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

Haining Fan and M. Anwar Hasan *Senior Member, IEEE*

Abstract

We show that multiplication complexities of n-term Karatsuba-Like formulae of $GF(2)[x]$ ($7 < n < 19$) presented 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 2-term multiplication algorithm and its extensions, i.e., n-term Karatsuba-like formula ($n > 2$), are often used to design subquadratic complexity $GF(2^n)$ multiplication algorithms. In [1], for $1 < n < 19$, Montgomery presents 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], [3], [4] and [5]. 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]. Unless otherwise stated, we assume that all polynomials considered here are in $GF(2)[x]$. The CRT for $GF(2)[x]$ states that:

Haining Fan is with the Department of Computer Science, Tsinghua University, Beijing, China. Most of this work was done when he was at the University of Waterloo. M. Anwar Hasan is with the Department of Electrical and Computer Engineering University of Waterloo, Waterloo, Canada. E-mails: hfan@vlsi.uwaterloo.ca and ahasan@ece.uwaterloo.ca.

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 $r(x) \bmod m(x)$ such that $r(x) \equiv r_i(x) \pmod{m_i(x)}$, where $1 \leq i \leq t$. A formula for $r(x)$ is

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

II. Improved $M(n)$

Let $deg(a(x))$ denote the degree of $a(x)$, and $deg(a(x)) < n$ and $deg(b(x)) < n$. 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 $m_i(x)$ ($1 \leq i \leq t$) are chosen such that $deg(m(x)) > 2n-2$. Then $A_i(x) = a(x) \bmod m_i(x)$ and $B_i(x) = b(x) \bmod m_i(x)$ 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 $A_i(x)B_i(x) \bmod m_i(x)$ are computed, and each requires $M(deg(m_i(x)))$ multiplications. 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 ($1 \leq w \leq 2n-2$) 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, p.34]. 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 $1 \leq w \leq 2n-2$, $c(x) = \sum_{i=0}^{2n-2} c_i x^i$ and $m(x)$ be polynomials with $deg(m(x)) = 2n-1-w$. Given $c_{2n-2}, c_{2n-3}, \cdots, c_{2n-1-w}$ and $r(x) = c(x) \bmod m(x)$, then $d(x) = r(x) + h_w(x)$ is equal to $c(x)$, where $h_w(x)$ is defined as:

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

Proof:

If $1 \leq i \leq w$, then we claim that

$$e(h_i, j) = c_j, \tag{1}$$

where $2n-2 \geq j \geq 2n-i-1$.

Since $deg(m(x)x^{w-i}) = 2n-i-1$ $(1 \leq i \leq w)$, we have $e(m(x)x^{w-i}, 2n-i-1) = 1$. Therefore, we obtain

$$\begin{aligned} & e(h_i, 2n-i-1) \\ = \;& e(h_{i-1}, 2n-i-1) + [c_{2n-i-1} + e(h_{i-1}, 2n-i-1)] * e(m(x)x^{w-i}, 2n-i-1) \\ = \;& c_{2n-i-1} \quad (\text{since } \; 1+1=0 \text{ in } \; GF(2)). \end{aligned} \tag{2}$$

For $i=1$, (2) is simplified as $e(h_1, 2n-2) = c_{2n-2}$, i.e., statement (1) is true.

Now we consider $2 \leq i \leq w$. Since the polynomial $m(x)x^{w-i}$ is of degree $2n-i-1$, for $2n-2 \geq j \geq 2n-i$, we can write $e(m(x)x^{w-i}, j) = 0$. Therefore, from the definition of $h_i(x)$, we have

$$e(h_i, j) = e(h_{i-1}, j), \tag{3}$$

where $2n-2 \geq j \geq 2n-i$.

From (2) and (3), we know that statement (1) is true for $1 \leq i \leq w$.

Especially, (1) shows that $e(h_w, j) = c_j$ for $2n-2 \geq j \geq 2n-1-w$. Since $deg(r(x)) < 2n-1-w$, it is clear that $e(d, j) = e(h_w, j) = c_j$ for $2n-2 \geq j \geq 2n-1-w$. 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 can write $c_H(x) = d_H(x)$.

Since $deg(m(x)) = 2n-1-w > deg(c_L(x))$, we have $c_L(x) = c_L(x) \bmod m(x)$. Similarly, we have $d_L(x) = d_L(x) \bmod m(x)$. The construction of $h_w(x)$ shows that $0 = h_w(x) \bmod m(x)$. This leads to $r(x) \equiv d(x) \pmod{m(x)}$. So we have $(c_L(x) \bmod m(x)) = (d_L(x) \bmod m(x))$, 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 $f_{51} = x^5+x^2+1$.

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 $a_{n-1}b_{n-3}+b_{n-1}a_{n-3}+a_{n-2}b_{n-2}$.

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}

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

The authors thank the reviewers for their useful comments. 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, Mar. 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, Sept. 2004.

[4] J.-C. Bajard, L. Imbert and G. A. Jullien, “Parallel Montgomery Multiplication in $GF(2^k)$ Using Trinomial Residue Arithmetic,” *Proc. 17th IEEE Symposium on Computer Arithmetic (ARITH 2005)*, pp. 164-171, June 2005.

[5] J.-C. Bajard, L. Imbert and C. Nègre. “Arithmetic Operations in Finite Fields of Medium Prime Characteristic using the Lagrange Representation.” *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1167-1177, Sept. 2006.