Journal of Complexity 26 (2010) 172–186

Contents lists available at ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

On multiplication in finite fields

Murat Cenk [a], Ferruh Özbudak [b,*]

[a] Department of Mathematics and Computer Science, Cankaya University, Balgat, Ankara, Turkey

[b] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

ARTICLE INFO

Article history:
Received 25 April 2009
Accepted 11 October 2009
Available online 26 November 2009

Keywords:
Finite fields
Algebraic function fields
Bilinear complexity

ABSTRACT

We present a method for multiplication in finite fields which gives multiplication algorithms with improved or best known bilinear complexities for certain finite fields. Our method generalizes some earlier methods and combines them with the recently introduced complexity notion $\widehat{M}_q(\ell)$, which denotes the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain the coefficients of the product of two arbitrary ℓ-term polynomials modulo x^ℓ in $\mathbb{F}_q[x]$. We study our method for the finite fields $\mathbb{F}_{q^n}$, where $2 \leq n \leq 18$ and $q = 2, 3, 4$ and we improve or reach the currently best known bilinear complexities. We also give some applications in cryptography.

1. Introduction

Let $\mathbb{F}_q$ be a finite field and $n > 1$ be an integer. Let $\mathbb{F}_{q^n}^{\perp}$ be the dual of $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. Then the rank $R(\mathbb{F}_{q^n}/\mathbb{F}_q)$ over $\mathbb{F}_q$ is defined to be

$$\min\left\{\ell \in \mathbb{N} \mid \exists u_i, v_i \in \mathbb{F}_{q^n}^{\perp}, w_i \in \mathbb{F}_{q^n} \text{ such that } \forall a, b \in \mathbb{F}_{q^n}, ab = \sum_{i=1}^{\ell} u_i(a)v_i(b)w_i\right\}.$$

$R(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is also denoted by $\mu_q(n)$ and it is called the *bilinear complexity of multiplication in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$. It corresponds to the minimum number of $\mathbb{F}_q$ bilinear multiplications in order to multiply two arbitrary elements of $\mathbb{F}_{q^n}$. Winograd [27] showed that this complexity is $\geq 2n - 1$, and it is equal to $2n - 1$ if and only if $n \leq \frac{1}{2}q + 1$. Algorithms obtaining the lower bound are based on interpolation algorithms on the rational function field [27]. D.V. Chudnovsky and G.V. Chudnovsky [14]

* Corresponding author.
E-mail addresses: mcenk@cankaya.edu.tr (M. Cenk), ozbudak@metu.edu.tr (F. Özbudak).

0885-064X/$ – see front matter © 2010 Published by Elsevier Inc.
doi:10.1016/j.jco.2009.11.002

generalized this idea to algebraic function fields (of one variable) over $\mathbb{F}_q$. Shokrollahi [22] obtained optimal algorithms for the multiplication in certain finite fields using the principle of D.V. and G.V. Chudnovsky algorithm and the elliptic curves. Shparlinski, Tsfasman and Vladut [23] gave the asymptotic bounds for multiplication in finite fields by using curves with many points. Ballet [2,3] generalized Shokrollahi's work to the algebraic function fields of genus g. Ballet and Rolland [4] gave a generalization of D.V. Chudnovsky and G.V. Chudnovsky multiplication algorithm by interpolating not only degree one places but also interpolating on degree two places. Moreover, Ballet, Rolland, Chaumine and Brigand in [4–7] have improved the asymptotic bounds given by Shparlinski, Tsfasman and Vladut in [23]. Arnaud [1] presented a method using local expansions with multiplicity 2 and places of degree one and two. In [8], new upper bounds of the bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are obtained by proving the existence of certain types of non-special divisors of degree $g-1$ in the algebraic function fields of genus g defined over $\mathbb{F}_q$. Moreover, concerning the use of places of degree greater than one, Ballet and Rolland use places of degree one, two and four to improve the asymptotic bilinear complexity of multiplication in the extensions of $\mathbb{F}_2$ in [10].

In this paper, we use algebraic function fields of one variable with places of arbitrary degrees and moreover we use some places not only once but also many times. Here many times refers to using first $u_i > 1$ coefficients instead of the first ($u_i = 1$) coefficient in the local expansion of a place P_i (see the map φ in Section 3). The proposed method is a generalization of the methods introduced in [14,23, 22,2–7,1,8,9]. In the papers cited above, mostly degree one places are used only. Among these papers, only [4–7,1,8,9] use places of degree greater than one. In these papers, [4–9] use only places of degree one and degree two but always with $u_i = 1$, i.e., using places only once. In [1], only places of degree one and degree two are used and all of such places are used at most 2 times.

In order to use places of arbitrary degree, one needs a measure to estimate the contribution of such places in the bilinear complexity. Here, we use the recently introduced complexity notion $\widehat{M}_q(\ell)$ for this purpose [12]. Recall that $\widehat{M}_q(\ell)$ is the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain coefficients of the product of two arbitrary ℓ-term polynomials modulo x^ℓ in $\mathbb{F}_q[x]$. We observe that in order to get the best linear complexities using our method, one needs to solve an optimization problem using $\widehat{M}_q(\ell)$ and curves with many points over finite fields. Here, curves with many points refer to curves with many degree one and higher degree points, where the complexity notion $\widehat{M}_q(\ell)$ indicates the weight of degree ℓ points of the curve in the optimization problem. Here, we would like to remark that local expansions and higher degree points of curves over finite fields have been shown to be very useful in algebraic geometry codes and low discrepancy sets and sequences (see, for example [28,29,19,20]). One of our motivations in this paper comes from these results in algebraic geometry codes and low discrepancy sets and sequences. We improve or reach the best known bilinear complexities in $\mathbb{F}_{q^n}$ where $2 \le n \le 18$ and $q = 2, 3, 4$ by searching and optimizing the suitable places and multiplicities in the proposed method. Moreover, our method gives explicit multiplication formulae immediately. We also give some applications to cryptography.

The rest of the paper is organized as follows: we introduce complexity notions and a brief review of algebraic function fields in Section 2. The proposed method is presented in Section 3. In Section 4, we obtain currently best known upper bounds for the bilinear complexity $\mu_q(n)$ of multiplication for $2 \le n \le 18$ and $q = 2, 3, 4$ which includes our some of improvements. Using the method of Section 3, we obtain some improvements. In Section 5, we give an example of computing multiplicative complexity of finite fields with large number of elements used in cryptography. The proposed method gives explicit formulae easily. We illustrate how to obtain explicit formulae reaching the upper bounds of Section 3 with an example in Section 6.

2. Preliminaries

2.1. Some complexity notions

The notation $\mu_q(n)$ represents the *bilinear complexity of multiplication in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$. It corresponds to the minimum number of $\mathbb{F}_q$ bilinear multiplications in order to multiply two arbitrary elements of $\mathbb{F}_{q^n}$. There is a related but different complexity notion. Let $M_q(n)$ denote the number of multiplications needed in $\mathbb{F}_q$ in order to multiply two arbitrary n-term polynomials in $\mathbb{F}_q[x]$ (cf. [13,15,16,25–27]). Here a polynomial is called an n-term polynomial in $\mathbb{F}_q[x]$ if it is of the form

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x].$$

As reduction modulo an irreducible polynomial in $\mathbb{F}_q[x]$ can be performed without multiplications in $\mathbb{F}_q$, we have

$$\mu_q(n) \le M_q(n). \tag{2.1}$$

However $\mu_q(n)$ and $M_q(n)$ are not necessarily equal in general. Using a polynomial basis $\{1, \xi, \xi^2, \ldots, \xi^{n-1}, \ldots, \xi^{2n-2}\}$ for $\mathbb{F}_{q^{2n-1}}$ over $\mathbb{F}_q$, it is easy to show that

$$M_q(n) \le \mu_q(2n-1).$$

We will need another complexity notion in this paper. For a positive integer ℓ, let $\widehat{M}_q(\ell)$ denote the multiplicative complexity of computing the coefficients of the product of two ℓ-term polynomials modulo x^ℓ over $\mathbb{F}_q$. In other words, $\widehat{M}_q(\ell)$ is the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain the first ℓ coefficients of the product of two arbitrary ℓ-term polynomials in $\mathbb{F}_q[x]$. It is not difficult to obtain useful upper bounds on $\widehat{M}_q(\ell)$ for certain values ℓ. For example we have $\widehat{M}_q(2) \le 3$, $\widehat{M}_q(3) \le 5$, $\widehat{M}_q(4) \le 8$ and $\widehat{M}_q(5) \le 11$ for any prime power q (cf. [13, Proposition 1]).

2.2. A brief review of algebraic function fields

We start with the basics of the algebraic function fields. The details in this subsection can be found in [24].

An algebraic function field $F/\mathbb{F}_q$ of one variable over $\mathbb{F}_q$ is an extension field $F \supseteq \mathbb{F}_q$ such that F is a finite extension of $\mathbb{F}_q(x)$ for some element $x \in F$ which is transcendental over $\mathbb{F}_q$. A valuation ring of the function field $F/\mathbb{F}_q$ is a ring $\mathcal{O} \subseteq F$ with the properties $\mathbb{F}_q \subset \mathcal{O} \subset F$ and for any $z \in F$, either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$. A place of P of the function field $F/\mathbb{F}_q$ is the maximal ideal of some valuation ring $\mathcal{O}$ of $F/\mathbb{F}_q$. We will denote the set of all places of $F/\mathbb{F}_q$ as $\mathbb{P}_F$. If $\mathcal{O}$ is a valuation ring of $F/\mathbb{F}_q$ and P is its maximal ideal, then $\mathcal{O}$ is uniquely determined by P hence we denote $\mathcal{O}$ by $\mathcal{O}_P$.

$F_P := \mathcal{O}_P/P$ is called the residue class field of P. The map $x \to x(P)$ from F to $F_P \cup \{\infty\}$ is called the residue class map with respect to P. Degree of P is $[F_P : \mathbb{F}_q] := \deg P$.

The free abelian group which is generated by the places of $F/\mathbb{F}_q$ is called the divisor group of $F/\mathbb{F}_q$ and it is denoted by $\mathcal{D}_F$. A divisor is a formal sum $D = \sum_{P \in \mathbb{P}_F} n_P P$ with $n_P \in \mathbb{Z}$, almost all $n_P = 0$. The support of D is defined by $\operatorname{supp} D := \{\mathbb{P} \in \mathbb{P}_F | n_P \neq 0\}$. A divisor of the form $D = P$ with $P \in \mathbb{P}_F$ is called a prime divisor. Two divisor $D = \sum n_P P$ and $D' = \sum n'_P P$ are added coefficientwise. For $Q \in \mathbb{P}_F$ and $D = \sum n_P P \in \mathcal{D}_F$ we define $v_Q(D) = n_Q$. A partial ordering on $\mathcal{D}_F$ is defined by

$$D_1 \le D_2 \Longleftrightarrow v_P(D_1) \le v_P(D_2)$$

for any $P \in \mathbb{P}_F$. A divisor $D \ge 0$ is called positive. The degree of a divisor is defined by

$$\deg D := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \deg P$$

and $\deg : \mathcal{D} \to \mathbb{Z}$ is a group homomorphism.

Let $0 \neq x \in F$ and Z (respectively N) be the set of zeros (poles) of x in $\mathbb{P}_F$. Then $(x)_0 := \sum_{P \in Z} v_P(x)P$ is called the zero divisor of x, $(x)_\infty := \sum_{P \in N}(-v_P(x))P$ is called the pole divisor of x and $(x) := (x)_0 - (x)_\infty$ is called the principal divisor of x.

The set $\mathcal{P}_F := \{(x) | 0 \neq x \in F\}$ is defined as the group of principal divisors of $F/\mathbb{F}_q$. The factor group

$$\mathcal{C} := \mathcal{D}_F/\mathcal{P}_F$$

is called the divisor class group. The divisor class of D, denoted by $[D]$, is the corresponding element in the factor group $\mathcal{C}_F$. For $D_1, D_2 \in \mathcal{D}_F$, we denote $D_1 \sim D_2$ if $[D_1] = [D_2]$.

For a divisor $A \in \mathcal{D}_F$ we set

$$\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{\infty\}.$$

$\mathcal{L}(A)$ is a vector space over $\mathbb{F}_q$. If A' is a divisor equivalent to A then $\mathcal{L}(A) \cong \mathcal{L}(A')$. For $A \in \mathcal{D}_F$, the integer $\dim A := \dim \mathcal{L}(A)$ is called the dimension of the divisor A. The genus of $F/\mathbb{F}_q$ is defined by

$$g := \max\{\deg A - \dim A + 1 \mid A \in \mathcal{D}_F\}.$$

For $A \in \mathcal{D}_F$,

$$i(A) := \dim A - \deg A + g - 1$$

is called the index of speciality of A. Any divisor $A \in \mathcal{D}_F$ is called non-special if $i(A) = 0$; otherwise A is called special.

3. The method

Let $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$. Let $P_1, \ldots, P_N$ be distinct places of arbitrary degrees. Assume that Q is a place of degree n. Let $\mathcal{O}_Q$ be the valuation ring of the place Q. Note that the residue field $\mathcal{O}_Q/Q$ is isomorphic to $\mathbb{F}_{q^n}$. Let D be a divisor such that $\operatorname{supp} D \cap \{Q, P_1, P_2, \ldots, P_N\} = \emptyset$. Let $\mathcal{L}(D)$ be the Riemann–Roch space of D. Assume also that the evaluation map Ev_Q from $\mathcal{L}(D)$ to the residue field $\mathcal{O}_Q/Q$ is onto. For $1 \leq i \leq N$, let t_i be a local parameter at P_i. For $f \in \mathcal{L}(2D)$, let

$$f = \alpha_{i,0} + \alpha_{i,1} t_i + \alpha_{i,2} t_i^2 + \cdots$$

be the local expansion at P_i with respect to t_i, where $\alpha_{i,0}, \alpha_{i,1}, \ldots \in \mathbb{F}_{q^{\deg(P_i)}}$. Let u_i be a positive integer and consider the $\mathbb{F}_q$-linear map

$$\begin{aligned} \varphi_i : \mathcal{L}(2D) &\rightarrow \left(\mathbb{F}_{q^{\deg(P_i)}}\right)^{u_i} \\ f &\rightarrow \left(\alpha_{i,0}, \alpha_{i,1}, \ldots, \alpha_{i,u_i-1}\right). \end{aligned}$$

Let φ be the $\mathbb{F}_q$-linear map given by

$$\begin{aligned} \varphi : \mathcal{L}(2D) &\rightarrow \left(\mathbb{F}_{q^{\deg(P_1)}}\right)^{u_1} \times \left(\mathbb{F}_{q^{\deg(P_2)}}\right)^{u_2} \times \cdots \times \left(\mathbb{F}_{q^{\deg(P_N)}}\right)^{u_N} \\ f &\rightarrow (\varphi_1(f), \varphi_2(f), \ldots, \varphi_N(f)). \end{aligned} \tag{3.1}$$

Finally we assume that the map φ is injective.

Theorem 3.1. *Under the notation and assumptions as above we have*

$$\mu_q(n) \leq \sum_{i=1}^{N} \mu_q(\deg(P_i)) \widehat{M}_{q^{\deg(P_i)}}(u_i). \tag{3.2}$$

Proof. Let $\{h_\ell : 1 \leq \ell \leq n\}$ be a fixed basis of $\mathcal{L}(D)$ over $\mathbb{F}_q$. Moreover we choose and fix $h'_1, \ldots, h'_m$ such that $\{h_\ell : 1 \leq \ell \leq n\} \cup \{h'_k : 1 \leq k \leq m\}$ is a basis of $\mathcal{L}(2D)$. We consider $\mathrm{Ev}_Q(h_1), \ldots, \mathrm{Ev}_Q(h_n)$, $\mathrm{Ev}_Q(h'_1), \ldots, \mathrm{Ev}_Q(h'_m) \in \mathcal{O}_Q/Q \cong \mathbb{F}_{q^n}$ as constants since $h_1, \ldots, h_n, h'_1, \ldots, h'_m$ are fixed. Similarly, we consider $\varphi(h_1), \ldots, \varphi(h_n), \varphi(h'_1), \ldots, \varphi(h'_m) \in \left(\mathbb{F}_{q^{\deg(P_1)}}\right)^{u_1} \times \cdots \times \left(\mathbb{F}_{q^{\deg(P_N)}}\right)^{u_N}$ as constants. For $f \in \mathcal{L}(2D)$, there is no cost for bilinear complexity in obtaining $\varphi(f)$. Indeed, as

$$f = \sum_{\ell=1}^{n} c_\ell h_\ell + \sum_{k=1}^{m} d_k h'_k$$

with $c_1 \ldots, c_n, d_1, \ldots, d_m \in \mathbb{F}_q$, we obtain $\varphi(f)$ using only multiplications with constants $\varphi(h_1), \ldots, \varphi(h_n), \varphi(h'_1), \ldots, \varphi(h'_m)$ and additions as in

$$\varphi(f) = c_1\varphi(h_1) + \cdots + c_n\varphi(h_n) + d_1\varphi(h'_1) + \cdots + d_m\varphi(h'_m).$$

Similarly for $f \in \mathcal{L}(2D)$, there is no cost for bilinear complexity in obtaining $\mathrm{Ev}_Q(f)$. Note that the evaluation map from $\mathcal{L}(2D)$ to $\mathrm{Ev}_Q(f)$ is surjective but not necessarily injective.

We identify $\mathcal{L}(D)$ with $\mathcal{O}_Q/Q \cong \mathbb{F}_{q^n}$ without any cost on bilinear complexity. For given $\alpha, \beta \in \mathbb{F}_{q^n} \cong \mathcal{O}_Q/Q$, let f_1, f_2 be corresponding functions in $\mathcal{L}(D)$. We obtain the coefficients $a_1, \ldots, a_n$, $b_1, \ldots, b_m$ such that

$$f_1 = a_1h_1 + \cdots + a_nh_n, \qquad f_2 = b_1h_1 + \cdots + b_nh_n \tag{3.3}$$

without any cost in bilinear complexity.

Note that $f_1f_2 \in \mathcal{L}(2D)$. The only cost on bilinear complexity stems from obtaining the coefficients $c_1, \ldots, c_n, d_1, \ldots, d_m \in \mathbb{F}_q$, where

$$f_1f_2 = \sum_{\ell=1}^{n} c_\ell h_\ell + \sum_{k=1}^{m} d_k h'_k$$

using the coefficients $a_1, \ldots, a_n, b_1, \ldots, b_n$ given in (3.3). Indeed the product $\alpha\beta \in \mathbb{F}_{q^n}$ is obtained using $\mathrm{Ev}_Q(f_1f_2)$ without any extra cost in bilinear complexity provided that the coefficients $c_1, \ldots, c_n, \ldots, d_m \in \mathbb{F}_q$ are known.

Using our arguments above, we obtain the coefficients $c_1, \ldots, c_n, d_1, \ldots, d_m \in \mathbb{F}_q$ from

$$\varphi(f_1f_2) = (\varphi_1(f_1f_2), \varphi_2(f_1f_2), \ldots, \varphi_N(f_1f_2)).$$

We will complete the proof by showing that the cost of obtaining $\varphi_i(f_1f_2)$ using the coefficients $a_1, \ldots, a_n, b_1, \ldots, b_n$ is at most

$$\mu_q(\deg(P_i))\widehat{M}_{q^{\deg(P_i)}}(u_i)$$

for each $1 \le i \le N$.

Let $1 \le i \le N$ be an integer and

$$\varphi_i(f_1) = (\alpha_{i,0}, \alpha_{i,1}, \ldots, \alpha_{i,u_i-1}), \qquad \varphi_i(f_2) = (\beta_{i,0}, \beta_{i,1}, \ldots, \beta_{i,u_i-1}).$$

Note that the coordinates $\alpha_{i,0}, \ldots, \alpha_{i,u_i-1}, \beta_{i,0}, \ldots, \beta_{i,u_i-1} \in \mathbb{F}_{q^{\deg(P_i)}}$ and they are obtained using the coefficients $a_1, \ldots, a_n, b_1, \ldots, b_n$ and the constants $\varphi_i(h_1), \ldots, \varphi_i(h_n)$ without any cost.

For a transcendental x over $\mathbb{F}_{q^{\deg(P_i)}}$, we consider the polynomial ring $\mathbb{F}_{q^{\deg(P_i)}}[x]$. Let $p_1^{(i)}(x), p_2^{(i)}(x) \in \mathbb{F}_{q^{\deg(P_i)}}[x]$ be polynomials given by

$$\begin{aligned} p_1^{(i)}(x) &= \alpha_{i,0} + \alpha_{i,1}x + \cdots + \alpha_{i,u_i-1}x^{u_i-1}, \\ p_2^{(i)}(x) &= \beta_{i,0} + \beta_{i,1}x + \cdots + \beta_{i,u_i-1}x^{u_i-1}. \end{aligned}$$

Let $p^{(i)}(x) = p_1^{(i)}(x)p_2^{(i)}(x)$ and $\gamma_0^i, \gamma_1^i, \ldots, \gamma_{u_i-1}^i \in \mathbb{F}_{q^{\deg(P_i)}}$ be the first u_i terms of $p(x)$. Namely, let $\gamma_0^i, \gamma_1^i, \ldots, \gamma_{u_i-1}^i \in \mathbb{F}_{q^{\deg(P_i)}}$ such that

$$p^{(i)}(x) \equiv \gamma_0^i + \gamma_1^i x + \cdots + \gamma_{u_i-1}^i x^{u_i-1} \bmod x^{u_i} \in \mathbb{F}_{q^{\deg(P_i)}}[x].$$

It is clear that

$$\varphi_i(f_1f_2) = (\gamma_0^i, \gamma_1^i, \ldots \gamma_{u_i-1}^i).$$

The cost of obtaining the first u_i terms $\gamma_0^i, \gamma_1^i, \ldots \gamma_{u_i-1}^i$ of the polynomial $p^{(i)}(x)$ using the polynomials $p_1^{(i)}(x), p_2^{(i)}(x)$ is at most

$$\mu_q(\deg(P_i))\widehat{M}_{q^{\deg(P_i)}}(u_i).$$

This completes the proof. □

Using Theorem 3.1 we obtain explicit algorithms for multiplications in $\mathbb{F}_{q^n}$. The conditions of the following theorem guarantee that the assumptions of Theorem 3.1 are satisfied.

Theorem 3.2. *Let $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$. Let g be the genus of F. Let $P_1, P_2, \dots, P_N$ be distinct places of arbitrary degrees of F. Let $u_1, u_2, \dots, u_N$ be arbitrary positive integers. Assume that*

(1) *there exists a non-special divisor of degree $g-1$,*
(2) *there exists a place of degree n,*
(3) $\sum_{i=1}^{N} \deg(P_i)u_i > 2n + 2g - 2$.

Then assumptions in Theorem 3.1 hold and we have

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

Proof. Let G be a non-special divisor of degree $g-1$. Let Q be a place of degree n. Let D_1 be the effective divisor given by $D_1 = G+Q$. As $D_1 \ge G$, we have that D_1 is non-special again (cf. Remark I.6.9, item (f) [24]). Hence

$$\dim \mathcal{L}(D_1) = \deg(D_1) + 1 - g = (n + g - 1) + 1 - g = n.$$

Using Strong Approximation Theorem (cf. Theorem I.6.4 [24]) we obtain a divisor D of F such that

$$D \sim D_1 \quad \text{and} \quad \operatorname{supp} D \cap \{Q, P_1, P_2, \dots, P_N\} = \emptyset.$$

Hence D is non-special (cf. Remark 1.6.9, item (c)) and the map Ev_Q from $\mathcal{L}(D)$ to the residue field $\mathcal{O}_Q/Q$ is onto. Let φ be the $\mathbb{F}_q$-linear map from $\mathcal{L}(2D)$ to $\left(\mathbb{F}_{q^{\deg(P_1)}}\right)^{u_1} \times \left(\mathbb{F}_{q^{\deg(P_2)}}\right)^{u_2} \times \cdots \times \left(\mathbb{F}_{q^{\deg(P_N)}}\right)^{u_N}$ given by (3.1). It remains to prove that φ is injective. But the kernel of φ is $\mathcal{L}(2D - \sum u_iP_i)$ and as the degree of the divisor $2D - \sum u_iP_i < 0$ by the assumption (3), the kernel is $\{0\}$. So φ is injective. □

Remark 3.3. Under the notation and assumptions of Theorem 3.2, consider the subcase that $N = N_1 + N_2$, P_i is a degree one place for $1 \le i \le N_1$ and P_i is a degree two place for $N_1 + 1 \le i \le N_1 + N_2$. Moreover let $u_i = 1$ for $1 \le i \le N_1+N_2$. Note that $\mu_q(1) = 1$, $\mu_q(2) = 3$ (cf. [27]), and $\widehat{M}_{q^{\deg(P_i)}}(1) = 1$ for any $\deg(P_i)$. Therefore the condition (3) of Theorem 3.2 becomes

$$N_1 + 2N_2 > 2n + 2g - 2,$$

and the bound of Theorem 3.2 on $\mu_q(n)$ becomes

$$\mu_q(n) \le N_1 + 3N_2.$$

These coincide with the corresponding result of Ballet and Rolland in [4].

Remark 3.4. By Theorem 3.2, in order to obtain better upper bounds on $\mu_q(n)$, we need algebraic function fields with full constant field $\mathbb{F}_q$, with small genus g, and with enough number of rational places of suitable degrees. It is well known that finding algebraic function fields over $\mathbb{F}_q$ with fixed small genus g and many rational places is not easy (cf. [18, Chapter 4]). In Theorem 3.2, as $\deg(P_i)$ and u_i are further parameters to be chosen, the condition (3) is weaker than the corresponding condition in [4, Theorem 2.2].

Using $u = 2$ for degree one places and $u = 1$ for degree two places in Theorem 3.2, we obtain the following corollary.

Corollary 3.5. *Let $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$. Let g be the genus of F. Assume there exist at least N_1 degree one and at least N_2 degree two places of F. If*

(1) *there exists a non-special divisor of degree $g-1$,*
(2) *there exists a place of degree n,*
(3) $2N_1 + 2N_2 > 2n + 2g - 2$,

then we have

$$\mu_q(n) \le 3n + \frac{3g}{2}.$$

Proof. We use N_1 degree one places with $u = 2$ and N_2 degree two places with $u = 1$. Since we have $2N_1 + 2N_2 > 2n + 2g - 2$, then φ is injective with rank $2n + g - 1$. Therefore we can choose N_1' degree one places from degree one places and N_2' degree two places from degree two places such that $2n + g - 1 \le 2N_1' + 2N_2' \le 2n + g$. Then we get

$$\mu_q(n) \le 3N_1' + 3N_2' \le 3\left(n + \frac{g}{2}\right) = 3n + \frac{3g}{2}. \quad \square$$

We compare Corollary 3.5 with the corresponding results in [4]. The bound of Corollary 3.5 is at least as good as the bounds of [4, Theorem 2.2] and [7, Theorem 2.1]. The condition (3) of Corollary 3.5 is weaker as the corresponding condition of [4] and [7] is $N_1 + 2N_2 > 2n + 2g - 2$. The other conditions of Corollary 3.5 are the same as the ones in [4]. Therefore Corollary 3.5 gives improved bounds on $\mu_q(n)$ compared to the ones in [4].

For some explicit algebraic function fields, the map φ in (3.1) becomes injective for suitable choices of the places $P_1, \ldots, P_N$ and the divisor D even $\sum_{i=1}^{N} \deg(P_i)u_i = 2n + g - 1$ holds. We state such a result in the following theorem.

Theorem 3.6. *Let $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$. Let g be genus of F. Let $P_1, \ldots, P_N$ be distinct places of arbitrary degrees of F. Let $u_1, u_2, \ldots, u_N$ be arbitrary integers. Assume that*

(1) *there exists a non-special divisor D of degree $n + g - 1$,*
(2) *there exists a place of degree n,*
(3) $\sum_{i=1}^{N} \deg(P_i)u_i = 2n + g - 1$.

Let φ be the $\mathbb{F}_q$-linear map from $\mathcal{L}(2D)$ to $\left(\mathbb{F}_{q^{\deg(P_1)}}\right)^{u_1} \times \cdots \times \left(\mathbb{F}_{q^{\deg(P_N)}}\right)^{u_N}$ given in (3.1). If φ is injective then

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

Proof. As D is non-special, $\dim(\mathcal{L}(D)) = \deg D + 1 - g = n$. Moreover supp $(D) \cup \{Q\} = \emptyset$ and hence the evaluation map Ev_Q from $\mathcal{L}(D)$ to $\mathcal{O}_Q/Q$ is bijective. Note that supp $(D) \cup \{P_1, \ldots, P_N\} = \emptyset$ as well. The result follows from Theorem 3.1. $\square$

Remark 3.7. It is enough to assume D is a non-special divisor of degree $n + g - 1$. Using Strong Approximation Theorem (cf. Theorem I.6.4 [24]), we can always obtain D' from such D with $D' \sim D$ and $\operatorname{supp} D' \cap \{Q, P_1, P_2, \ldots, P_N\} = \emptyset$.

Remark 3.8. In the case of places only of degree one and two and with $u = 1$, the conditions of Theorem 3.6 are exactly equivalent to the conditions of Theorem 2.2 in [7]. Moreover, The same bound was given in [4] under certain conditions on q and n only for degree one and degree two places with $u = 1$. The conditions on q and n in [4] seem to come from the choice of a non-special divisor D with extra conditions. In our case the extra conditions refer to the injectivity of the map φ, even when $\sum_{i=1}^{N} \deg(P_i)u_i = 2n + g - 1$. We give explicit examples of algebraic function fields satisfying this criteria in our improvements.

The following example shows that Theorem 3.1 gives an improved bound for $\mathbb{F}_{3^9}$.

Example 3.9. Let $q = 3$ and $n = 9$. Using the results in the literature, to the best of our knowledge, the best upper bound is $\mu_3(9) \leq 27$, which can be derived by two alternative methods as follows. Using [13,16,26], we obtain the upper bounds on $M_3(9)$ as 36, 34 and 27, respectively. Hence by [13] and (2.1) we get $\mu_3(9) \leq 27$. For the method in [4], we have considered all algebraic function fields of genus 0 and 1. Let E be elliptic curve $y^2 = x^3 + x + 2$ over $\mathbb{F}_3$. It has 4 degree one places, 6 degree two places and 8 degree three places. As $4+2\cdot 6 < 2\cdot 9+1-1$, the method of [4] cannot be applied directly. Using 3 degree one places, 6 degree two places, and 1 degree three places, all with $u = 1$ as in [4], we obtain that $\mu_3(9) \leq 3\cdot 1+6\cdot 3+6\cdot 1 = 27$. Now we improve this to $\mu_3(9) \leq 26$ using Theorem 3.6 together with $u = 2$ for some places. We take 2 degree one places with $u = 2$, 2 degree one places with $u = 1$, and 6 degree two places with $u = 1$. Therefore we obtain that $\mu_3(9) \leq 2\cdot 3+2\cdot 1+6\cdot 3 = 26$. We find an explicit formula of such an algorithm via Theorem 3.6, which can be found in Appendix. The description and details of finding explicit formula for $\mu_3(9) \leq 26$ are given in Section 6.

4. Multiplication in finite fields $\mathbb{F}_{q^n}$ for $2 \leq n \leq 18$ and $q = 2, 3, 4$

In this section, for $2 \leq n \leq 18$ and $q = 2, 3, 4$, we obtain the best known (upper) bounds on $\mu_q(n)$ using the various methods in the literature and the proposed method in this paper. In particular, we indicate some improvements obtained using the proposed method on certain values of $\mu_q(n)$.

To the best of our knowledge, for this range of values of q and n, the best known (upper) bounds on $\mu_q(n)$ are obtained using the following methods:

(i) The methods based on the idea of D.V. Chudnovsky and G.V. Chudnovsky [14], which are presented in the [2–4,7].

(ii) The observation in (2.1) together with results presented in [12,13,15,16,26,27].

(iii) A well known method when n is a composite number which is as follows: Let $k, \ell \geq 2$ be positive integers with $n = k\cdot\ell$. As $\mathbb{F}_{q^\ell}$ is a subfield of $\mathbb{F}_{q^n}$, it immediately follows from the definitions of $\mu_q(n)$, $\mu_{q^\ell}(k)$ and $\mu_q(\ell)$ that

$$\mu_q(n) \leq \mu_{q^\ell}(k)\cdot\mu_q(\ell). \tag{4.1}$$

(iv) The proposed method.

Now we give some of the improvements that are obtained by using the proposed method explicitly. We start with multiplication in $\mathbb{F}_{3^n}$. For the cases $n = 9, 11, 13, 15, 17, 18$, we improve the best known bounds given in [13,16]. Throughout the paper we use the notation of Magma [11] for presenting the places and the divisor of algebraic function fields.

In Example 3.9, it is already explained how to obtain $\mu_3(9) \leq 26$. For the other improvements in characteristic three in this section, we again use the same elliptic curve E given in Example 3.9. Recall that E has 4 degree one places, 6 degree two places and 8 degree three places. For each choice of the paces and the divisors given below, it is easy to verify, for example using Magma as in Section 6, that the corresponding map φ in (3.1) is injective and hence the proposed method applies.

In order to show that $\mu_3(11) \leq 34$, it is enough to take 2 degree one places with $u = 2$, 2 degree one places with $u = 3$ and 6 degree two places with $u = 1$ with the choice of $D = (x^{11}+2x^9+x^7+x^6+x^4+x^3+2x^2+x+1, y+x^{10}+2x^7+2x^5+2x^4+2x^3+x+2)$.

In order to obtain $\mu_3(13) \leq 42$, we use 4 degree one places with $u = 2$, 6 degree two places with $u = 1$ and 2 degree three places with $u = 1$ with the choice of $D = (x^{13}+2x^{12}+x^{11}+2x^{10}+x^9+x^8+x^7+2x^4+2x^3+1, y+x^{12}+x^{11}+2x^{10}+2x^9+x^7+x^5+2x^4+2x^3)$.

On the other hand, taking 4 degree one places with $u = 3$, 6 degree two places with $u = 1$ and 2 degree three places with $u = 1$ gives $\mu_3(15) \leq 50$ where D can be selected as $(x^{15}+2x^{13}+2x^{12}+2x^{11}+x^{10}+x^8+x^5+2x+2, y+2x^{13}+x^{12}+x^{11}+2x^{10}+x^9+2x^5+x^4+x^3+2x^2+2x)$.

When we choose $D = (x^{17}+2x^{16}+2x^{15}+x^{13}+x^10+2x^9+x^8+x^7+2x^6+2x^5+2x^2+x+1, y+2x^{15}+x^{14}+2x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^2+2)$, another improved bound $\mu_3(17) \leq 58$ is obtained by using 2 degree one places with $u = 2$, 2 degree one places with $u = 3$, 6 degree two places with $u = 1$ and 4 degree three places with $u = 1$.

Finally, $\mu_3(18) \le 62$ is obtained by taking 3 degree one places with $u = 2$, 1 degree one places with $u = 3$, 6 degree two places with $u = 1$ and 5 degree three places with $u = 1$ where one can use $D = (x^{18}+2x^{17}+2x^{16}+x^{15}+x^{11}+2x^{10}+x^4+2x+2, y+2x^{17}+x^{14}+x^{13}+2x^{12}+2x^8+x^6+2x^5+x^4)$.

Next we show that the proposed method improves or reach the currently best known bilinear complexities in $\mathbb{F}_{4^n}$ for $n = 11$, 13 and 17. In order to show that $\mu_4(11) \le 30$, $\mu_4(13) \le 37$ and $\mu_4(17) \le 53$ we use the proposed method as follows. Let $\mathbb{F}_4 = \{0, 1, w, w+1\}$ where w is a root of $x^2 + x + 1 \in \mathbb{F}_2[x]$. Let

$$E_1 : y^2 + wy = x^3 + x^2 + wx + 1,$$
$$E_2 : y^2 + w^2xy + wy = x^3 + wx + w^2,$$
$$E_3 : y^2 + y = x^3 + x^2 + w^2x + w$$

be elliptic curves over $\mathbb{F}_4$. E_1 has 7 degree one places, 7 degree two places and 14 degree three places. E_2 has 6 degree one places, 9 degree two places and 16 degree three places. Finally, E_3 has 5 degree one places, 10 degree two places and 20 degree three places.

The bound $\mu_4(11) \le 30$ can be obtained using the proposed method together with E_1. When we use 1 degree one place with $u = 2$, 6 degree one places with $u = 1$ and 7 degree two places with $u = 1$, we get $\mu_4(11) \le 30$. Note that the same bound is also obtained by the method of [4]. If we use E_2 then we obtain $\mu_4(11) \le 30$ by using 6 degree one places and 8 degree two places.

The improved bound $\mu_4(13) \le 37$ can be obtained by using E_2. Let $\{P_1, \dots, P_6, Q_1, \dots, Q_9\}$ be a set of places where P_i 's are of degree one and Q_i's are of degree two. Those are

$$P_1 = \infty, \quad P_2 = (x, y+1), \quad P_3 = (x, y+x+w^2), \quad P_4 = (x+w^2, y+w),$$
$$P_5 = (x+1, y), \quad P_6 = (x+1, y+x), \quad Q_1 = (x+w), \quad Q_2 = (x^2+x+w^2, y),$$
$$Q_3 = (x^2+x+w^2, y+w^2x+w), \quad Q_4 = (x^2+w^2x+1, y+w),$$
$$Q_5 = (x^2+w^2x+1, y+w^2x), \quad Q_6 = (x^2+w^2x+w^2, y+x),$$
$$Q_7 = (x^2+w^2x+w^2, y+wx+w), \quad Q_8 = (x^2+wx+w, y+x+w^2),$$
$$Q_9 = (x^2+wx+w, y+wx+1).$$

When we use 2 degree one places, P_1, P_2, with $u = 2$, 4 degree one places, $P_3, \dots, P_6$ with $u = 1$ and 9 degree two places, $Q_1, \dots, Q_9$ with $u = 1$, we obtain $\mu_4(13) \le 37$ where one can use $D = (x^{13} + w^2x^{12} + x^{11} + x^{10} + wx^9 + x^8 + wx^7 + wx^4 + x^2 + x + w, y + wx^{12} + x^{11} + w^2x^{10} + w^2x^9 + w^2x^8 + wx^7 + w^2x^6 + wx^5 + w^2x^4 + x^3 + x^2 + x + w^2)$.

The bound $\mu_4(17) \le 53$ can be obtained by using two methods, the proposed method and method introduced in [4]. When we use the elliptic curve E_2 with 2 degree one places with $u = 2$, 4 degree one places with $u = 1$ and 9 degree two places with $u = 1$, we get $\mu_4(17) \le 53$. On the other hand, using E_3 with 5 degree one places with $u = 1$, 10 degree two places with $u = 1$ and 3 degree three places with $u = 1$ gives the same bound.

We summarize the results of this section in Table 1. The symbol $*$ denotes an improvement by using the proposed method compared to the best known values in the literature. In this table, we indicate the methods that achieve the bounds in the corresponding columns. These are the methods (i), (ii), (iii) or (iv) explained in the beginning of Section 4.

5. Application

Finite field multiplication is widely used in many areas such as cryptography and coding theory. For example, in elliptic curve cryptography, finite fields with large number of elements are used. Some of the suitable finite fields are proposed by NIST (National Institute of Standards and Technology) [17]. In that list, it is suggested to use the fields with 2^{163}, 2^{233}, 2^{283}, 2^{409} and 2^{571} elements. Now, we will compute the multiplicative complexity for multiplication in $\mathbb{F}_{2^{163}}$ using the proposed method. The most suitable elliptic curve over $\mathbb{F}_2$ (up to isomorphism) is $y^2 + y = x^3 + x + 1$ which has 1 degree one place, 2 degree two places, 4 degree three places, 5 degree four places, 8 degree five places, 8 degree six places, 16 degree seven places and 25 degree eight places. We take 1 degree one place with $u = 5$, 2 degree two places with $u = 2$, 4 degree three places with $u = 1$, 5 degree four places with $u = 1$, 8

Table 1
Bounds for $\mu_q(n)$ for $2 \leq n \leq 18$ and $q = 2, 3, 4$.

n	$\mu_2(n)$	Method	$\mu_3(n)$	Method	$\mu_4(n)$	Method
2	3	(ii)	3	(ii)	3	(ii)
3	6	(ii)	6	(ii)	6	(ii)
4	9	(ii)	9	(ii)	8	(ii)
5	13	(ii)	12	(ii)	11	(ii)
6	15	(iii)	15	(ii)	14	(ii)
7	22	(ii)	19	(ii)	17	(ii)
8	24	(iii)	21	(iii)	20	(ii)
9	30	(ii)	26*	(iv)	23	(ii)
10	33	(iii)	27	(iii)	27	(ii)
11	39	(ii)	34*	(iv)	30	(i), (iv)
12	42	(iii)	36	(iii)	33	(iii)
13	48	(ii)	42*	(iv)	37*	(iv)
14	51	(iii)	45	(iii)	39	(iii)
15	54	(iii)	50*	(iv)	45	(iii)
16	60	(iii)	54	(iii)	45	(iii)
17	67	(ii)	58*	(iv)	53	(i), (iv)
18	69	(ii)	62*	(iv)	51	(iii)

degree five places with $u = 1$, 8 degree six places with $u = 1$, 15 degree seven places with $u = 1$ and 11 degree eight places with $u = 1$. Therefore we obtain

$$\mu_2(163) \leq 11 + 2 \cdot 9 + 4 \cdot 6 + 5 \cdot 9 + 8 \cdot 13 + 8 \cdot 15 + 15 \cdot 22 + 11 \cdot 24 = 916,$$

where we use Table 1 and $\widehat{M}_2(5) \leq 11$, $\widehat{M}_4(2) \leq 3$ [12]. On the other hand, the best we can expect from Karatsuba algorithm (together with (2.1)) is $\mu_2(163) \leq N$, where N is an integer with $N > 2187$, since it is given in [26] that $M_2(128) \leq 2187$.

The finite field $\mathbb{F}_{3^{97}}$ is used in pairing based cryptography [13,21]. In order to compute $\mu_3(97)$ by using the proposed method, it would be better to use the elliptic curve $y^2 = x^3 + x^2 + 2x + 1$ which has 3 degree one places, 6 degree two places, 11 degree three places, 15 degree four places and 42 degree five places. When we use 3 degree one places with $u = 3$, 6 degree two places with $u = 1$, 11 degree three places with $u = 1$, 15 degree four places with $u = 1$ and 16 degree five places with $u = 1$, we obtain

$$\mu_3(97) \leq 3 \cdot 5 + 6 \cdot 3 + 11 \cdot 6 + 15 \cdot 9 + 16 \cdot 12 = 426$$

where we use Table 1 and $\widehat{M}_3(3) \leq 5$ [13]. Note that Karatsuba algorithm (together with (2.1)) gives $\mu_3(97) \leq 1554$ [26].

6. Multiplication in $\mathbb{F}_{3^9}$

In this section, we will give the details of obtaining an explicit formula for multiplication in $\mathbb{F}_{3^9}$ by using an elliptic curve. In Example 3.9, we gave the known bounds and we showed that the proposed method provides an improved bound $\mu_3(9) \leq 26$. Now, we will give the details of how the formula for multiplication $\mathbb{F}_{3^9}$ with $\mu_3(9) \leq 26$ is obtained explicitly.

Consider the elliptic curve $E : y^2 = x^3 + x + 2$ over $\mathbb{F}_3$. Let $\{P_1, \ldots, P_4, Q_1, \ldots, Q_6\}$ be a set of places where P_i's are of degree one and Q_i's are of degree two. Those are

$$P_1 = \infty, \quad P_2 = (x + 1, y), \quad P_3 = (x + 2, y + 1), \quad P_4 = (x + 2, y + 2),$$
$$Q_1 = (x), \quad Q_2 = (x^2 + 2x + 2, y), \quad Q_3 = (x^2 + 1, y + x), \quad Q_4 = (x^2 + 1, y + 2x),$$
$$Q_5 = (x^2 + x + 2, y + 1), \quad Q_6 = (x^2 + x + 2, y + 2).$$

When we use P_1 and P_2 with $u = 1$, P_3 and P_4 with $u = 2$ and $Q_1, \ldots, Q_6$ with $u = 1$, the map φ defined in Section 3 becomes injective. In order to find an explicit formula, we need to find the local parameters of P_3 and P_4. The local parameters t_3 and t_4 corresponding to P_3 and P_4 respectively are

$$t_3 = \frac{y}{(x^2 + x + 2)} + \frac{1}{(x^2 + x + 2)}, \qquad t_4 = \frac{y}{(x^2 + x + 2)} + \frac{2}{(x^2 + x + 2)}.$$

Let us choose

$$\mathcal{D} = (x^9 + x^8 + x^5 + 2x^3 + 2x^2 + 2x + 1, y + x^7 + x^6 + 2x^5 + x + 1).$$

Then a basis $\{f_1, f_2, \ldots, f_{18}\}$ of $\mathcal{L}(2\mathcal{D})$ containing the basis of $\mathcal{L}(\mathcal{D})$ is

$$f_1 = \frac{x^7y}{f} + \frac{(2x^8 + 2x^7 + x^6 + 2x^4 + x^3 + x^2 + 2x + 2)}{f},$$

$$f_2 = \frac{x^6y}{f} + \frac{(x^8 + 2x^6 + x^5 + x^4 + 2x^3 + 1)}{f},$$

$$f_3 = \frac{x^5y}{f} + \frac{(2x^8 + 2x^5 + x^3 + x + 1)}{f}, \qquad f_4 = \frac{x^4y}{f} + \frac{(2x^8 + x^7 + x^4 + 2x^2 + x + 2)}{f}$$

$$f_5 = \frac{x^3y}{f} + \frac{(x^8 + x^6 + x^4 + x^3 + 2x^2 + x)}{f}, \qquad f_6 = \frac{x^2y}{f} + \frac{(x^7 + x^5 + x^3 + x^2 + 2x + 1)}{f}$$

$$f_7 = \frac{xy}{f} + \frac{(2x^8 + 2x^7 + x^6 + 2x^2 + 2x)}{f}, \qquad f_8 = \frac{y}{f} + \frac{(2x^7 + 2x^6 + x^5 + 2x + 2)}{f}, \qquad f_9 = 1$$

$$f_{10} = \frac{(x^{14} + x^{13} + 2x^{12} + x^{10} + 2x^8 + x^7 + x^5 + x^3 + 2x^2)y}{f^2} + \frac{(x^{18} + 2x^{17} + 2x^{16} + 2x^{15} + 2x^{13} + 2x^{12} + 2x^{10} + x^9 + x^8 + 2x^7 + 2x^4 + 2x)}{f^2}$$

$$f_{11} = \frac{(x^{13} + x^{12} + 2x^{11} + x^9 + 2x^7 + x^6 + x^4 + x^2 + 2x)y}{f^2} + \frac{(x^{17} + 2x^{16} + 2x^{15} + 2x^{14} + 2x^{12} + 2x^{11} + 2x^9 + x^8 + x^7 + 2x^6 + 2x^3 + 2)}{f^2}$$

$$f_{12} = \frac{(x^{12} + x^{11} + 2x^{10} + x^8 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + x)y}{f^2} + \frac{(x^{16} + 2x^{15} + 2x^{14} + 2x^{13} + 2x^{11} + 2x^{10} + x^9 + 2x^8 + x^6 + x^4 + x^3 + x + 1)}{f^2}$$

$$f_{13} = \frac{(x^{11} + x^{10} + 2x^9 + x^7 + x^5 + x^3 + 2x^2)y}{f^2} + \frac{(x^{15} + 2x^{14} + 2x^{13} + 2x^{12} + 2x^{10} + x^9 + x^8 + 2x^4 + 2x)}{f^2}$$

$$f_{14} = \frac{(x^{10} + x^9 + 2x^8 + x^6 + x^4 + x^2 + 2x)y}{f^2} + \frac{(x^{14} + 2x^{13} + 2x^{12} + 2x^{11} + 2x^9 + x^8 + x^7 + 2x^3 + 2)}{f^2}$$

$$f_{15} = \frac{(x^9 + x^8 + 2x^7 + 2x^5 + 2x^4 + 2x^3 + x)y}{f^2} + \frac{(x^{13} + 2x^{12} + 2x^{11} + 2x^{10} + x^9 + 2x^8 + x^6 + x^5 + x^4 + x^3 + x + 1)}{f^2}$$

$$f_{16} = \frac{(x^8 + x^7 + 2x^6 + 2x^5 + x^3 + 2x^2)y}{f^2} + \frac{(x^{12} + 2x^{11} + 2x^{10} + x^9 + x^8 + 2x)}{f^2}$$

$$f_{17} = \frac{(x^7 + x^6 + 2x^5 + 2x^4 + x^2 + 2x)y}{f^2} + \frac{(x^{11} + 2x^{10} + 2x^9 + x^8 + x^7 + 2)}{f^2}$$

$$f_{18} = \frac{(x^6 + 2x^5 + x^4 + x)y}{f^2} + \frac{(x^{10} + 2x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)}{f^2}$$

where $\{f_1, f_2, \ldots, f_9\}$ is a basis of $\mathcal{L}(\mathcal{D})$ and $f = x^9 + x^8 + x^5 + 2x^3 + 2x^2 + 2x + 1$.

Now consider the elements $a = \sum_{i=1}^{9} a_i f_i \in \mathcal{L}(\mathcal{D})$ and $b = \sum_{i=1}^{9} b_i f_i \in \mathcal{L}(\mathcal{D})$. Let $c = \sum_{i=1}^{18} c_i f_i$ be the product of a and b given by

$$\left(\sum_{i=1}^{9} a_i f_i\right) \cdot \left(\sum_{i=1}^{9} b_i f_i\right) = \sum_{i=1}^{18} c_i f_i. \tag{6.1}$$

Then we get the following system of linear equations

$$\underbrace{\begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 - m_3 - m_5 \\ m_6 \\ m_7 - m_6 - m_8 \\ m_9 - m_{11} \\ m_{10} - m_9 - m_{11} \\ m_{12} + m_{13} \\ m_{14} - m_{12} \\ m_{15} - m_{16} \\ m_{17} - m_{15} - m_{16} \\ m_{18} - m_{19} \\ m_{20} - m_{18} - m_{19} \\ m_{21} + m_{222} \\ m_{23} - m_{21} - m_{22} \\ m_{24} + m_{25} \\ m_{26} - m_{24} + m_{25} \end{bmatrix}}_{M} = \underbrace{\begin{bmatrix} 0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0 \\ 0&2&2&2&0&0&1&2&1&2&1&1&0&0&2&2&1&1 \\ 0&1&0&2&0&0&2&2&1&0&0&2&0&0&2&0&0&2 \\ 0&2&2&0&0&0&1&2&0&0&0&1&1&1&2&2&2&0 \\ 2&0&2&1&2&2&1&1&1&0&0&0&0&0&0&0&0&0 \\ 2&2&1&2&1&0&1&2&0&0&0&0&0&0&0&0&0&0 \\ 2&1&1&2&0&1&0&2&1&0&2&1&0&2&1&0&2&1 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&1&0&2&0&1&1&2&2&2&1&1&2&0&2 \\ 2&2&2&2&1&1&2&2&0&0&1&1&0&2&0&2&2&2 \\ 1&0&1&1&0&1&0&0&1&2&0&0&2&2&0&0&2&2 \\ 0&1&1&0&1&0&0&0&0&0&1&1&2&1&2&2&0&2 \\ 1&2&1&2&0&0&0&1&1&2&0&0&2&2&0&0&2&2 \\ 2&1&2&0&0&0&1&0&0&0&1&1&2&1&2&2&0&2 \\ 0&0&0&1&1&0&0&2&1&2&0&0&1&2&1&1&0&2 \\ 2&1&2&2&2&1&2&0&0&1&2&2&1&1&1&2&1&2 \\ 0&2&2&2&1&1&1&1&1&1&1&1&0&1&0&2&2&0 \\ 1&1&1&1&0&1&0&1&0&0&1&1&1&0&1&0&2&2 \end{bmatrix}}_{G} \underbrace{\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \\ c_9 \\ c_{10} \\ c_{11} \\ c_{12} \\ c_{13} \\ c_{15} \\ c_{16} \\ c_{17} \\ c_{18} \end{bmatrix}}_{C}$$

where multiplications m_i for $1 \leq i \leq 26$, are given in Appendix.

Since G is invertible, we have $C = G^{-1} \cdot M$. Then we can find the multiplication in $\mathbb{F}_{3^9}$ by using $\text{Ev}_Q(c)$ where we choose

$$Q = (x^9 + 2x^8 + x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2, y + x^8 + 2x^6 + 2x^4 + x^3 + 1).$$

The explicit formula is given in the Appendix.

Acknowledgments

We would like to thank the anonymous reviewers for their insightful and useful comments that improved the paper.

The authors were partially supported by TÜBİTAK under Grant No. TBAG-107T826.

Appendix

We give an explicit formula for multiplication in $\mathbb{F}_{3^9}$. We represent $\mathbb{F}_{3^9}$ as the field $\mathbb{F}_3(w) = \mathbb{F}_3[x]/(p(x))$ where w is the root of the irreducible polynomial $p(x) = x^9 + 2x^8 + x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2$. Let $\alpha = \sum_{i=1}^{9} a_i \xi_i$, $\beta = \sum_{i=1}^{9} b_i \xi_i$, and $\gamma = \sum_{i=1}^{9} c_i \xi_i \in \mathbb{F}_{3^9}$ with

$$\left(\sum_{i=1}^{9} a_i \xi_i\right) \cdot \left(\sum_{i=1}^{9} b_i \xi_i\right) = \sum_{i=1}^{9} c_i \xi_i,$$

where $\{\xi_i, \xi_2, \dots, \xi_9\}$ is a basis of $\mathbb{F}_{3^9}$ over $\mathbb{F}_3$ such that

$$\begin{aligned}
\xi_1 &= w^8 + 2w^7 + w^6 + w^4 + 2w^3 + 2w^2 + 2,\\
\xi_2 &= w^7 + 2w^6 + w^5 + w^3 + 2w^2 + 2w,\\
\xi_3 &= 2w^8 + w^7 + w^6 + w^5 + 2w^4 + w^3 + 2w^2 + 2,\\
\xi_4 &= w^8 + w^7 + w^6 + 2w^5 + w^3 + w,\\
\xi_5 &= w^8 + w^6 + 2w^5 + w^4 + 2w^3 + 2w + 1,\\
\xi_6 &= w^8 + 2w^5 + w^4 + w^2 + 2w + 2,\\
\xi_7 &= w^8 + w^5 + w^4 + 2w^2 + 2,\\
\xi_8 &= 2w^8 + 2w^7 + 2w^5 + 2w^4 + 2w^3 + w^2,\\
\xi_9 &= 1.
\end{aligned}$$

The following explicit formula consisting of the 26 multiplications in $\mathbb{F}_3$ gives γ from α and β. We first define the multiplications m_i, for $1 \le i \le 26$ and then we give the formula for obtaining the coefficients of γ using these multiplications.

$$\begin{aligned}
m_1 &= a_9b_9\\
m_2 &= (2a_2 + 2a_3 + 2a_4 + a_7 + 2a_8 + a_9)(2b_2 + 2b_3 + 2b_4 + b_7 + 2b_8 + b_9)\\
m_3 &= (a_2 + 2a_8 + 2a_4 + 2a_7 + a_9)(b_2 + 2b_8 + 2b_4 + 2b_7 + b_9)\\
m_4 &= (a_8 + 2\,a_4 + a_9 + 2\,a_3)(b_8 + 2\,b_4 + b_9 + 2\,b_3)\\
m_5 &= (2a_2 + a_7 + 2a_3 + 2a_8)(2b_2 + b_7 + 2b_3 + 2b_8)\\
m_6 &= (2a_1 + a_9 + a_7 + 2a_3 + a_8 + a_4 + 2a_5 + 2a_6)\\
&\quad \times (2b_1 + b_9 + b_7 + 2b_3 + b_8 + b_4 + 2b_5 + 2b_6)\\
m_7 &= (a_1 + a_9 + 2a_7 + 2a_6 + 2a_2)(b_1 + b_9 + 2b_7 + 2b_6 + 2b_2)\\
m_8 &= (2a_2 + a_3 + 2a_4 + a_7 + a_5 + 2a_8 + 2a_1)(2b_2 + b_3 + 2b_4 + b_7 + b_5 + 2b_8 + 2b_1)\\
m_9 &= (2a_1 + a_2 + a_3 + 2a_4 + a_6 + 2a_8 + a_9)(2b_1 + b_2 + b_3 + 2b_4 + b_6 + 2b_8 + b_9)\\
m_{10} &= (2a_1 + a_2 + a_3 + 2a_4 + a_6 + a_9)(2b_1 + b_2 + b_3 + 2b_4 + b_6 + b_9)\\
m_{11} &= a_8b_8\\
m_{12} &= (a_1 + a_5 + a_9 + 2a_7)(b_1 + b_5 + b_9 + 2b_7)\\
m_{13} &= (2a_2 + 2a_1 + a_5 + 2a_3 + 2a_4 + 2a_7 + 2a_8 + a_6)\\
&\quad \times (2b_2 + 2b_1 + b_5 + 2b_3 + 2b_4 + 2b_7 + 2b_8 + b_6)\\
m_{14} &= (2a_5 + a_9 + a_7 + 2a_2 + 2a_3 + 2a_4 + 2a_8 + a_6)\\
&\quad \times (2b_5 + b_9 + b_7 + 2b_2 + 2b_3 + 2b_4 + 2b_8 + b_6)\\
m_{15} &= (a_1 + a_3 + a_9 + a_4 + a_6)(b_1 + b_3 + b_9 + b_4 + b_6)\\
m_{16} &= (a_2 + a_5 + a_3)(b_2 + b_5 + b_3)\\
m_{17} &= (a_1 + 2a_3 + a_9 + a_4 + a_6 + a_2 + a_5)(b_1 + 2b_3 + b_9 + b_4 + b_6 + b_2 + b_5)\\
m_{18} &= (a_1 + a_9 + 2a_2 + a_3 + 2a_4 + a_8)(b_1 + b_9 + 2b_2 + b_3 + 2b_4 + b_8)\\
m_{19} &= (a_2 + 2a_1 + a_7 + 2a_3)(b_2 + 2b_1 + b_7 + 2b_3)\\
m_{20} &= (a_9 + 2a_4 + a_8 + a_7)(b_9 + 2b_4 + b_8 + b_7)\\
m_{21} &= (a_5 + a_9 + a_4 + 2a_8)(b_5 + b_9 + b_4 + 2b_8)\\
m_{22} &= (2a_1 + 2a_4 + 2a_3 + a_6 + 2a_7 + a_2 + 2a_5)(2b_1 + 2b_4 + 2b_3 + b_6 + 2b_7 + b_2 + 2b_5)\\
m_{23} &= (a_9 + 2a_8 + 2a_1 + 2a_3 + a_6 + 2a_7 + a_2)(b_9 + 2b_8 + 2b_1 + 2b_3 + b_6 + 2b_7 + b_2)\\
m_{24} &= (a_9 + 2a_2 + a_7 + 2a_3 + a_6 + 2a_4 + a_5 + a_8)\\
&\quad \times (b_9 + 2b_2 + b_7 + 2b_3 + b_6 + 2b_4 + b_5 + b_8)\\
m_{25} &= (a_2 + a_3 + a_6 + a_4 + a_8 + a_1)(b_2 + b_3 + b_6 + b_4 + b_8 + b_1)\\
m_{26} &= (a_9 + a_7 + 2a_6 + a_5 + 2a_8 + a_1)(b_9 + b_7 + 2b_6 + b_5 + 2b_8 + b_1).
\end{aligned}$$

The coefficients of $\gamma \in \mathbb{F}_{3^9}$ are found by using the following equations.

$$\begin{aligned}
c_1 &= (2m_6 + m_{11} + m_{10} + m_{13} + m_{14} + 2m_{16} + 2m_{17} + 2m_{19} + m_{25} + 2m_{26} \\
&\quad + 2m_{20} + 2m_{21} + 2m_{22} + 2m_2 + m_1) \\
c_2 &= (m_6 + 2m_9 + 2m_{10} + m_{15} + m_{16} + 2m_{17} + 2m_{18} + 2m_{19} + 2m_{25} + m_{26} \\
&\quad + m_{20} + m_{21} + m_{23} + 2m_2 + m_3 + 2m_5 + m_4) \\
c_3 &= (m_6 + 2m_9 + 2m_{10} + m_{13} + m_{14} + m_{15} + 2m_{16} + m_{19} + 2m_{24} + 2m_{25} \\
&\quad + m_{20} + m_{22} + 2m_{23} + 2m_2 + 2m_3 + m_5 + 2m_4) \\
c_4 &= (m_7 + 2m_8 + m_9 + m_{11} + 2m_{10} + m_{13} + m_{14} + m_{15} + m_{17} + m_{18} + 2m_{19} \\
&\quad + m_{25} + 2m_{26} + m_{21} + m_{22} + m_2 + m_1 + m_5 + 2m_4) \\
c_5 &= (2m_6 + m_7 + 2m_8 + 2m_9 + 2m_{11} + m_{10} + 2m_{13} + 2m_{14} + 2m_{18} + m_{19} \\
&\quad + m_{25} + 2m_{26} + m_2 + 2m_1) \\
c_6 &= (2m_6 + 2m_9 + 2m_{10} + 2m_{12} + 2m_{13} + 2m_{15} + 2m_{17} + m_{18} + 2m_{19} \\
&\quad + 2m_{25} + m_{26} + m_{22} + 2m_{23} + m_2 + m_1) \\
c_7 &= (m_6 + 2m_7 + m_8 + m_{12} + m_{13} + 2m_{15} + m_{16} + 2m_{18} + 2m_{19} + m_{24} \\
&\quad + m_{25} + m_{20} + 2m_{21} + 2m_{22} + 2m_1 + 2m_3 + m_5 + 2m_4) \\
c_8 &= (m_6 + 2m_{11} + 2m_{10} + 2m_{12} + m_{13} + 2m_{14} + m_{16} + m_{17} + 2m_{19} \\
&\quad + 2m_{24} + 2m_{26} + 2m_{20} + 2m_{21} + 2m_{23} + m_1 + 2m_3) \\
c_9 &= (2m_6 + 2m_9 + m_{11} + 2m_{13} + 2m_{14} + 2m_{15} + 2m_{17} + 2m_{18} + m_{19} + m_{24} \\
&\quad + 2m_{25} + 2m_{26} + 2m_{21} + m_{22} + m_{23} + 2m_5 + m_4).
\end{aligned}$$

References

[1] N. Arnaud, Evaluation Dérivée, Multiplication dans les Corps finis et codes correcteurs, Ph.D. dissertation, Université de la Méditerranée, France, 2006.

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

[3] S. Ballet, Quasi-optimal algorithms for multiplication in the extension of degree 13, 14, and 15, Journal of Pure and Applied Algebra 171 (2002) 149–164.

[4] S. Ballet, R. Rolland, Multiplication algorithm in a finite field and tensor rank of the multiplication, Journal of Algebra 272/1 (2004) 173–185.

[5] S. Ballet, J. Chaumine, On the bounds of the bilinear complexity of multiplication in some finite fields, Applicable Algebra in Engineering, Communication and Computing 15 (2004) 205–211.

[6] S. Ballet, D. Le Brigand, R. Rolland, On an application of the definition field descent of a tower of function filed, in: Colloque International Arithmetic, Geometry and Coding Theory 2005 (AGCT 10), in: Société Mathématiques de France, sér. Séminaires et Congrés, vol. 21, 2009, pp. 187–203.

[7] S. Ballet, An improvement of the construction of the D.V. and G.V. Chudnovsky algorithm for multiplication in finite fields, Theoretical Computer Science 352 (2006) 293–305.

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

[9] S. Ballet, A note on the tensor rank of the multiplication in certain finite fields, in: J. Hirschfeld, J. Chaumine, R. Rolland (Eds.), Algebraic Geometry and its Applications (Proceedings of Symposium of Algebraic Geometry and Applications, Tahiti, 7–11 mai 2007), in: Number Theory and its Applications, vol. 5, World Scientific, 2008, pp. 332–342.

[10] S. Ballet, R. Rolland, Asymptotical bounds for the tensor rank of the multiplication in finite extensions of $\mathbb{F}_2$, preprint IML 2008, web site IML.

[11] W. Bosma, J. Cannon, C. CPlayoust, The Magma algebra system I. The user language, Journal of Symbolic Computation 24 (3–4) (1997) 235–265.

[12] M. Cenk, F. Özbudak, Improved polynomial multiplication formulas over $\mathbb{F}_2$ using Chinese Remainder Theorem, IEEE Transactions on Computers 58 (4) (2009) 572–576.

[13] M. Cenk, F. Özbudak, Efficient multiplication in $\mathbb{F}_{3^{\ell m}}$, $m \geq 1$ and $5 \leq \ell \leq 18$, in: Africacrypt 2008, in: Lecture Notes in Computer Science, vol. 5023, Springer-Verlag, 2008, pp. 406–414.

[14] D.V. Chudnovsky, G.V. Chudnovsky, Algebraic complexities and algebraic curves over finite fields, Journal of Complexity 4 (1988) 285–316.

[15] H. Fan, M.A. Hasan, Comments on five, six, and seven-term Karatsuba-like formulae, IEEE Transactions on Computers 56 (5) (2007) 716–717.

[16] P.L. Montgomery, Five, six, and seven-term Karatsuba-like formulae, IEEE Transactions on Computers 54 (3) (2005) 362–369.

[17] National Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-2, 2000.

[18] H. Niederreiter, C. Xing, Rational Points on Curves Over Finite Fields: Theory and Applications, Cambridge University Press, Cambridge, UK, 2001.
[19] H. Niederreiter, F. Özbudak, Constructions of digital nets using global function fields, Acta Arithmetica 105 (3) (2002) 279–302.
[20] H. Niederreiter, F. Özbudak, Improved asymptotoic bounds for codes using distinguished divisors of global function fields, SIAM Journal on Discrete Mathematics 21 (4) (2007) 865–899.
[21] D. Page, N.P. Smart, Hardware implementation of finite fields of characteristic three, in: CHESS 2003, in: Lecture Notes in Computer Science, vol. 2523, Springer-Verlag, 2003, pp. 539–539.
[22] M.A. Shokrollahi, Optimal algortihms for multiplication in certain finite fields using algebraic curves, SIAM Journal on Computing 21 (6) (1992) 1193–1198.
[23] I.E. Shparlinski, M.A. Tsfasman, S.G. Vladut, Curves with many points and multiplication in finite fields, in: Lecture Notes in Mathematics, vol. 1518, Springer, Berlin, 1992, pp. 145–169.
[24] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993.
[25] B. Sunar, A generalized method for constructing subquadratic complexity $GF(2^k)$ multipliers, IEEE Transactions on Computers 53 (9) (2004) 1097–1105.
[26] A. Weimerskirch, C. Paar, Generalizations of the Karatsuba algorithm for polynomial multiplication. Avaliable at: http://eprint.iacr.org/2006/224.
[27] S. Winograd, Arithmetic Complexity of Computations, SIAM, 1980.
[28] C.P. Xing, H. Niederreiter, Low-discrepancy sequences obtained from algebraic function-fields over finite-fields, Acta Arithmetica 72 (3) (1995) 281–298.
[29] C.P. Xing, H. Niederreiter, K.Y. Lam, Constructions of algebraic-geometry codes, IEEE Transactions on Information Theory 45 (4) (1999) 1186–1193.