Obtaining More Karatsuba-Like Formulae over the Binary Field

Haining Fan, Ming Gu, Jiaguang Sun and Kwok-Yan Lam

Abstract

The aim of this paper is to find more Karatsuba-like formulae for a fixed set of moduli polynomials in $GF(2)[x]$. To this end, a theoretical framework is established. We first generalize the division algorithm, and then present a generalized definition of the remainder of integer division. Finally, a previously generalized Chinese remainder theorem is used to achieve our initial goal. As a by-product of the generalized remainder of integer division, we rediscover Montgomery's N-$residue$ and present a systematic interpretation of definitions of Montgomery's multiplication and addition operations.

Index Terms

Karatsuba algorithm, polynomial multiplication, Chinese remainder theorem, Montgomery algorithm, finite field.

I. Introduction

Efficient $GF(2^n)$ multiplication operation is important in cryptosystems. The main advantage of subquadratic multipliers is that their low asymptotic space complexities make it possible to implement VLSI multipliers for large values of n. The Karatsuba algorithm, which was invented by Karatsuba in 1960 [1], provides a practical solution for subquadratic $GF(2^n)$ multipliers [2]. Because time and space complexities of these multipliers depend on low-degree Karatsuba-like formulae, much effort has been devoted to obtain Karatsuba-like formulae with low multiplication complexity. Using the Chinese remainder theorem (CRT), Lempel, Seroussi and Winograd obtained a quasi-linear upper bound of the multiplicative complexity of multiplying

Haining Fan, Ming Gu, Jiaguang Sun and Kwok-Yan Lam are with the School of Software, Tsinghua University, Beijing, China. E-mails: {fhn, guming, sunjg, lamky}@tsinghua.edu.cn

two polynomials over finite fields [3]. Weimerskirch and Paar generalized the Karatsuba algorithm and showed how to use it with the least number of operations [4]. Based on an exhaustive search method, Montgomery presented Karatsuba-like formulae which multiply two polynomials of degree at most 4, 5, or 6 in $GF(2)[x]$ [5]. He also obtained new upper bounds on the multiplication complexity of n-term (degree $n-1$) polynomials for some small n. Recently, some bounds in [5] were improved by Fan and Hasan [6], Cenk and Özbudak [7], Oseledets [8] and Cenk, Koç and Özbudak [9].

Apart from Weimerskirch and Paar's method, the above methods can be classified into two categories: the exhaustive search method [5] [8] and the CRT-based method [3] [6] [7] [8] [9]. The exhaustive search method can find all n-term Karatsuba-like formulae for a fixed value of n, but its drawback is obvious, namely, it can only be used for small values of n. The CRT-based method is suitable for both small and large values of n, but only one n-term Karatsuba-like formula can be derived once the set of moduli polynomials is chosen.

The purpose of this paper is to find more Karatsuba-like formulae for a fixed set of moduli polynomials in $GF(2)[x]$. To this end, a theoretical framework is established. We first generalize the division algorithm, and then present a generalized definition of the remainder of integer division. As a by-product of these generalizations, we find that the residue class determined by this generalized remainder turns out to be Montgomery's $N\text{-}residue$ [11]; and furthermore, we present a systematic interpretation of definitions of Montgomery's multiplication and addition operations. Finally, a previously generalized CRT is used to achieve our initial goal.

The remainder of this article is organized as follows: We present the generalized division algorithm in Section II. After presenting two examples in Section III, we summarize a method to obtain more Karatsuba-like formulae. Finally, concluding remarks are made in Section IV.

II. A Generalization of the Division Algorithm

A. A Generalization of the Division Algorithm

The integer division algorithm is the basis of the congruence theory.

Theorem 1 (The division algorithm): $\forall 0 < m,\ a \in \mathbb{Z}$, there exist unique integers q' and r' with $0 \le r' < m$ such that $a = m \cdot q' + r'$.

Based on Theorem 1, we have the classical definition of the remainder of a modulo m, i.e., *Definition 1:* $\forall 0 < m,\ a \in \mathbb{Z}$, the remainder of a modulo m is defined as $a \bmod m := r' = a - mq'$, where r' and q' are unique integers determined by Theorem 1.

More precisely, r' in Theorem 1 is called the least non-negative remainder. In the following, we will use $\langle a \rangle_m$ to denote $a \bmod m$. Before we present the proposed generalization of Theorem 1, we introduce another generalization of the division algorithm.

Theorem 2 (The 1st generalization of the division algorithm): $\forall 0 < m,\ a,\ d \in \mathbb{Z}$, there exist unique integers q' and r' with $d \le r' < m + d$ such that $a = mq' + r'$.

Especially, if $d = -\lfloor \frac{m}{2} \rfloor$ then $-\lfloor \frac{m}{2} \rfloor \le r' < m - \lfloor \frac{m}{2} \rfloor$. In this case, r' is called the least absolute remainder. As an application of this generalization, the original Euclidean algorithm for integers can be slightly speeded up [10, Exercise 3.13 and 3.30].

Let $\mathbb{Z}_m^* = \{i | i \in \mathbb{Z}_m \text{ and } \gcd(i, m) = 1\}$ be the multiplicative group of $\mathbb{Z}_m$ and "$\cdot$" denote the multiplication operation in $\mathbb{Z}$. The second generalization of the division algorithm is as follows.

Proposition 3 (The 2nd generalization of the division algorithm): $\forall 0 < m,\ a \in \mathbb{Z}$. Let $R^{-1} \in \mathbb{Z}_m^*$ be the multiplicative inverse of $R \in \mathbb{Z}_m^*$. Then there exist unique integers q and r with $0 \le r < m$ such that $a = m \cdot q + R^{-1} \cdot r$.

Proof:

$\because$ R^{-1} is the multiplicative inverse of R in $\mathbb{Z}_m^*$,

$\therefore$ $\exists u \in \mathbb{Z}$ such that $1 = um + RR^{-1}$.

$\therefore a = aum + aRR^{-1}$.

By the division algorithm, there exist unique integers q'' and r'' such that $aR = mq'' + r''$, where $0 \le r'' = \langle aR \rangle_m < m$. Therefore, $a = aum + (aR)R^{-1}$ can be rewritten as

$$\begin{aligned} a &= aum + (mq'' + r'')R^{-1} \\ &= aum + mq''R^{-1} + R^{-1}r'' \\ &= (au + q''R^{-1})m + R^{-1}r'' \end{aligned}$$

$\therefore$ There exist integers $q = (ua + q''R^{-1})$ and $r = r'' = \langle aR \rangle_m$ with $0 \le r < m$ such that $a = mq + R^{-1}r$.

To prove the uniqueness, we assume, on the contrary, that there exist q_1, q_2, and $0 \le r_1, r_2 < m$ such that $a = m \cdot q_1 + R^{-1} \cdot r_1 = m \cdot q_2 + R^{-1} \cdot r_2$.

If $r_1 = r_2$ then it is easy to prove that $q_1 = q_2$.

For the case $r_1 \neq r_2$, since $(m, R^{-1}) = 1$ and m divides $0 = a - a = m(q_1 - q_2) + R^{-1} \cdot (r_1 - r_2)$, we have $r_1 = r_2$. This is a contradiction. □

Obviously, Proposition 3 becomes Theorem 1 when $R = R^{-1} = 1$.

Because the classical definition of the remainder of a modulo m, i.e., $\langle a \rangle_m$ in Definition 1, is based on the classical division algorithm Theorem 1, and we have just generalized Theorem 1 to Proposition 3, the unique integer $r = \langle aR \rangle_m$ appeared in the proof of Proposition 3 can be naturally viewed as a generalization of $\langle a \rangle_m$, i.e.,

Definition 2 (A generalized remainder of a modulo m): $\forall 0 < m,\ a \in \mathbb{Z}$ and $R \in \mathbb{Z}_m^*$. The generalized remainder of a modulo m w.r.t. R is defined as $\langle a \rangle_{(m,R)} := \langle a \cdot R \rangle_m$.

The reader may be familiar with $\langle aR \rangle_m$. In fact, it corresponds to the $N\text{-}residue$ of a defined by Montgomery in [11]. Montgomery's representation involves only one parameter R. Using the generalized division algorithm, we can readily deal with two or more R's. The following equation is such an example, and it will be used in the next section.

$$\langle ab \rangle_{(m,R_c)} = \left\langle aR_a \cdot bR_b \cdot \frac{R_c}{R_a R_b} \right\rangle_m = \left\langle \langle a \rangle_{(m,R_a)} \cdot \langle b \rangle_{(m,R_b)} \cdot \frac{R_c}{R_a R_b} \right\rangle_m . \tag{1}$$

B. A Systematic Interpretation of Definitions of Montgomery's Multiplication and Addition Operations

Let $a = m \cdot q_a + R^{-1} \cdot r_a$ and $b = m \cdot q_b + R^{-1} \cdot r_b$ be two positive integers, whose $N\text{-}residues$ correspond to $r_a = \langle a \rangle_{(m,R)} = \langle a \cdot R \rangle_m$ and $r_b = \langle b \rangle_{(m,R)} = \langle b \cdot R \rangle_m$ respectively. In Montgomery's representation, the addition operation "$\oplus$", i.e., $r_a \oplus r_b := \langle r_a + r_b \rangle_m$, is defined the same as that in $\mathbb{Z}_m$. But the definition of the multiplication operation "$\otimes$" is different, which is defined as $r_a \otimes r_b := \langle r_a \cdot r_b \cdot R^{-1} \rangle_m$. The reason that operation "$\otimes$" is defined in this way, not other expressions, can be traced back to the N-residue of $a \cdot b$, which is uniquely determined by the generalized division algorithm. Or, more precisely, expanding $a \cdot b = (m \cdot q_a + R^{-1} \cdot r_a)(m \cdot q_b + R^{-1} \cdot r_b)$ as

$$a \cdot b = m(mq_a q_b + q_a R^{-1} r_b + q_b R^{-1} r_a) + R^{-1}(R^{-1} \cdot r_a \cdot r_b)$$

and expressing $(R^{-1} \cdot r_a \cdot r_b)$ as $R^{-1} \cdot r_a \cdot r_b = m\lfloor \frac{R^{-1} \cdot r_a \cdot r_b}{m} \rfloor + \langle R^{-1} \cdot r_a \cdot r_b \rangle_m$ by the division algorithm, we have

$$a \cdot b = m\left(mq_a q_b + q_a R^{-1} r_b + q_b R^{-1} r_a + R^{-1} \lfloor \frac{R^{-1} \cdot r_a \cdot r_b}{m} \rfloor\right) + R^{-1}[\langle R^{-1} \cdot r_a \cdot r_b \rangle_m].$$

By Proposition 3 and Definition 2, the integer $\langle R^{-1}\cdot r_a\cdot r_b\rangle_m = \langle (a\cdot b)R\rangle_m$ in the square brackets just corresponds to the N-$residue$ of $a \cdot b$.

The definition of Montgomery's addition operation of N-$residues$ can also be interpreted similarly: expressing $a+b$ by the generalized division algorithm as

$$\begin{aligned} a+b &= (m\cdot q_a + R^{-1}\cdot r_a) + (m\cdot q_b + R^{-1}\cdot r_b) \\ &= m(q_a+q_b) + R^{-1}(r_a+r_b) \\ &= m\left(q_a+q_b+R^{-1}\lfloor\frac{r_a+r_b}{m}\rfloor\right) + R^{-1}\langle r_a+r_b\rangle_m, \end{aligned}$$

the integer $\langle r_a+r_b\rangle_m$ corresponds to Montgomery's summation of two N-$residues$ r_a and r_b, i.e., $r_a \oplus r_b$.

C. A Generalization of the CRT

The following is an integer version of the CRT.

Theorem 4 (CRT): Let $t>1$, $m_1, m_2, \cdots, m_t$ be pairwisely coprime positive integers, $M = \prod_{i=1}^{t} m_i$ and $M_i = \frac{M}{m_i}$. Then the unique solution y modulo M to the system of linear congruences $\langle y\rangle_{m_i} = y_i'$ is

$$y = \left\langle \sum_{i=1}^{t} y_i' \cdot M_i \cdot \left\langle M_i^{-1}\right\rangle_{m_i} \right\rangle_M , \tag{2}$$

where $\left\langle M_i^{-1}\right\rangle_{m_i}$ is the multiplicative inverse of M_i in $\mathbb{Z}_{m_i}^*$ and $1 \le i \le t$.

In the above subsection, we have presented a generalized definition of the remainder of integer division. Therefore, it is natural to seek the solution to the system of the generalized linear congruences $\langle y\rangle_{(m_i,R_i)} = y_i$. This consideration leads to a rediscovery of the following generalized CRT [12]:

Theorem 5 (A generalized CRT): Let $t>1$, $m_1, m_2, \cdots, m_t$ be pairwisely coprime positive integers, $M = \prod_{i=1}^{t} m_i$, $M_i = \frac{M}{m_i}$ and $R_i \in \mathbb{Z}_{m_i}^*$. Then the unique solution y modulo M to the system of generalized linear congruences $\langle y\rangle_{(m_i,R_i)} = y_i$ is

$$y = \left\langle \sum_{i=1}^{t} y_i \cdot M_i \cdot \left\langle \left\langle M_i^{-1}\right\rangle_{m_i} \cdot \left\langle R_i^{-1}\right\rangle_{m_i} \right\rangle_{m_i} \right\rangle_M , \tag{3}$$

where $\left\langle M_i^{-1}\right\rangle_{m_i}$ and $\left\langle R_i^{-1}\right\rangle_{m_i}$ are multiplicative inverses of M_i and R_i in $\mathbb{Z}_{m_i}^*$ respectively and $1 \le i \le t$.

The correctness of this theorem is clear since the system of linear congruences $\langle y\rangle_{(m_i,R_i)} = \langle y\cdot R_i\rangle_{m_i} = y_i$ is equivalent to the system of linear congruences $\langle y\rangle_{m_i} = \langle y_i\cdot R_i^{-1}\rangle_{m_i}$, which has the solution (3) by (2).

Until now, we have focussed only on the ring $\mathbb{Z}_m$. In fact, these results can be transferred to the polynomial ring $F[x]$ without essential modification, where F is a field. For simplicity, we do not rewrite them here.

III. Obtaining More Karatsuba-Like Formulae in $GF(2)[x]$

We now use the above results to obtain more Karatsuba-like formulae for a fixed set of moduli polynomials in $GF(2)[x]$. Two examples are presented first to illustrate the main idea.

A. 3-term Karatsuba-like Formulae

This example provides all 3-term Karatsuba-like formulae that can be derived from the generalized CRT Theorem 5. These formulae compute $C = \sum_{i=0}^{4} c_i x^i = AB = (a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0)$ in $GF(2)[x]$ using 6 multiplications.

For the purpose of comparison, we first present the formula derived from the conventional CRT. The moduli polynomials used in this example are $f_\infty = x - \infty$, $f_0 = x$, $f_1 = x+1$ and $f_2 = x^2+x+1$. We will not present the detailed procedure to construct the whole Karatsuba-like formula. Instead, we present only the computation procedure of the term $\left\langle y_2'\cdot M_2\cdot \left\langle M_2^{-1}\right\rangle_{f_2}\right\rangle_M$ appeared in the conventional CRT, which will be called the product term in the following.

For moduli polynomial $f_2 = x^2+x+1$. We first compute parameters $M = f_0\cdot f_1\cdot f_2 = x^4+x$, $M_2 = \frac{M}{f_2} = x^2+x$ and $\langle M_2^{-1}\rangle_{f_2} = 1$. Then we compute the product term as follows:

$$
\begin{aligned}
& \left\langle \langle AB\rangle_{f_2}\cdot M_2\cdot \langle M_2^{-1}\rangle_{f_2}\right\rangle_M \\
= & \left\langle \langle\langle A\rangle_{f_2}\cdot\langle B\rangle_{f_2}\rangle_{f_2}\cdot M_2\cdot\langle M_2^{-1}\rangle_{f_2}\right\rangle_M \\
= & \left\langle \langle[(a_1+a_2)x+(a_0+a_2)]\cdot[(b_1+b_2)x+(b_0+b_2)]\rangle_{f_2}\cdot(x^2+x)\cdot 1\right\rangle_M \\
= & \left\langle \left\langle m_4x^2+(m_3+m_4+m_5)x+m_3\right\rangle_{f_2}\cdot(x^2+x)\right\rangle_M \\
= & [(m_3+m_5)x+(m_3+m_4)]\cdot(x^2+x) \\
= & (m_3+m_5)x^3+(m_4+m_5)x^2+(m_3+m_4)x, \qquad (4)
\end{aligned}
$$

where $m_3 = (a_0+a_2)(b_0+b_2)$, $m_4 = (a_1+a_2)(b_1+b_2)$ and $m_5 = (a_0+a_1)(b_0+b_1)$.

After getting the two product terms corresponding to two other moduli polynomials $f_0 = x$ and $f_1 = x + 1$, we can obtain the CRT-based 3-term Karatsuba-like formula using the construction multiplication modulo $(x - \infty)^w$ [6, Lemma 2]. The formula is listed in table I as $\mathcal{F}_1$.

TABLE I

ALL 3-TERM KARATSUBA-LIKE FORMULAE OBTAINED FROM THEOREM 5

No.	(R_A, R_B)	c_i's	The six multiplications
$\mathcal{F}_1$	$(1,1)$, (x,x), $(x+1,x+1)$	$c_0 = m_0$ $c_1 = m_1 + m_2 + m_3 + m_4$ $c_2 = m_1 + m_4 + m_5$ $c_3 = m_0 + m_1 + m_3 + m_5$ $c_4 = m_2$	$m_0 = a_0b_0$ $m_1 = (a_0 + a_1 + a_2)(b_0 + b_1 + b_2)$ $m_2 = a_2b_2$ $m_3 = (a_0 + a_2)(b_0 + b_2)$ $m_4 = (a_1 + a_2)(b_1 + b_2)$ $m_5 = (a_0 + a_1)(b_0 + b_1)$
$\mathcal{F}_2$	$(x,1)$, $(1,x+1)$, $(x+1,x)$	$c_0 = m_0$ $c_1 = m_1 + m_2 + m_4 + m_5$ $c_2 = m_1 + m_3 + m_5$ $c_3 = m_0 + m_1 + m_3 + m_4$ $c_4 = m_2$,	$m_0 = a_0b_0$ $m_1 = (a_0 + a_1 + a_2)(b_0 + b_1 + b_2)$ $m_2 = a_2b_2$ $m_3 = (a_1 + a_2)(b_0 + b_2)$ $m_4 = (a_0 + a_1)(b_1 + b_2)$ $m_5 = (a_0 + a_2)(b_0 + b_1)$
$\mathcal{F}_3$	$(1,x)$, $(x+1,1)$, $(x,x+1)$	$c_0 = m_0$ $c_1 = m_1 + m_2 + m_4 + m_5$ $c_2 = m_1 + m_3 + m_5$ $c_3 = m_0 + m_1 + m_3 + m_4$ $c_4 = m_2$	$m_0 = a_0b_0$ $m_1 = (a_0 + a_1 + a_2)(b_0 + b_1 + b_2)$ $m_2 = a_2b_2$ $m_3 = (a_0 + a_2)(b_1 + b_2)$ $m_4 = (a_1 + a_2)(b_0 + b_1)$ $m_5 = (a_0 + a_1)(b_0 + b_2)$

Now we present the new formula derived from the generalized CRT Theorem 5. We need to generalize the two remainders $\langle A\rangle_{f_2} = \langle A\rangle_{(f_2,1)}$ and $\langle B\rangle_{f_2} = \langle B\rangle_{(f_2,1)}$ appeared in (4) to $\langle A\rangle_{(f_2,R_A)}$ and $\langle B\rangle_{(f_2,R_B)}$, where R_A and R_B belong to the multiplicative group $GF(2)[x]/(f_2)^* = \{1, x, x+1\}$. Setting $(R_A, R_B) = (x, 1)$, we have $\langle A\rangle_{(f_2,R_A)} = \langle A\cdot x\rangle_{f_2} = (a_0+a_1)x+(a_1+a_2)$

and $\langle R_A^{-1}\rangle_{f_2} = x+1$. Then we obtain the following product term by (1).

$$
\begin{aligned}
& \big\langle \langle AB\rangle_{f_2} \cdot M_2 \cdot \langle M_2^{-1}\rangle_{f_2}\big\rangle_M \\
= \;& \big\langle \langle (A\cdot R_A \cdot R_A^{-1})\cdot(B\cdot R_B\cdot R_B^{-1})\rangle_{f_2} \cdot M_2 \cdot \langle M_2^{-1}\rangle_{f_2}\big\rangle_M \\
= \;& \big\langle \langle \langle A\rangle_{(f_2,R_A)} \cdot \langle B\rangle_{(f_2,R_B)}\rangle_{f_2} \cdot M_2 \cdot \langle M_2^{-1}\cdot R_A^{-1}\cdot R_B^{-1}\rangle_{f_2}\big\rangle_M \\
= \;& \big\langle \langle \langle A\rangle_{(f_2,x)} \cdot \langle B\rangle_{f_2}\rangle_{f_2} \cdot (x^2+x)\cdot(x+1)\big\rangle_M \\
= \;& \big\langle \langle [(a_0+a_1)x+(a_1+a_2)]\cdot[(b_1+b_2)x+(b_0+b_2)]\rangle_{f_2}\cdot(x^3+x)\big\rangle_M \\
= \;& \big\langle \langle m_4x^2+(m_3+m_4+m_5)x+m_3\rangle_{f_2}\cdot(x^3+x)\big\rangle_M \\
= \;& \big\langle [(m_3+m_5)x+(m_3+m_4)]\cdot(x^3+x)\big\rangle_{x^4+x} \\
= \;& (m_3+m_4)x^3+(m_3+m_5)x^2+(m_4+m_5)x,
\end{aligned}
$$

where $m_3=(a_1+a_2)(b_0+b_2)$, $m_4=(a_0+a_1)(b_1+b_2)$ and $m_5=(a_0+a_2)(b_0+b_1)$.

The remaining steps to construct the new 3-term Karatsuba-like formula are the same as those in the conventional CRT, and we list this new formula $\mathcal{F}_2$ in the middle of table I.

It is clear that the CRT-based formula $\mathcal{F}_1$ is symmetrical, namely, it does not change if we exchange "a" and "b" in m_i's. But if we exchange "a" and "b" in the new formula $\mathcal{F}_2$, we will obtain a brand new formula $\mathcal{F}_3$, which can be obtained by setting $(R_A,R_B)=(1,x)$. Therefore, formula $\mathcal{F}_2$ (or $\mathcal{F}_3$) is not symmetrical from this point of view.

Since there are 3 elements in $GF(2)[x]/(f_2)^* = \{1, x, x{+}1\}$, we have 9 different combinations of pair (R_A,R_B). For each of these pairs, we can obtain one 3-term Karatsuba-like formula. But some of them are the same. For example, the CRT-based formula $\mathcal{F}_1$, which is derived by setting $(R_A,R_B)=(1,1)$, can also be obtained by setting $(R_A,R_B)=(x,x)$ or $(R_A,R_B)=(x+1,x+1)$. In table I, all three distinct formulae are listed. Here we note that f_2 is the only moduli polynomial that the generalized CRT can be applied to because there is only one element, i.e., 1, in either $GF(2)[x]/(f_0)^*$ or $GF(2)[x]/(f_1)^*$.

B. Another 9-term Karatsuba-like Formula

A 9-term CRT-based Karatsuba-like formula, which computes $C=\sum_{i=0}^{16} c_ix^i = A\cdot B = \sum_{i=0}^{8} a_ix^i \cdot \sum_{i=0}^{8} b_ix^i$ in $GF(2)[x]$, was given in [7]. They selected the moduli polynomials $(x-\infty)^3$, $f_{11}^3=x^3$, $f_{12}^3=(x+1)^3$, $f_{21}=x^2+x+1$, $f_{31}=x^3+x+1$ and $f_{32}=x^3+x^2+1$.

In the following, we will also use these moduli polynomials and derive a new Karatsuba-like formula by generalizing product terms corresponding to moduli polynomials f_{31} and f_{32}.

For moduli polynomial f_{31}, we select $R_A = R_B = x$ and compute $\langle A\rangle_{(f_{31},R_A)} = \langle A\cdot x\rangle_{f_{31}}$ and $\langle B\rangle_{(f_{31},R_B)} = \langle B\cdot x\rangle_{f_{31}}$ first. Then we compute its product term as follows.

$$\begin{aligned} & \left\langle \langle AB\rangle_{f_{31}} \cdot M_{31} \cdot \left\langle \frac{1}{M_{31}} \right\rangle_{f_{31}} \right\rangle_M \\ = & \left\langle \langle \langle A\rangle_{(f_{31},R_A)} \cdot \langle B\rangle_{(f_{31},R_B)}\rangle_{f_{31}} \cdot M_{31} \cdot \left\langle \frac{1}{M_{31}} \cdot \frac{1}{R_A\cdot R_B} \right\rangle_{f_{31}} \right\rangle_M . \end{aligned}$$

For moduli polynomial f_{32}, we select $R_A = R_B = x+1$ and perform similar computation. Finally, we can obtain a new formula. This formula also consists of 30 multiplication m_i's. Except for m_9 and m_{11}, all other m_i's are the same as those in [7]. Careful comparison shows that coefficient c_{13} in [7] is a summation of 20 m_i's, but every c_i in the new formula is a summation of no more than 19 m_i's. However, if we set $R_A = R_B = x^2$ for f_{31} and $R_A = R_B = x$ for f_{32}, we will obtain another formula in which c_{13} is a summation of 21 m_i's.

Summarizing the method used in the above two examples, we can obtained an algorithm to derive more Karatsuba-like formulae in $GF(2)[x]$, namely,

1. For each moduli polynomial f_i, define $S_i = GF(2)[x]/(f_i)^*$;
2. For each pair $(R_A, R_B) \in S_i \times S_i$, derive a formula using the generalized CRT;
3. Save this formula if it is a new one.

IV. Conclusions

We have generalized the division algorithm, and presented a method to obtain more n-term Karatsuba-like formulae in $GF(2)[x]$ for a fixed set of moduli polynomials. These new n-term formulae have the same multiplication complexity as that obtained from the conventional CRT. As for the addition complexity, we have checked some 4, 5, 6, 7, 8, and 9-term new formulae, but have not found obvious advantage or disadvantage. Even though, the proposed method can provide us with a broader understanding of Karatsuba-like formulae.

Acknowledgment

The work was supported by NSFC under grant No. 60970147.

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

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

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

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

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

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

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

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

$$m_9 = (a_0 + a_1 + a_2 + a_5 + a_7 + a_8)(b_0 + b_1 + b_2 + b_5 + b_7 + b_8);$$

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

$$m_{11} = (a_0 + a_1 + a_2 + a_4 + a_7 + a_8)(b_0 + b_1 + b_2 + b_4 + b_7 + b_8);$$

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

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

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

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

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

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

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

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

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

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

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

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

$$m_{24} = a_0 b_0;$$

$$m_{25} = a_1 b_1;$$

$$m_{26} = a_7 b_7;$$

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

$$m_{28} = a_6 b_6;$$

$$m_{29} = a_8 b_8;$$

$$m_{30} = a_2 b_2;$$

$$
\begin{aligned}
c_0 &= m_{24};\\
c_1 &= m_{24}+m_{25}+m_{23};\\
c_2 &= m_{22}+m_{24}+m_{30}+m_{25};\\
c_3 &= m_{22}+m_{30}+m_{23}+m_{13}+m_{20}+m_{10}+m_{14}+m_{4}+m_{16}+m_{7}\\
&\quad +m_{8}+m_{12}+m_{18}+m_{6}+m_{3}+m_{21}+m_{28}+m_{29}+m_{27};\\
c_4 &= m_{24}+m_{25}+m_{23}+m_{10}+m_{2}+m_{5}+m_{4}+m_{16}+m_{9}+m_{17}\\
&\quad +m_{8}+m_{18}+m_{6}+m_{11}+m_{19}+m_{21}+m_{28}+m_{29}+m_{26};\\
c_5 &= m_{22}+m_{24}+m_{30}+m_{25}+m_{1}+m_{10}+m_{2}+m_{14}+m_{4}+m_{16}\\
&\quad +m_{17}+m_{12}+m_{6}+m_{15}+m_{19}+m_{29}+m_{26}+m_{27};\\
c_6 &= m_{22}+m_{24}+m_{30}+m_{23}+m_{13}+m_{20}+m_{2}+m_{5}+m_{4}+m_{6}\\
&\quad +m_{15}+m_{19}+m_{21}+m_{28}+m_{27};\\
c_7 &= m_{24}+m_{1}+m_{16}+m_{7}+m_{8}+m_{12}+m_{6}+m_{15}+m_{19}+m_{21}\\
&\quad +m_{28}+m_{29}+m_{26};\\
c_8 &= m_{24}+m_{25}+m_{23}+m_{1}+m_{9}+m_{17}+m_{7}+m_{12}+m_{18}+m_{15}\\
&\quad +m_{19}+m_{3}+m_{29}+m_{26}+m_{27};\\
c_9 &= m_{22}+m_{24}+m_{30}+m_{25}+m_{1}+m_{16}+m_{9}+m_{7}+m_{18}+m_{15}\\
&\quad +m_{11}+m_{29};\\
c_{10} &= m_{22}+m_{30}+m_{23}+m_{13}+m_{1}+m_{20}+m_{10}+m_{14}+m_{4}+m_{16}\\
&\quad +m_{9}+m_{7}+m_{21}+m_{28}+m_{29}+m_{27};\\
c_{11} &= m_{24}+m_{25}+m_{23}+m_{1}+m_{10}+m_{2}+m_{5}+m_{4}+m_{16}+m_{9}\\
&\quad +m_{7}+m_{18}+m_{6}+m_{3}+m_{21}+m_{28}+m_{29}+m_{26};\\
c_{12} &= m_{22}+m_{24}+m_{30}+m_{25}+m_{10}+m_{2}+m_{14}+m_{4}+m_{9}+m_{8}\\
&\quad +m_{12}+m_{11}+m_{19}+m_{3}+m_{29}+m_{26}+m_{27};\\
c_{13} &= m_{22}+m_{24}+m_{30}+m_{23}+m_{13}+m_{1}+m_{20}+m_{2}+m_{5}+m_{4}\\
&\quad +m_{16}+m_{17}+m_{12}+m_{18}+m_{15}+m_{11}+m_{21}+m_{28}+m_{27};\\
c_{14} &= m_{21}+m_{28}+m_{29}+m_{26};\\
c_{15} &= m_{29}+m_{26}+m_{27};\\
c_{16} &= m_{29};
\end{aligned}
$$

REFERENCES

[1] A. Karatsuba, "The complexity of computations," Proc. Steklov Inst. Math. vol. 211, pp.169-183, 1995.

[2] A. Karatsuba and Y. Ofman, "Multiplication of Multidigit Numbers on Automata," *Soviet Physics-Doklady (English translation)*, vol. 7, no. 7, pp. 595-596, 1963.

[3] A. Lempel, G. Seroussi and S. Winograd, "On the Complexity of Multiplication in Finite Fields," *Theoretical Computer Science*, vol. 22, pp. 285-296, 1983

[4] A. Weimerskirch, and C. Paar, "Generalizations of the Karatsuba Algorithm for Efficient Implementations," $http://eprint.iacr.org/2006/224$, 2003.

[5] P. L. Montgomery, "Five, Six, and Seven-Term Karatsuba-Like Formulae," *IEEE Transactions on Computers*, vol. 54, no. 3, pp. 362-369, Mar. 2005.

[6] H. Fan and M. A. Hasan, "Comments on "Five, Six, and Seven-Term Karatsuba-Like Formulae"," *IEEE Transactions on Computers*, vol. 56, no. 5, pp. 716-717, May 2007.

[7] M. Cenk and F. Özbudak, "Improved Polynomial Multiplication Formulas over $\mathbb{F}_2$ Using Chinese Remainder theorem," *IEEE Transactions on Computers*, vol. 58, no. 4, pp. 572-576, April 2009.

[8] I. Oseledets, "Optimal Karatsuba-like formulae for certain bilinear forms in $GF(2)$," *Linear Algebra and its Applications*, vol. 429 pp. 2052-2066, 2008.

[9] M. Cenk, Ç. K. Koç and F. Özbudak, "Polynomial Multiplication over Finite Fields using Field Extensions and Interpolation," *Proc. 19th IEEE International Symposium on Computer Arithmetic*, 2009.

[10] J. V. Z. Gathen and J. Gerhard, "Modern Computer Algebra," Cambridge Univ. Press, First ed., 1999, Second ed., 2003.

[11] P. L. Montgomery, "Modular multiplication without trial division," *Mathematics of Computation*, 44(170), pp. 519-521, 1985.

[12] T. M. Apostol, "Introduction to Analytic Number Theory," Springer, 1976.