RESULTS ON COMPLEXITY OF MULTIPLICATION OVER FINITE FIELDS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

MURAT CENK

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

FEBRUARY 2009

Approval of the thesis:

RESULTS ON COMPLEXITY OF MULTIPLICATION OVER FINITE FIELDS

submitted by **MURAT CENK** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Ersan Akyıldız
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak
Head of Department, **Cryptography**

Prof. Dr. Ferruh Özbudak
Supervisor, **Department of Mathematics, METU**

Examining Committee Members:

Assoc. Prof. Dr. Ali Doğanaksoy
Department of Mathematics, METU

Prof. Dr. Ferruh Özbudak
Institute of Applied Mathematics, METU

Assoc. Prof. Dr. Emrah Çakçak
Department of Mathematics, METU

Dr. Zülfükar Saygı
Department of Mathematics, TOBB ETU

Dr. Burcu Gülmez Temur
Department of Mathematics, Atılım University

Date:

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: MURAT CENK

Signature :

ABSTRACT

RESULTS ON COMPLEXITY OF MULTIPLICATION OVER FINITE FIELDS

Cenk, Murat
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

February 2009, 62 pages

Let n and ℓ be positive integers and $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ such that $\ell deg(f(x)) < 2n - 1$, where q is 2 or 3. We obtain an effective upper bound for the multiplication complexity of n-term polynomials modulo $f(x)^\ell$. This upper bound allows a better selection of the moduli when Chinese Remainder Theorem is used for polynomial multiplication over $\mathbb{F}_q$. We give improved formulae to multiply polynomials of small degree over $\mathbb{F}_q$. In particular we improve the best known multiplication complexities over $\mathbb{F}_q$ in the literature in some cases. Moreover, we present a method for multiplication in finite fields improving finite field multiplication complexity $\mu_q(n)$ for certain values of q and n. We use local expansions, the lengths of which are further parameters that can be used to optimize the bounds on the bilinear complexity, instead of evaluation into residue class field. We show that we obtain improved bounds for multiplication in $\mathbb{F}_{q^n}$ for certain values of q and n where $2 \leq n \leq 18$ and $q = 2, 3, 4$.

Keywords: Polynomial Multiplication, Finite Field Multiplications, Multiplicative Complexity

ÖZ

SONLU CİSİMLERDE ÇARPMA KARMAŞIKLIĞI ÜZERİNE SONUÇLAR

Cenk, Murat
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Şubat 2009, 62 sayfa

Üzerinde çalışılan cismin eleman sayısı olan q, 2 veya 3 olmak üzere, n ve ℓ pozitif tamsayı, $f(x)$ indirgenemez polinom ve $\ell deg(f(x)) < 2n-1$ olsun. Bu tezde $\mathbb{F}_q$ üzerine n-terimli poinomların mod $f(x)^\ell$ indirgemesine göre çarpım karmaşıklığı üzerine üst sınırlar elde edildi. Bu üst sınır Çinli Kalan Teoreminde daha iyi modülüs polinomları seçilmesine olanak tanıdı. Boylece $\mathbb{F}_q$ üzerine küçük dereceli polinom çarpımları için literarürde olan en iyi sonuçlardan daha iyi sonuçlar geliştirildi. Ek olarak belirli n ve q için $\mu_q(n)$ olan sonlu cisim çarpma karmaşıklığı üzerinde gelişmeler elde edildi. Burada, sınıf cisimlerinde değerlendirme yerine lokal genişlemeler kullanarak sınırlar üzerinde optimizasyonlar elde edildi. Belirli q ve n değerleri olan $q = 2, 3, 4$ ve $2 \leq n \leq 18$ için $\mathbb{F}_{q^n}$'de geliştirilmiş çarpmalar elde edildi.

Anahtar Kelimeler: Polinom Çarpmı, Sonlu cisim Çarpmı, Çarpımsal Karmaşıklık

To my father, my beloved wife Derya and my child Emre...

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to Prof. Dr. Ferruh Özbudak for his guidance, advice, encouragement and insight throughout the research. Without him, I couldn't have completed this thesis. It was honour for me to work with him and to benefit from his experiences.

I also wish to present my sincere thanks to Prof. Dr. Ersan Akyıldız who have always supported and encouraged me during my study.

I owe special thanks to my parents for their unconditional love, faithfulness and endless support all times in my life.

Special thanks go to my wife Derya for her support, encouragement, help and love during this difficult process. I also wish to present my special thanks to my dear son Emre because he shared his father with many papers, homeworks and computers for 4 years.

TABLE OF CONTENTS

CHAPTERS

LIST OF TABLES

TABLES

CHAPTER 1

INTRODUCTION

Finite field multiplication plays an important role in public key cryptography and coding theory. Public key cryptographic applications accomplished in very large finite fields. For example, one needs a finite field of at least 2^{160} elements for elliptic curve cryptography. For that reason efficient finite field multiplication has become a crucial part of such applications. A finite field with q^n elements is denoted by $\mathbb{F}_{q^n}$ where q is a prime power and $n \geq 1$. The elements of $\mathbb{F}_{q^n}$ can be represented by n-term polynomials over $\mathbb{F}_q$. Field elements can be multiplied in terms of ordinary multiplication of polynomials and modular reduction of the result product by the defining polynomial of the finite field. The reduction step has no multiplicative complexity [11, p.8]. So finite field multiplication is directly related to the polynomial multiplication.

A direct approach to polynomial multiplication is the schoolbook method. For multiplying two arbitrary 2-term polynomials, this algorithms requires 4 multiplications. Karatsuba-Ofman or simply Karatsuba algorithm [5, 6] is a well-known subquadratic polynomial multiplication algorithm. Karatsuba algorithm decreases the number of multiplications from 4 multiplications to 3 multiplications for multiplying two arbitrary 2-term polynomials. Weimerskirch and Paar [9] generalized Karatsuba algorithm and gave a detailed account of its variants. Toom-Cook [8, 3] method is another related method which gives the best result in many cases where it can be applied directly. Toom-Cook method cannot be applied directly for the multiplication of n-term polynomials over a finite field $\mathbb{F}_q$, if n is sufficiently large compared to q. In [11], Winograd studied the polynomial multiplication problem over arbitrary fields and, among other things, the use of Chinese Remainder Theorem (CRT) for this problem was explained. Sunar [10] gave applications and hardware implementations of CRT for polynomial multiplication over $\mathbb{F}_2$. Montgomery [7] gave explicit formulae for polynomial multiplication which improve multiplication complexity (see Section 2 for a definition of multiplication complexity). Recently Fan and Hasan [4] gave further improvements of multiplication complexity of polynomial multiplication over $\mathbb{F}_2$ using CRT. Up to our knowledge [4] gives the best known complexity bounds for polynomial multiplication over $\mathbb{F}_2$ in the literature.

Let $\mathbb{F}_q$ be a finite field and $n > 1$ be an integer. Let $\mathbb{F}_{q^n}^{\perp}$ be 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

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

$R(\mathbb{F}_{q^n}/\mathbb{F}_q)$ 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 $\mathbb{F}_q$ multiplications in order to multiply two arbitrary elements of $\mathbb{F}_{q^n}$. Winograd [11] 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 [11]. D. V. Chudnovsky and G. V. Chudnovsky [23] generalized this idea to algebraic function fields (of one variable) over $\mathbb{F}_q$. Shokrollahi [27] 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 [28] gave the asymptotic bounds for multiplication in finite fields by using curves with many points. Ballet [16], [17] generalized Shokrollahi's work to the algebraic function fields of genus g. Ballet and Rolland [18] gave a generalization of D. V. Chudnovsky and G. V. Chudnovsky multiplication algorithm by interpolating not only degree 1 places but also interpolating on degree 2 places. In [19], 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 $g - 1$ in the algebraic function fields of genus g defined over $\mathbb{F}_q$.

We classify our contributions in four parts. In Chapter 2 we give a new method for polynomial multiplication over finite fields using field extensions and polynomial interpolation. Our method uses polynomial interpolation as Toom-Cook method, and we also use field extensions. Furthermore, our method works also when Toom-Cook method cannot be applied directly. We obtain explicit formulae improving the previous results in many cases. In some cases over $\mathbb{F}_2$ the bounds we obtain are the same with the recent bounds obtained by Fan and Hasan in [4].

In Chapter 3, we obtain an effective upper bound for the multiplication complexity of n-term polynomials modulo $f(x)^\ell$ where ℓ is a positive integer and $f(x)$ is an irreducible polynomial over $\mathbb{F}_2$. This upper bound allows a better selection of the moduli when Chinese Remainder Theorem is used for polynomial multiplication over $\mathbb{F}_2$. We give improved formulae in order to multiply polynomials of small degree over $\mathbb{F}_2$. In particular we improve the best known multiplication complexities over $\mathbb{F}_2$ in the literature in some cases.

In Chapter 4, using a method based on CRT for polynomial multiplication over $\mathbb{F}_3$ and suitable reductions, we obtained an efficient multiplication method for finite fields of characteristic 3. For $5 \leq \ell \leq 18$, we show that our method gives canonical multiplication formulae over $\mathbb{F}_{3^{\ell m}}$ for any integer $m \geq 1$ with the best multiplicative complexity improving the bounds in [7]. Moreover, we give an explicit formula in the case $\mathbb{F}_{3^{6\cdot 97}}$.

In Chapter 5, we present a method for multiplication in finite fields improving $\mu_q(n)$ for certain values of q and n. We use local expansions, the lengths of which are further parameters that can be used to optimize the bounds on the bilinear complexity, instead of evaluation into residue class field. Our basic principle is still based on the method of D. V. Chudnovsky and G. V. Chudnovsky [23]. The main idea in the new method can be summarized as follows: 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.

CHAPTER 2

POLYNOMIAL MULTIPLICATION OVER FINITE FIELDS USING FIELD EXTENSIONS AND INTERPOLATION

In this chapter we give a new method for polynomial multiplication over finite fields using field extensions and polynomial interpolation. Our method uses polynomial interpolation as Toom-Cook method and we also use field extensions. Furthermore, our method works also when Toom-Cook method cannot be applied directly. We obtain explicit formulae improving the previous results in many cases. In some cases over $\mathbb{F}_2$ the bounds we obtain are the same with the recent bounds obtained by Fan and Hasan in [4].

This chapter is organized as follows: In the next section we give some background and describe some well-known methods of polynomial multiplication. Our method is explained with illustrative examples in Section 2.2. We apply our method to polynomial multiplication over $\mathbb{F}_2$ and $10, 11$ and 12-term polynomial multiplication bounds are determined in Section 2.3.

2.1 BACKGROUND

Let $\mathcal{R}$ be an arbitrary commutative ring with identity and $\mathcal{R}[x]$ denote the ring of polynomials over $\mathcal{R}$ with indeterminate x. For an integer $n \geq 1$, a polynomial of the form

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathcal{R}[x]$$

is called an *n-term polynomial* over $\mathcal{R}$. Throughout this chapter, if not stated otherwise, an n-term polynomial $A(x)$ means an n-term polynomial with the indeterminate x over an arbitrary commutative ring with identity.

For an integer $n \geq 1$, the *complexity of polynomial multiplication* for n-term polynomials is the minimum number $M(n)$ of multiplications needed in order to multiply two arbitrary n-term polynomials.

Throughout this chapter $\mathbb{F}_q$ denotes a finite field with q elements. For a prime power q and an integer $n \geq 1$, the *complexity of polynomial multiplication over* $\mathbb{F}_q$ for n-term polynomials is the minimum number $M_q(n)$ of multiplications over $\mathbb{F}_q$ needed to multiply two arbitrary n-term polynomials over $\mathbb{F}_q$. We note that $M_q(n) \leq M(n)$.

We now summarize the schoolbook method, Karatsuba algorithm and the related generalization by Weimerskirch and Paar, the recent work by Montgomery, and Toom-Cook method.

2.1.1 SCHOOLBOOK METHOD

Consider two n-term polynomials

$$A(x) = \sum_{i=0}^{n-1} a_i x^i, \quad B(x) = \sum_{i=0}^{n-1} b_i x^i.$$

The schoolbook multiplication gives us the product $C(x)$ of $A(x)$ and $B(x)$ to be

$$C(x) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j x^{i+j} .$$

Therefore using this method we get

$$M(n) \leq n^2. \tag{2.1}$$

2.1.2 KARATSUBA ALGORITHM AND WEIMERSKIRCH-PAAR GENERALIZATION

Karatsuba algorithm [5] gives better upper bounds on $M(n)$. For example, consider two 2-term polynomials,

$$A(x) = a_0 + a_1 x, \quad B(x) = b_0 + b_1 x.$$

The Karatsuba algorithm computes the product $C(x) = A(x)B(x)$ as

$$C(x) = a_1 b_1 x^2 + [(a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1]x + a_0 b_0.$$

Here we need just three multiplications: $a_0 b_0$, $(a_0 + a_1)(b_0 + b_1)$ and $a_1 b_1$. Hence we obtain $M(2) \leq 3$, while the schoolbook method gives only $M(2) \leq 4$.

Weimerskirsh and Paar [9] gave a detailed complexity analysis of Karatsuba algorithm for different cases. Specifically, if the number of coefficients of polynomials are composite integers, say nm, then we can write $A(x) = \sum_{s=0}^{m-1} A_s(x)x^{ns} \in \mathcal{R}[x]$ where $A_s(x) \in \mathcal{R}[x]$ is an n-term polynomial for each $0 \leq s \leq m-1$. Let $\mathfrak{R} = \mathcal{R}[x]$, which is again a commutative ring with identity. Now, $A(x)$ can be considered as an m-term polynomial over $\mathfrak{R}$, where each of its coefficients are n-term polynomials over $\mathcal{R}$. After writing $B(x)$ in the same way and applying Karatsuba algorithm, it is found that

$$M(nm) \leq M(n)M(m). \tag{2.2}$$

If the number of coefficient is $n = 2m+1$ where $m \geq 1$, then we can write

$$A(x) = A_0(x) + A_1(x)x^m, \quad B(x) = B_0(x) + B_1(x)x^m \ ,$$

where A_0, B_0 are degree $m-1$ polynomials and A_1, B_1 are degree m polynomials. Then

$$A(x)B(x) = A_0B_0 + [(A_0 + A_1)(B_0 + B_1) - A_1B_1 - A_0B_0]x^m + A_1B_1x^{2m}.$$

Therefore we arrive to the following bound of [9]:

$$M(2m+1) \leq M(m) + 2M(m+1) \tag{2.3}$$

for odd $n = 2m+1$ where $m \geq 1$.

2.1.3 MONTGOMERY'S CONTRIBUTION

Montgomery [7] observed, among other things, that one multiplication is redundant in (2.3). Hence

$$M(2m+1) \leq 2M(m+1) + M(m) - 1, \quad (m \geq 1). \tag{2.4}$$

Montgomery also gave explicit formulae for $n = 5, 6, 7$, which imply $M(5) \leq 13$, $M(6) \leq 17$ and $M(7) \leq 22$. Using these formulae for $n = 5, 6, 7$ recursively, he also obtained improvements on $M(n)$ for some larger values of n. These improvements are tabulated in [7, Table 1 in page 367].

2.1.4 TOOM-COOK METHOD

Let $\mathcal{F}$ be an arbitrary field. For $n \geq 1$, assume that $\mathcal{F}$ has at least $2n-2$ distinct elements (or "point"s) $\alpha_1, ..., \alpha_{2n-2}$. Toom-Cook method [8], [3] uses these $2n-2$ distinct elements of

$\mathcal{F}$ and the point at "∞" in order to compute the product of two arbitrary n-term polynomials from $\mathcal{F}$. If there are enough elements in $\mathcal{F}$, then this method needs $(2n-1)$ multiplications over $\mathcal{F}$ in order to multiply two arbitrary n-term polynomials over $\mathcal{F}$. We refer to a recent paper [1] for the details. Hence if $q \geq 2n-2$, then Toom-Cook method gives

$$M_q(n) \leq 2n - 1. \tag{2.5}$$

However if $\mathcal{F}$ is a finite field $\mathbb{F}_q$ and n is large enough, this method cannot be applied directly (see also [7, Subsection 6.1]). For example, if $q = 7$ and $n = 5$, then as $2n - 2 = 8 > 7 = q$, we cannot apply Toom-Cook method. Among schoolbook method, Karatsuba algorithm and Montgomery's improvements, the best result for $M_7(5)$ is $M_7(5) \leq 13$ (see [7, Table 1]). Note that Toom-Cook method gives $M_7(3) = 5$ and $M_7(2) = 3$. Therefore using Toom-Cook method recursively and (2.4), we obtain that

$$M_7(5) \leq 2M_7(3) + M_7(2) - 1 \leq 2 \cdot 5 + 3 - 1 = 12,$$

which is better than the upper bound $M_7(5) \leq 13$ obtained from Montgomery's formulae for 5-term polynomials. In the next section we will improve, for example, this bound to $M_7(5) \leq 11$ (see Example 2.2.5) and then we will improve this bound to $M_7(5) = 10$ (see Example 2.3.5) which is optimal and for that reason we use equality.

Remark 2.1.1 *It follows from the definitions that the inequalities on (2.2) and (2.4) on $M(n)$ also hold if $M(n)$ is replaced with $M_q(n)$, where q is a prime power.*

2.2 NEW METHOD FOR POLYNOMIAL MULTIPLICATION OVER FINITE FIELDS

Let q be a prime power. Using Toom-Cook method we have

$$\begin{array}{lll} M_{q^2}(n) & \leq 2n-1 & \text{for } n \leq \frac{q^2+2}{2}, \text{ and} \\ M_q(n) & \leq 2n-1 & \text{for } n \leq \frac{q+2}{2}. \end{array}$$

Toom-Cook method cannot be applied directly for obtaining an upper bound on $M_q(n)$ if $n > \frac{q+2}{2}$. In the beginning of this section, we will show that by modifying Toom-Cook method and using the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$, we can obtain new formulae and improved upper bounds on $M_q(n)$ for $n \leq \frac{q^2+2}{2}$. Then, we will generalize our results using the extensions $\mathbb{F}_{q^m}/\mathbb{F}_q$ for arbitrary integers $m \geq 2$ and obtain new formulae and improved upper bounds on $M_q(n)$ for larger values of n as well.

The following definition is useful.

Definition 2.2.1 *Let q be a prime power and $m \geq 2$ be an integer. Let $\mu_q(m)$ be the smallest number of multiplications needed over $\mathbb{F}_q$ for multiplying two arbitrary elements of $\mathbb{F}_{q^m}$. In the definition of $\mu_q(m)$, multiplying two arbitrary elements of $\mathbb{F}_q$ is counted but multiplying an element of $\mathbb{F}_q$ with a constant in $\mathbb{F}_q$ is not counted.*

Any polynomial multiplication formula over $\mathbb{F}_q$ can be used for finite field multiplication because the elements of finite fields can be represented by polynomials. In order to multiply two elements of finite field, the elements are multiplied like polynomials and then the product is reduced using reduction polynomial of the finite field. The reduction step has no multiplicative cost. So we can assume that we have $\mu_q(n) \leq M_q(n)$.

Lemma 2.2.2 *Let q be a prime power. We have $\mu_q(2) \leq 3$.*

Proof. Karatsuba algorithm [5] gives the result. ■

Now we give our first improvement using the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$.

Proposition 2.2.3 *Let q be a prime power. Assume that $\frac{q+2}{2} < n \leq \frac{q^2+2}{2}$. There exists a formula for multiplying two arbitrary n-term polynomials over $\mathbb{F}_q$ which gives*

$$M_q(n) \leq 6n - 2q - 5. \tag{2.6}$$

Proof. Assume that $n > \frac{q+2}{2}$. We use Toom-Cook type evaluations over $\mathbb{F}_{q^2}$ using the point ∞, all elements of $\mathbb{F}_q$ and $2n-q-2$ elements from $\mathbb{F}_{q^2} \backslash \mathbb{F}_q$. These need at most $q+1$ multiplications in $\mathbb{F}_q$ due to the point ∞ and the elements of $\mathbb{F}_q$ and at most $2n - q - 2$ multiplications over $\mathbb{F}_{q^2}$ due to the chosen $2n - q - 2$ elements of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Using Lemma 2.2.2 we obtain that

$$M_q(n) \leq q + 1 + \mu_q(2)(2n - q - 2) \leq 6n - 2q - 5.$$

■

Remark 2.2.4 *In the proof of Proposition 2.2.3, if we know that a multiplication corresponding to an evaluation and contributing to the upper bound (2.6) also appears in another evaluation, then we call such a multiplication an overlap. Since the proof of Proposition 2.2.3 does not take such overlaps into account, if we know the existence of such overlaps in a particular case, then the upper bound (2.6) can be improved. In Example 2.2.6 we will illustrate such a situation.*

In the following example we demonstrate how to find the formula of Proposition 2.2.3 explicitly.

Example 2.2.5 *Let* $q = 7$ *and* $n = 5$*. Note that* $x^2 - 3 \in \mathbb{F}_7[x]$ *is irreducible and let* $w \in \mathbb{F}_{49}$ *with* $w^2 = 3$*. Let* $a = a_0 + a_1 + \cdots + a_4x^4$ *and* $b = b_0 + b_1x + \cdots + b_4x^4$ *be two arbitrary* 5*-term polynomials over* $\mathbb{F}_7$*. We need to compute* $c_0, c_1, \ldots, c_8 \in \mathbb{F}_7$ *such that*

$$(a_0 + a_1x + ... + a_4x^4)(b_0 + b_1x + ... + b_4x^4) = c_0 + c_1x + ... + c_8x^8.$$

Using the elements $0, 1, \ldots, 6$ *of* $\mathbb{F}_7$*,* $w \in \mathbb{F}_{49} \setminus \mathbb{F}_7$ *and the point* ∞*, we obtain the following system of* $2n - 1 = 9$ *equations:*

$$\begin{aligned}
x = 0 \Rightarrow &\quad a_0b_0 = c_0 \\
x = 1 \Rightarrow &\quad (a_0 + a_1 + ... + a_4)(b_0 + b_1 + ... + b_4) = (c_0 + c_1 + ... + c_8) \\
x = 2 \Rightarrow &\quad (a_0 + 2a_1 + ... + 2^4a_4)(b_0 + 2b_1 + ... + 2^4b_4) = (c_0 + 2c_1 + ... + 2^8c_8) \\
x = 3 \Rightarrow &\quad (a_0 + 3a_1 + ... + 3^4a_4)(b_0 + 3b_1 + ... + 3^4b_4) = (c_0 + 3c_1 + ... + 3^8c_8) \\
x = 4 \Rightarrow &\quad (a_0 + 4a_1 + ... + 4^4a_4)(b_0 + 4b_1 + ... + 4^4b_4) = (c_0 + 4c_1 + ... + 4^8c_8) \\
x = 5 \Rightarrow &\quad (a_0 + 5a_1 + ... + 5^4a_4)(b_0 + 5b_1 + ... + 5^4b_4) = (c_0 + 5c_1 + ... + 5^8c_8) \\
x = 6 \Rightarrow &\quad (a_0 + 6a_1 + ... + 6^4a_4)(b_0 + 6b_1 + ... + 6^4b_4) = (c_0 + 6c_1 + ... + 6^8c_8) \\
x = w \Rightarrow &\quad (a_0 + wa_1 + .. + w^4a_4)(b_0 + wb_1 + .. + w^4b_4) = (c_0 + wc_1 + .. + w^8c_8) \\
x = \infty \Rightarrow &\quad a_4b_4 = c_8
\end{aligned}$$

We use the following notations for the products at the left hand side of equations above. Note that we reduce the products with respect to mod 7 and mod $(w^2 - 3)$*.*

$$\begin{aligned}
D_0 &= a_0b_0\\
D_1 &= (a_0+a_1+a_2+a_3+a_4)(b_0+b_1+b_2+b_3+b_4)\\
D_2 &= (a_0+2a_1+4a_2+a_3+2a_4)(b_0+2b_1+4b_2+b_3+2b_4)\\
D_3 &= (a_0+3a_1+2a_2+6a_3+4a_4)(b_0+3b_1+2b_2+6b_3+4b_4)\\
D_4 &= (a_0+4a_1+2a_2+a_3+4a_4)(b_0+4b_1+2b_2+b_3+4b_4)\\
D_5 &= (a_0+5a_1+4a_2+6a_3+2a_4)(b_0+5b_1+4b_2+6b_3+2b_4)\\
D_6 &= (a_0+6a_1+a_2+6a_3+a_4)(b_0+6b_1+b_2+6a_3+b_4)\\
\overline{D}_7 &= (a_0+3a_2+2a_4+(a_1+3a_3)w)(b_0+3b_2+2b_4+(b_1+3b_3)w)\\
D_8 &= a_4b_4.
\end{aligned}$$

As it is seen $\overline{D}_7$ is the only product over $\mathbb{F}_{49}$. If we expand $\overline{D}_7$, then we get

$$\overline{D}_7 = t_1t'_1 + [(t_1+t_2)(t'_1+t'_2) - t_1t'_1 - t_2t'_2]w + t_2t'_2w^2$$

where

$$t_1 = (a_0+3a_2+2a_4),\ t'_1 = (b_0+3b_2+2b_4),\ t_2 = (a_1+3a_3),\ t'_2 = (b_1+3b_3).$$

Substituting $w^2 = 3$ we obtain

$$\overline{D}_7 = D'_7 + D''_7w,$$

where D'_7 and D''_7 are the multiplications over $\mathbb{F}_7$ with

$$\begin{aligned}
D'_7 = {} & t_1t'_1 + 3t_2t'_2,\\
D''_7 = {} & [(t_1+t_2)(t'_1+t'_2) - t_1t'_1 - t_2t'_2].
\end{aligned}$$

We have

$$\begin{bmatrix} c_0\\ c_1\\ c_2\\ c_3\\ c_4\\ c_5\\ c_6\\ c_7\\ c_8 \end{bmatrix} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2w & 3w+2 & w+5 & 6w+6 & 6w+1 & w+2 & 3w+5 & 6w & w\\
0 & 6 & 5 & 3 & 3 & 5 & 6 & 0 & 6\\
0 & 6 & 6 & 1 & 6 & 1 & 1 & 0 & 0\\
0 & 6 & 3 & 5 & 5 & 3 & 6 & 0 & 0\\
0 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 0\\
6 & 6 & 6 & 6 & 6 & 6 & 6 & 0 & 0\\
5w & 4w+4 & 6w+5 & w+3 & w+4 & 6w+2 & 4w+3 & w & 6w\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}\begin{bmatrix} D_0\\ D_1\\ D_2\\ D_3\\ D_4\\ D_5\\ D_6\\ \overline{D}_7\\ D_8 \end{bmatrix}$$

Using $\overline{D}_7 = D'_7 + D''_7 w$ and $c_0, c_1, \ldots, c_8 \in \mathbb{F}_7$ we get an explicit formula for the coefficients as

$$\begin{aligned}
c_0 &= D_0 \\
c_1 &= 2D_1 + 5D_2 + 6D_3 + D_4 + 2D_5 + 5D_6 + 4D''_7 \\
c_2 &= 6D_1 + 5D_2 + 3D_3 + 3D_4 + 5D_5 + 6D_6 + 6D_8 \\
c_3 &= 6D_1 + 6D_2 + D_3 + 6D_4 + D_5 + D_6 \\
c_4 &= 6D_1 + 3D_2 + 5D_3 + 5D_4 + 3D_5 + 6D_6 \\
c_5 &= 6D_1 + 5D_2 + 4D_3 + 3D_4 + 2D_5 + D_6 \\
c_6 &= 6D_0 + 6D_1 + 6D_2 + 6D_3 + 6D_4 + 6D_5 + 6D_6 \\
c_7 &= 4D_1 + 5D_2 + 3D_3 + 4D_4 + 2D_5 + 3D_6 + 3D''_7 \\
c_8 &= D_8
\end{aligned} \tag{2.7}$$

Since D''_7 requires 3 multiplications in $\mathbb{F}_7$, this shows that we can multiply 5-term polynomials over $\mathbb{F}_7$ with 11 multiplications in $\mathbb{F}_7$.

By Proposition 2.2.3 we have $M_2(3) \leq 9$. In the next example using 3 overlaps (cf. Remark 2.2.4) we will improve it to $M_2(3) \leq 6$.

Example 2.2.6 *Let $q = 2$ and $n = 3$. Let $w \in \mathbb{F}_4 \setminus \mathbb{F}_2$ with $w^2 + w + 1 = 0$. Let $a_0 + a_1 x + x_2 x^2$ and $b_0 + b_1 x + b_2 x^2$ be two arbitrary 3-term polynomials over $\mathbb{F}_2$. We need to compute $c_0, c_1, c_2, c_3, c_4 \in \mathbb{F}_2$ such that*

$$(a_0 + a_1 x + a_2 x^2)(b_0 + b_1 x + b_2 x^2) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4.$$

Using the elements 0, 1 of $\mathbb{F}_2$, $w, w^2 \in \mathbb{F}_4 \setminus \mathbb{F}_2$ and the point ∞ we obtain the following matrix equation:

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & w+1 & w & 1 \\ 0 & 1 & w & w+1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_0 b_0 \\ (a_0 + a_1 + a_2)(b_0 + b_1 + b_2) \\ (a_0 + w a_1 + w^2 a_2)(b_0 + w b_1 + w^2 b_2) \\ (a_0 + w^2 a_1 + w^4 a_2)(b_0 + w^2 b_1 + w^4 b_2) \\ a_2 b_2 \end{bmatrix}$$

Let us denote

$$\begin{aligned}
\overline{D}_2 &= (a_0 + w a_1 + w^2 a_2)(b_0 + w b_1 + w^2 b_2), \\
\overline{D}_3 &= (a_0 + w^2 a_1 + w^4 a_2)(b_0 + w^2 b_1 + w^4 b_2).
\end{aligned}$$

In the proof of Proposition 2.2.3, each of the contributions of $\overline{D}_2$ and $\overline{D}_3$ to the upper bound (2.6) are counted as 3*. Using* $w^2 + w + 1 = 0$*, we obtain that*

$$\overline{D}_2 = [(a_0 + a_2)(b_0 + b_2) + (a_1 + a_2)(b_1 + b_2)] + w[(a_0 + a_1)(b_0 + b_1) + (a_0 + a_2)(b_0 + b_2)],$$

and

$$\overline{D}_3 = [(a_0 + a_1)(b_0 + b_1) + (a_1 + a_2)(b_1 + b_2)] + w[(a_0 + a_2)(b_0 + b_2) + (a_0 + a_1)(b_0 + b_1)].$$

The counted multiplications in Proposition 2.2.3 for $\overline{D}_1$ *are*

$$(a_0 + a_2)(b_0 + b_2),\ (a_1 + a_2)(b_1 + b_2),\ (a_0 + a_1)(b_0 + b_1),$$

and for $\overline{D}_2$ *are*

$$(a_0 + a_1)(b_0 + b_1),\ (a_1 + a_2)(b_1 + b_2),\ (a_0 + a_2)(b_0 + b_2).$$

It is clear that there are at least 3 *overlaps: each of the multiplications for* $\overline{D}_1$ *are counted again for* $\overline{D}_2$*. Therefore we obtain that* $M_2(3) \le (6n - 2q - 5) - 3 = 6$.

In the rest of this section we give our generalizations. The first one is a straightforward generalization of Proposition 2.2.3. Recall that $\mu_q(m)$ is defined in Definition 2.2.1.

Proposition 2.2.7 *Let q be a prime power and m ≥ an integer. Assume that* $\frac{q+2}{2} < n \le \frac{q^m+2}{2}$*. There exists a formula for multiplying two arbitrary n-term polynomials over* $\mathbb{F}_q$ *which gives*

$$M_q(n) \le q + 1 + \mu_q(m)(2n - q - 2). \tag{2.8}$$

Proof. By changing $\mu_q(2) \le 3$ with $\mu_q(m)$ and applying the similar arguments in the proof of Proposition 2.2.3, we complete the proof. ■

It follows from Definition 2.2.1 that if m_1, m_2 are positive integers and $m_1 \mid m_2$, then $\mu_q(m_1) \le \mu_q(m_2)$. Indeed as $\mathbb{F}_{q^{m_1}}$ is a subfield of $\mathbb{F}_{q^{m_2}}$, any formula for multiplying two arbitrary elements of $\mathbb{F}_{q^{m_2}}$ can be used for multiplying two arbitrary elements of $\mathbb{F}_{q^{m_1}}$. Moreover if $1 \le m_1 \le m_2$ are positive integers with $m_1 \nmid m_2$, then in all cases we know that the upper bound on $\mu_q(m_1)$ is less than or equal to the upper bound on $\mu_q(m_2)$. Therefore we would like to use all suitable finite fields of small size in order to obtain a better upper bound on $M_q(n)$. Using this idea now we give our general result which improves Proposition 2.2.7. First we give some notation. Let $S_q(k)$ be the number of elements in $\mathbb{F}_{q^k} \setminus \mathbb{F}_{q^d}$ where $d|k$. In other words,

$$S_q(k) = \#\{\alpha \in \mathbb{F}_{q^k} \mid \alpha \notin \mathbb{F}_{q^d} \text{ for all } d|k\}. \tag{2.9}$$

Theorem 2.2.8 *Let q be a prime power and $m \geq 2$ an integer. For an integer $n > \frac{q+2}{2}$ assume it holds that*

$$2n - 2 \leq q + \sum_{2 \leq k \leq m} S_q(k), \tag{2.10}$$

where $S_q(k)$ is defined in (2.9). There exists a formula for multiplying two arbitrary n-term polynomials over $\mathbb{F}_q$ which gives

$$M_q(n) \leq 1 + q + \sum_{2 \leq k < m} \mu_q(k) S_q(k) + \mu_q(m)(2n - 2 - q - \sum_{2 \leq k < m} S_q(k)). \tag{2.11}$$

Proof. Let $\bar{m}$ be the least common multiple of the integers $1, 2, \ldots, m$ and $\mathcal{F} = \mathbb{F}_{q^{\bar{m}}}$. It is clear that $\mathbb{F}_{q^k}$ is a subfield of $\mathcal{F}$ for each $2 \leq k \leq m$. By assumption (2.10), apart from the point at ∞, we can choose $2n - 2$ elements of $\mathcal{F}$ such that exactly q of them are from $\mathbb{F}_q$, for $2 \leq k < m$ exactly $S_q(k)$ of them are from $\mathbb{F}_{q^k}$ and $\left(2n - 2 - q - \sum_{2 \leq k < m} S_q(k)\right)$ of them are from $\mathbb{F}_{q^m}$. Using the method in the proofs of Propositions 2.2.3 and Proposition 2.2.7, we observe that Toom-Cook type evaluations at the point ∞ and at the elements of $\mathbb{F}_q$ contribute to $M_q(n)$ by at most $q + 1$ multiplications. For each $2 \leq k < m$, Toom-Cook type evaluations at the chosen elements of $\mathbb{F}_{q^k}$ contribute to $M_q(n)$ by at most $\mu_q(k) S_q(k)$ multiplications. Finally, Toom-Cook type evaluations at the $\left(2n - 2 - q - \sum_{2 \leq k < m} S_q(k)\right)$ chosen elements of $\mathbb{F}_{q^m}$ contribute to $M_q(n)$ by at most $\mu_q(m)\left(2n - 2 - q - \sum_{2 \leq k < m} S_q(k)\right)$. This completes the proof. ■

Remark 2.2.9 *As in Proposition 2.2.3 and Remark 2.2.4, we can improve the upper bound (2.11) of Theorem 2.2.8 if we know the existence of overlaps. We provide such an example in Section 2.3.*

2.3 IMPROVED BOUNDS FOR MULTIPLYING 10, 11 AND 12-TERM POLYNOMIALS OVER $\mathbb{F}_2$

In this section we show the existence of some overlaps in Theorem 2.2.8 for $q = 2$ and we will apply the results to $n = 10$, 11 and 12. Therefore we obtain formulae giving

$$M_2(10) \leq 36, \; M_2(11) \leq 42, \; \text{and } M_2(12) \leq 45. \tag{2.12}$$

We note that using [7, Table 1 in page 367] one would only get

$$M_2(10) \leq 39,\ M_2(11) \leq 46,\ \text{and } M_2(12) \leq 51.$$

However, a recent paper [4] shows that $M_2(10) \leq 35$, $M_2(10) \leq 40$ and $M_2(10) \leq 44$ by using Chinese Remainder Theorem. We will also obtain the same bound in [4] by using a mixed method given at the end of this section.

The following proposition will be used to show the bounds (2.12).

Proposition 2.3.1 *Let $q = 2$, $w \in \mathbb{F}_4$ with $w^2 + w + 1 = 0$, $\alpha \in \mathbb{F}_8$ with $\alpha^3 + \alpha + 1 = 0$ and $\gamma \in \mathbb{F}_{16}$ with $\gamma^4 + \gamma + 1 = 0$. For an integer $n \geq 1$, let $A(x) = \sum_{i=0}^{n-1} a_i x^i$ and $B(x) = \sum_{i=0}^{n-1} b_i x^i$ be two arbitrary n-term polynomials over $\mathbb{F}_2$. In computing the product $A(x)B(x)$ using the method of Theorem 2.2.8:*

i) the total number of multiplications needed for the evaluation at the elements of the set $\{w, w^2\}$ is at most 3, instead of $\mu_2(2) \cdot 2 \leq 6$,

ii) the total number of multiplications needed for the evaluation at the elements of the set $\left\{\alpha, \alpha^2, \alpha^3\right\}$ (respectively $\left\{\alpha^3, \alpha^6, \alpha^5\right\}$) is at most 6, instead of $\mu_2(3) \cdot 3 \leq 18$,

ii) the total number of multiplications needed for the evaluation at the elements of the set $\left\{\gamma, \gamma^2, \gamma^4, \gamma^8\right\}$ (respectively $\left\{\gamma^3, \gamma^6, \gamma^{12}, \gamma^9\right\}$ and $\left\{\gamma^7, \gamma^{14}, \gamma^{13}, \gamma^{11}\right\}$) is at most 9, instead of $\mu_2(4) \cdot 4 \leq 36$.

Proof. We give a detailed proof of item i) only as the proofs of the items ii) and iii) are similar. Let $w_1 = w$ and $w_2 = w^2$. Let $I_0 = \{0 \leq i \leq n-1 : i \not\equiv 0 \mod 3\}$, $I_1 = \{0 \leq i \leq n-1 : i \not\equiv 1 \mod 3\}$ and $I_2 = \{0 \leq i \leq n-1 : i \not\equiv 2 \mod 3\}$. Using the relation $w_1^2 = w_1 + 1$ we obtain that

$$A(w_1) = A_0 + w_1 A_1,\ B(w_1) = B_0 + w_1 B_1,$$

where $A_0, A_1, B_0, B_1 \in \mathbb{F}_2$ are given by

$$A_0 = \sum_{i \in I_1} a_i,\ A_1 = \sum_{i \in I_0} a_i,\ B_0 = \sum_{i \in I_1} b_i,\ B_1 = \sum_{i \in I_0} b_i.$$

Then, using a Karatsuba type argument, we get

$$A(w_1)B(w_1) = (A_0 B_0 + A_1 B_1) + w_1 \left[(A_0 + A_1)(B_0 + B_1) + A_0 B_0\right].$$

We note that

$$A_0 + A_1 = \sum_{i\in I_2} a_i, \text{ and } B_0 + B_1 = \sum_{i\in I_2} b_i.$$

The counted multiplications for the evaluation at w_1 in the method of Theorem 2.2.8 are

$$A_0B_0 = \left(\sum_{i\in I_1} a_i\right)\left(\sum_{i\in I_1} b_i\right), \quad A_1B_1 = \left(\sum_{i\in I_0} a_i\right)\left(\sum_{i\in I_0} b_i\right), \text{ and}$$
$$(A_0 + A_1)(B_0 + B_1) = \left(\sum_{i\in I_2} a_i\right)\left(\sum_{i\in I_2} b_i\right). \tag{2.13}$$

Since w_1 and w_2 are conjugates of each other we have $w_2^2+w_2+1 = 0$. So we have $w_2^2 = w_2+1$ and we obtain that

$$A(w_2) = \overline{A}_0 + w_2\overline{A}_1, \; B(w_2) = \overline{B}_0 + w_2\overline{B}_1,$$

where $\overline{A}_0 = A_0, \; \overline{A}_1 = A_1, \; \overline{B}_0 = B_0,$ and $\overline{B}_1 = B_1 \in \mathbb{F}_2$. It is seen that multiplications needed for the evaluation at w and multiplications needed for the evaluation at w^2 are the same, and hence the total number of evaluations needed for the elements of $\{w, w^2\}$ is 3. This completes the proof of item i). ■

Example 2.3.2 *Let $q = 2$ and w, α, γ be as defined in proposition 2.3.1. We first consider 10-term polynomials over $\mathbb{F}_2$. As $2 \cdot 10 - 2 = 18$, using the method of Theorem 2.2.8, apart from the point at ∞, it is enough to choose the following 18 evaluation points:*

$$\{0,1\}, \{w, w^2\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^5\}, \{\gamma, \gamma^2, \gamma^4, \gamma^8\}, \{\gamma^3, \gamma^6, \gamma^{12}, \gamma^9\}.$$

Using Proposition 2.3.1 and the method of Theorem 2.2.8 we obtain existence of an explicit formula for multiplying two 10-term polynomials over $\mathbb{F}_2$ which gives

$$M_2(10) \leq 1 + 2 + 3 + 6 + 6 + 9 + 9 = 36.$$

Next we consider 11-term polynomials over $\mathbb{F}_2$. We have $2 \cdot 11 - 2 = 20$ and apart from the point at ∞ we consider the following 20 points:

$$\{0,1\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^5\}, \{\gamma, \gamma^2, \gamma^4, \gamma^8\}, \{\gamma^3, \gamma^6, \gamma^{12}, \gamma^9\}, \{\gamma^7, \gamma^{14}, \gamma^{13}, \gamma^{11}\}.$$

Hence we obtain

$$M_2(11) \leq 1 + 2 + 6 + 6 + 9 + 9 + 9 = 42.$$

Finally we consider 12*-term polynomials over* $\mathbb{F}_2$*. We have* $2 \cdot 12 - 2 = 22$ *and apart from the point at* ∞ *we consider the following* 22 *points:*

$$\{0,1\},\{w,w^2\},\{\alpha,\alpha^2,\alpha^4\},\{\alpha^3,\alpha^6,\alpha^5\},\{\gamma,\gamma^2,\gamma^4,\gamma^8\},\{\gamma^3,\gamma^6,\gamma^{12},\gamma^9\},\{\gamma^7,\gamma^{14},\gamma^{13},\gamma^{11}\}.$$

Then we get

$$M_2(12) \leq 1+2+3+7+7+9+9+9 = 45.$$

In order to attain the bounds given in [4] we will use the following Corollary of Theorem 2.2.8. The proof can be seen in in [2] and it is described for $q \geq 2n-1$. However, one can easily modify the proof in [2] for our case by working in a large enough field extension.

Corollary 2.3.3 *Let $a(x)$ and $b(x)$ be n-term polynomials over $\mathbb{F}_q$. If ℓ coefficients of the product $a(x) \cdot b(x)$ is known then $(2n-2-\ell)$ elements of $\mathbb{F}_q$ are enough for the method described in Theorem 2.2.8 to find a formula for $a(x) \cdot b(x)$.*

The following proposition will be used for further improvements.

Proposition 2.3.4 *Let $a(x) = \sum_{i=0}^{n-1} a_i x^i$ and $b(x) = \sum_{i=0}^{n-1} b_i x^i$ be n-term polynomials over $\mathbb{F}_q$ and let $c(x) = \sum_{i=0}^{2n-2} c_i x^i$ be their product. It always holds*
$c_0 = a_0 b_0, \quad c_1 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1,$
$c_2 = (a_0 + a_2)(b_0 + b_2) - a_0 b_0 - a_2 b_2 + a_1 b_1$
$c_{2n-2} = a_{n-1} b_{n-1}, \quad c_{2n-3} = (a_{n-1} + a_{n-2})(b_{n-1} + b_{n-2}) - a_{n-1} b_{n-1} - a_{n-2} b_{n-2}$ $c_{2n-4} = (a_{n-1} + a_{n-3})(b_{n-1} + b_{n-3}) - a_{n-1} b_{n-1} - a_{n-3} b_{n-3} + a_{n-2} b_{n-2}$

Proof of the proposition is obvious. Note that c_0 and c_{2n-2} are the products corresponding to evaluations at 0 and ∞. After using those points the cost of each of c_1 and c_{2n-3} is 2 multiplications. Similarly, the cost of each of c_2 and c_{2n-4} is 2 multiplications when we use c_0, c_1, c_{2n-2} and c_{2n-3}. The following example shows the use of Corollary 5.2.5 in the method of interpolation.

Example 2.3.5 *Consider* 5*-term polynomial multiplication over* $\mathbb{F}_7$*. Since* $7 < 2.5 - 2$*, we have* $M_7(5) > 2.5 - 1 = 9$*. In Example 2.2.5 we found that* $M_7(5) \leq 11$*. Now we will find the* *optimal bound $M_7(5) = 10$ by using interpolation and Corollary 5.2.5. Now using the points of $\mathbb{F}_7$, ∞ and the known coefficient $c_1 = (a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1$ in the equation*

$$(a_0 + a_1x + ... + a_4x^4)(b_0 + b_1x + ... + b_4x^4) = c_0 + c_1x + ... + c_8x^8.$$

we get:

$$\begin{aligned}
x = 0 \Rightarrow &\quad a_0b_0 = c_0\\
x = 1 \Rightarrow &\quad (a_0 + a_1 + ... + a_4)(b_0 + b_1 + ... + b_4) = (c_0 + c_1 + ... + c_8)\\
x = 2 \Rightarrow &\quad (a_0 + 2a_1 + ... + 2^4a_4)(b_0 + 2b_1 + ... + 2^4b_4) = (c_0 + 2c_1 + ... + 2^8c_8)\\
x = 3 \Rightarrow &\quad (a_0 + 3a_1 + ... + 3^4a_4)(b_0 + 3b_1 + ... + 3^4b_4) = (c_0 + 3c_1 + ... + 3^8c_8)\\
x = 4 \Rightarrow &\quad (a_0 + 4a_1 + ... + 4^4a_4)(b_0 + 4b_1 + ... + 4^4b_4) = (c_0 + 4c_1 + ... + 4^8c_8)\\
x = 5 \Rightarrow &\quad (a_0 + 5a_1 + ... + 5^4a_4)(b_0 + 5b_1 + ... + 5^4b_4) = (c_0 + 5c_1 + ... + 5^8c_8)\\
x = 6 \Rightarrow &\quad (a_0 + 6a_1 + ... + 6^4a_4)(b_0 + 6b_1 + ... + 6^4b_4) = (c_0 + 6c_1 + ... + 6^8c_8)\\
x = \infty \Rightarrow &\quad a_4b_4 = c_8
\end{aligned}$$

and $c_1 = (a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1$. If we construct the system of linear equations in $\mathbb{F}_7$, like in Example 2.2.5, we see that matrix of the linear system is invertible. Therefore we get $M_7(5) = 10$, since 7 multiplications comes from elements of $\mathbb{F}_7$, 1 multiplication is counted for ∞ and 2 multiplications are counted for c_1.

Now consider again polynomials over $\mathbb{F}_2$. First $n = 10$. As $2 \cdot 10 - 2 = 18$, using the method of Theorem 2.2.8, apart from the point at ∞, it is enough to choose 18 evaluation points. If we use c_{16}, c_{15}, c_1 and c_2 given in Proposition 2.3.4, it is enough to choose $18 - 4 = 14$ evaluation points. Let us choose

$$\{0, 1\}, \{w, w^2\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^5\}, \{\gamma, \gamma^2, \gamma^4, \gamma^8\}$$

which gives $M_2(10) \leq 1 + 2 + 3 + 6 + 6 + 9 + 8 = 35$. For $n = 11$ we use

$$\{0, 1\}, \{w, w^2\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^5\}, \{\gamma, \gamma^2, \gamma^4, \gamma^8\}, \{\gamma^3, \gamma^6, \gamma^{12}, \gamma^9\}$$

together with c_1 and c_{19}. Then it is obtained that $M_2(11) \leq 40$ since c_1 and c_{19} cost 4 multiplications. Similarly, if we use c_{16}, c_{15}, c_1 and c_2 instead of using points in the set $\{\gamma^7, \gamma^{14}, \gamma^{13}, \gamma^{11}\}$ in the computation of $M_2(12)$ we decreased the number of multiplications from 45 to 44 since the cost of c_{16}, c_{15}, c_1 and c_2 is 8 while the cost of $\{\gamma^7, \gamma^{14}, \gamma^{13}, \gamma^{11}\}$ is 9 multiplications.

CHAPTER 3

IMPROVED POLYNOMIAL MULTIPLICATION FORMULAE OVER $\mathbb{F}_2$ USING CHINESE REMAINDER THEOREM

Let $n, \ell \geq 1$ be integers and $f(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial such that $\ell deg(f(x)) < 2n-1$. We obtain an effective upper bound for the multiplication complexity $M_{f,\ell}(n)$ of n-term polynomials modulo $f(x)^\ell$. We refer to Notation 3.1.1 for a definition of $M_{f,\ell}(n)$. This upper bound allows a better selection of the moduli when CRT is used for polynomial multiplication over $\mathbb{F}_2$ (see Example 3.2.5 below). We get improved formulae to multiply polynomials of small degree over $\mathbb{F}_2$. In particular, we improve the best known multiplication complexities over $\mathbb{F}_2$ in the literature in some cases.

This chapter is organized as follows. We give some background and notation in the next section. In Section 3, we give our upper bound on $M_{f,\ell}(n)$ in Theorem 3.2.2. It depends on a new parameter $\lambda(\ell)$ introduced in Notation 3.2.1. We also give some effective upper bounds on $\lambda(\ell)$ in Proposition 3.2.4. We show that combining these results with CRT algorithm implies new explicit multiplication formulae for n-term polynomials over $\mathbb{F}_2$. In particular we obtain improvements on the best known multiplication complexities bounds over $\mathbb{F}_2$. As examples of the new explicit formulae we present such formulae for 5-term and 9-term polynomials in Section 3.3.

3.1 BACKGROUND

Let $\mathbb{F}_2$ be the field with two elements and $deg(a(x))$ denote the degree of $a(x) \in \mathbb{F}_2[x]$. Unless otherwise stated, all polynomials considered in this chapter are in $\mathbb{F}_2[x]$. Throughout the chapter we fix an integer $n \geq 1$. A polynomial $A(x)$ of the form

$$A(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1}$$

is called an n-term polynomial. $M(n)$ denotes the minimum number of multiplications needed in $\mathbb{F}_2$ in order to multiply two arbitrary n-term polynomials. We note that $M(n)$ is also called *the multiplication complexity of n-term polynomials.*

A crucial idea in [4] is the use of CRT effectively for the design of polynomial multiplication algorithms (see also [11]). We refer to [4], [11] and the references in [4] for further details and other applications of CRT for the design of polynomial multiplication algorithms.

We first introduce some notation. Let $f(x)$ be an irreducible polynomial and $\ell \geq 1$ be an integer such that

$$deg(f(x)^{\ell}) = \ell \; deg(f(x)) < 2n - 1. \tag{3.1}$$

Notation 3.1.1 *For arbitrary n-term polynomials $\sum_{i=0}^{n-1} a_i x^i$ and $\sum_{i=0}^{n-1} b_i x^i$, let $\sum_{i=0}^{deg(f(x)^{\ell})-1} \overline{c_i} x^i$ be the uniquely determined polynomial satisfying*

$$\sum_{i=0}^{deg(f(x)^{\ell})-1} \overline{c_i} x^i = \left(\sum_{i=0}^{n-1} a_i x^i\right)\left(\sum_{i=0}^{n-1} b_i x^i\right) \mod f(x)^{\ell}. \tag{3.2}$$

Let $M_{f,\ell}(n)$ denote the minimum number of multiplications needed in $\mathbb{F}_2$ in order to determine $\sum_{i=0}^{deg(f(x)^{\ell})-1} \overline{c_i} x^i$satisfying (3.2) from arbitrary n-term polynomials $\sum_{i=0}^{n-1} a_i x^i$ and $\sum_{i=0}^{n-1} b_i x^i$. We also call $M_{f,\ell}(n)$ as the multiplication complexity of n-term polynomials modulo $f(x)^{\ell}$.

Let $w \geq 1$ be an integer such that

$$w < 2n - 1. \tag{3.3}$$

Notation 3.1.2 *For n-term polynomials $\sum_{i=0}^{n-1} a_i x^i$ and $\sum_{i=0}^{n-1} b_i x^i$, let $\sum_{i=0}^{2n-2} c_i x^i$ be the polynomial defined by*

$$\sum_{i=0}^{2n-2} c_i x^i = \left(\sum_{i=0}^{n-1} a_i x^i\right)\left(\sum_{i=0}^{n-1} b_i x^i\right). \tag{3.4}$$

Recall that in the literature obtaining the last w coefficients $c_{2n-2}, c_{2n-3}, ..., c_{2n-1-w}$ of $\sum_{i=0}^{n-1} c_i x^i$ defined in (3.4) is referred as multiplication of n-term polynomials $\sum_{i=0}^{n-1} a_i x^i$ and $\sum_{i=0}^{n-1} b_i x^i$ modulo $(x - \infty)^w$ *(see, for example [11, p. 34] or [4], Section 2). Let $M_{(x-\infty),w}(n)$ denote the minimum number of multiplications needed in $\mathbb{F}_2$ in order to obtain the last w coefficients*

$c_{2n-2}, c_{2n-3}, ..., c_{2n-1-w}$ of $\sum_{i=0}^{n-1} c_i x^i$ defined in (3.4) for arbitrary n-term polynomials $\sum_{i=0}^{n-1} a_i x^i$ and $\sum_{i=0}^{n-1} b_i x^i$.

Remark 3.1.3 *The restrictions in (3.1) and (3.3) follow from the following simple observation. Assume that $M_{f,\ell}(n)$ is defined as in Notation 3.1.1 for an irreducible polynomial $f(x)$ and an integer $\ell \geq 1$ not necessarily satisfying (3.1). Similarly assume that $M_{(x-\infty),w}(n)$ is defined as in Notation 3.1.2 also for $w = 2n-1$. If $\ell deg(f(x)) \geq 2n-1$ then $M_{f,\ell}(n) = M(n)$ and hence $M_{f,\ell}(n)$ is superfluous. Similarly, if $w = 2n-1$ then $M_{(x-\infty),w}(n) = M(n)$.*

The method in [4] can be summarized as follows. Let $t \geq 1$ be an integer. Let $f_1(x), ..., f_t(x)$ be distinct irreducible polynomials and $\ell_1, ..., \ell_t$ be positive integers such that for the polynomial $m(x) = \prod_{i=0}^{t} f_i(x)^{\ell_i}$, we have

$$w + deg(m(x)) = w + \sum_{i=1}^{t} \ell_i deg(f_i(x)) \geq 2n-1. \tag{3.5}$$

It follows from CRT algorithm (see [11]), namely using Theorem 1 and Lemma 2 in [4], that we have

$$M(n) \leq M_{(x-\infty),w}(n) + \sum_{i=1}^{t} M_{f_i,\ell_i}(n). \tag{3.6}$$

In [4], the following bound on $M_{f,\ell}(n)$ has been used:

$$M_{f,\ell}(n) \leq M(\ell\ deg(f(x))). \tag{3.7}$$

Our crucial observation is an improvement of the bound (3.7). In the next section we give this improvement.

3.2 IMPROVED $M(n)$

In order to give our improvement on the bound (3.7), we first need to introduce another notation. Recall that unless otherwise stated explicitly, all polynomials considered in this chapter are in $\mathbb{F}_2[x]$.

Notation 3.2.1 *Let $R = \mathbb{F}_2[x]$ be the ring of polynomials over $\mathbb{F}_2$ in variable x, $\ell \geq 1$ be an integer and*

$$\begin{aligned} A(Y) &= a_0(x) + a_1(x)Y + ... + a_{\ell-1}(x)Y^{\ell-1} \\ B(Y) &= b_0(x) + b_1(x)Y + ... + b_{\ell-1}(x)Y^{\ell-1} \end{aligned}$$

be two ℓ-term polynomials in the polynomial ring $R[Y]$ over R. Let $c_0(x), ..., c_{2\ell-2}(x) \in R$ be given by

$$c_0(x) + c_1(x)Y + ... + c_{2\ell-2}(x)Y^{2\ell-2} = A(Y)B(Y). \tag{3.8}$$

Note that the identity in (3.8) is a polynomial identity in $R[Y]$ and the polynomials $c_0(x)$, $c_1(x)$, $c_2(x)$, …, $c_{2\ell-2}(x) \in R$ are the coefficients of the polynomial $A(Y)B(Y) \in R[Y]$. Let $\lambda(\ell)$ denote the minimum number of multiplications needed in R in order to determine the coefficients $c_0(x), c_1(x), ..., c_{\ell-1}(x)$ defined in (3.8) for arbitrary ℓ-term polynomials $A(Y)$ and $B(Y)$.

In the next theorem, using Notation (3.2.1), we give our improvement of the bound (3.7).

Theorem 3.2.2 *Let $f(x)$ be an irreducible polynomial and $\ell \geq 1$ be an integer such that $\ell\ deg(f(x)) < 2n - 1$. We have*

$$M_{f,\ell}(n) \leq \lambda(\ell)M(deg(f)). \tag{3.9}$$

Proof. Let $A(x)$ be an n-term polynomial and $\overline{A}(x)$ be the uniquely determined polynomial of degree strictly less than $\ell\ deg(f(x))$ such that $\overline{A}(x) \equiv A(x) \mod f(x)^\ell$. Let $a_0(x), a_1(x), ..., a_{\ell-1}(x)$ be uniquely determined polynomials such that

$$\overline{A}(x) = a_0(x) + a_1(x)f(x) + ... + a_{\ell-1}(x)f(x)^{\ell-1}$$

and $deg(a_i(x)) < deg(f(x))$ for $0 \leq i \leq \ell - 1$. Let $\overline{B}(x)$ and $b_0(x), b_1(x), ..., b_{\ell-1}(x)$ be defined similarly. Note that $a_i(x)$ and $b_j(x)$, are obtained without any multiplication, where $0 \leq i, j \leq \ell - 1$. Let $R = \mathbb{F}_2[x]$ and $\widetilde{A}(Y)$ and $\widetilde{B}(Y)$ be the polynomials in $R[Y]$ such that

$$\begin{aligned}\widetilde{A}(Y) &= a_0(x) + a_1(x)Y + ... + a_{\ell-1}(x)Y^{\ell-1}\\ \widetilde{B}(Y) &= b_0(x) + b_1(x)Y + ... + b_{\ell-1}(x)Y^{\ell-1}.\end{aligned}$$

Define $\widetilde{C}(Y) = \widetilde{A}(Y)\widetilde{B}(Y)$ and let $c_0(x), c_1(x), ..., c_{\ell-1}(x) \in R$ be the first ℓ coefficients of $\widetilde{C}(Y)$. Since the coefficients of $A(x)B(x) \mod f(x)^\ell$ is the same as the coefficients of $\widetilde{A}(Y)\widetilde{B}(Y) \mod Y^\ell$ and $Y^i \equiv 0 \mod Y^\ell$ for $i \geq \ell$, $M_{f,\ell}(n)$ refers to computing the first ℓ coefficients of $\widetilde{A}(Y)\widetilde{B}(Y)$. Therefore the first ℓ coefficients $c_0(x), c_1(x), ..., c_{\ell-1}(x)$ can be obtained from $A(x)$ and $B(x)$ with at most $\lambda(\ell)$ multiplications of certain coefficients of $\widetilde{A}(Y)$ and $\widetilde{B}(Y)$ in R. Since each coefficient of $\widetilde{A}(Y)$ and $\widetilde{B}(Y)$ is a $deg(f(x))$-term polynomial over $\mathbb{F}_2$, any multiplication can be done with $M(deg(f(x)))$ multiplications over $\mathbb{F}_2$. ■

Remark 3.2.3 *Let* $1 \leq w < 2n-1$ *be an integer. Recall that the notation* $M_{(x-\infty),w}(n)$ *is given in Notation 3.1.2. It is clear that* $M(1) = 1$*. Using similar methods as in Theorem 3.2.2 we obtain that*

$$M_{(x-\infty),w}(n) \leq \lambda(w)M(1) = \lambda(w).$$

Some effective upper bounds of $\lambda(\ell)$ is given in the following proposition which will be used to get improvements on $M_{f,\ell}(n)$ and $M(n)$.

Proposition 3.2.4 *For an integer* $\ell \geq 1$*, let* $\lambda(\ell)$ *be the integer defined in Notation 3.2.1. We have* $\lambda(3) \leq 5$*,* $\lambda(4) \leq 8$*,* $\lambda(5) \leq 11$*,* $\lambda(6) \leq 15$*,* $\lambda(7) \leq 19$*,* $\lambda(8) \leq 24$*, and* $\lambda(9) \leq 29$*.*

Proof. We give an explicit proof of $\lambda(6) \leq 15$. Let $A(x)$ and $B(x)$ be arbitrary n-term polynomials, $C(x) = A(x)B(x)$ and $c_0, c_1, c_2, c_3, c_4, c_5$ be the first 6 coefficients of $C(x)$. Then

$$\begin{aligned}
c_0 &= D_0\\
c_1 &= D_{01} + D_0 + D_1\\
c_2 &= D_{02} + D_0 + D_1 + D_2\\
c_3 &= D_{03} + D_{12} + D_0 + D_1 + D_2 + D_3\\
c_4 &= D_{04} + D_{13} + D_0 + D_1 + D_2 + D_3 + D_4,\\
c_5 &= D_{05} + D_{14} + D_{23} + D_0 + D_1 + D_2 + D_3 + D_4 + D_5
\end{aligned}$$

where $D_i = a_i b_i$ and $D_{st} = (a_s + a_t)(b_s + b_t)$. Then
$\lambda(6) \leq \#\{D_0, D_1, D_2, D_3, D_4, D_5, D_{01}, D_{02}, D_{03}, D_{04}, D_{05}, D_{12}, D_{13}, D_{14}, D_{23}\} = 15$. We prove the other statements of the proposition similarly. ■

In the next example we illustrate that it is not difficult to obtain an explicit formula giving the bound on $M_{f,\ell}(n)$ implied by Theorem 3.2.2 and Proposition 3.2.4.

Example 3.2.5 *Let* $f(x) = x^2 + x + 1$ *and* $A(x), B(x)$ *be n-term polynomials over* $\mathbb{F}_2$ *with* $n \geq 6$*. In this example, we will obtain an explicit formula giving* $M_{f,3}(n) \leq 15$*. Let* $\overline{A}(x)$ *be the uniquely determined polynomial of degree strictly less than 6 such that* $\overline{A}(x) \equiv A(x) \mod f^3$*, and assume that* $\overline{A}(x) = \sum_{i=0}^{5} a_i x^i$*. Using the equations* $f = x^2 + x + 1$*,* $x^2 = f + x + 1$*,* $x^3 = xf + f + 1$*,* $x^4 = f^2 + f + x$ *and* $x^5 = (f^2 + f + 1)x + f + 1$ *we get*

$$\overline{A}(x) = a_0(x) + a_1(x)f(x) + a_2 f^2(x) \text{ and } deg(a_i(x)) < deg(f(x))$$

where

$$\begin{aligned}a_0(x) &= (a_2 + a_1 + a_5 + a_4)x + a_0 + a_5 + a_2 + a_3,\\ a_1(x) &= (a_3 + a_5)x + a_2 + a_4 + a_3 + a_5,\\ a_2(x) &= a_4 + a_5 x.\end{aligned}$$

Let $\overline{B}(x)$ and $b_0(x), b_1(x), b_2(x)$ be defined similarly. Let $R = \mathbb{F}_2[x]$ and $\widetilde{A}(Y), \widetilde{B}(Y)$ be polynomials in $R[Y]$ such that

$$\begin{aligned}\widetilde{A}(Y) &= a_0(x) + a_1(x)Y + a_2(x)Y^2,\\ \widetilde{B}(Y) &= b_0(x) + b_1(x)Y + b_2(x)Y^2.\end{aligned}$$

Let $\widetilde{C}(Y) = \widetilde{A}(Y)\widetilde{B}(Y)$ and $c_0(x), c_1(x), c_2(x) \in R$ be the first 3 coefficients of $\widetilde{C}(Y)$. Since the coefficients of $A(x)B(x) \mod f(x)^3$ are the same as the coefficients of $\widetilde{A}(Y)\widetilde{B}(Y) \mod Y^3$ and $Y^i \equiv 0 \mod Y^3$ for $i \geq 3$, $M_{f,3}(n)$ refers to computing the first 3 coefficients of $\widetilde{A}(Y)\widetilde{B}(Y)$. Those coefficients are given by

$$\begin{aligned}c_0(x) &= a_0(x)b_0(x),\\ c_1(x) &= (a_0(x) + a_1(x))(b_0(x) + b_1(x)) +\\ &\quad a_0(x)b_0(x) + a_1(x)b_1(x),\\ c_2(x) &= (a_0(x) + a_2(x))(b_0(x) + b_2(x)) +\\ &\quad a_0(x)b_0(x) + a_1(x)b_1(x) + a_2(x)b_2(x).\end{aligned} \tag{3.10}$$

In (3.10), the only required multiplications are:

$$\begin{aligned}&a_0(x)b_0(x),\\ &a_1(x)b_1(x),\\ &a_2(x)b_2(x),\\ &(a_0(x) + a_1(x))(b_0(x) + b_1(x)),\\ &(a_0(x) + a_2(x))(b_0(x) + b_2(x)).\end{aligned}$$

There are 5 multiplications and each of them is a multiplication of 2-term polynomials over $\mathbb{F}_2$. Using the fact that $M(2) = 3$ we obtain that $M_{f,3}(n) \leq 5 \cdot 3 = 15$.

In Table 3.1, we list some improvements on the upper bound on $M_{f,\ell}(n)$ compared to the corresponding bound of [4]. Combining Theorem 3.2.2, Remark 4.1.5, Proposition 3.2.4 and (4.2) we obtain improvements on the upper bounds $M(n)$. In Table 3.2 we list some of our improvements.

For the range of indices i and j in Table 3.1 and Table 3.2, f_{ij} denotes an irreducible polynomial of degree i over $\mathbb{F}_2$ which are defined as follows: $f_{11} = x, f_{12} = x+1, f_{21} = x^2+x+1, f_{31} =$

$x^3+x+1, f_{32} = x^3+x^2+1, f_{41} = x^4+x+1, f_{42} = x^4+x^3+1, f_{43} = x^4+x^3+x^2+x+1, f_{51} = x^5+x^2+1$.

For each n in Table 3.2, we have selected the moduli polynomials such that the inequality in (3.5) is satisfied and the upper bound in (4.2) is as small as possible.

Table 3.1: Upper Bounds for $M_{f,\ell}(n)$ over $\mathbb{F}_2$

f	l	$M_{f,\ell}(n)$[4]	New $M_{f,\ell}(n)$
f_{11}, f_{12}	3	6	5
f_{11}, f_{12}	4	9	8
f_{11}, f_{12}	5	13	11
f_{11}, f_{12}	6	17	15
f_{11}, f_{12}	7	22	19
f_{11}, f_{12}	8	26	24
f_{11}, f_{12}	9	31	29
f_{21}	3	17	15
f_{21}	4	26	24
f_{21}	5	35	33
f_{31}, f_{32}	3	31	30

Remark 3.2.6 *In Table 3.2 for $n = 5$ we have*

$$\begin{aligned} M(5) &\leq M_{(x-\infty),3}(5) + M_{f_{11},3}(5) + M_{f_{12},1}(5) + M_{f_{21},1}(5) \\ &\leq 5 + 5 + 1 + 3 = 14. \end{aligned}$$

We observe that the parts of the algorithm corresponding to $M_{(x-\infty),3}(5)$ and $M_{f_{11},3}(5)$ use a common product (which is a_2b_2 in the corresponding explicit formula in the Appendix), so the upper bound on $M(5)$ is decreased by one. We refer to the Appendix for the complete explicit formula.

Remark 3.2.7 *For $n = 5$, although the multiplication complexity for the proposed algorithm is the same with the corresponding one in [7], the number of additions is improved. Namely, the number of additions in [7] for 5-term polynomials is 72 while the proposed formula contains 62 additions. Similarly, for $n = 7$, although the upper bounds on the multiplication complexities are the same, we improve the number of additions from 216 to 182. This improvement in the number of additions follows from using a different set of the moduli polynomials for $n = 7$.*

Table 3.2: Upper Bounds for $M(n)$ over $\mathbb{F}_2$

n	$M(n)$[7]	$M(n)$[4]	New $M(n)$	Moduli polynomials
2	3	3	3	$(x-\infty), f_{11}, f_{12}$
3	6	6	6	$(x-\infty), f_{11}, f_{12}, f_{21}$
4	9	9	9	$(x-\infty), f_{11}^2, f_{12}^2, f_{21}$
5	13	14	13*	$(x-\infty)^3, f_{11}^3, f_{12}, f_{21}$
6	17	18	18	$(x-\infty)^2, f_{11}^2, f_{12}^2, f_{21}, f_{31}$
7	22	22	22*	$(x-\infty)^3, f_{11}^3, f_{12}^2, f_{21}, f_{31}$
8	27	26	26	$(x-\infty)^3, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}$
9	34	31	30*	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{21}, f_{31}, f_{32}$
10	39	35	35	$(x-\infty)^3, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}$
11	46	40	39*	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{21}, f_{31}, f_{32}, f_{41}$
12	51	44	44	$(x-\infty)^3, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}$
13	60	49	48*	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}$
14	66	53	53	$(x-\infty)^3, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}$
15	75	59	57*	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}$
16	81	64	63*	$(x-\infty)^3, f_{11}^4, f_{12}^4, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}$
17	94	69	68*	$(x-\infty)^3, f_{11}^3, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}, f_{51}$
18	102	75	73*	$(x-\infty)^4, f_{11}^3, f_{12}^3, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}, f_{51}$

Multiplications listed in Table 3.2 occur quite often in practical situations. For example, multiplying two 9^ℓ-term polynomials recursively using our 9-term algorithm (which is also given explicitly in the Appendix) requires $(30)^\ell$ multiplications while the algorithms in [4] and [7] requires $(31)^\ell$ and $(34)^\ell$. If $\ell = 3$, this means that 27000 multiplications using our algorithm, while 29791 and 39304 multiplications using algorithms in [4] and [7], respectively.

In Table 3.2, we list our improvements up to 18-term polynomials since the corresponding tables in [4] and [7] give values only up to 18-term polynomials. In fact, our improvements in Table 3.1 yield improved $M(n)$ for $n > 18$ as well. For example, if the moduli polynomials $(x-\infty)^4, f_{11}^3, f_{12}^3, f_{21}^2, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}, f_{51}$ are used, then the proposed method gives $M(19) \leq 79$ while the method in [4] gives $M(19) \leq 81$ and the formulae in [7] gives $M(19) \leq 111$.

3.3 EXPLICIT FORMULAE FOR $n = 5$ AND $n = 9$

In the section, we give explicit formulae having the bounds of Table 3.2 for $n = 5$ and $n = 9$.

First we begin with an explicit formula for multiplying two arbitrary 5-term polynomials over $\mathbb{F}_2$. Let $A(x) = \sum_{i=0}^{4} a_i x^i$ and $B(x) = \sum_{i=0}^{4} b_i x^i$ be polynomials over $\mathbb{F}_2$. Let $C(x) = \sum_{i=0}^{8} c_i x^i \in \mathbb{F}_2[x]$ be the polynomial defined by $C(x) = A(x)B(x)$. Using our method, we obtain the following explicit formula consisting of the 13 multiplications. We first define the multiplications m_i for $1 \leq i \leq 13$ and then we give the formula for obtaining the coefficients of the polynomial $C(x)$ using these multiplications.

$m_1 = a_0 b_0,$

$m_2 = a_1 b_1,$

$m_3 = a_2 b_2,$

$m_4 = a_3 b_3,$

$m_5 = a_4 b_4,$

$m_6 = (a_0 + a_1)(b_0 + b_1),$

$m_7 = (a_0 + a_2)(b_0 + b_2),$

$m_8 = (a_2 + a_4)(b_2 + b_4),$

$m_9 = (a_3 + a_4)(b_3 + b_4),$

$m_{10} = (a_0 + a_2 + a_3)(b_0 + b_2 + b_3)$

$m_{11} = (a_1 + a_2 + a_4)(b_1 + b_2 + b_4),$

$m_{12} = (a_0 + a_3 + a_1 + a_4)(b_0 + b_3 + b_1 + b_4),$

$m_{13} = (a_0 + a_1 + a_2 + a_3 + a_4)(b_0 + b_1 + b_2 + b_3 + b_4).$

$c_0 = m_1,$

$c_1 = m_6 + m_1 + m_2,$

$c_2 = m_7 + m_1 + m_3 + m_2,$

$c_3 = m_1 + m_{13} + m_{12} + m_{10} + m_8 + m_3 + m_5 + m_4$

$c_4 = m_6 + m_1 + m_2 + m_{13} + m_{10} + m_{11} + m_9 + m_5 + m_4,$

$c_5 = m_7 + m_1 + m_3 + m_2 + m_{13} + m_{11} + m_{12} + m_5$

$c_6 = m_8 + m_3 + m_5 + m_4,$

$c_7 = m_9 + m_4 + m_5,$

$c_8 = m_5.$

Next we give a formula for multiplying two arbitrary 9-term polynomials over $\mathbb{F}_2$ with 30 multiplications. Similarly we consider $A(x) = \sum_{i=0}^{8} a_i x^i$ and $B(x) = \sum_{i=0}^{8} b_i x^i$ as two arbitrary 9-term polynomials over $\mathbb{F}_2$ and we define $C(x) = \sum_{i=0}^{16} c_i x^i$ as their product. The formula is given after the definition of 30 multiplications m_i, for $1 \leq i \leq 30$.

$m_1 = (a_2 + a_7 + a_6 + a_3 + a_0 + a_1 + a_5 + a_4 + a_8)(b_2 + b_7 + b_6 + b_3 + b_0 + b_1 + b_5 + b_4 + b_8)$,

$m_2 = (a_2 + a_6 + a_0 + a_4 + a_8)(b_2 + b_6 + b_0 + b_4 + b_8)$,

$m_3 = (a_1 + a_8 + a_5 + a_2 + a_3)(b_1 + b_8 + b_5 + b_2 + b_3)$,

$m_4 = (a_0 + a_2 + a_5 + a_8 + a_3 + a_6)(b_0 + b_2 + b_5 + b_8 + b_3 + b_6)$,

$m_5 = (a_0 + a_3 + a_6 + a_1 + a_4 + a_7)(b_0 + b_3 + b_6 + b_1 + b_4 + b_7)$,

$m_6 = (a_0 + a_3 + a_7 + a_4 + a_5)(b_0 + b_3 + b_7 + b_4 + b_5)$,

$m_7 = (a_1 + a_8 + a_3 + a_2 + a_6)(b_1 + b_8 + b_3 + b_2 + b_6)$,

$m_8 = (a_2 + a_5 + a_4 + a_6)(b_2 + b_5 + b_4 + b_6)$,

$m_9 = (a_2 + a_6 + a_3 + a_4)(b_2 + b_6 + b_3 + b_4)$,

$m_{10} = (a_1 + a_7 + a_5 + a_3)(b_1 + b_7 + b_5 + b_3)$,

$m_{11} = (a_0 + a_6 + a_7 + a_1 + a_4 + a_8)(b_0 + b_6 + b_7 + b_1 + b_4 + b_8)$,

$m_{12} = (a_0 + a_3 + a_6 + a_5 + a_7)(b_0 + b_3 + b_6 + b_5 + b_7)$,

$m_{13} = (a_0 + a_1 + a_5 + a_4 + a_8)(b_0 + b_1 + b_5 + b_4 + b_8)$,

$m_{14} = (a_1 + a_4 + a_7 + a_2 + a_5 + a_8)(b_1 + b_4 + b_7 + b_2 + b_5 + b_8)$,

$m_{15} = (a_0 + a_3 + a_7 + a_1 + a_8 + a_6)(b_0 + b_3 + b_7 + b_1 + b_8 + b_6)$,

$m_{16} = (a_1 + a_4 + a_8 + a_3 + a_5)(b_1 + b_4 + b_8 + b_3 + b_5)$,

$m_{17} = (a_0 + a_3 + a_7 + a_2 + a_4)(b_0 + b_3 + b_7 + b_2 + b_4)$,

$m_{18} = (a_1 + a_4 + a_8 + a_5 + a_6)(b_1 + b_4 + b_8 + b_5 + b_6)$,

$m_{19} = (a_0 + a_7 + a_5 + a_2 + a_6)(b_0 + b_7 + b_5 + b_2 + b_6)$,

$m_{20} = (a_2 + a_7 + a_6 + a_3)(b_2 + b_7 + b_6 + b_3)$,

$m_{21} = (a_6 + a_8)(b_6 + b_8)$,

$m_{22} = (a_0 + a_2)(b_0 + b_2)$,

$m_{23} = (a_0 + a_1)(b_0 + b_1)$,

$m_{24} = a_0 b_0$,

$m_{25} = a_1 b_1$,

$m_{26} = a_7 b_7$,

$m_{27} = (a_7 + a_8)(b_7 + b_8)$,

$m_{28} = a_6 b_6$,

$m_{29} = a_8 b_8$,

$m_{30} = a_2 b_2$.

$c_0 = m_{24},$

$c_1 = m_{23} + m_{24} + m_{25},$

$c_2 = m_{22} + m_{24} + m_{30} + m_{25},$

$c_3 = m_{29} + m_{18} + m_3 + m_{16} + m_8 + m_7 + m_6 + m_{30} + m_{22} + m_{23} + m_{13} + m_{20} + m_{10} + m_{14} + m_{12} + m_4 + m_{27} + m_{21} + m_{28},$

$c_4 = m_5 + m_4 + m_{11} + m_{12} + m_7 + m_3 + m_9 + m_{15} + m_{10} + m_{23} + m_{24} + m_{25} + m_2 + m_{21} + m_{28} + m_{29} + m_{26},$

$c_5 = m_{27} + m_{26} + m_{29} + m_1 + m_{10} + m_{22} + m_{24} + m_{30} + m_{25} + m_2 + m_4 + m_{14} + m_{15} + m_6 + m_{19} + m_{17} + m_{12} + m_{16},$

$c_6 = m_{27} + m_{13} + m_{20} + m_{22} + m_{24} + m_{30} + m_5 + m_4 + m_{15} + m_6 + m_{19} + m_{23} + m_2 + m_{21} + m_{28},$

$c_7 = m_{21} + m_{28} + m_{29} + m_{26} + m_{24} + m_1 + m_{16} + m_8 + m_{12} + m_7 + m_{15} + m_6 + m_{19},$

$c_8 = m_1 + m_{24} + m_{25} + m_{11} + m_{16} + m_8 + m_3 + m_{19} + m_{15} + m_{18} + m_{23} + m_{27} + m_{26} + m_{29},$

$c_9 = m_{22} + m_{24} + m_{30} + m_{25} + m_1 + m_{17} + m_{12} + m_8 + m_{11} + m_3 + m_9 + m_{19} + m_6 + m_{29},$

$c_{10} = m_{13} + m_1 + m_{20} + m_{10} + m_{22} + m_{30} + m_{23} + m_4 + m_{14} + m_{17} + m_{12} + m_8 + m_{11} + m_{21} + m_{28} + m_{29} + m_{27},$

$c_{11} = m_{17} + m_{12} + m_8 + m_{11} + m_{18} + m_6 + m_3 + m_1 + m_{10} + m_5 + m_4 + m_{23} + m_{24} + m_{25} + m_2 + m_{21} + m_{28} + m_{29} + m_{26},$

$c_{12} = m_{27} + m_{26} + m_{29} + m_9 + m_{15} + m_6 + m_{18} + m_{11} + m_7 + m_{17} + m_{16} + m_4 + m_{14} + m_2 + m_{10} + m_{22} + m_{24} + m_{30} + m_{25},$

$c_{13} = m_9 + m_{19} + m_3 + m_{16} + m_{17} + m_6 + m_{30} + m_{22} + m_{24} + m_{23} + m_1 + m_{13} + m_{20} + m_2 + m_{12} + m_5 + m_4 + m_{27} + m_{21} + m_{28},$

$c_{14} = m_{21} + m_{28} + m_{29} + m_{26},$

$c_{15} = m_{27} + m_{26} + m_{29},$

$c_{16} = m_{29}.$

CHAPTER 4

EFFICIENT MULTIPLICATION in $\mathbb{F}_{3^{\ell m}}$, $m \geq 1$ AND $5 \leq \ell \leq 18$

The finite fields of characteristic three are useful for pairing-based cryptography. Therefore, special attention has been given to $\mathbb{F}_{3^m}$, recently. The elements of $\mathbb{F}_{3^m}$ can be represented by at most $(m-1)$ degree polynomials over $\mathbb{F}_3$. To multiply elements of $\mathbb{F}_{3^m}$ one can use Karatsuba method [5] or Montgomery formulae [7], which are among the main algorithms used in every finite field. On the other hand, for finite fields of fixed characteristics, there are other methods that give more efficient algorithms for polynomial multiplication than Karatsuba and Montgomery in some cases. Some of those methods are Chinese Remainder Theorem (CRT) method [11] and Discrete Fourier Transform (DFT) method. In [12, 13], using DFT method, multiplication formula in [14] for $\mathbb{F}_{3^{6m}}$ is improved.

In this chapter, using a method based on CRT for polynomial multiplication over $\mathbb{F}_3$ and suitable reductions, we obtain an efficient multiplication method for finite fields of characteristic 3. For $5 \leq \ell \leq 18$, we show that our method gives canonical multiplication formulae over $\mathbb{F}_{3^{\ell m}}$ for any $m \geq 1$ with the best multiplicative complexity improving the bounds in [7]. Moreover, we give explicit formula in the case $\mathbb{F}_{3^{6\cdot 97}}$.

The rest of this chapter is organized as follows. In Section 2, we introduce our method. Applying our method we obtain explicit formulae in Section 3. We also compare our results with the previous results in Section 3. We conclude this chapter in Section 4.

4.1 THE METHOD

Let $n \geq 1$ be an integer. Let $\mathbb{F}_q$ be a finite field with q elements where $q = 3^n$. Unless stated otherwise, all polynomials considered here are in $\mathbb{F}_3[x]$. A polynomial $A(x)$ of the form

$$A(x) = a_0 + a_1 x + ... + a_{n-1}x^{n-1}, \ a_{n-1} \neq 0$$

is called an n-term polynomial. $M(n)$ denotes the minimum number of multiplications needed in $\mathbb{F}_3$ in order to multiply two arbitrary n-term polynomials. We note that $M(n)$ is also called multiplicative complexity of n-term polynomials. Let $n \geq 1$ be an integer, $f(x)$ be an irreducible polynomial and $\ell \geq 1$ be an integer such that

$$\ell \ deg(f(x)) < 2n - 1.$$

Let $A(x)$ and $B(x)$ be two arbitrary n-term polynomials, $C(x) = A(x)B(x)$ and $\overline{A}(x), \overline{B}(x), \overline{C}(x)$ be the uniquely determined polynomials of degree strictly less than $\ell \ deg(f(x))$ such that

$$\overline{A}(x) \equiv A(x) \bmod f(x)^\ell, \ \overline{B}(x) \equiv B(x) \bmod f(x)^\ell, \ \overline{C}(x) \equiv C(x) \bmod f(x)^\ell.$$

Notation 4.1.1 *Let $M_{f,\ell}(n)$ denote the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain $\overline{C}(x)$ from given n-term polynomials $A(x)$ and $B(x)$. Obtaining such $\overline{C}(x)$ from $A(x)$ and $B(x)$ is called multiplication of n-term polynomials modulo $f(x)^\ell$.*

Let $1 \leq w \leq 2n - 2$ be an integer and $C(x) = c_0 + c_1 x + ... + c_{2n-2}x^{2n-2}$. Obtaining the last w coefficients $c_{2n-2}, c_{2n-3}, ..., c_{2n-1-w}$ of $C(x)$ is defined as the multiplication of n-term polynomials modulo $(x - \infty)^w$ [11, 4].

Notation 4.1.2 *Let $M_{(x-\infty),w}(n)$ denote the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain $c_{2n-2}, c_{2n-3}, ..., c_{2n-1-w}$ from given n-term polynomials $A(x)$ and $B(x)$.*

CRT method for finite field polynomial multiplication can be summarized as follows. For $1 \leq i \leq t$, let $m_i(x) = f_i(x)^{\ell_i}$ be the ℓ_i-th power ($\ell_i \geq 1$) of an irreducible polynomial $f_i(x)$ such that $deg(m(x)) \geq 2n - 1$ where $m(x) = \prod_{i=1}^{t} m_i(x)$. Assume that $f_1(x), ..., f_t(x)$ are distinct. Let $w \geq 1$ be an integer which corresponds to multiplication modulo $(x - \infty)^w$ (see [4] and [11, p. 34]). It follows from CRT algorithm that if

$$w + \sum_{i=1}^{t} \ell_i \ deg(f_i(x)) \geq 2n - 1 \tag{4.1}$$

then

$$M(n) \leq M_{(x-\infty),w}(n) + \sum_{i=1}^{t} M_{f,\ell}(n). \tag{4.2}$$

The value of $M_{f,\ell}(n)$ can be bounded from above by $M(deg(f^{\ell})) \leq M(\ell \cdot deg(f))$. For example in [4], $M_{f,\ell}(n) \leq M(\ell \cdot deg(f))$ is used for binary fields. In Chapter 3, we improved the estimate of $M_{f,\ell}(n)$ for the binary field $\mathbb{F}_2$. The same techniques also work for any finite field $\mathbb{F}_q$, in particular for $\mathbb{F}_3$. Before giving the improvement, we give the following definition.

Definition 4.1.3 *Let $R = \mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$ in variable x, $\ell \geq 1$ be an integer and*

$$A(Y) = a_0(x) + a_1(x)Y + ... + a_{\ell-1}(x)Y^{\ell-1}, \; B(Y) = b_0(x) + b_1(x)Y + ... + b_{\ell-1}(x)Y^{\ell-1}$$

be two ℓ-term polynomials in the polynomial ring $R[Y]$ over R. Let $c_0(x), ..., c_{2\ell-2}(x) \in R$ be given by

$$c_0(x) + c_1(x)Y + ... + c_{2\ell-2}(x)Y^{2\ell-2} = A(Y)B(Y).$$

Let $\lambda(\ell)$ denote the minimum number of multiplications needed in R in order to obtain $c_0(x), c_1(x), ..., c_{\ell-1}(x)$.

For the sake of completeness we prefer to give the following theorem which is given in Chapter 3.

Theorem 4.1.4 *Let $f(x)$ be an irreducible polynomial and $\ell \geq 1$ be an integer such that $\ell \; deg(f(x)) < 2n - 1$. We have*

$$M_{f,\ell}(n) \leq \lambda(\ell)M(deg(f)). \tag{4.3}$$

Remark 4.1.5 *Let $1 \leq w \leq 2n-1$ be an integer. Recall that the notation $M_{(x-\infty),w}(n)$ is given in Notation 4.1.2. It is clear that $M(1) = 1$. Using similar methods as in Theorem 4.1.4 we also obtain that*

$$M_{(x-\infty),w}(n) \leq \lambda(w)M(1) = \lambda(w).$$

Corollary 4.1.6 *$M_{x,w}(n)$ corresponds to computing the first w coefficients $c_0, c_1, ..., c_{w-1}$ of $c(x)$ and $M_{x,w}(n) = M_{(x-\infty),w}(n) \leq \lambda(w)$.*

Some effective upper bounds for $\lambda(\ell)$ is given in the following lemma which contributes to improvements on $M_{f,\ell}(n)$.

Proposition 4.1.7 *$\lambda(3) \leq 5$, $\lambda(4) \leq 8$, $\lambda(5) \leq 11$, $\lambda(6) \leq 15$, $\lambda(7) \leq 19$, $\lambda(8) \leq 24$, and $\lambda(9) \leq 29$.*

Proof. We use a Karatsuba type method (cf., for example in [9]). Here we present an explicit proof of $\lambda(3) \leq 5$ only. The other statements can be proved similarly (see also [9]). Let $A(x)$ and $B(x)$ be arbitrary n-term polynomials, $C(x) = A(x)B(x)$ and c_0, c_1, c_2 be the first 3 coefficients of $C(x)$. Then

$$\begin{aligned} c_0 &= D_0 \\ c_1 &= D_{01} - D_0 - D_1 \\ c_2 &= D_{02} + D_1 - D_0 - D_2 \end{aligned}$$

where $D_i = a_i b_i$ and $D_{st} = (a_s + a_t)(b_s + b_t)$. Then

$$\lambda(3) \leq \#\{D_0, D_1, D_2, D_{01}, D_{02}\} = 5.$$

This completes the proof of $\lambda(3) \leq 5$. ■

In Table 4.1, we list some improvements on the upper bound on $M_{f,\ell}(n)$. Note that computation of $M_{f,\ell}(n)$ can be done by first computing the polynomial multiplication then reducing the result modulo f^{ℓ}. Therefore we compare our bounds with bounds in [7]. For the range of indices i and j in Table 4.1 and Table 4.2, f_{ij} denotes an irreducible polynomial of degree i over $\mathbb{F}_3$ which are defined as follows: $f_{11} = x, f_{12} = x + 1, f_{13} = x + 2, f_{21} = x^2 + 1, f_{22} = x^2 + x + 2, f_{23} = x^2 + 2x + 2, f_{31} = x^3 + 2x + 1, f_{32} = x^3 + 2x + 2, f_{33} = x^3 + 2x^2 + 2x + 2, f_{34} = x^3 + x^2 + x + 2, f_{35} = x^3 + x^2 + 2, f_{36} = x^3 + 2x^2 + x + 1, f_{37} = x^3 + x^2 + 2x + 1, f_{38} = x^3 + 2x^2 + 1.$

4.2 BOUNDS FOR $\mathbb{F}_{3^{\ell m}}$, $m \geq 1$ AND $5 \leq \ell \leq 18$

In this section, up to our knowledge, we give the best known bounds for n-term polynomial multiplication over $\mathbb{F}_3$ for $5 \leq n \leq 18$ and we give an explicit formula for multiplication in $\mathbb{F}_{3^{6m}}$ which is used in id-based cryptography for efficient Tate paring computations. Using Theorem 4.1.4, Proposition 4.1.7 and (4.2), the bounds in Table 4.2 are obtained.

Table 4.1: Upper Bounds for $M_{f,\ell}(n)$ over $\mathbb{F}_3$

f	l	$M_{f,\ell}(n)$[7]	New $M_{f,\ell}(n)$
f_{11}, f_{12}, f_{13}	3	6	5
f_{11}, f_{12}, f_{13}	4	9	8
f_{11}, f_{12}, f_{13}	5	13	11
f_{11}, f_{12}, f_{13}	6	17	15
f_{11}, f_{12}, f_{13}	7	22	19
f_{11}, f_{12}, f_{13}	8	27	24
f_{11}, f_{12}, f_{13}	9	34	29
f_{21}, f_{22}, f_{23}	3	17	15
f_{21}, f_{22}, f_{23}	4	27	24
f_{21}, f_{22}, f_{23}	5	39	33
$f_{31}, ..., f_{38}$	3	34	30

Note that we can conclude from Table 4.2

$$M(n) \leq \begin{cases} 3n-3 & \text{if} \quad 2 \leq n \leq 6 \\ 4n-9 & \text{if} \quad 7 \leq n \leq 18. \end{cases}$$

The bounds in Table 4.2 is also valid for any polynomial multiplication over $\mathbb{F}_{3^m}$ because of the following Theorem.

Theorem 4.2.1 *The formulae for the product of two arbitrary n-term polynomials over* $\mathbb{F}_3$ *are also valid for multiplication of two arbitrary n-term polynomials over* $\mathbb{F}_{3^m}$*, where m is any positive integer.*

Proof. The proof can be found in [15]. ■

The finite fields of $\mathbb{F}_{3^{6m}}$, where m is prime are used in id-based cryptography for efficient computation of the Tate pairing. In [14], multiplication in $\mathbb{F}_{3^{6m}}$ is used with 18 multiplications in $\mathbb{F}_{3^m}$. In [12, 13], the number of multiplications in $\mathbb{F}_{3^{6m}}$ is decreased to 15 multiplications in $\mathbb{F}_{3^m}$. We give a formula in the next example for 6 term polynomial multiplication over $\mathbb{F}_3$ which requires 15 multiplications in $\mathbb{F}_3$. Since the formula for multiplication of two arbitrary n-term polynomials over $\mathbb{F}_3$ is also valid for multiplication of two arbitrary n-term polynomials over $\mathbb{F}_{3^m}$, where m is any positive integer, the formula given in the next example can be used for the multiplication in $\mathbb{F}_{3^{6m}}$ with 15 multiplications in $\mathbb{F}_{3^m}$. The following example

Table 4.2: Upper Bounds for $M(n)$ over $\mathbb{F}_3$

n	$M(n)$[7]	New $M(n)$	Modulus polynomials
2	3	3	$(x-\infty), f_{11}, f_{12}$
3	6	6	$(x-\infty), f_{11}^2, f_{12}, f_{13}$
4	9	9	$(x-\infty), f_{11}^2, f_{12}, f_{13}, f_{21}$
5	13	12	$(x-\infty), f_{11}^2, f_{12}, f_{13}, f_{21}, f_{22}$
6	17	15	$(x-\infty)^2, f_{11}, f_{12}, f_{13}, f_{21}, f_{22}, f_{23}$
7	22	19	$(x-\infty)^2, f_{11}^2, f_{12}^2, f_{13}, f_{21}, f_{22}, f_{23}$
8	27	23	$(x-\infty)^3, f_{11}^3, f_{12}^2, f_{13}, f_{21}, f_{22}, f_{23}$
9	34	27	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{13}^2, f_{21}, f_{22}, f_{23}$
10	39	31	$(x-\infty)^3, f_{11}^3, f_{12}^2, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}$
11	46	35	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{13}^3, f_{21}, f_{22}, f_{23}, f_{31}$
12	51	39	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}$
13	60	43	$(x-\infty)^3, f_{11}^3, f_{12}^2, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}$
14	66	47	$(x-\infty)^3, f_{11}^2, f_{12}^2, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}, f_{34}$
15	75	51	$(x-\infty)^2, f_{11}^2, f_{12}^2, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}, f_{34}, f_{35}$
16	81	55	$(x-\infty)^3, f_{11}^3, f_{12}^2, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}, f_{34}, f_{35}$
17	94	59	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{13}^3, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}, f_{34}, f_{35}$
18	102	63	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}, f_{34}, f_{35}, f_{36}$

compares our formula and the formula given in [12, 13].

Example 4.2.2 *In this example, we give an explicit formula for* 6*-term polynomial multiplication over* $\mathbb{F}_3$*. Let* $A(x) = \sum_{i=0}^{5} a_i x^i$ *and* $B(x) = \sum_{i=0}^{5} b_i x^i$ *be polynomials over* $\mathbb{F}_3$*. Let* $C(x) = \sum_{i=0}^{10} c_i x^i \in \mathbb{F}_3[x]$ *be the polynomial defined by* $C(x) = A(x)B(x)$*. We obtain the following explicit formula consisting of* 15 *multiplications. We first define the multiplications* m_i *for* $1 \leq i \leq 15$ *and then we give the formula for obtaining the coefficients of the polynomial* $C(x)$ *using these multiplications.*

$m_1 = (a_0 + a_1 + a_2 + a_3 + a_4 + a_5)(b_0 + b_1 + b_2 + b_3 + b_4 + b_5),$

$m_2 = (a_0 + a_1)(b_0 + b_1),$

$m_3 = a_0 b_0,$

$m_4 = a_1 b_1,$

$m_5 = (a_1 - a_3 - a_5 + a_2)(b_1 - b_3 - b_5 + b_2),$

$m_6 = (a_0 - a_2 - a_4 + a_1 - a_5)(b_0 - b_2 - b_4 + b_1 - b_5),$

$m_7 = (a_0 - a_2 + a_4 + a_1 - a_3 + a_5)(b_0 - b_2 + b_4 + b_1 - b_3 + b_5),$

$m_8 = (a_0 - a_2 + a_4)(b_0 - b_2 + b_4),$

$m_9 = (a_1 - a_3 + a_5)(b_1 - b_3 + b_5),$

$m_{10} = (a_0 - a_1 + a_2 - a_3 + a_4 - a_5)(b_0 - b_1 + b_2 - b_3 + b_4 - b_5),$

$m_{11} = (a_0 + a_2 - a_4 - a_3)(b_0 + b_2 - b_4 - b_3),$

$m_{12} = (a_0 - a_4 + a_3 + a_1 - a_5)(b_0 - b_4 + b_3 + b_1 - b_5),$

$m_{13} = (a_0 + a_2 - a_4 + a_3)(b_0 + b_2 - b_4 + b_3),$

$m_{14} = (a_1 - a_3 - a_5 - a_2)(b_1 - b_3 - b_5 - b_2),$

$m_{15} = a_5 b_5,$

$c_0 = m_3,$

$c_1 = (m_2 - m_3 - m_4),$

$c_2 = -m_{15} + m_6 - m_{13} - m_{12} + m_{11} - m_{14} - m_8 + m_9 - m_{10} - m_1,$

$c_3 = m_{13} + m_5 + m_{10} - m_{11} - m_{14} - m_1 - m_7 + m_8 + m_9,$

$c_4 = m_{13} - m_5 + m_6 - m_{10} + m_{14} - m_{12} + m_8 - m_9 - m_1,$

$c_5 = -m_1 + m_{10} - m_6 - m_5 + m_7 - m_8 - m_9 - m_{12} - m_{11},$

$c_6 = -m_6 + m_{13} - m_1 + m_{12} - m_{11} + m_{14} - m_8 + m_9 - m_{10},$

$c_7 = -m_{13} - m_5 + m_{10} + m_{11} + m_{14} - m_1 - m_7 + m_8 + m_9,$

$c_8 = -m_3 - m_6 - m_{13} + m_5 - m_1 - m_{10} + m_{12} - m_{14} + m_8 - m_9,$

$c_9 = -m_1 - m_2 + m_3 + m_4 + m_5 + m_6 + m_7 - m_8 - m_9 + m_{10} + m_{11} + m_{12},$

$c_{10} = m_{15}.$

We will show that multiplication in $\mathbb{F}_{3^{6\cdot 97}}$ can be done with 15 multiplications in $\mathbb{F}_{3^{97}}$. Let us construct,

$$\begin{aligned}\mathbb{F}_{3^{97}} &\cong \mathbb{F}_3[x]/(x^{97} + x^{16} + 2),\\ \mathbb{F}_{3^{6\cdot 97}} &\cong \mathbb{F}_{3^{97}}[y]/(y^6 + y - 1).\end{aligned}$$

Let $\alpha, \beta, \gamma \in \mathbb{F}_{3^{6\cdot 97}}$ such that $\alpha = \sum_{i=0}^{5} a_i y^i$, $\beta = \sum_{i=0}^{5} b_i y^i$ and $\gamma = \alpha \cdot \beta = \sum_{i=0}^{5} c_i y^i$. Then the coefficients of γ can be found as follows: First compute the coefficients of $\left(\sum_{i=0}^{5} a_i y^i\right)\left(\sum_{i=0}^{5} b_i y^i\right)$ and then reduce it modulo $y^6 + y - 1$. Therefore, using the formula given above we get

$c_0 = -m_{15} - m_1 + m_{10} - m_6 - m_5 + m_7 - m_8 - m_9 - m_{12} - m_{11},$

$c_1 = m_{15} + m_2 - m_3 - m_4 + m_5 - m_7 - m_8 + m_{10} - m_{11} + m_{12} + m_{13} + m_{14},$

$c_2 = -m_3 + m_5 + m_4 - m_6 - m_1 - m_2 - m_8 + m_9 - m_{13},$

$c_3 = -m_3 - m_5 + m_7 - m_1 - m_8 - m_9 - m_{13} - m_{15},$

$c_4 = m_6 + m_{13} - m_{12} - m_{11} - m_8 - m_{10} - m_5 - m_7 + m_2 - m_3 - m_4,$

$c_5 = m_{14} - m_8 + m_9 - m_{10} - m_6 + m_{13} - m_1 + m_3 - m_{11} + m_{12}.$

Now, we give the multiplication formula for $\mathbb{F}_{3^{6\cdot 97}}$ given in [13]. $\mathbb{F}_{3^{6\cdot 97}}$ is constructed in [12, 13] using tower field representation, i.e.

$$\begin{aligned}
\mathbb{F}_{3^{97}} &\cong \mathbb{F}_3[x]/(x^{97} + x^{16} + 2),\\
\mathbb{F}_{3^{2\cdot 97}} &\cong \mathbb{F}_{3^{97}}[y]/(y^2 + 1),\\
\mathbb{F}_{3^{6\cdot 97}} &\cong \mathbb{F}_{3^{2\cdot 97}}[z]/(z^3 - z - 1).
\end{aligned}$$

Let $\alpha, \beta \in \mathbb{F}_{3^{6\cdot 97}}$ be give as:

$$\alpha = a_0 + a_1 s + a_2 r + a_3 rs + a_4 r^2 + a_5 r^2 s,$$

$$\beta = b_0 + b_1 s + b_2 r + b_3 rs + b_4 r^2 + b_5 r^2 s,$$

where $a_0, \ldots, a_5, b_0, \ldots, b_5 \in \mathbb{F}_{3^{97}}$, $s \in \mathbb{F}_{3^{2\cdot 97}}$ and $r \in \mathbb{F}_{3^{6\cdot 97}}$ are roots of $y^2 + 1$ and $z^3 - z - 1$, respectively. Let $\gamma = \alpha\beta$ be

$$\gamma = c_0 + c_1 s + c_2 r + c_3 rs + c_4 r^2 + c_5 r^2 s.$$

The coefficients $c_0, ..., c_5 \in \mathbb{F}_{3^{97}}$ of the product can be computed as follows:

$m_0 = (a_0 + a_2 + a_4)(b_0 + b_2 + b_4),$

$m_1 = (a_0 + a_1 + a_2 + a_3 + a_4 + a_5)(b_0 + b_1 + b_2 + b_3 + b_4 + b_5),$

$m_2 = (a_1 + a_3 + a_5)(b_1 + b_3 + b_5),$

$m_3 = (a_0 + sa_2 - a_4)(b_0 + sb_2 - b_4),$

$m_4 = (a_0 + a_1 + sa_2 + sa_3 - a_4 - a_5)(b_0 + b_1 + sb_2 + sb_3 - b_4 - b_5),$

$m_5 = (a_1 + sa_3 - a_5)(b_1 + sb_3 - b_5),$

$m_6 = (a_0 - a_2 + a_4)(b_0 - b_2 + b_4),$

$m_7 = (a_0 + a_1 - a_2 - a_3 + a_4 + a_5)(b_0 + b_1 - b_2 - b_3 + b_4 + b_5),$

$m_8 = (a_1 - a_3 + a_5)(b_1 - b_3 + b_5),$

$m_9 = (a_0 - sa_2 - a_4)(b_0 - sb_2 - b_4),$

$m_{10} = (a_0 + a_1 - sa_2 - sa_3 - a_4 - a_5)(b_0 + b_1 - sb_2 - sb_3 - b_4 - b_5),$

$m_{11} = (a_1 - sa_3 - a_5)(b_1 - sb_3 - b_5),$

$m_{12} = a_4 b_4,$

$m_{13} = (a_4 + a_5)(b_4 + b_5),$

$m_{14} = a_5 b_5,$

$c_0 = -m_0 + m_2 + (s+1)m_3 - (s+1)m_5 - (s-1)m_9 + (s-1)m_{11} - m_{12} + m_{14},$

$c_1 = m_0 - m_1 + m_2 - (s+1)m_3 + (s+1)m_4 - (s+1)m_5 + (s-1)m_9 -,$

$(s-1)m_{10} + (s-1)m_{11} - m_{12} - m_{13} + m_{14},$

$c_2 = -m_0 + m_2 + m_6 - m_8 + m_{12} - m_{14},$

$c_3 = m_0 - m_1 + m_2 - m_6 + m_7 - m_8 - m_{12} + m_{13} - m_{14},$

$c_4 = m_0 - m_2 - m_3 + m_5 + m_6 - m_8 - m_9 + m_{11} + m_{12} - m_{14},$

$c_5 = m_0 + m_1 - m_2 + m_3 - m_4 + m_5 - m_6 + m_7 - m_8 + m_9 - m_{10} + m_{11} - m_{12} + m_{13} - m_{14}.$

Therefore, the formula in [12, 13] contains multiplication by $\mp s$, $\mp(s+1)$ *and* $\mp(s-1)$*, where* $s \in \mathbb{F}_{3^{2\cdot 97}}$ *is a root of* y^2+1*. For both our proposed formula and the formula in [13], the number of multiplications is 15. The number of additions for our proposed formula is 137. Note that there are multiplications of form* $(s \mp 1)m_i$ *in the formula in [13]. Here* $s \notin \mathbb{F}_3$*. In calculation of the number of additions, if we disregard the multiplication by s for the formula in [13], and if we consider the cost of each multiplication of the form* $(s \mp 1)m_i$ *for the formula in [13] as 1 addition only, then the number of additions for the formula in [13] is still 138. Moreover, in our formula the only nonzero coefficients are* ∓ 1 *and we do not need to introduce intermediate field extensions like* $\mathbb{F}_{3^{2\cdot 97}}$ *containing* $s \notin \mathbb{F}_3$*. Therefore it seems that our construction would be preferable to the construction in [12, 13].*

CHAPTER 5

ON MULTIPLICATION IN FINITE FIELDS

Let $\mathbb{F}_q$ be a finite field and $n > 1$ be an integer. Let $\mathbb{F}_{q^n}^{\perp}$ be 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

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

$R(\mathbb{F}_{q^n}/\mathbb{F}_q)$ 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 $\mathbb{F}_q$ multiplications in order to multiply two arbitrary elements of $\mathbb{F}_{q^n}$. In this chapter, we present a method for multiplication in finite fields improving $\mu_q(n)$ for certain values of q and n. We use local expansions, the lengths of which are further parameters that can be used to optimize the bounds on the bilinear complexity, instead of evaluation into residue class field. Basic principle is still based on the method of D. V. Chudnovsky and G. V. Chudnovsky. The main idea can be summarized as follows: 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 below). We obtain improved bounds for multiplication in $\mathbb{F}_{q^n}$, where $2 \leq n \leq 18$ and $q = 2, 3, 4$ by searching to optimize the algorithm of D. V. Chudnovsky and G. V. Chudnovsky and by using the complexity notion introduce in 5.1.1.

The rest of chapter is organized as follows: We introduce complexity notions and a brief review of algebraic function fields in the next section. The proposed method is presented in Section 3. In Section 4, we obtain upper bounds for the bilinear complexity $\mu_q(n)$ of multiplication for $2 \leq n \leq 18$ and $q = 2, 3, 4$. 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 elements used in cryptography. Our 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.

5.1 PRELIMINARIES

5.1.1 SOME COMPLEXITY NOTIONS

Let $\mu_q(n)$ represent *the bilinear complexity of multiplication in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$. It corresponds to the minimum number of $\mathbb{F}_q$ 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. [22], [4], [7], [9] [11], [9], [10]). Here, a polynomial is called an n-term polynomial in $\mathbb{F}_q[x]$ if it is of the form

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},\ a_i \in \mathbb{F}_q.$$

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

$$\mu_q(n) \leq M_q(n). \tag{5.1}$$

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

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

We will need another complexity notion in this chapter. For a positive integer ℓ, let $\widehat{M}_q(\ell)$ denote 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 $\widehat{M}_q(2) \leq 3$, $\widehat{M}_q(3) \leq 5$, $\widehat{M}_q(4) \leq 8$ and $\widehat{M}_q(5) \leq 11$ for any prime power q (cf. [22, Proposition 1]).

5.1.2 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 [29].

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 $O \subseteq F$ with the properties $K\mathbb{F}_q \subset O \subset F$ and for any $z \in F$, either $z \in O$ or $z^{-1} \in O$. A place of P of the function field $F/\mathbb{F}_q$ is the maximal ideal of some valuation ring O of $F/\mathbb{F}_q$. We will denote the set of all places of $F/\mathbb{F}_q$ as $\mathbb{P}_F$. If O is a valuation ring of $F/\mathbb{F}_q$ and P is its maximal ideal, then O is uniquely determined by P. Hence we denote O by O_P.

$F_P := O_P/P$ 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 $[F_P : \mathbb{F}_q] := degP$.

The free abelian group which is generated by the places of $F/\mathbb{F}_q$ is denoted by $\mathcal{D}_F$, called the divisor group of $F/\mathbb{F}_q$. A divisor is a formal sum $D = \sum_{P \in \mathbb{P}_F} n_P P$ with $n_P \in \mathbb{Z}$, with almost all $n_P = 0$. The support of D is defined by 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

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

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

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

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 we define $(x)_0 := \sum_{P \in Z} v_P(x)P$, called the zero divisor of x, and $(x)_\infty := \sum_{P \in N}(-v_P(x))P$, called the pole divisor of x, and $(x) := (x)_0 - (x)_\infty$, 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

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

is called the divisor class group. The divisor class of D, denoted by $[D]$, is the corresponding element in the factor group 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

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

$\mathcal{L}(A)$ 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 defined by $\dim A := \dim \mathcal{L}(A)$ is called the dimension of the divisor A. The genus of $F/\mathbb{F}_q$ is defined by

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

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.

5.2 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 F of arbitrary degrees. Assume that Q is a place of degree n. Let O_Q be the valuation ring of the place Q. Note that the residue field O_Q/Q is isomorphic to $\mathbb{F}_{q^n}$. Let D be a divisor such that $\text{supp} D \cap \{Q, P_1, P_2, \ldots, P_N\} = \emptyset$. 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 O_Q/Q is onto. For $1 \le i \le N$, 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

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

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

$$\begin{array}{rcl} \varphi : \mathcal{L}(2D) & \to & \left(\mathbb{F}_{q^{\deg(P_1)}}\right)^{u_1} \times \left(\mathbb{F}_{q^{\deg(P_2)}}\right)^{u_2} \times \cdots \times \left(\mathbb{F}_{q^{\deg(P_N)}}\right)^{u_N} \\ f & \to & (\varphi_1(f), \varphi_2(f), \ldots, \varphi_N(f)). \end{array} \tag{5.2}$$

Finally we assume that the map φ is injective.

Theorem 5.2.1 *Under the notation and assumptions as above we have*

$$\mu_q(n) \le \sum_{i=1}^{N} \mu_q(\deg(P_i)) \widehat{M}_{q^{\deg(P_i)}}(u_i). \tag{5.3}$$

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 $\mathrm{Ev}_Q(h_1), \ldots, \mathrm{Ev}_Q(h_n), \mathrm{Ev}_Q(h'_m), \ldots, \mathrm{Ev}_Q(h'_m) \in O_Q/Q \cong \mathbb{F}_{q^n}$ 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

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

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 $O_Q/Q \cong \mathbb{F}_{q^n}$ without any cost on bilinear complexity. For given $\alpha, \beta \in \mathbb{F}_{q^n} \cong O_Q/Q$, 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

$$f_1 = a_1h_1 + \ldots + a_nh_n, \;\; f_2 = b_1h_1 + \ldots + b_nh_n \tag{5.4}$$

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 (5.4). 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 $1 \leq i \leq N$.

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

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

Note that the coordinates $\alpha_{i,0}, \dots, \alpha_{i,u_i-1}, \beta_{i,0}, \dots, \beta_{i,u_i-1} \in \mathbb{F}_{q^{\deg(P_i)}}$ and they are obtained using the coefficients $a_1, \dots, a_n, b_1, \dots, b_n$ and the constants $\varphi_i(h_1), \dots, \varphi_i(h_n)$ 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

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

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

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

It is clear that

$$\varphi_i(f_1 f_2) = (\gamma_0^i, \gamma_1^i, \dots \gamma_{u_i-1}^i).$$

The cost of obtaining the first u_i terms $\gamma_0^i, \gamma_1^i, \dots \gamma_{u_i-1}^i$ 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 5.2.1 we obtain explicit algorithms for multiplications in $\mathbb{F}_{q^n}$. The conditions of the following theorem guarantee that the assumptions of Theorem 5.2.1 are satisfied.

Theorem 5.2.2 *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 we have

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

Proof. Let G be a 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 $D_1 \geq G$, we have that D_1 is non-special again (cf. Remark I.6.9, item (f) [29]). Hence

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

Using Strong Approximation Theorem (cf. Theorem I.6.4 [29]) we obtain a divisor D of F such that

$$D \sim D_1 \text{ and } \mathrm{supp} D \cap \{Q, P_1, P_2, \cdots, P_N\} = \emptyset.$$

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 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 (5.2). It remains to prove that φ is injective.

Assume the contrary. Then there exists a nonzero $f \in \mathcal{L}(2D)$ such that

$$v_{P_1}(f) \geq u_1,\ v_{P_2}(f) \geq u_2, \ldots,\ v_{P_N}(f) \geq u_N.$$

This implies that

$$f \in \mathcal{L}(2D - u_1P_1 - u_2P_2 - \cdots - u_NP_N). \tag{5.5}$$

Note that

$$deg(2D) = 2degD = 2(n + g - 1). \tag{5.6}$$

Using (5.5) and (5.6), as f is nonzero, we obtain that $2(n + g - 1) \geq \sum_{i=1}^{N} u_iP_i$ which gives a contradiction to the hypothesis. ■

Remark 5.2.3 *Under the notation and assumptions of Theorem 5.2.2, consider the subcase that $N = N_1 + N_2$, P_i is a degree 1 place for $1 \leq i \leq N_1$ and P_i is a degree 2 place for $N_1 + 1 \leq i \leq N_1 + N_2$. Moreover let $u_i = 1$ for $1 \leq i \leq N_1 + N_2$. Note that $\mu_q(1) = 1$, $\mu_q(2) = 3$*

(cf. [11]), and $\widehat{M}_{q^{\deg(P_i)}}(1) = 1$ *for any* $\deg(P_i)$*. Therefore the condition (3) of Theorem 5.2.2 becomes*

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

and the bound of Theorem 5.2.2 on $\mu_q(n)$ *becomes*

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

These coincide with the corresponding result of Ballet and Rolland in [18].

Remark 5.2.4 *By Theorem 5.2.2, 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.[25, Chapter 4]). In Theorem 5.2.2, as* $\deg(P_i)$ *and* u_i *are further parameters to be chosen, the condition (3) is weaker than the corresponding condition in [18, Theorem 2.2].*

Using $u = 2$ for degree 1 places and $u = 1$ for degree 2 places in Theorem 5.2.2, we obtain the following corollary.

Corollary 5.2.5 *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 1 and at least* N_2 *degree 2 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

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

Proof. We use N_1 degree 1 places with $u = 2$ and N_2 degree 2 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 1 places from degree 1 places and N_2' degree 2 places from degree 2 places such that $2n + g - 1 \leq 2N_1' + 2N_2' \leq 2n + g$. Then we get

$$\mu_q(n) \leq 3N_1' + 3N_2' \leq 3(n + \frac{g}{2}) = 3n + \frac{3g}{2}.$$

■

We compare Corollary 5.2.5 with the corresponding results in [18]. The bound of Corollary 5.2.5 is at least as good as the bounds of [18, Theorem 2.2] and [19, Theorem 2.1]. The condition (3) of Corollary 5.2.2 is weaker as the corresponding condition of [18] and [19] is $N_1 + 2N_2 > 2n + 2g - 2$. The other conditions of Corollary 5.2.5 are the same as the ones in [18]. Therefore Corollary 5.2.5 gives improved bounds on $\mu_q(n)$ compared to the ones in [18].

For some explicit algebraic function fields, the map φ in (5.2) 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 5.2.6 *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 place of degree n,

(2) $\sum_{i=1}^{N} \deg(P_i)u_i = 2n + g - 1$,

(3) there exists a non-special divisor D of degree $n + g - 1$.

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 (5.2). If φ is injective then

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

Proof. As D is non-special, $\dim(\mathcal{L}(D)) = degD + 1 - g = n$. Moreover $\text{supp}(D) \cup \{Q\} = \emptyset$ and hence the evaluation map Ev_Q from $\mathcal{L}(D)$ to O_Q/Q is bijective. Note that $\text{supp}(D) \cup \{P_1, \ldots, P_N\} = \emptyset$ as well. The result follows from Theorem 5.2.1. ■

Remark 5.2.7 *In Theorem 5.2.6 it is enough to assume that D is a non-special divisor of degree $n + g - 1$. Using Strong Approximation Theorem (cf. Theorem I.6.4 [29]), we can always obtain D' from such D with $D' \sim D$ and* $\mathrm{supp}D' \cup \{Q, P_1, P_2, \ldots, P_N\}$.

Remark 5.2.8 *The same bound of Theorem 5.2.6 was given in [19] under certain conditions on q and n only for degree 1 and degree 2 places with $u = 1$. The condition on q and n in [19] seems to come from choice of non-special divisor D with extra conditions. In our case the extra conditions refers 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 5.2.6 gives an improved bound for $\mathbb{F}_{3^9}$.

Example 5.2.9 *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 [22], [7] and [9], we obtain the upper bounds on $M_3(9)$ as 36, 34 and 27, respectively. Hence by [22] and (5.1) we get $\mu_3(9) \leq 27$. For the method in [18], 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 1 places, 6 degree 2 places and 8 degree three places. As $4 + 2 \cdot 6 < 2 \cdot 9 + 1 - 1$, the method of [18] cannot be applied directly. Using 3 degree 1 places, 6 degree 2 places, and 1 degree three places, all with $u = 1$ as in [18], we obtain that $\mu_3(9) \leq 3\cdot1+6\cdot3+6\cdot1 = 27$. Now we improve this to $\mu_3(9) \leq 26$ using Theorem 5.2.6 together with $u = 2$ for some places. We take 2 degree 1 places with $u = 2$, 2 degree 1 places with $u = 1$, and 6 degree 2 places with $u = 1$. Therefore we obtain that $\mu_3(9) \leq 2\cdot3+2\cdot1+6\cdot3 = 26$. We find an explicit formula of such an algorithm via Theorem 5.2.6, which can be found in Appendix A. The description and details of finding explicit formula for $\mu_3(9) \leq 26$ are given in Section 5.5.*

5.3 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 our proposed method in this chapter. In particular, we indicate some improvements obtained using our 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 $\mu_q(n)$ in the literature is obtained using the following methods:

(i) The methods based on the idea of D.V. Chudnovsky and G.V. Chudnovsky [23], which are presented in the [16], [17], [18], [19].

(ii) The observation in (5.1) together with results presented in [9], [7], [4], [22], [21].

(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

$$\mu_q(n) \leq \mu_{q^\ell}(k) \cdot \mu_q(\ell). \tag{5.7}$$

5.3.1 MULTIPLICATION IN $\mathbb{F}_{2^n}$

Using [11], [9], [7], [4] and [21], we get $\mu_2(2) = 3$, $\mu_2(3) = 6$, $\mu_2(4) \leq 9$, $\mu_2(5) \leq 13$, $\mu_2(7) \leq 22$, $\mu_2(9) \leq 30$, $\mu_2(11) \leq 39$, $\mu_2(13) \leq 48$ and $\mu_2(17) \leq 68$.

For $n = 6, 8, 10, 12, 14, 16, 18$, using (5.7) with $\ell = 2$ we obtain

$$\mu_2(n) \leq \mu_{2^2}(n/2) \cdot \mu_2(2) = 3\mu_4(n/2).$$

The bounds $\mu_4(n/2)$ for $n = 6, 8, 10, 12, 14, 16, 18$ are in Table 1. Then we get $\mu_2(6) \leq 15$, $\mu_2(8) \leq 24$, $\mu_2(10) \leq 33$, $\mu_2(12) \leq 42$, $\mu_2(14) \leq 51$, $\mu_2(16) \leq 60$, and $\mu_2(18) \leq 69$.

For $n = 15$, using (5.7) with $\ell = 3$ we obtain

$$\mu_2(15) \leq \mu_{2^3}(5) \cdot \mu_2(3) = 6\mu_8(5) = 54,$$

where we use $\mu_8(5) = 9$ (cf. [11]).

5.3.2 MULTIPLICATION IN $\mathbb{F}_{3^n}$

Using [11], [7] and [22], we get $\mu_3(2) = 3$, $\mu_3(3) = 6$, $\mu_3(4) \leq 9$, $\mu_3(5) \leq 12$, $\mu_3(6) \leq 15$ and $\mu_3(7) \leq 19$.

For $n = 8, 10, 12, 14, 16$, using (5.7) with $\ell = 2$ we obtain

$$\mu_3(n) \leq \mu_{3^2}(n/2) \cdot \mu_3(2) = 3\mu_9(n/2).$$

Recall that $\mu_9(4) = 7$, $\mu_9(5) = 9$ and $\mu_9(6) = 12$, (cf. [11]). The methods in [4] and [22] give $\mu_9(7) \leq 15$, $\mu_9(8) \leq 18$. Then we obtain $\mu_3(8) \leq 21$, $\mu_3(10) \leq 27$, $\mu_3(12) \leq 36$, $\mu_3(14) \leq 45$ and $\mu_3(16) \leq 54$.

For the cases $n = 9, 11, 13, 15, 17, 18$, we improve the best known bounds given in [22] and [7], by using the method given in this chapter. Throughout this chapter we use the notation of Magma [20] for presenting the places and the divisor of algebraic function fields. It is easy to verify that our choices of the places and the divisor imply that the map φ in (5.2) is injective using Magma as in Section 6.

In Example 5.2.9, it is explained how to obtain $\mu_3(9) \leq 26$.

When we use the same curve given in Example 5.2.9, we obtain the improved bounds. Note that the places of this elliptic curve are given in Section 6.

In order to show that $\mu_2(11) \leq 34$ it is enough to take 2 degree 1 places with $u = 2$, 2 degree 1 places with $u = 3$ and 6 degree 2 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 $\mu_2(13) \leq 42$, we use 4 degree 1 places with $u = 2$, 6 degree 2 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 1 places with $u = 3$, 6 degree 2 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 1 places with $u = 2$, 2 degree 1 places with $u = 3$, 6 degree 2 places with $u = 1$ and 4 degree three places with $u = 1$.

Finally, $\mu_3(18) \leq 62$ is obtained by taking 3 degree 1 places with $u = 2$, 1 degree 1 places with $u = 3$, 6 degree 2 places with $u = 1$ and 5 degree three places with $u = 1$ where one can use

$D = (x^{18}+2x^{17}+2x^{16}+x^{15}+x^{11}+2x^{10}+x^4+2x+2, y+2x^{17}+x^{14}+x^{13}+2x^{12}+2x^8+x^6+2x^5+x^4).$

5.3.3 MULTIPLICATION IN $\mathbb{F}_{4^n}$

Using the methods in [11], [4] and [21], we obtain $\mu_4(2) = 3, \mu_4(3) = 5, \mu_4(4) = 8, \mu_4(5) \leq 11$, $\mu_4(6) \leq 14, \mu_4(7) \leq 17, \mu_4(8) \leq 20, \mu_4(9) \leq 23$ and $\mu_4(10) \leq 27$.

For $n = 12, 14, 16$, using (5.7) with $\ell = 2$ we obtain

$$\mu_4(n) \leq \mu_{4^2}(n/2) \cdot \mu_4(2) = 3\mu_{16}(n/2).$$

Recall that $\mu_{16}(6) = 11, \mu_{16}(7) = 13, \mu_{16}(8) = 15$ and $\mu_{16}(9) = 17$ (cf. [11]). Therefore we obtain, $\mu_4(12) \leq 33, \mu_4(14) \leq 39, \mu_4(16) \leq 45$ and $\mu_4(18) \leq 51$.

In order to show that $\mu_4(11) \leq 30, \mu_4(13) \leq 37$ and $\mu_4(17) \leq 53$ 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

$$\begin{aligned} E_1 &: \; y^2 + wy = x^3 + x^2 + wx + 1, \\ E_2 &: \; y^2 + w^2xy + wy = x^3 + wx + w^2, \\ E_3 &: \; y^2 + y = x^3 + x^2 + w^2x + w \end{aligned}$$

be elliptic curves over $\mathbb{F}_4$. E_1 has 7 degree 1 places, 7 degree 2 places and 14 degree 3 places. E_2 has 6 degree 1 places, 9 degree 2 places and 16 degree 3 places. Finally, E_3 has 5 degree 1 places, 10 degree 2 places and 20 degree 3 places.

The bound $\mu_4(11) \leq 30$ can be obtained using the method described in this chapter by using E_1. When we use 1 degree 1 place with $u = 2$, 6 degree 1 places with $u = 1$ and 7 degree 2 places with $u = 1$, we get $\mu_4(11) \leq 30$. Note that the same bound is also obtained by the method of [18]. If we use E_2 then we obtain $\mu_4(11) \leq 30$ by using 6 degree one places and 8 degree 2 places.

The improved bound $\mu_4(13) \leq 37$ can be obtained by using E_2. Let the set $\{P_1, \ldots, P_6, Q_1, \ldots, Q_9\}$ be places of degrees 1 and 2 of E_2 where P_i's are degree 1 places for $1 \leq i \leq 6$ and Q_j's are degree 2 places for $1 \leq j \leq 9$. Those are

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

When we use 2 degree 1 places, P_1, P_2, with $u = 2$, 4 degree 1 places, $P_3, \ldots, P_6$ with $u = 1$ and 9 degree 2 places, $Q_1, \ldots, Q_9$ with $u = 1$, we obtain $\mu_4(13) \leq 37$ 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 $\mu_4(17) \leq 53$ can be obtained by using two methods, the proposed method and method introduced in [18]. When we use the elliptic curve E_2 with 2 degree 1 places with $u = 2$, 4 degree 1 places with $u = 1$ and 9 degree 2 places with $u = 1$, we get $\mu_4(17) \leq 53$. On the other hand, using E_3 with 5 degree 1 places with $u = 1$, 10 degree 2 places with $u = 1$ and 3 degree 3 places with $u = 1$ gives the same bound.

We summarize the results of this section in Table 5.1. The symbol $*$ denotes an improvement by using the proposed method compared to the best known values in the literature.

5.4 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) [24]. 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 for our method over $\mathbb{F}_2$ (up to isomorphism) is $y^2 + y = x^3 + x + 1$ which has 1 degree 1 places, 2 degree 2 places, 4 degree 3 places, 5 degree 4 places, 8 degree 5 places, 8 degree 6 places, 16 degree 7 places and 25 degree 8 places. We take 1 degree 1 places with $u = 5$, 2 degree 2 places with $u = 2$, 4 degree 3 places with $u = 1$, 5 degree 4 places with $u = 1$, 8 degree 5 places with $u = 1$, 8

Table 5.1: Bounds for $\mu_q(n)$ for $2 \leq n \leq 18$ and $q = 2, 3, 4$

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

degree 6 places with $u = 1$, 15 degree 7 places with $u = 1$ and 11 degree 8 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 5.1 and $\widehat{M}_2(5) \leq 11$, $\widehat{M}_4(2) \leq 3$ [21]. On the other hand, the best we can expect from Karatsuba algorithm (together with (5.1)) is $\mu_2(163) \leq N$, where N is an integer with $N > 2187$, since it is given in [9] that $M_2(128) \leq 2187$.

The finite field $\mathbb{F}_{3^{97}}$ is used in pairing based cryptography [22], [26]. 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 1 places, 6 degree 2 places, 11 degree 3 places, 15 degree 4 places and 42 degree 5 places. When we use 3 degree 1 places with $u = 3$, 6 degree 2 places with $u = 1$, 11 degree 3 places with $u = 1$, 15 degree 4 places with $u = 1$ and 16 degree 5 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 5.1 and $\widehat{M}_3(3) \leq 5$ [22] . Note that Karatsuba algorithm (together with (5.1)) gives $\mu_3(97) \leq 1554$ [9].

5.5 EXPLICIT FORMULA FOR 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 elliptic curves. In Example 5.2.9, 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 places of degrees 1 and 2 where P_i's are degree 1 places for $1 \leq i \leq 4$ and Q_j's are degree 2 places for $1 \leq j \leq 6$. Those are

$$\begin{aligned}
&P_1 = \infty,\ P_2 = (x+1, y),\ P_3 = (x+2, y+1),\ P_4 = (x+2, y+2),\\
&Q_1 = (x),\ Q_2 = (x^2+2x+2, y),\ Q_3 = (x^2+1, y+x),\ Q_4 = (x^2+1, y+2x),\\
&Q_5 = (x^2+x+2, y+1),\ Q_6 = (x^2+x+2, y+2).
\end{aligned}$$

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 5.2 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

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

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

$$\begin{aligned}
&f_1 = \tfrac{x^7y}{f} + \tfrac{(2x^8+2x^7+x^6+2x^4+x^3+x^2+2x+2)}{f},\ f_2 = \tfrac{x^6y}{f} + \tfrac{(x^8+2x^6+x^5+x^4+2x^3+1)}{f},\\
&f_3 = \tfrac{x^5y}{f} + \tfrac{(2x^8+2x^5+x^3+x+1)}{f},\ f_4 = \tfrac{x^4y}{f} + \tfrac{(2x^8+x^7+x^4+2x^2+x+2)}{f}\\
&f_5 = \tfrac{x^3y}{f} + \tfrac{(x^8+x^6+x^4+x^3+2x^2+x)}{f},\ f_6 = \tfrac{x^2y}{f} + \tfrac{(x^7+x^5+x^3+x^2+2x+1)}{f}\\
&f_7 = \tfrac{xy}{f} + \tfrac{(2x^8+2x^7+x^6+2x^2+2x)}{f}, f_8 = \tfrac{y}{f} + \tfrac{(2x^7+2x^6+x^5+2x+2)}{f},\ f_9 = 1\\
&f_{10} = \tfrac{(x^{14}+x^{13}+2x^{12}+x^{10}+2x^8+x^7+x^5+x^3+2x^2)y}{f^2} + \tfrac{(x^{18}+2x^{17}+2x^{16}+2x^{15}+2x^{13}+2x^{12}+2x^{10}+x^9+x^8+2x^7+2x^4+2x)}{f^2}\\
&f_{11} = \tfrac{(x^{13}+x^{12}+2x^{11}+x^9+2x^7+x^6+x^4+x^2+2x)y}{f^2} + \tfrac{(x^{17}+2x^{16}+2x^{15}+2x^{14}+2x^{12}+2x^{11}+2x^9+x^8+x^7+2x^6+2x^3+2)}{f^2}\\
&f_{12} = \tfrac{(x^{12}+x^{11}+2x^{10}+x^8+2x^6+2x^5+2x^4+2x^3+x)y}{f^2} + \tfrac{(x^{16}+2x^{15}+2x^{14}+2x^{13}+2x^{11}+2x^{10}+x^9+2x^8+x^6+x^4+x^3+x+1)}{f^2}\\
&f_{13} = \tfrac{(x^{11}+x^{10}+2x^9+x^7+x^5+x^3+2x^2)y}{f^2} + \tfrac{(x^{15}+2x^{14}+2x^{13}+2x^{12}+2x^{10}+x^9+x^8+2x^4+2x)}{f^2}\\
&f_{14} = \tfrac{(x^{10}+x^9+2x^8+x^6+x^4+x^2+2x)y}{f^2} + \tfrac{(x^{14}+2x^{13}+2x^{12}+2x^{11}+2x^9+x^8+x^7+2x^3+2)}{f^2}
\end{aligned}$$

$$f_{15} = \frac{(x^9+x^8+2x^7+2x^5+2x^4+2x^3+x)y}{f^2} + \frac{(x^{13}+2x^{12}+2x^{11}+2x^{10}+x^9+2x^8+x^6+x^5+x^4+x^3+x+1)}{f^2}$$
$$f_{16} = \frac{(x^8+x^7+2x^6+2x^5+x^3+2x^2)y}{f^2} + \frac{(x^{12}+2x^{11}+2x^{10}+x^9+x^8+2x)}{f^2}$$
$$f_{17} = \frac{(x^7+x^6+2x^5+2x^4+x^2+2x)y}{f^2} + \frac{(x^{11}+2x^{10}+2x^9+x^8+x^7+2)}{f^2}$$
$$f_{18} = \frac{(x^6+2x^5+x^4+x)y}{f^2} + \frac{(x^{10}+2x^8+x^6+x^5+x^4+x^3+x^2+x+1)}{f^2}$$

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

$$\left(\sum_{i=1}^{9} a_i f_i\right) \cdot \left(\sum_{i=1}^{9} b_i f_i\right) = \sum_{i=1}^{18} c_i f_i. \tag{5.8}$$

When we evaluate P_1 and P_2 with $u = 1$, P_3 and P_4 with u=2 and $Q_1, \ldots, Q_6$ with $u = 1$ in the equation (5.8), 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 below.

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

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

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 $\gamma = \sum_{i=1}^{9} c_i\xi_i \in \mathbb{F}_{3^9}$ such that

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

where $\{\xi_i, \xi_2, \ldots, \xi_9\}$ 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 $1 \leq i \leq 26$ and then we give the formula for obtaining the coefficients of γ using these multiplications.

$$\begin{aligned}
m_1 &= a_9 b_9 \\
m_2 &= (2a_2 + 2a_3 + 2a_4 + a_7 + 2a_8 + a_9)(2b_2 + 2b_3 + 2b_4 + b_7 + 2b_8 + b_9) \\
m_3 &= (a_2 + 2a_8 + 2a_4 + 2a_7 + a_9)(b_2 + 2b_8 + 2b_4 + 2b_7 + b_9) \\
m_4 &= (a_8 + 2\,a_4 + a_9 + 2\,a_3)(b_8 + 2\,b_4 + b_9 + 2\,b_3) \\
m_5 &= (2a_2 + a_7 + 2a_3 + 2a_8)(2b_2 + b_7 + 2b_3 + 2b_8) \\
m_6 &= (2a_1 + a_9 + a_7 + 2a_3 + a_8 + a_4 + 2a_5 + 2a_6)(2b_1 + b_9 + b_7 + 2b_3 + b_8 + b_4 + 2b_5 + 2b_6) \\
m_7 &= (a_1 + a_9 + 2a_7 + 2a_6 + 2a_2)(b_1 + b_9 + 2b_7 + 2b_6 + 2b_2) \\
m_8 &= (2a_2 + a_3 + 2a_4 + a_7 + a_5 + 2a_8 + 2a_1)(2b_2 + b_3 + 2b_4 + b_7 + b_5 + 2b_8 + 2b_1) \\
m_9 &= (2a_1 + a_2 + a_3 + 2a_4 + a_6 + 2a_8 + a_9)(2b_1 + b_2 + b_3 + 2b_4 + b_6 + 2b_8 + b_9) \\
m_{10} &= (2a_1 + a_2 + a_3 + 2a_4 + a_6 + a_9)(2b_1 + b_2 + b_3 + 2b_4 + b_6 + b_9) \\
m_{11} &= a_8 b_8
\end{aligned}$$

$$\begin{aligned}
m_{12} &= (a_1 + a_5 + a_9 + 2a_7)(b_1 + b_5 + b_9 + 2b_7) \\
m_{13} &= (2a_2 + 2a_1 + a_5 + 2a_3 + 2a_4 + 2a_7 + 2a_8 + a_6)(2b_2 + 2b_1 + b_5 + 2b_3 + 2b_4 + 2b_7 + 2b_8 + b_6) \\
m_{14} &= (2a_5 + a_9 + a_7 + 2a_2 + 2a_3 + 2a_4 + 2a_8 + a_6)(2b_5 + b_9 + b_7 + 2b_2 + 2b_3 + 2b_4 + 2b_8 + b_6) \\
m_{15} &= (a_1 + a_3 + a_9 + a_4 + a_6)(b_1 + b_3 + b_9 + b_4 + b_6) \\
m_{16} &= (a_2 + a_5 + a_3)(b_2 + b_5 + b_3) \\
m_{17} &= (a_1 + 2a_3 + a_9 + a_4 + a_6 + a_2 + a_5)(b_1 + 2b_3 + b_9 + b_4 + b_6 + b_2 + b_5) \\
m_{18} &= (a_1 + a_9 + 2a_2 + a_3 + 2a_4 + a_8)(b_1 + b_9 + 2b_2 + b_3 + 2b_4 + b_8) \\
m_{19} &= (a_2 + 2a_1 + a_7 + 2a_3)(b_2 + 2b_1 + b_7 + 2b_3) \\
m_{20} &= (a_9 + 2a_4 + a_8 + a_7)(b_9 + 2b_4 + b_8 + b_7) \\
m_{21} &= (a_5 + a_9 + a_4 + 2a_8)(b_5 + b_9 + b_4 + 2b_8) \\
m_{22} &= (2a_1 + 2a_4 + 2a_3 + a_6 + 2a_7 + a_2 + 2a_5)(2b_1 + 2b_4 + 2b_3 + b_6 + 2b_7 + b_2 + 2b_5) \\
m_{23} &= (a_9 + 2a_8 + 2a_1 + 2a_3 + a_6 + 2a_7 + a_2)(b_9 + 2b_8 + 2b_1 + 2b_3 + b_6 + 2b_7 + b_2) \\
m_{24} &= (a_9 + 2a_2 + a_7 + 2a_3 + a_6 + 2a_4 + a_5 + a_8)(b_9 + 2b_2 + b_7 + 2b_3 + b_6 + 2b_4 + b_5 + b_8) \\
m_{25} &= (a_2 + a_3 + a_6 + a_4 + a_8 + a_1)(b_2 + b_3 + b_6 + b_4 + b_8 + b_1) \\
m_{26} &= (a_9 + a_7 + 2a_6 + a_5 + 2a_8 + a_1)(b_9 + b_7 + 2b_6 + b_5 + 2b_8 + b_1)
\end{aligned}$$

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

$c_1 = (2\,m_6 + m_{11} + m_{10} + m_{13} + m_{14} + 2\,m_{16} + 2\,m_{17} + 2\,m_{19} + m_{25} + 2\,m_{26} + 2\,m_{20} + 2\,m_{21} + 2\,m_{22} + 2\,m_2 + m_1)$

$c_2 = (m_6 + 2\,m_9 + 2\,m_{10} + m_{15} + m_{16} + 2\,m_{17} + 2\,m_{18} + 2\,m_{19} + 2\,m_{25} + m_{26} + m_{20} + m_{21} + m_{23} + 2\,m_2 + m_3 + 2\,m_5 + m_4)$

$c_3 = (m_6 + 2\,m_9 + 2\,m_{10} + m_{13} + m_{14} + m_{15} + 2\,m_{16} + m_{19} + 2\,m_{24} + 2\,m_{25} + m_{20} + m_{22} + 2\,m_{23} + 2\,m_2 + 2\,m_3 + m_5 + 2\,m_4)$

$c_4 = (m_7 + 2\,m_8 + m_9 + m_{11} + 2\,m_{10} + m_{13} + m_{14} + m_{15} + m_{17} + m_{18} + 2\,m_{19} + m_{25} + 2\,m_{26} + m_{21} + m_{22} + m_2 + m_1 + m_5 + 2\,m_4)$

$c_5 = (2\,m_6 + m_7 + 2\,m_8 + 2\,m_9 + 2\,m_{11} + m_{10} + 2\,m_{13} + 2\,m_{14} + 2\,m_{18} + m_{19} + m_{25} + 2\,m_{26} + m_2 + 2\,m_1)$

$c_6 = (2\,m_6 + 2\,m_9 + 2\,m_{10} + 2\,m_{12} + 2\,m_{13} + 2\,m_{15} + 2\,m_{17} + m_{18} + 2\,m_{19} + 2\,m_{25} + m_{26} + m_{22} + 2\,m_{23} + m_2 + m_1)$

$c_7 = (m_6 + 2\,m_7 + m_8 + m_{12} + m_{13} + 2\,m_{15} + m_{16} + 2\,m_{18} + 2\,m_{19} + m_{24} + m_{25} + m_{20} + 2\,m_{21} + 2\,m_{22} + 2\,m_1 + 2\,m_3 + m_5 + 2\,m_4)$

$c_8 = (m_6 + 2\,m_{11} + 2\,m_{10} + 2\,m_{12} + m_{13} + 2\,m_{14} + m_{16} + m_{17} + 2\,m_{19} + 2\,m_{24} + 2\,m_{26} + 2\,m_{20} + 2\,m_{21} + 2\,m_{23} + m_1 + 2\,m_3)$

$c_9 = (2\,m_6 + 2\,m_9 + m_{11} + 2\,m_{13} + 2\,m_{14} + 2\,m_{15} + 2\,m_{17} + 2\,m_{18} + m_{19} + m_{24} + 2\,m_{25} + 2\,m_{26} + 2\,m_{21} + m_{22} + m_{23} + 2\,m_5 + m_4)$

CHAPTER 6

CONCLUSION

In chapter 2, we give a method for polynomial multiplication over finite fields using field extensions and polynomial interpolation. Using this method we obtained explicit formulae which improved the previous results. We analyzed the n-term polynomial multiplications over $\mathbb{F}_2$, where $n \in \{10, 11, 12\}$, in detail.

Let $n, \ell \geq 1$ be integers and $f(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial. In chapter 3, we give an effective upper bound on $M_{f,\ell}(n)$ (see Notation 3.1.1). This upper bound allows a better selection of the moduli when Chinese Remainder Theorem is used for polynomial multiplication over $\mathbb{F}_2$. We also get improved formulae to multiply polynomials of small degree over $\mathbb{F}_2$. In Table 3.2 we demonstrate that we improve the best known multiplication complexities in the literature in some cases.

In Chapter 4, for each $5 \leq \ell \leq 18$ we obtain a canonical multiplication formula in $\mathbb{F}_{3^{\ell m}}$ which is valid for any $m \geq 1$. To the best of our knowledge, these formulae have the best known multiplication complexity in the literature improving the bounds in [7]. Moreover, we give an explicit formula in the case $\mathbb{F}_{3^{6 \cdot 97}}$.

In chapter 5, we present a method for multiplication in finite fields improving $\mu_q(n)$ for certain values of q and n. We use local expansions, the lengths of which are further parameters that can be used to optimize the bounds on the bilinear complexity, instead of evaluation into residue class field. Our basic principle is still based on the method of D. V. Chudnovsky and G. V. Chudnovsky. The main idea in the method is to use algebraic function fields of one variable with places of arbitrary degrees and to use some places not only once but many times. Moreover, we show that we obtain improved bounds for multiplication in $\mathbb{F}_{q^n}$ for certain values of q and n where $2 \leq n \leq 18$ and $q = 2, 3, 4$.

REFERENCES

[1] M. Bodrato and A. Zanoni, “Integer and Polynomial Multiplication: Towards Optimal Toom-Cook Matrices”, *Proceedings of the ISSAC 2007 conference*, Ontario, Canada, July 29-August 1, 2007, ACM press.

[2] P. Bürgisser, M. Clausen and M. A. Shokrollahi, *Algebraic Complexity Theory*, Springer, 1997.

[3] S. A. Cook,*On the Minimum Computation Time of Functions*. pages 51-77, Thesis, Harvard University, Cambridge, MA, 1966.

[4] H. Fan and M. Anwar Hasan, Comments on “Five, Six, and Seven-Term Karatsuba-Like Formulae”, *IEEE Transactions on Computers*, vol. 56, no. 5, pp. 716-717, 2007.

[5] A. Karatsuba and Y. Ofman, “Multiplication of multidigit numbers by automata”, *Soviet Physics-Doklady*, (7):595-596, 1963.

[6] D. E. Knuth, *The Art of Computer Programming: Seminumerical Algorithms*, Volume 2, Second Edition, Addison-Wesley, 1981.

[7] P. L. Montgomery,“ Five, six, and seven-term Karatsuba-like formulae”, *IEEE Transactions on Computers*, 54(3):362-369, March 2005.

[8] A. L. Toom, “The complexity scheme of functional elements realizing the multiplication of integers”, *Soviet Mathematics*, 3:714-716, 1963.

[9] A. Weimerskirch and C. Paar,“Generalizations of the Karatsuba Algorithm for Polynomial Multiplication”, http://eprint.iacr.org/2006/224, 2008.

[10] B. Sunar, “A Generalized Method for Constructing Subquadratic Complexity $GF(2^k)$ Multipliers”, *IEEE Transactions on Computers*, vol. 53, no. 9, pp. 1097-1105, 2004.

[11] S. Winograd, *Arithmetic Complexity of Computations,* SIAM, 1980.

[12] E. Gorla, C. Puttmann and J. Shokrollahi,“Explicit formulas for efficient multiplication in $\mathbb{F}_{3^{6m}}$”, in *Selected Areas in Cryptography (SAC2007)* (Also avaliable at http://www.arxiv.org/PS_cache/arxiv/pdf/0708/0708.3014v1.pdf).

[13] J. Shokrollahi, E. Gorla and C. Puttmann, “Efficient FPGA-Based Multipliers for $\mathbb{F}_{3^{97}}$ and $\mathbb{F}_{3^{6\cdot 97}}$”, in *Field Programmable Logic and Applications (FPL 2007)* (Also avaliable at http://www.arxiv.org/PS_cache/arxiv/pdf/0708/0708.3022v1.pdf).

[14] T. Kerins, W. P. Marnane, E. M. Popovici, and P. S. L. M. Barreto, “Efficient hardware for the tate pairing calculation in characteristic three”, in *Cryptographic Hardware and Embedded Systems, CHES2005, ser. Lecture Notes in Computer Science*, J. R. Rao and B. Sunar, Eds., vol. 3659. Springer- Verlag, 2005, pp. 412-426.

[15] M. D. Wagh and S. D. Morgera, “A new structured design method for convolutions over finite fields, Part I”, *IEEE Transactions on Information Theory*, 29(4):583-594, 1983.

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

[17] Ballet, S., “Quasi-optimal algorithms for multiplication in the extension of degree 13, 14, and 15”, *J. Pure Appl. Algebra*, 171, 149 -164 (2002).

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

[19] Ballet, S., “On the tensor rank of the multiplication in the finite field”, *J. Number Theory* (2007), in press, available at doi:10.1016/j.jnt.2007.06.010.

[20] Bosma, W., Cannon, J., CPlayoust, C, “The Magma algebra system. I. The user language”, *J. Symbolic Comput.*, 24(3-4), 235-265 (1997).

[21] Cenk, M., Özbudak, F., “Improved Polynomial Multiplication Formulae over $\mathbb{F}_2$ Using Chinese Remainder Theorem”, *IEEE Transactions on Computers*, to appear.

[22] Cenk, M., Özbudak, F., ”Efficient multiplication in $\mathbb{F}_{3^{\ell m}}$, $m \geq 1$ and $5 \leq \ell \leq 18$“, In Africacrypt 2008 volume 5023 of *Lecture Notes in Computer Science*, 406-414 Springer - Verlag.

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

[24] National Institute of Standards and Technology., “Digital Signature Standard”, *FIPS Publication 186-2*, February 2000.

[25] Niederreiter, H., Xing, C., *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge University Press, Cambridge, UK (2001).

[26] Page, D., Smart, N. P., “Hardware implementation of finite fields of characteristic three”, In CHESS 2003 volume 2523 of *Lecture Notes in Computer Science*, 539-539 Springer - Verlag.

[27] Shokrollahi, M. A.: Optimal algortihms for multiplication in certain finite fields using algebraic curves. SIAM J. Comput. 21 (6), 1193 - 1198 (1992).

[28] Shparlinski, I. E., Tsfasman, M. A., Vladut, S. G., “Curves with many points and multiplication in finite fields”, *Lecture Notes in Mathematics*, Vol. 1518, Springer, Berlin, pp. 145 - 169 (1992,).

[29] Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer, Berlin (1993).

VITA

Murat Cenk received the B.Sc. degree in Mathematics and Physics Education from Middle East Technical University in 2000 and M.Sc. degree in Mathematics and Computer Science from Cankaya University in 2003, in Ankara Turkey. He worked in Cankaya University at the department of Mathematics and Computer Science as research assistant between 2001 and 2005. He has been working as instructor in the same university since 2005. His research interests are finite fields, public key cryptography, efficient arithmetic for public key cryptography, coding theory, algebraic function fields over finite fields and algebra.

Publications

1. M. Cenk, F. Özbudak, "Improved Polynomial Multiplication Formulae over $\mathbb{F}_2$ Using Chinese Remainder Theorem", *IEEE Transactions on Computers*, to appear.

2. M. Cenk, F. Özbudak, "Efficient multiplication in $\mathbb{F}_{3^{\ell m}}$, $m \geq 1$ and $5 \leq \ell \leq 18$", In Africacrypt 2008 volume 5023 of *Lecture Notes in Computer Science*, pp. 406-414, 2008, Springer - Verlag.

3. M. Cenk, F. Özbudak, "On Multiplication in Finite Fields", 8th Central European Conference on Cryptography, Graz, 2008.

4. M. Cenk, F. Özbudak, "Isomorphism Classes of Ordinary Elliptic Curves Over Finite Fields of Characteristic 3", *Mathematical Methods in Engineering* with Editors K. Taş, J. A. Tenreiro Machado, D. Baleanu, pp. 151 - 158, Springer, 2007.

5. M. Cenk, F. Özbudak, "Eliptik Egri Kriptografi ve Aritmetigi", I. Ulusal Kriptoloji Sempozyumu, 2005, ODTU, Ankara.

6. M. Cenk, F. Özbudak, "Isomorphism Classes of Elliptic Curves Over Finite Fields of Characteristic 3", *II. Ulusal Kriptoloji Sempozyumu*, 2006, ODTU, Ankara.

7. M. Cenk, O. Yayla, "Ayrık Logaritma Problemini Kullanan E-imza“, *Ulusal Elektronik Imza Sempozyumu*, 2006, Ankara (Poster).

8. M. Cenk, F. Özbudak, ”Rings of Low Multiplicative Complexity and Fast Multiplication in Finite Fields F_{2^N}“, *Bilgi Güvenligi ve Kriptoloji Konferansı*, 2007, Ankara (Poster).

9. M. Cenk, F. Özbudak, “Efficient Multiplication in Finite Fields of Characteristic 3 and 5 for Pairing Based Cryptography”, *Bilgi Güvenligi ve Kriptoloji Konferansı*, 2008, Ankara.