2016).

Keywords
Algebraic function field · Tower of function fields · Tensor rank · Algorithm · Finite field · Modular curve · Shimura curve

Mathematics Subject Classification 14Q05 · 14Q20 · 11Y16 · 12Y05

1 Introduction

1.1 Notation

Let $\mathbb{F}_q$ be a finite field with $q$ elements where $q$ is a prime power and let $\mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-extension of degree $n$. The multiplication of two elements of $\mathbb{F}_{q^n}$ is an $\mathbb{F}_q$-bilinear map from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$.
onto $\mathbb{F}_{q^n}$. It can be considered as an $\mathbb{F}_q$-linear map from the tensor product $\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ onto $\mathbb{F}_{q^n}$. Consequently it can be also viewed as an element $T$ of $\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ where $\mathbb{F}_{q^n}^*$ denotes the dual of $\mathbb{F}_{q^n}$. More precisely, when $T$ is expressed as

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

where $x_i^* \in \mathbb{F}_{q^n}^*$, $y_i^* \in \mathbb{F}_{q^n}$ and $c_i \in \mathbb{F}_{q^n}$, the following holds for any $x, y \in \mathbb{F}_{q^n}$:

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

**Definition 1** The minimal number of summands in a decomposition of the multiplication tensor $T$ is called the tensor rank of the multiplication in the extension field $\mathbb{F}_{q^n}$ (or bilinear complexity of the multiplication) and is denoted by $\mu_q(n)$:

$$\mu_q(n) = \min \left\{ r \mid T = \sum_{i=1}^{r} x_i^* \otimes y_i^* \otimes c_i \right\}.$$

It is known that the tensor $T$ can have a symmetric decomposition:

$$T = \sum_{i=1}^{r} x_i^* \otimes x_i^* \otimes c_i.$$

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

$$\mu_{q}^{\text{sym}}(n) = \min \left\{ r \mid T = \sum_{i=1}^{r} x_i^* \otimes y_i^* \otimes c_i \right\}.$$

From an asymptotical point of view, let us define the following

$$M_{q}^{\text{sym}} = \limsup_{k \to \infty} \frac{\mu_{q}^{\text{sym}}(k)}{k},$$

$$m_{q}^{\text{sym}} = \liminf_{k \to \infty} \frac{\mu_{q}^{\text{sym}}(k)}{k}.$$

### 1.2 Known results

The original algorithm of D. V. and G. V. Chudnovsky introduced in [11] is symmetric by definition and leads to the following results from [3,7] and [9]:

**Theorem 3** Let $q$ be a prime power and let $n > 1$ be an integer. Let $F/\mathbb{F}_q$ be an algebraic function field of genus $g$ and $N_k$ be the number of places of degree $k$ in $F/\mathbb{F}_q$. Suppose $F/\mathbb{F}_q$ is such that $2g + 1 \leq q^{\frac{n+1}{2}}(q^{\frac{1}{2}} - 1)$ then:

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

$$\mu_{q}^{\text{sym}}(n) \leq 2n + g - 1.$$
(ii) if \( N_1 + 2N_2 > 2n + 2g - 2 \) and there exists a non-special divisor of degree \( g - 1 \), then

\[
\mu_{q}^{\text{sym}}(n) \leq 3n + 2g.
\]

**Theorem 4** Let \( q \) be a power of a prime \( p \) and let \( n \) be an integer. Then the symmetric tensor rank \( \mu_{q}^{\text{sym}}(n) \) is linear with respect to the extension degree; more precisely, there exists a constant \( C_q \) such that for any integer \( n > 1 \),

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

From different versions of symmetric algorithms of Chudnovsky type applied to good towers of algebraic function fields of type Garcia–Stichtenoth attaining the Drinfeld–Vladut bounds of order one, two or four, different authors have obtained uniform bounds for the tensor rank of multiplication, namely general expressions for \( C_q \), such as the following best currently published estimates:

**Theorem 5** Let \( q = p^r \) be a power of a prime \( p \) and let \( n \) be an integer \( > 1 \). Then:

(i) If \( q = 2 \), then \( \mu_{q}^{\text{sym}}(n) \leq 15.46n \) (cf. [6, Corollary 29] and [10])

(ii) If \( q = 3 \), then \( \mu_{q}^{\text{sym}}(n) \leq 7.732n \) (cf. [6, Corollary 29] and [10])

(iii) If \( q \geq 4 \), then \( \mu_{q}^{\text{sym}}(n) \leq 3 \left( 1 + \frac{4}{\pi}p \frac{q}{q - 3 + 2(p - 1) \frac{q}{q + 1}} \right) n \) (cf. [9])

(iv) If \( p \geq 5 \), then \( \mu_{p}^{\text{sym}}(n) \leq 3 \left( 1 + \frac{8}{3p - 5} \right) n \) (cf. [9])

(v) If \( q \geq 4 \), then \( \mu_{q^2}^{\text{sym}}(n) \leq 2 \left( 1 + \frac{p}{q - 3 + (p - 1) \frac{q}{q + 1}} \right) n \) (cf. [1] and [9])

(vi) If \( p \geq 5 \), then \( \mu_{p^2}^{\text{sym}}(n) \leq 2 \left( 1 + \frac{2}{p - \frac{1}{16}} \right) n \) (cf. [9])

### 1.3 New results

The main goal of the paper is to improve the upper bounds for \( \mu_{q}^{\text{sym}}(n) \) from the previous theorem for the assertions concerning the extensions of finite fields \( \mathbb{F}_{p^2} \) and \( \mathbb{F}_p \) where \( p \) is a prime number. One of main ideas used in this paper was introduced in [4] by the first author thanks to the use of the Chebyshev Theorem (or also called the Bertrand Postulate) to bound the gaps between prime numbers. More precisely, the aim was to construct families of modular curves \( \{ X_i \} \) with increasing genus \( g_i \) attaining the Drinfeld–Vladut bound as dense as possible. This means that these families of modular curves have the maximum possible ratio of the number of \( \mathbb{F}_{p^2} \)-rational points to the genus and such that the sequence of their genera is as dense as possible, namely \( \lim_{i \to \infty} \frac{g_i + 1}{g_i} = 1 \). Later, motivated by [4], the approach of using such bounds on gaps between prime numbers (e.g. Baker–Harman–Pintz) was also used in the preprint [13] in order to improve the upper bounds of \( \mu_{p^2}^{\text{sym}}(n) \) where \( p \) is a prime number. In our paper, we improve all the known uniform upper bounds for \( \mu_{p^2}^{\text{sym}}(n) \) and \( \mu_{p}^{\text{sym}}(n) \) for \( p \geq 5 \). This article is an expansion of a paper which was presented at The Tenth International Workshop on Coding and Cryptography (WCC17) [8].
2 New upper bounds

In this section, we give new better upper bounds for the symmetric tensor rank of multiplication in certain extensions of finite fields $\mathbb{F}_{p^2}$ and $\mathbb{F}_p$. In order to do that, we construct suitable families of modular curves defined over $\mathbb{F}_{p^2}$ and $\mathbb{F}_p$. In this aim, we need explicit prime number density theorems, usually called theorems of type Hoheisel. In particular, by a result of Baker et al. [2, Theorem 1] established in 2001 and by a recent result established by Dudek [12] in 2016, we directly deduce the following result:

**Theorem 6** 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 $\alpha = \frac{21}{40}$ with the value of $x_\alpha$ that can in principle be determined effectively, or $\alpha = \frac{2}{3}$ with $x_\alpha = \exp(\exp(33.217))$.

**Proof** It is known that there exists a real number $x_\alpha$ such that for all $x > x_\alpha$, the interval $[x - x^\alpha, x]$ with $\alpha = \frac{21}{40}$ contains prime numbers by a result of Baker, Harman and Pintz [2, Theorem 1]. In particular, if $l_k > x_\alpha$ denotes the $k$-th prime number, it means that the interval $[l_k, l_k + l_k^\alpha]$ contains the $k + 1$-th prime number $l_{k+1}$. Moreover, the value of $x_\alpha$ can in principle be determined, according to the authors. However, to our knowledge, this computation has not been realized yet.

For a bigger $\alpha = \frac{2}{3}$, Dudek obtained recently in [12, Theorem 1.1] an explicit bound $x_\alpha \geq \exp(\exp(33.217))$. More precisely, Dudek proves that there exists a prime between cubes, namely the interval $[n^3, (n + 1)^3]$ contains a prime number for sufficiently large numbers $n$. From this result, we can directly deduce that there exists a prime in the interval $[x, x + 3x^\frac{2}{3}]$ for all sufficiently large $x$. Moreover, he makes the result explicit, in that he determines numerically a lower bound for which this result is valid, namely for $x \geq \exp(\exp(33.217))$. Then, if we put $[x, x + 3x^\frac{2}{3}] = [x, x + x^\alpha]$, we deduce that $\alpha = \frac{2}{3} + \epsilon$ with $\epsilon < \frac{\ln 3}{\exp(\exp(33.217))}$ for any $x > \exp(\exp(33.217))$. \qed

2.1 The case of the quadratic extensions of prime fields

**Proposition 7** Let $p \geq 5$ be a prime number, and let $x_\alpha$ be the constant from Theorem 6.

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

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

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

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

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

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

\( \copyright \) Springer
(iii) Asymptotically the following inequality holds for any $p \geq 5$:

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

**Proof** First, let us consider the characteristic $p$ such that $p \neq 11$. Then it is known ([16, Corollary 4.1.21] and [15, proof of Theorem 3.9]) that the modular curve $X_k = X_0(11l_k)$, where $l_k$ is the $k$-th prime number, is of genus $g_k = l_k$ and satisfies

$$N_1(X_k(\mathbb{F}_{p^2})) \geq (p - 1)(g_k + 1),$$

where $N_1(X_k(\mathbb{F}_{p^2}))$ denotes the number of rational points over $\mathbb{F}_{p^2}$ of the curve $X_k$. Let us consider an integer $n > 1$. Then there exist two consecutive prime numbers $l_k$ and $l_{k+1}$ such that

$$(p - 1)(l_{k+1} + 1) > 2n + 2l_{k+1} - 2 \quad (5)$$

and

$$(p - 1)(l_k + 1) \leq 2n + 2l_k - 2 \quad (6)$$

(here we use the fact that $p \geq 5$). Let us consider the algebraic function field $F_{k+1}/\mathbb{F}_{p^2}$ associated to the curve $X_{k+1}$ of genus $l_{k+1}$ defined over $\mathbb{F}_{p^2}$. Denoting by $N_1(F_k/\mathbb{F}_{p^2})$ the number of places of degree $i$ of $F_k/\mathbb{F}_{p^2}$, we get

$$N_1(F_{k+1}/\mathbb{F}_{p^2}) \geq (p - 1)(l_{k+1} + 1) > 2n + 2l_{k+1} - 2.$$
in the notation of loc. cit. Let us take an integer \( n > 1 \). There exist two consecutive prime numbers \( l_k \) and \( l_{k+1} \) such that
\[
2(p - 1)(l_{k+1} + 1) > 2n + 2(2l_{k+1} + 1) - 2
\]
and
\[
2(p - 1)(l_k + 1) < 2n + 2(2l_k + 1) - 2,
\]
i.e.
\[
(p - 1)(l_k + 1) > n + 2l_k + 1
\tag{7}
\]
and
\[
(p - 1)(l_{k+1} + 1) < n + 2l_{k+1}.
\tag{8}
\]

Let us consider the algebraic function field \( F_{k+1}/\mathbb{F}_p^2 \) associated to the curve \( X_{k+1} \) of genus \( g_{k+1} = 2l_{k+1} + 1 \) defined over \( \mathbb{F}_p^2 \). We have
\[
N_1(F_{k+1}/\mathbb{F}_p^2) \geq 2(p - 1)(l_{k+1} + 1) > 2n + 4l_{k+1}.
\]

As before \( l_{k+1} \leq (1 + \epsilon(l_k))l_k \), with \( \epsilon(l_k) = l_k^{\alpha - 1} \). It is also easy to check that the inequality \( 2g + 1 \leq q^\frac{3n}{2} (q^\frac{1}{2} - 1) \) of Theorem 3 holds when \( q \) is a power of 11, which follows from the fact that
\[
11^{4l_k + \frac{9}{2}(11^{\frac{1}{2}} - 1)} \geq 8l_k + 3.
\]

Thus, for any integer \( n \geq (p - 3)x_{\alpha} + p - 1 \), the algebraic function field \( F_{k+1}/\mathbb{F}_p^2 \) satisfies Theorem 3, so
\[
\mu_{p^2}^{\text{sym}}(n) \leq 2n + 2l_{k+1} \leq 2n + 2(1 + \epsilon(l_k))l_k
\]
with \( l_k \leq n - \frac{p - 1}{p - 3} \) by (8).

We remark that as \( l_k \leq n - \frac{p - 1}{p - 3} \), \( \epsilon(l_k) \leq \epsilon_p(n) = (\frac{n}{p - 3})^{\alpha - 1} \), which gives the second inequality of the proposition.

Finally, when \( n \to +\infty \), the prime numbers \( l_k \to +\infty \), thus both for \( p \neq 11 \) and \( p = 11 \) the corresponding \( \epsilon_p(n) \to 0 \). So in the two cases we obtain
\[
M_{p^2}^{\text{sym}} \leq 2 \left( 1 + \frac{1}{p - 3} \right).
\]

\[ \Box \]

**Remark 8** It is easy to see that the bounds obtained in Proposition 7 are generally better than the best known bounds (v) and (vi) recalled in Theorem 5. Indeed, it is sufficient to consider the asymptotic bounds which are deduced from them and to see that for any prime \( p \geq 5 \) we have
\[
\frac{1}{p - 3} < \frac{p}{p - 3 + (p - 1)} \frac{1}{p - 7} \quad \text{and} \quad \frac{1}{p - 3} < \frac{2}{p - 16} \quad \text{respectively.}
\]

**Remark 9** Note that the bounds obtained in [13, Corollary 28] also concern the symmetric tensor rank of multiplication in the finite fields even if it is not mentioned. Indeed, the distinction between \( \mu_q^{\text{sym}}(n) \) and \( \mu_q(n) \) was exploited only from [14]. So, we can compare our Proposition 7 with Corollary 8 there. Firstly, note that the bounds in [13, Corollary 28] are only valid for \( p \geq 7 \). Moreover, the only bound which is better than our bounds is the asymptotic bound [13, Corollary 28, Bound (vi)] given for an unknown sufficiently large \( n \), contrary to our uniform bound with \( \alpha = \frac{2}{3} \) for \( n \geq \exp(\exp(33.217)) \).
2.2 The case of prime fields

**Proposition 10** Let \( p \geq 5 \) be a prime number, let \( x_\alpha \) be defined as in Theorem 6, and \( \epsilon_p(n) \) as in Proposition 7.

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

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

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

\[
\mu_p^{\text{sym}}(n) \leq 3 \left( 1 + \frac{\frac{4}{3}(1 + \epsilon_p(n))}{p - 3} \right) n - \frac{4(1 + \epsilon_p(n))(p - 1)}{p - 3} + 1.
\]

(iii) Asymptotically the following inequality holds for any \( p \geq 5 \):

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

**Proof** It suffices to consider the same families of curves as in the proof of Proposition 7.

When \( p \neq 11 \) we take \( X_k = X_0(11l_k) \), where \( l_k \) is the \( k \)-th prime number. These curves are defined over \( \mathbb{F}_p \), hence, we can consider the associated algebraic function fields \( F_k/\mathbb{F}_p \) defined over \( \mathbb{F}_p \) and we have \( N_1(F_k/\mathbb{F}_p^2) = N_1(F_k/\mathbb{F}_p) + 2N_2(F_k/\mathbb{F}_p) \geq (p - 1)(l_k + 1) \), since \( F_k/\mathbb{F}_p^2 = F_k/\mathbb{F}_p \otimes_{\mathbb{F}_p} \mathbb{F}_p^2 \) for any \( k \). Note that the genus of the algebraic function fields \( F_k/\mathbb{F}_p \) is also \( g_k = l_k \), since the genus is preserved under descent.

Given an integer \( n > 1 \), there exist two consecutive prime numbers \( l_k \) and \( l_{k+1} \) such that

\[
(p - 1)(l_{k+1} + 1) > 2n + 2l_{k+1} - 2
\]

and

\[
(p - 1)(l_k + 1) \leq 2n + 2l_k - 2.
\]

Let us consider the algebraic function field \( F_{k+1}/\mathbb{F}_p \) associated to the curve \( X_{k+1} \) of genus \( l_{k+1} \) defined over \( \mathbb{F}_p \). We get

\[
N_1(F_{k+1}/\mathbb{F}_p) + 2N_2(F_{k+1}/\mathbb{F}_p) \geq (p - 1)(l_{k+1} + 1) > 2n + 2l_{k+1} - 2.
\]

As before \( l_{k+1} \leq (1 + \epsilon(l_k))l_k \), with \( \epsilon(l_k) = l_k^{a-1} \), and from the proof of the previous proposition we know that the inequality \( 2g + 1 \leq q^{\frac{2}{2\alpha}} \left( q^{\frac{1}{2}} - 1 \right) \) of Theorem 3 holds. Consequently, for any integer \( n \geq \frac{p - 3}{2} x_\alpha + \frac{p + 1}{2} \), the algebraic function field \( F_{k+1}/\mathbb{F}_p \) satisfies Theorem 3, part ii) since by [5, Theorem 11 (i)] there always exists a non-special divisor of degree \( g_{k+1} - 1 \) for \( p \geq 5 \). So

\[
\mu_p^{\text{sym}}(n) \leq 3n + 2l_{k+1} \leq 3n + 2(1 + \epsilon(l_k))l_k
\]

with \( l_k \leq \frac{2n}{p-3} - \frac{p+1}{p-3} \) by (10). As before, \( \epsilon(l_k) \leq \epsilon_p(n) = \left( \frac{2n}{p-3} \right)^{a-1} \).

When \( p = 11 \) we use once again the family of curves \( X_k = X_0(23l_k) \). They are defined over \( \mathbb{F}_p \), hence we can consider the associated algebraic function fields \( F_k/\mathbb{F}_p \) over \( \mathbb{F}_p \) and we have \( N_1(F_k/\mathbb{F}_p^2) = N_1(F_k/\mathbb{F}_p) + 2N_2(F_k/\mathbb{F}_p) \geq 2(p - 1)(l_k + 1) \). The genus of the algebraic function fields \( F_k/\mathbb{F}_p \) defined over \( \mathbb{F}_p \) is also \( g_k = 2l_k + 1 \) since the genus is preserved under descent.
Given an integer \( n > 1 \), there exist two consecutive prime numbers \( l_k \) and \( l_{k+1} \) such that
\[
2(p - 1)(l_{k+1} + 1) > 2n + 2(2l_{k+1} + 1) - 2
\]
and
\[
2(p - 1)(l_k + 1) \leq 2n + 2(2l_k + 1) - 2,
\]
i.e.
\[
(p - 1)(l_{k+1} + 1) > n + 2l_{k+1} \tag{11}
\]
and
\[
(p - 1)(l_k + 1) \leq n + 2l_k. \tag{12}
\]

Let us consider the algebraic function field \( F_{k+1}/\mathbb{F}_p \) associated to the curve \( X_{k+1} \) of genus \( g_{k+1} = 2l_{k+1} + 1 \) defined over \( \mathbb{F}_p \). We get
\[
N_1(F_{k+1}/\mathbb{F}_p) + 2N_2(F_{k+1}/\mathbb{F}_p) \geq 2(p - 1)(l_{k+1} + 1) > 2n + 2(2l_{k+1} + 1) - 2.
\]

As above \( l_{k+1} \leq (1 + \epsilon(l_k))l_k \), with \( \epsilon(l_k) = l_k^{g_k} - 1 \), and the inequality \( 2g + 1 \leq q^{n-1}(q^2 - 1) \) of Theorem 3 holds. Consequently, for any integer \( n \geq (p - 3)x_0 + p - 1 \), the algebraic function field \( F_{k+1}/\mathbb{F}_p \) satisfies Theorem 3, part ii) since, as before, there exists a non-special divisor of degree \( g_{k+1} - 1 \) by [5, Theorem 11 (i)]. So,
\[
\mu_p^{\mathrm{sym}}(n) \leq 3n + 2g_{k+1} \leq 3n + 2(2l_{k+1} + 1) \leq 3n + 2(1 + \epsilon)l_k
\]
with \( l_k \leq \frac{n}{p-3} - \frac{p-1}{p-3} \) by (12). We can also bound \( \epsilon(l_k) \leq \epsilon_p(n) = \left(\frac{-n}{p-3}\right)^{\alpha-1} \).

Finally, when \( n \to +\infty \), the prime numbers \( l_k \to +\infty \), thus both for \( p \neq 11 \) and \( p = 11, \epsilon_p(n) \to 0 \). So we obtain \( M_p^{\mathrm{sym}} \leq 3 \left(1 + \frac{4}{p-3}\right) \). \( \square \)

**Remark 11** It is easy to see that the bounds obtained in Proposition 10 are generally better than the best known bounds (iii) and (iv) recalled in Theorem 5. Indeed, it is sufficient to consider the asymptotic bounds which are deduced from them and to see that for any prime \( p \geq 5 \) we have \( \frac{4}{p-3} < \frac{5p}{5p-11p+11p+1} \) and \( \frac{4}{p-3} < \frac{8}{5p-5} \) respectively.

**Acknowledgements** The first author wishes to thank Sary Drappeau, Olivier Ramaré, Hugues Randriambololona, Joël Rivat and Serge Vladuts for valuable discussions. The second author, tragically deceased in April 2017, was partially supported by ANR Globes ANR-12-JS01-0007-01 and by the Russian Academic Excellence Project ‘5-100’.

**References**

1. Arnaud N.: Évaluations dérivés, multiplication dans les corps finis et codes correcteurs. PhD thesis, Université de la Méditerranée, Institut de Mathématiques de Luminy (2006).
2. Baker R., Harman G., Pintz J.: The difference between consecutive primes, II. Proc. Lond. Math. Soc. **83**(3), 532–562 (2001).
3. Ballet S.: Curves with many points and multiplication complexity in any extension of \( \mathbb{F}_q \). Finite Fields Their Appl. **5**, 364–377 (1999).
4. Ballet S.: On the tensor rank of the multiplication in the finite fields. J. Number Theory **128**, 1795–1806 (2008).
5. Ballet S., Le Brigand D.: 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**, 293–310 (2006).
6. Ballet S., Pieltant J.: Tower of algebraic function fields with maximal Hasse–Witt invariant and tensor rank of multiplication in any extension of \( F_2 \) and \( F_3 \). J. Pure Appl. Algebra \textbf{222}(5), 1069–1086 (2018).
7. Ballet S., Rolland R.: Multiplication algorithm in a finite field and tensor rank of the multiplication. J. Algebra \textbf{272}(1), 173–185 (2004).
8. Ballet S., Zykin A.: Dense families of modular curves, prime numbers and uniform symmetric tensor rank of multiplication in certain finite fields. In: Proceedings of The Tenth International Workshop on Coding and Cryptography (2017). \url{http://wcc2017.suai.ru/proceedings.html}.
9. Ballet S., Pieltant J., Rambaud M., Sijsling J.: On some bounds for symmetric tensor rank of multiplication in finite fields. Contemp. Math. Am. Math. Soc. \textbf{686}, 93–121 (2017).
10. Cenk M., Özbudak F.: On multiplication in finite fields. J. Complex. \textbf{26}(2), 172–186 (2010).
11. Chudnovsky D., Chudnovsky G.: Algebraic complexities and algebraic curves over finite fields. J. Complex. \textbf{4}, 285–316 (1988).
12. Dudek A.: An explicit result for primes between cubes. Funct. Approx. Commentarii Math. \textbf{55}(2), 177–197 (2016).
13. Randriambololona H.: Divisors of the form \( 2d - g \) without sections and bilinear complexity of multiplication in finite fields. ArXiv e-prints (2011).
14. Randriambololona H.: Bilinear complexity of algebras and the Chudnovsky–Chudnovsky interpolation method. J. Complex. \textbf{28}(4), 489–517 (2012).
15. Shparlinski I., Tsfasman M., Vlăduț S.: Curves with many points and multiplication in finite fields. In: Stichtenoth H., Tsfasman M.A. (eds.) Coding Theory and Algebraic Geometry, vol. 1518, pp. 145–169. Lectures Notes in MathematicsSpringer, Berlin (1992).
16. Tsfasman M., Vlăduț S.: Algebraic-Geometric Codes. Kluwer Academic Publishers, Dordrecht (1991).

\textbf{Publisher’s Note} Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.