Comments on Montgomery's "Five, Six, and Seven-Term Karatsuba-Like Formulae"

Haining Fan and M. Anwar Hasan

Abstract

We show that multiplication complexities of n-term Karatsuba-Like formulae ($7 < n < 19$) in the above paper can be further improved using the Chinese Remainder Theorem and the construction multiplication modulo $(x-\infty)^w$.

Index Terms

Karatsuba algorithm, polynomial multiplication, finite field.

I. Introduction

The Karatsuba-Ofman multiplication algorithm and its generalizations, i.e., n-term Karatsuba-like formula ($n > 2$), are often used to design subquadratic complexity software and hardware $GF(2^n)$ multiplication algorithms. In [1], five, six, and seven-term Karatsuba-like formulae for $GF(2)[x]$ are presented. These formulae have the lowest values of the multiplication complexity $M(n)$, which is defined as the minimum number of multiplications needed to multiply two n-term polynomials $a(x) = \sum_{i=0}^{n-1} a_i x^i$ and $b(x) = \sum_{i=0}^{n-1} b_i x^i$ in $GF(2)[x]$.

Applying the Chinese Remainder Theorem (CRT) for the design of polynomial multiplication algorithms is well known in the literature [2]. In this comment, we use the CRT and the construction multiplication modulo $(x-\infty)^w$ to improve values of $M(n)$ ($7 < n < 19$) obtained in [1]. From now on, we assume that all polynomials are in $GF(2)[x]$. The CRT for $GF(2)[x]$ states that:

Theorem 1: Let $m_1(x), m_2(x), \cdots, m_t(x)$ be pairwisely coprime polynomials, and $m(x) = \prod_{i=1}^{t} m_i(x)$. Then for any polynomials $r_1(x), r_2(x), \cdots, r_t(x)$, there is a unique polynomial $r(x) \pmod{m(x)}$ such that $r(x) \equiv r_i(x) \pmod{m_i(x)}$, where $1 \le i \le t$ and

$$r(x) = \sum_{i=1}^{t} r_i(x) \left(\frac{m(x)}{m_i(x)} \right) \left(\left(\frac{m(x)}{m_i(x)} \right)^{-1} \mod m_i(x) \right).$$

II. IMPROVED $M(n)$

When the CRT is used to compute the product $c(x) = \sum_{i=0}^{2n-2} c_i x^i = a(x)b(x)$, first, a set of modulus polynomials $m_i(x)$ $(1 \le i \le t)$ are chosen such that $deg(m(x)) > 2n-2$. Then $A_i(x) = a(x) \pmod{m_i(x)}$ and $B_i(x) = b(x) \pmod{m_i(x)}$ are computed. Since the operation of the reduction modulo a fixed polynomial $m_i(x)$ may be converted to subtraction operations, this step involves no multiplications. Next, the t products $A_i(x)B_i(x) \pmod{m_i(x)}$ are computed, and each requires $M(deg(m_i(x)))$ multiplications, where $deg(m_i(x))$ denotes the degree of $m_i(x)$. Finally, $c(x)$ is obtained via the CRT. This step needs no multiplication operations since multiplying by a fixed polynomial may be converted to addition operations.

Therefore, the minimum number of multiplications needed to multiply $a(x)$ and $b(x)$, i.e., $M(n) = \sum_{i=1}^{t} M(deg(m_i(x)))$, depends on the set of modulus polynomials. In order to minimize $M(n)$, these polynomials are selected such that $deg(m(x)) = 2n-1$. However, if we know the w $(1 \le w \le 2n-2)$ coefficients $c_{2n-2}, c_{2n-3}, \cdots, c_{2n-1-w}$, the degree of $m(x)$ can be reduced to $2n-1-w$. This construction is referred to the multiplication modulo $(x-\infty)^w$ [2]. Let $e(f,i)$ denote the coefficient of x^i in $f(x)$. The following lemma is a formal statement of this construction.

Lemma 2: Let $1 \le w \le 2n-2$, $c(x) = \sum_{i=0}^{2n-2} c_i x^i$ and $m(x)$ be polynomials with $deg(c(x)) \le 2n-2$ and $deg(m(x)) = 2n-1-w$, respectively. Given $c_{2n-2}, c_{2n-3}, \cdots, c_{2n-1-w}$ and $r(x) = c(x) \pmod{m(x)}$, then $d(x) = r(x) + h_w(x)$ is equal to $c(x)$, where $h_w(x)$ is defined as:

$$\begin{cases} h_0(x) = m(x)x^{w-1}, \\ h_i(x) = h_{i-1}(x) + (c_{2n-1-i} + e(h_{i-1}, 2n-1-i))m(x)x^{w-i}, \quad 1 \le i \le w. \end{cases}$$

Proof: Since $deg(m(x)x^{w-i}) = 2n-1-i$, we know that $e(h_i, 2n-1-i) = c_{2n-1-i}$ and $e(h_i, j) = e(h_{i-1}, j)$ for $2n-2 \ge j \ge 2n-i$. By induction on i we know that $e(h_w, j) = c_j$ for $2n-2 \ge j \ge 2n-1-w$. Since $deg(r(x)) < 2n-1-w$, it is clear that $e(d,j) = e(h_w, j) = c_j$ for $2n-2 \ge j \ge 2n-1-w$. Therefore, if $c(x)$ and $d(x)$ are uniquely rewritten as $c(x) = c_H(x)x^{2n-1-w} + c_L(x)$ and $d(x) = d_H(x)x^{2n-1-w} + d_L(x)$, where $c_L(x)$ and $d_L(x)$ are polynomials of degrees less than $2n-1-w$, we know that $c_H(x) = d_H(x)$.

Since $deg(m(x)) = 2n-1-w > deg(c_L(x))$, we have $c_L(x) = c_L(x) \pmod{m(x)}$. Similarly, we have $d_L(x) = d_L(x) \pmod{m(x)}$. The construction of $h_w(x)$ shows that $0 = h_w(x) \pmod{m(x)}$. This leads to $r(x) = d(x) \pmod{m(x)}$. So we have $(c_L(x) \pmod{m(x)}) = (d_L(x) \pmod{m(x)})$, i.e. $c_L(x) = d_L(x)$. This completes the proof. □

Using the CRT and this construction, we obtain improved values of $M(n)$ $(7 < n < 19)$ and they are given in Table I. In the table, f_{ij} denotes the j-th irreducible polynomial of degree i over $GF(2)$, e.g., $f_{11} = x$, $f_{12} = x+1$, $f_{21} = x^2+x+1$, $f_{31} = x^3+x+1$, $f_{32} = x^3+x^2+1$, $f_{41} = x^4+x+1$, $f_{42} = x^4+x^3+1$, $f_{43} = x^4+x^3+x^2+x+1$ and $f_{51} = x^5+x^2+1$.

TABLE I

UPPER BOUND FOR $M(n)$

n	$M(n)$ [1]	New Bound	Modulus polynomials
2	3	3	$(x-\infty)$, f_{11}, f_{12}
3	6	6	$(x-\infty)$, f_{11}, f_{12}, f_{21}
4	9	10	$(x-\infty)$, f_{11}^2, f_{12}^2, f_{21}
5	13	14	$(x-\infty)^3$, f_{11}^2, f_{12}^2, f_{21}
6	17	18	$(x-\infty)^2$, f_{11}^2, f_{12}^2, f_{21}, f_{31}
7	22	22	$(x-\infty)$, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}
8	27	26	$(x-\infty)^3$, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}
9	34	31	$(x-\infty)$, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}
10	39	35	$(x-\infty)^3$, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}
11	46	40	$(x-\infty)$, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}
12	51	44	$(x-\infty)^3$, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}
13	60	49	$(x-\infty)$, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}
14	66	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	$(x-\infty)^3$, f_{11}^2, f_{12}^2, f_{21}^2, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}
16	81	64	$(x-\infty)^2$, f_{11}^2, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}, f_{51}
17	94	69	$(x-\infty)^3$, f_{11}^3, f_{12}^2, f_{21}, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}, f_{51}
18	102	75	$(x-\infty)^3$, f_{11}^3, f_{12}^2, f_{21}^2, f_{31}, f_{32}, f_{41}, f_{42}, f_{43}, f_{51}

$Remarks$:

1. Values of $M(4) = 9$ and $M(5) = 13$ of [1] have been used for obtaining new bounds.

2. While computations of $(x-\infty)$ and $(x-\infty)^2$ require 1 and 3 multiplications, respectively, computing $(x-\infty)^3$ requires 5 multiplications: $a_{n-1}b_{n-1}$, $(a_{n-1}+a_{n-2})(b_{n-1}+b_{n-2})+a_{n-1}b_{n-1}+a_{n-2}b_{n-2}$ and $a_{n-1}b_{n-3}+b_{n-1}a_{n-3}+a_{n-2}b_{n-2}$.

3. Detailed descriptions and examples of constructing the n-term Karatsuba-like formulae using the set of modulus polynomials can be found in the literature, e.g., [3].

ACKNOWLEDGMENT

This work was supported in part by NSERC Discovery and NSERC Strategic Project grants awarded to Dr. Hasan.

REFERENCES

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

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

[3] 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.