2009 19th IEEE International Symposium on Computer Arithmetic

Polynomial Multiplication over Finite Fields using Field Extensions and Interpolation

Murat Cenk
Department of Mathematics and Computer Science
Cankaya University, Ankara, Turkey
mcenk@cankaya.edu.tr

Çetin Kaya Koç
University of California Santa Barbara, USA &
City University of Istanbul, Turkey
koc@cs.ucsb.edu

Ferruh Özbudak
Department of Mathematics and Institute of Applied Mathematics
Middle East Technical University, Ankara, Turkey
ozbudak@metu.edu.tr

Abstract

A method for polynomial multiplication over finite fields using field extensions and polynomial interpolation is introduced. The proposed method uses polynomial interpolation as Toom-Cook method together with field extensions. Furthermore, the proposed method can be used when Toom-Cook method cannot be applied directly. Explicit formulae improving the previous results in many cases are obtained.

1 Introduction

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 [6, 7] 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 [10] generalized Karatsuba algorithm and gave a detailed account of its variants. Recently, Montgomery [8] improved some of those results by giving explicit formulae for multiplying two arbitrary n-term polynomials, where $n \in \{5, 6, 7\}$. Toom-Cook [9, 4] 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 this paper we give a 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 [5].

The paper 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 3. We apply our method to polynomial multiplication over $\mathbb{F}_2$ and $10, 11$ and 12-term polynomial multiplication bounds are determined in Section 4. In Section 5 we discuss the efficiency of the proposed method. We conclude this paper in Section 6.

2 Background

Let $\mathcal{R}$ be an arbitrary commutative ring with identity and $\mathcal{R}[x]$ denote the ring of polynomials over $\mathcal{R}$ with the inde-

1063-6889/09 $25.00 © 2009 IEEE
DOI 10.1109/ARITH.2009.11

terminate 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 the paper, if not stated otherwise, an n-term polynomial $A(x)$ means an n-term polynomial with 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 the paper, $\mathbb{F}_q$ 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 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

$$M(n) \leq n^2. \tag{1}$$

2.2 Karatsuba Algorithm and Weimerskirch-Paar Generalization

Karatsuba algorithm [6] gives better upper bounds on $M(n)$. For example, consider two 2-term polynomials,

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

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 [10] 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

$$M(nm) \leq M(n)M(m). \tag{2}$$

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

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

where A_0, B_0 are degree $m-1$ polynomials and A_1, B_1 are degree m polynomials. Then $A(x)B(x) = A_0 B_0 + [(A_0 + A_1)(B_0 + B_1) - A_1 B_1 - A_0 B_0]x^m + A_1 B_1 x^{2m}$. Therefore we arrive to the following bound of [10]:

$$M(2m+1) \leq M(m) + 2M(m+1) \tag{3}$$

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

2.3 Montgomery's Contribution

Montgomery [8] observed, among other things, that one multiplication is redundant in (3). Hence

$$M(2m+1) \leq 2M(m+1) + M(m) - 1, \quad (m \geq 1). \tag{4}$$

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 the Table 1 in [8].

2.4 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 [9], [4] 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, 2] for the details. Hence if $q \geq 2n-2$, then Toom-Cook method gives

$$M_q(n) \leq 2n - 1. \tag{5}$$

However if $\mathcal{F}$ is a finite field $\mathbb{F}_q$ and n is large enough, this method cannot be applied directly (see also [8, 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 [8, Table 1]). Note that Toom-Cook method gives $M_7(3) = 5$ and $M_7(2) = 3$. Therefore using Toom-Cook method recursively and (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 1) and then we will improve this bound to $M_7(5) = 10$ (see Example 3) which is optimal and therefore we use equality.

Remark 1 *It follows from the definitions that the inequalities on (2) and (4) on $M(n)$ also hold if $M(n)$ is replaced with $M_q(n)$, where q is a prime power.*

3 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 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 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 element 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 1 *Let q be a prime power. We have $\mu_q(2) \leq 3$.*

Proof. Karatsuba algorithm [6] gives the result.

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

Proposition 1 *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*

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

Proof. Assume that $n > \frac{q+2}{2}$. We use Toom-Cook type evaluations over $\mathbb{F}_{q^2}$ using the point ∞, q elements of $\mathbb{F}_q$ and $2n-q-2$ elements from $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Here and throughout the paper, for sets $\mathcal{A}$ and $\mathcal{B}$, the notation $\mathcal{A} \setminus \mathcal{B}$ denotes the subset of $\mathcal{A}$ excluding the elements of $\mathcal{B}$. 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 1 we obtain that

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

Remark 2 *In the proof of Proposition 1, if we know that a multiplication corresponding to an evaluation and contributing to the upper bound (6) also appears in another evaluation, then we call such a multiplication an overlap. Since the proof of Proposition 1 does not take such overlaps into account, if we know the existence of such overlaps in a particular case, then the upper bound (6) can be improved. In Example 2 we will illustrate such a situation.*

In the following example we demonstrate how to find the formula of Proposition 1 explicitly.

Example 1 *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:*

$x = 0 \Rightarrow a_0b_0 = c_0$
$x = 1 \Rightarrow (a_0 + ... + a_4)(b_0 + ... + b_4) = (c_0 + ... + c_8)$
$x = 2 \Rightarrow (a_0 + ... + 2^4a_4)(b_0 + ... + 2^4b_4) = (c_0 + ... + 2^8c_8)$
$x = 3 \Rightarrow (a_0 + ... + 3^4a_4)(b_0 + ... + 3^4b_4) = (c_0 + ... + 3^8c_8)$
$x = 4 \Rightarrow (a_0 + ... + 4^4a_4)(b_0 + ... + 4^4b_4) = (c_0 + ... + 4^8c_8)$
$x = 5 \Rightarrow (a_0 + ... + 5^4a_4)(b_0 + ... + 5^4b_4) = (c_0 + ... + 5^8c_8)$

$x = 6 \Rightarrow (a_0+...+6^4a_4)(b_0+...+6^4b_4) = (c_0+...+6^8c_8)$
$x = w \Rightarrow (a_0+..+w^4a_4)(b_0+..+w^4b_4) = (c_0+..+w^8c_8)$
$x = \infty \Rightarrow a_4b_4 = c_8$

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).

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

As it is seen $\overline{D}_7$ *is the only product over* $\mathbb{F}_{49}$. *If we expand* $\overline{D}_7$, *then we get*
$\overline{D}_7 = t_1t_1' + [(t_1+t_2)(t_1'+t_2') - t_1t_1' - t_2t_2']w + t_2t_2'w^2$, *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*

$$\overline{D}_7 = D_7' + D_7''w,$$

where D_7' *and* D_7'' *are the multiplications over* $\mathbb{F}_7$ *with*

$$\begin{aligned} D_7' &= t_1t_1' + 3t_2t_2', \\ D_7'' &= [(t_1+t_2)(t_1'+t_2') - t_1t_1' - t_2t_2']. \end{aligned}$$

For any matrix A, *let* A^T *denote the transpose of* A. *Then we have* $C^T = VD^T$ *where*
$C = \begin{bmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 \end{bmatrix}$,
$D = \begin{bmatrix} D_0 & D_1 & D_2 & D_3 & D_4 & D_5 & D_6 & \overline{D}_7 & D_8 \end{bmatrix}$,
and

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2w & 3w+2 & w+5 & 6w+6 & 6w+1 & w+2 & 3w+5 & 6w & w \\ 0 & 6 & 5 & 3 & 3 & 5 & 6 & 0 & 6 \\ 0 & 6 & 6 & 1 & 6 & 1 & 1 & 0 & 0 \\ 0 & 6 & 3 & 5 & 5 & 3 & 6 & 0 & 0 \\ 0 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 0 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 & 0 & 0 \\ 5w & 4w+4 & 6w+5 & w+3 & w+4 & 6w+2 & 4w+3 & w & 6w \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

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*

$$\begin{aligned} c_0 &= D_0 \\ c_1 &= 2D_1 + 5D_2 + 6D_3 + D_4 + 2D_5 + 5D_6 + 4D_7'' \\ c_2 &= 6D_1 + 5D_2 + 3D_3 + 3D_4 + 5D_5 + 6D_6 + 6D_8 \\ c_3 &= 6D_1 + 6D_2 + D_3 + 6D_4 + D_5 + D_6 \\ c_4 &= 6D_1 + 3D_2 + 5D_3 + 5D_4 + 3D_5 + 6D_6 \\ c_5 &= 6D_1 + 5D_2 + 4D_3 + 3D_4 + 2D_5 + D_6 \\ c_6 &= 6D_0 + 6D_1 + 6D_2 + 6D_3 + 6D_4 + 6D_5 + 6D_6 \\ c_7 &= 4D_1 + 5D_2 + 3D_3 + 4D_4 + 2D_5 + 3D_6 + 3D_7'' \\ c_8 &= D_8 \end{aligned} \tag{7}$$

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 1 we have $M_2(3) \leq 9$. In the next example using 3 overlaps (cf. Remark 2) we will improve it to $M_2(3) \leq 6$.

Example 2 *Let* $q = 2$ *and* $n = 3$. *Let* $w \in \mathbb{F}_4 \setminus \mathbb{F}_2$ *with* $w^2+w+1 = 0$. *Let* $a_0+a_1x+a_2x^2$ *and* $b_0+b_1x+b_2x^2$ *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*

$$(a_0+a_1x+a_2x^2)(b_0+b_1x+b_2x^2) = c_0+c_1x+\ldots+c_4x^4.$$

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:*

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & w+1 & w & 1 \\ 0 & 1 & w & w+1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_0b_0 \\ (a_0+a_1+a_2)(b_0+b_1+b_2) \\ (a_0+wa_1+w^2a_2)(b_0+wb_1+w^2b_2) \\ (a_0+w^2a_1+w^4a_2)(b_0+w^2b_1+w^4b_2) \\ a_2b_2 \end{bmatrix}$$

Let us denote

$$\begin{aligned} \overline{D}_2 &= (a_0+wa_1+w^2a_2)(b_0+wb_1+w^2b_2), \\ \overline{D}_3 &= (a_0+w^2a_1+w^4a_2)(b_0+w^2b_1+w^4b_2). \end{aligned}$$

In the proof of Proposition 1, each of the contributions of $\overline{D}_2$ *and* $\overline{D}_3$ *to the upper bound (6) are counted as* 3. *Using* $w^2+w+1 = 0$, *we obtain that*

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

and

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

The counted multiplications in Proposition 1 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* $M_2(3) \leq (6n-2q-5)-3 = 6$.

In the rest of this section we give our generalizations. The first one is a straightforward generalization of Proposition 1. Recall that $\mu_q(m)$ is defined in Definition 1.

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

$$M_q(n) \leq q+1+\mu_q(m)(2n-q-2). \tag{8}$$

Proof. By changing $\mu_q(2) \leq 3$ with $\mu_q(m)$ and applying the similar arguments in the proof of Proposition 1, we complete the proof.

It follows from Definition 1 that if m_1, m_2 are positive integers and $m_1 \mid m_2$, then $\mu_q(m_1) \leq \mu_q(m_2)$. Here and throughout the paper, for two positive integers m_1 and m_2, the notation $m_1 \mid m_2$ denotes that m_1 divides 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 $1 \leq m_1 \leq m_2$ are positive integers with $m_1 \nmid m_2$, then in all cases we know 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. 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,

$$S_q(k) = \#\{\alpha \in \mathbb{F}_{q^k} \mid \alpha \notin \mathbb{F}_{q^d} \text{ for all } d|k\}. \tag{9}$$

Theorem 1 *Let q be a prime power and $m \geq 2$ an integer. For an integer $n > \frac{q+2}{2}$ assume it holds that*

$$2n - 2 \leq q + \sum_{2 \leq k \leq m} S_q(k), \tag{10}$$

where $S_q(k)$ is defined in (9). There exists a formula for multiplying two arbitrary n-term polynomials over $\mathbb{F}_q$ which gives

$$\begin{aligned} M_q(n) \leq \quad & 1 + q + \textstyle\sum_{2 \leq k < m} \mu_q(k) S_q(k) + \\ & \mu_q(m)(2n - 2 - q - \textstyle\sum_{2 \leq k < m} S_q(k)). \end{aligned} \tag{11}$$

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 (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 1 and Proposition 2, 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 3 *As in Proposition 1 and Remark 2, we can improve the upper bound (11) of Theorem 1 if we know the existence of overlaps. We provide such an example in Section 4.*

4 Improved Bounds for Multiplying 10, 11 and 12-term Polynomials over $\mathbb{F}_2$

In this section, we will give a mixed method which provides improved bounds. Then we show existence of some overlaps in Theorem 1 for $q = 2$ in detail and we will apply the results to $n = 10, 11$ and 12 by using the mixed method. The following fact will be combined by the proposed method to obtain the mixed method.

Fact 1 *Let $a(x)$ and $b(x)$ be n-term polynomials over $\mathbb{F}_q$. If ℓ coefficients of the product $a(x) \cdot b(x)$ are known then $(2n - 2 - \ell)$ elements of $\mathbb{F}_q$ are enough for finding other coefficients of the product $a(x) \cdot b(x)$ with $(2n - 2 - \ell)$ multiplications in $\mathbb{F}_q$.*

We refer to [3, p. 30] for the proof of this fact. Note that since we count the point ∞ as an evaluation point, it is enough to use $(2n - 2 - \ell)$ points. The following proposition gives some coefficients of the product polynomial with efficient number of multiplications. Therefore, we can use this proposition for further improvements.

Proposition 3 *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*
$c_0 = a_0 b_0,\ c_1 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1,$
$c_2 = (a_0 + a_2)(b_0 + b_2) - a_0 b_0 - a_2 b_2 + a_1 b_1,$
$c_{2n-2} = a_{n-1} b_{n-1},\ c_{2n-3} = (a_{n-1} + a_{n-2})(b_{n-1} + b_{n-2}) - a_{n-1} b_{n-1} - a_{n-2} b_{n-2},\ c_{2n-4} = (a_{n-1} + a_{n-3})(b_{n-1} + b_{n-3}) - a_{n-1} b_{n-1} - a_{n-3} b_{n-3} + a_{n-2} b_{n-2}.$

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 how to use Proposition 3 and Fact 1.

Example 3 *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 1 it is found $M_7(5) \leq 11$. Now we will find the optimal bound $M_7(5) = 10$ by using interpolation and Proposition 3. Now using the points of $\mathbb{F}_7$, ∞ and the known coefficient $c_1 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1$ in the equation*

$$\left(\sum_{i=0}^{4} a_i x^i\right)\left(\sum_{i=0}^{4} b_i x^i\right) = \left(\sum_{i=0}^{8} c_i x^i\right),$$

we get
$x = 0 \Rightarrow a_0 b_0 = c_0,$
$x = 1 \Rightarrow (a_0 + a_1 + ... + a_4)(b_0 + b_1 + ... + b_4) =$

$(c_0 + c_1 + ... + c_8)$,
$x = 2 \Rightarrow (a_0 + 2a_1 + ... + 2^4 a_4)(b_0 + 2b_1 + ... + 2^4 b_4) = (c_0 + 2c_1 + ... + 2^8 c_8)$,
$x = 3 \Rightarrow (a_0 + 3a_1 + ... + 3^4 a_4)(b_0 + 3b_1 + ... + 3^4 b_4) = (c_0 + 3c_1 + ... + 3^8 c_8)$,
$x = 4 \Rightarrow (a_0 + 4a_1 + ... + 4^4 a_4)(b_0 + 4b_1 + ... + 4^4 b_4) = (c_0 + 4c_1 + ... + 4^8 c_8)$,
$x = 5 \Rightarrow (a_0 + 5a_1 + ... + 5^4 a_4)(b_0 + 5b_1 + ... + 5^4 b_4) = (c_0 + 5c_1 + ... + 5^8 c_8)$,
$x = 6 \Rightarrow (a_0 + 6a_1 + ... + 6^4 a_4)(b_0 + 6b_1 + ... + 6^4 b_4) = (c_0 + 6c_1 + ... + 6^8 c_8)$,
$x = \infty \Rightarrow a_4 b_4 = c_8$,
and $c_1 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1$. *If we construct the system of linear equations in* $\mathbb{F}_7$ *like in Example 1, we see that the matrix of the linear system is invertible. Therefore we get* $M_7(5) = 10$ *since 7 multiplications comes from the elements of* $\mathbb{F}_7$*, 1 multiplication is counted for* ∞ *and 2 multiplications are counted for* c_1.

The proposed method described in Section 3 can be combined with Fact 1 and Proposition 3 as in Example 3. We call this method as the mixed method. Now we will find the polynomial multiplication bounds for $n = 10, 11$ and 12 over $\mathbb{F}_2$ by using the mixed method. However, in order to find better results we need to find all possible overlaps. The following proposition is for the case $\mathbb{F}_2$.

Proposition 4 *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 1:*

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 $\{\alpha, \alpha^2, \alpha^4\}$ *(respectively* $\{\alpha^3, \alpha^6, \alpha^5\}$*) is at most* 6, *instead of* $\mu_2(3) \cdot 3 \leq 18$,

iii) the total number of multiplications needed for the evaluation at the elements of the set $\{\gamma, \gamma^2, \gamma^4, \gamma^8\}$ *(respectively* $\{\gamma^3, \gamma^6, \gamma^{12}, \gamma^9\}$ *and* $\{\gamma^7, \gamma^{14}, \gamma^{13}, \gamma^{11}\}$*) 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
$A(w_1)B(w_1) = (A_0 B_0 + A_1 B_1) + w_1[(A_0 + A_1)(B_0 + B_1) + A_0 B_0)]$.
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 1 are

$$\begin{aligned} A_0 B_0 &= \left(\sum_{i \in I_1} a_i\right)\left(\sum_{i \in I_1} b_i\right), \\ A_1 B_1 &= \left(\sum_{i \in I_0} a_i\right)\left(\sum_{i \in I_0} b_i\right), \\ (A_0 + A_1)(B_0 + B_1) &= \left(\sum_{i \in I_2} a_i\right)\left(\sum_{i \in I_2} b_i\right). \end{aligned} \tag{12}$$

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).

Remark 4 *The observation that is used in the proof of Proposition 4 can be used for any finite field* $\mathbb{F}_q$. *If* $\mathbb{F}_{q^d}$ *is the extension field of* $\mathbb{F}_q$ *then the total number of multiplications needed for the evaluation at the elements of the set* $S = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}\}$ *is equal to the total number of multiplications needed for the evaluations at the element* α *because the elements in* S *are all conjugates of each other and they are the roots of the reduction polynomial of* $\mathbb{F}_{q^d}$. *Note that overlaps are independent from the reduction polynomial of* $\mathbb{F}_{q^d}$. *However, if polynomial multiplication is used for finite field multiplication then the reduction polynomial affects the number of additions. In order to decrease the number of additions it would is better to chose the reduction polynomial having coefficients as low as possible such as binomial or trinomial.*

Now we will show how to find the polynomial multiplication bounds by using the mixed method.

Example 4 *Let $q = 2$ and w, α, γ be as defined in proposition 4. We first consider 10-term polynomials over $\mathbb{F}_2$. As $2 \cdot 10 - 2 = 18$, using the method of Theorem 1, apart from the point at ∞, it is enough to choose the following evaluation 18 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 4 and the method of Theorem 1 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 ∞ 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

$$M_2(12) \leq 1 + 2 + 3 + 7 + 7 + 9 + 9 + 9 = 47.$$

However, a recent paper [5] finds $M_2(10) \leq 35, M_2(11) \leq 40$ and $M_2(12) \leq 44$ by using Chinese Remainder Theorem. We will also obtain the same bound in [5] by using the mixed method as follows: First $n = 10$. As $2 \cdot 10 - 2 = 18$, using the method of Theorem 1, 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 3, 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 $M_2(11) \leq 40$ 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.

5 Efficiency of the Proposed Method

The proposed method provides multiplication algorithms which uses less number of multiplications than known methods. However, since the proposed method is based on the interpolation method, the number of additions may increase. The main question is the effect of those additions in practice. In this section, we discuss the efficiency of the proposed method.

In order to see the effect of additions, we will give timing results for 5-term polynomials over fields of characteristic 5. We compare the proposed method for 5-term polynomial multiplication over $\mathbb{F}_5$ with Montgomery's 5-term multiplication formula [8] and Karatsuba's 5-term multiplication formula [10]. Note that Mongomery's and Karatsuba's 5-term polynomial multiplication formulae use 13 and 15 multiplications in $\mathbb{F}_5$, respectively.

The proposed method provides a 5-term polynomial multiplication formula with 11 multiplications in $\mathbb{F}_5$ as follows. Let $a(x) = \sum_{i=0}^{4} a_i x^i$ and $b(x) = \sum_{i=0}^{4} b_i x^i$ be 5-term polynomials over $\mathbb{F}_5$ such that $a(x)b(x) = c(x) = \sum_{i=0}^{8} c_i x^i$. We use the 5 points from $\mathbb{F}_5, \infty, \alpha$ and β where $\alpha, \beta \in \mathbb{F}_{5^2}/\mathbb{F}_5$ such that $\alpha^2 + 3 = 0$ and $\beta^2 + 3 = 0$. Moreover, if we use the known coefficient $c_1 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1$, we obtain the multiplication formula. Note that the total number of multiplications needed for the evaluation at the elements of the set $\{\alpha, \beta\}$ is at most 3 multiplications in $\mathbb{F}_5$ by Remark 4. Therefore we find $M_5(5) \leq 11$. The explicit formula is the following:

$m_1 = a_0 b_0,\ m_2 = (a_0 + a_1)(b_0 + b_1),\ m_3 = a_1 b_1,$
$m_4 = (a_0 + a_1 + a_2 + a_3 + a_4)(b_0 + b_1 + b_2 + b_3 + b_4),$
$m_5 = (a_0 + 2a_1 + 4a_2 + 3a_3 + a_4)(b_0 + 2b_1 + 4b_2 + 3b_3 + b_4),$
$m_6 = (a_0 + 3a_1 + 4a_2 + 2a_3 + a_4)(b_0 + 3b_1 + 4b_2 + 2b_3 + b_4),$
$m_7 = (a_0 + 4a_1 + a_2 + 4a_3 + a_4)(b_0 + 4b_1 + b_2 + 4b_3 + b_4),$
$m_8 = a_4 b_4,\ m_9 = (a_0 + 2a_2 + 4a_4)(b_0 + 2b_2 + 4b_4)$
$m_{10} = (a_1 + 2a_3)(b_1 + 2b_3),$
$m_{11} = (a_1 + 2a_3 + a_0 + 2a_2 + 4a_4)(b_1 + 2b_3 + b_0 + 2b_2 + 4b_4).$
$c_0 = m_1,$
$c_1 = m_2 - m_1 - m_3,$
$c_2 = 2m_1 + 3m_4 + 4m_5 + 4m_6 + 3m_7 + 2m_8 + 4m_9 + 8m_{10},$
$c_3 = 2m_2 - 2m_1 - 2m_3 + 3m_4 + 2m_5 + 3m_6 + 2m_7 + 4m_{11} - 4m_9 - 4m_{10},$
$c_4 = 4m_1 + 4m_4 + 4m_5 + 4m_6 + 4m_7 + 4m_8,$
$c_5 = 4m_2 - 4m_1 - 4m_3 + 4m_4 + 2m_5 + 3m_6 + m_7,$
$c_6 = 3m_1 + m_4 + 2m_5 + 2m_6 + m_7 + 3m_8 + m_9 + 2m_{10},$
$c_7 = 3m_2 - 3m_1 - 3m_3 + m_4 + m_5 + 4m_6 + 4m_7 + m_{11} - m_9 - m_{10},$
$c_8 = m_8.$

In Table 1, we give timing comparisons among our explicit formula, Montgomery's 5-term polynomial multiplications [8] and Karatsuba's 5-term polynomial multiplication formula [10]. We implement the formulae recursively by using (2) for 5^k-term polynomial multiplications over $\mathbb{F}_5$, where $k \geq 1$. The implementation of formulae in the platform of a single-processor 3.00-GHZ Pentium 4 gives a slightly slower timing results for 5-term polynomials as indicated in Table 1. However, proposed explicit formula for

5-term polynomial multiplications over $\mathbb{F}_5$ is much better in timings compared to [8] and [10], especially for $k > 1$ because the number of multiplications dominates the number of additions for $k > 1$.

Table 1: Timings (μ sec) for $\mathbb{F}_5$ Polynomial Multiplication

n	Proposed Method	Montgomery	Karatsuba
5	0.14	0.12	0.09
25	3.58	3.83	3.98
125	49.6	62.08	69.12
625	652.8	944.64	1,075.2
3,125	16,896	32,481	37,376

Finally we give two examples of practical applications for which the number multiplications in polynomial multiplication formula is much more important than the number additions used in that formula.

Firstly we consider polynomial multiplication over large finite fields. Let $m > 1$ be an integer. It is well known that any n-term polynomial multiplication formula over $\mathbb{F}_q$ is valid for n-term polynomial multiplication over $\mathbb{F}_{q^m}$. If we apply the proposed formula over $\mathbb{F}_{q^m}$, the effect of addition will be negligible. For example, consider the proposed formula for 5-term polynomial multiplication formula over $\mathbb{F}_5$. When we use this proposed formula for 5-term polynomials over $\mathbb{F}_{5^m}$, we use 11 multiplications in $\mathbb{F}_{5^m}$ whereas Montgomery's formula uses 13 multiplications in $\mathbb{F}_{5^m}$ and Karatsuba's formula uses 15 multiplications in $\mathbb{F}_{5^m}$. Since the multiplication in $\mathbb{F}_{5^m}$ takes much more time than the addition in $\mathbb{F}_{5^m}$, the formula which uses less multiplication will produce faster polynomial multiplication.

Second we consider the multiplication of matrix polynomials. Multiplication of matrices takes much more time than their addition. In such an application, the number of multiplications will be more important parameter than the number of additions. For example, consider the 10-term binary matrix polynomials with coefficients of the size 512×512 matrices. In this case the multiplication of those matrices will take much more time than the additions of those matrices. So, the proposed method will give faster matrix multiplication of polynomials.

6 Conclusions

We gave 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 for n-term polynomial multiplications over $\mathbb{F}_2$, where $n \in \{10, 11, 12\}$, in detail. Moreover we discussed the efficiency of the proposed method.

Acknowledgments

A part of this paper was written while the third author was visiting Temasek Laboratories and Department of Mathematics at the National University of Singapore. He would like to thank both institutes for the hospitality. This research of the third author was supported by the DSTA grant R-394-000-025-422 with Temasek Laboratories in Singapore and NTU Research Grant No. M58110003. The first and the third authors were supported by TÜBİTAK under Grant No. TBAG-107T826.

References

[1] M. Bodrato and A. Zanoni. Integer and Polynomial Multiplication: Towards Optimal Toom-Cook Matrices, *Proceedings of the ISSAC 2007 Conference*, Ontario, Canada, pp. 17 - 24, ACM Press, July 29 - August 1, 2007, ACM press.

[2] M. Bodrato: Towards optimal Toom-Cook multiplication for univariate and multivariated polynomials in characteristic 2 and 0, Proc. WAIFI 2007, LNCS 4547, pp.116-133, June 2007.

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

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

[5] 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.

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

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

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

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

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