$GF(2^n)$ Subquadratic Polynomial Basis Multipliers for Some Irreducible Trinomials

Xi Xiong and Haining Fan

Abstract

The $GF(2^n)$ multiplication operation in polynomial basis can be represented as a matrix-vector product form, and the matrix is often called the Mastrovito matrix. The Toeplitz matrix-vector product approach has been used to design subquadratic shifted polynomial basis multipliers. In order to apply this approach to subquadratic polynomial basis multipliers, this Mastrovito matrix should be transformed into a Toeplitz matrix. In this paper, two transformation methods are proposed for irreducible trinomial $x^n + x^k + 1$, where $2k + 1 \leq n$.

I. Introduction

The space and time complexities are often used to measure the performance of a $GF(2^n)$ parallel multiplier. The existing multipliers can simply be classified into two categories: quadratic and subquadratic multipliers. Most subquadratic polynomial basis multipliers apply Karatsuba's algorithm, e.g., [1], [2], [3], [4], [5] and [6]. Recently, the optimal Toeplitz matrix-vector product (TMVP) formulae were used to design shifted polynomial basis multipliers [7], but this method has not been transplanted to polynomial bases.

In order to apply TMVP approach to subquadratic polynomial basis multipliers, the Mastrovito matrix should be transformed into a Toeplitz matrix. In this work, we will introduce two such transformation methods. Based on them, the subquadratic polynomial basis multipliers can also share the advantages of the TMVP approach, for example, low total gate delays.

II. Two Transformation Methods

Let $f(x) = x^n + x^k + 1$ $(2k+1 \leq n)$ be the irreducible trinomial generating $GF(2^n)$, and $X = (1, x, x^2, \cdots, x^{n-1})^T$ be the column vector of polynomial basis elements. Define $A = (a_0, a_1, \cdots, a_{n-1})^T$ be the coordinate column vector of the field element $a = X^T A = \sum_{i=0}^{n-1} a_i x^i$, and b, B, c and C are defined similarly. Let $c = \sum_{i=0}^{n-1} c_i x^i = X^T C = ab \bmod f(x)$ be the product of a and b in $GF(2^n)$.

In order to compute the coordinate column vector C of c, we may first multiply polynomials a and b:

$$s \quad = \quad ab = \sum_{t=0}^{2n-2} s_t x^t,$$

where

$$s_t = \begin{cases} \sum_{i=0}^{t} a_{t-i} b_i & 0 \leq t \leq n-1 \\ \sum_{i=t+1-n}^{n-1} a_{t-i} b_i & n \leq t \leq 2n-2. \end{cases} \tag{1}$$

Then we perform the reduction operation:

$$\begin{aligned} c \quad &= \quad s \bmod f(x) = \sum_{i=0}^{n-1} c_i x^i \\ &= \quad \sum_{t=0}^{n-1} s_t x^t + \sum_{t=n}^{2n-k-1} s_t (x^{t-n+k} + x^{t-n}) \\ &\quad + \sum_{t=2n-k}^{2n-2} s_t (x^{t-2n+2k} + x^{t-2n+k} + x^{t-n}) \\ &= \quad \sum_{t=0}^{n-1} s_t x^t + \sum_{t=k}^{n-1} s_{t+n-k} x^t + \sum_{t=0}^{n-k-1} s_{t+n} x^t \\ &\quad + \sum_{t=k}^{2k-2} s_{t+2n-2k} x^t + \sum_{t=0}^{k-2} s_{t+2n-k} x^t + \sum_{t=n-k}^{n-2} s_{t+n} x^t. \end{aligned} \tag{2}$$

These two steps can be combined into the following matrix-vector product form: $C = Z(b_0, b_1, \cdots, b_{n-1})^T$. The $n \times n$ dimensional matrix $Z = (z_{i,j})_{0 \leq i,j \leq n-1}$, which is called the Mastrovito matrix, is determined by the coefficients of A. Detailed description of Mastrovito matrix Z can be found in [8] and [9].

Definition 1: Let Z_i^j denote the $(j-i+1) \times n$ submatrix of Z formed by selecting rows $i, i+1, \cdots, j-1, j$, where $i \leq j$.

Matrix Z can be partitioned into two Toeplitz matrices: the upper $k \times n$ submatrix Z_0^{k-1} and the lower $(n-k) \times n$ submatrix Z_k^{n-1}, respectively [9]. In order to transform Z into a Toeplitz matrix, we propose

two transformation methods in the following.

A. Transformation 1

The first method is similar to that in the shifted polynomial basis case [7]. It also uses the following transformation matrix:

$$U_i = \begin{pmatrix} 0 & I_{n-i} \\ I_i & 0 \end{pmatrix},$$

where I_i is the $i \times i$ identity matrix.

Proposition 1: $T_1 = U_k Z$ is a Toeplitz matrix.

Proof: Since both Z_0^{k-1} and Z_k^{n-1} are Toeplitz matrices themselves and premultiplication of U_k to Z moves the upper k rows down below the lower $n-k$ rows of Z, we only need to derive explicit expressions of elements of row $n-k-1$ (the row $n-1$ of Z) and row $n-k$ (the row 0 of Z) of T_1, and prove that they satisfy the definition of a Toeplitz matrix. These two rows correspond to c_{n-1} and c_0 in (2) respectively.

From (1) and (2) we conclude that:

$$\begin{aligned} c_0 &= s_0 + s_n + s_{2n-k} \\ &= a_0 b_0 + \sum_{i=1}^{n-1} a_{n-i} b_i + \sum_{i=n-k+1}^{n-1} a_{2n-k-i} b_i, \end{aligned}$$

and

$$\begin{aligned} c_{n-1} &= s_{n-1} + s_{2n-k-1} \\ &= \sum_{i=0}^{n-1} a_{n-1-i} b_i + \sum_{i=n-k}^{n-1} a_{2n-k-1-i} b_i. \end{aligned}$$

Therefore, we have

$$z_{0,i} = \begin{cases} a_0 & i = 0, \\ a_{n-i} & 1 \le i \le n-k, \\ a_{n-i} + a_{2n-k-i} & n-k+1 \le i \le n-1, \end{cases}$$

and

$$z_{n-1,i} = \begin{cases} a_{n-i-1} & 0 \le i \le n-k-1, \\ a_{n-i-1} + a_{2n-k-i-1} & n-k \le i \le n-1. \end{cases}$$

Careful comparison shows that $z_{0,i} = z_{n-1,i-1}$ for $1 \leq i \leq n-1$, therefore $U_k Z$ is a Toeplitz matrix.

■

The transformation U_k is simple itself, but some elements in the last row of $U_k Z$, which is just row k of matrix Z, are sums of three terms like $a_i + a_j + a_k$. Or more precisely, the explicit expression of c_k is:

$$\begin{aligned} c_k &= s_k + s_n + s_{2n-k} + s_{k+n} \\ &= \sum_{i=0}^{k} a_{k-i}b_i + \sum_{i=1}^{n-1} a_{n-i}b_i + \sum_{i=n-k+1}^{n-1} a_{2n-k-i}b_i + \sum_{i=k+1}^{n-1} a_{n+k-i}b_i \\ &= a_k b_0 + \sum_{i=1}^{k} (a_{k-i} + a_{n-i})b_i + (a_{n-k-1} + a_{n-1})b_{k+1} + \sum_{i=k+2}^{n-1} (a_{n-i} + a_{2n-k-i} + a_{n+k-i})b_i. \end{aligned}$$

It is clear that the last $n-k-2$ elements in row k of Z are sums of three terms, i.e., $a_{n-i} + a_{2n-k-i} + a_{n+k-i}$. By the definition of a Toeplitz matrix, this implies there are $n-k-2$ rows each of which contains at least one element consists of three terms. In VLSI implementations, two XOR gate delays are required to compute these sums. In order to separate such delays, we propose the second transformation method as follows.

B. Transformation 2

Definition 2: Let $J_{i,j}$ represent the $n \times n$ elementary transformation matrix that adds row i to row j, and E be $\prod_{i=0}^{k-2} J_{i,i+k}$.

Proposition 2: $T_2 = U_{2k-1} Z E$ is a Toeplitz matrix whose each element is a sum of at most two terms.

Proof: We denote ZE as $\bar{Z}$. By definition 2, transformation E adds Z_0^{k-2} to Z_k^{2k-2}, and $\bar{Z}_k^{2k-2}$ is a Toeplitz matrix because Z_0^{k-1} and Z_k^{n-1} are two Toeplitz matrices. Now $\bar{Z}$ consists of three Toeplitz submatrices:

$$\bar{Z} = \begin{pmatrix} \bar{Z}_0^{k-1} \\ \bar{Z}_k^{2k-2} \\ \bar{Z}_{2k-1}^{n-1} \end{pmatrix} = \begin{pmatrix} Z_0^{k-1} \\ Z_0^{k-2} + Z_k^{2k-2} \\ Z_{2k-1}^{n-1}. \end{pmatrix}$$

We first prove that the $(2k-1) \times n$ submatrix

$$\begin{pmatrix} \bar{Z}_0^{k-1} \\ \bar{Z}_k^{2k-2} \end{pmatrix}$$

is a Toeplitz matrix. We only need to find out the relationship between row $k-1$ and row k, which correspond to c_{k-1} and $c_0 + c_k$ respectively:

$$\begin{aligned} c_{k-1} &= s_{k-1} + s_{k+n-1} \\ &= \sum_{i=0}^{k-1} a_{k-i-1} b_i + \sum_{i=k}^{n-1} a_{k+n-1-i} b_i, \\ c_0 + c_k &= s_0 + s_k + 2s_n + 2s_{2n-k} + s_{k+n} \\ &= s_0 + s_k + s_{k+n} \\ &= a_0 b_0 + \sum_{i=0}^{k} a_{k-i} b_i + \sum_{i=k+1}^{n-1} a_{k+n-i} b_i. \end{aligned}$$

A careful observation reveals that the first $n-1$ elements of row $k-1$ are equal to the last $n-1$ elements of row k. Therefore $\bar{Z}$ contains only two Toeplitz submatrices: $\bar{Z}_0^{2k-2}$ and $\bar{Z}_{2k-1}^{n-1}$. Because row 0 and row $n-1$ of $\bar{Z}$ are the same as those of Z, $U_{2k-1}ZE$ is a Toeplitz matrix by Proposition 1. ■

Since each element of $\bar{Z} = ZE$ is a sum of no more than two terms and premultiplication of U_{2k-1} to $\bar{Z}$ only moves the upper $2k-1$ rows down below the lower $n-2k+1$ rows of $\bar{Z}$, Toeplitz matrix T_2 can be computed in one XOR gate delay due to the parallelism.

III. Conclusion

In order to apply the TMVP approach to design subquadratic polynomial basis multipliers, we have presented two methods to transform the Mastrovito matrix Z into a Toeplitz matrix. The two transformations provide a gate delay trade-off between different design stages. Transformation 1 and its inverse need no gates, however, it takes 2 XOR gate delays to form the Mastrovito matrix. The number of the total XOR gate delays of transformation 2 is also two, but they were separated by the most time-consuming operation - TMVP: one is in transformation ZE and the other is in its inverse transformation $U_{2k-1}^{-1}T_2$.

ACKNOWLEDGMENT

The work was supported by NSFC under grant No. 60970147 and 973 project No. 2010CB328004.

REFERENCES

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

[2] Paar, C. : 'A New Architecture for a Parallel Finite Field Multiplier with Low Complexity Based on Composite Fields', *IEEE Transactions on Computers*, July 1996, vol. 45, no. 7, pp. 856-861

[3] Grabbe, C., Bednara, M., J. Shokrollahi, J. Teich, and J. von zur Gathen : 'FPGA Designs of parallel hign performance $GF(2^{233})$ Multipliers', *Proc. Int'l Symposium on Circuits and Systems (ISCAS 2003)*, 2003, vol. II, pp. 268-271

[4] Rodriguez-Henriquez, F., and Koc, C.K. : 'On fully parallel Karatsuba multipliers for $GF(2^m)$', *Proc. Int'l Conf. Computer Science and Technology (CST 2003)*, 2003, pp. 405-410

[5] von zur Gathen, J., and Shokrollahi, J. : 'Efficient FPGA-based Karatsuba Multipliers for Polynomials over F_2', *Proc. 12th Workshop on Selected Areas in Cryptography (SAC 2005)*, 2005

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

[7] Fan, H., and Hasan, M.A. : 'A New Approach to Subquadratic Space Complexity Parallel Multipliers for Extended Binary Fields', *IEEE Transactions on Computers*, Feb. 2007, vol. 56, no. 2, pp. 224-233

[8] Mastrovito, E.D. : 'VLSI schemes for Multiplication over Finite Field $GF(2^m)$', *Proc. 6th Int'l Conf. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-6)*, 1988, pp. 297-309

[9] Sunar, B., and Koc, C.K. : 'Mastrovito Multiplier for All Trinomials', *IEEE Transactions on Computers*, May 1999, vol. 48, no. 5, pp. 522-527

Authors' affiliations:

Xi Xiong and Haining Fan (Key Laboratory for Information System Security, Ministry of Education; Tsinghua National Laboratory for Information Science and Technology; School of Software, Tsinghua University, Beijing, China.)

E-mails: yqnyhdjn@gmail.com and fhn@tsinghua.edu.cn