Information Processing Letters 131 (2018) 33–38

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Efficient multiplier based on hybrid approach for Toeplitz matrix–vector product ☆

Ku-Young Chang [a], Sun-Mi Park [b], Dowon Hong [b,*], Changho Seo [b]

[a] Information Security Research Division, Electronics and Telecommunications Research Institute, 218 Gajeongro, Yuseong-gu, Daejeon, 34129, Republic of Korea

[b] Department of Applied Mathematics, Kongju National University, 56, Gongjudaehak-ro, Gongju-si, Chungnam, 32588, Republic of Korea

ARTICLE INFO

Article history:
Received 11 July 2015
Received in revised form 28 March 2017
Accepted 15 November 2017
Available online 21 November 2017
Communicated by X. Wu

Keywords:
Computational complexity
Toeplitz matrix–vector product
Subquadratic space complexity multiplier
Parallel multiplier
Hybrid multiplier

ABSTRACT

We propose a hybrid approach for a Toeplitz matrix–vector product (TMVP) of size $k \cdot 2^i 3^j$, where $k \geq 1$ and $i, j \geq 0$. It is possible to make trade-offs between time and space complexities for a TMVP by choosing values k, i, and j properly. We show that the multiplier based on the proposed hybrid TMVP approach has lower space as well as time complexities than other subquadratic space complexity multipliers for five fields recommended by NIST. Moreover, for those five fields, the space complexities of the proposed multiplier are reduced by a minimum 59% and a maximum 77% compared with quadratic space complexity multiplier.

1. Introduction

A Toeplitz matrix is an $n \times n$ matrix $T = [t_{i,j}]_{0 \leq i,j < n}$ such that $t_{i,j} = t_{i-1,j-1}$ for $1 \leq i, j < n$. Efficient computation for a Toeplitz matrix–vector product (TMVP) has received considerable attention since a binary extension field multiplication can be obtained by computing a TMVP over the binary field $\mathbb{F}_2$ ([1], [2]). A Toeplitz matrix and vector considered in this paper have their entries in $\mathbb{F}_2$. Fan and Hasan in [1] proposed a subquadratic approach for a TMVP of size l^i $(i > 0)$ using the recursive l-way split formula, where $l = 2$ or 3. It is possible to design subquadratic scheme for a TMVP of size $2^i 3^j$ $(i, j \geq 0)$ by combing the 2-way split and 3-way split approaches ([1, Section 2.3]). In [3], Hasan et al. proposed a modification of the TMVP of Fan and Hasan. They decompose the recursive l-way split formula for a TMVP of size $m = l^i$ into four independent blocks and then reduce the space complexity for a TMVP using a block recombination. However, the special form l^i of m may make the TMVP approach in [3] ineffective. If m is not a form of l^i, then an easy way to apply the TMVP approach in [3] is to expand sizes of the corresponding matrices and vectors into sizes of a form l^i by padding zero entries suitably. For example, if $m = 283$, the size of the TMVP is expanded into $2^9 = 512$, which is too large.

In this paper, we make a further study of the block recombination scheme proposed in [3]. We first extend the block decomposition for a TMVP of size $m = 2^i$ or 3^i into size $m = 2^i 3^j$ in Section 3, where $i, j \geq 0$. To this end, we give the definitions of four blocks for a TMVP of size $2^i 3^j$ and their complexities. Moreover, we apply the block recombination scheme to a k-TMVPs-and-add architecture

☆ This work was supported by Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korean government [17ZH1700, Development of storage and search technologies over encrypted database], the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (2016R1A4A1011761), and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2016R1D1A1B03931071).

* Corresponding author.
E-mail addresses: jang1090@etri.re.kr (K.-Y. Chang), smpark@kongju.ac.kr (S.-M. Park), dwhong@kongju.ac.kr (D. Hong), chseo@kongju.ac.kr (C. Seo).

https://doi.org/10.1016/j.ipl.2017.11.006
0020-0190/

Table 1
2-way and 3-way split formulae for TMVP.

2-way split	3-way split
$TV = \begin{bmatrix} T_1 & T_0 \\ T_2 & T_1 \end{bmatrix} \begin{bmatrix} V_0 \\ V_1 \end{bmatrix} = \begin{bmatrix} P_0 + P_2 \\ P_1 + P_2 \end{bmatrix}$,	$TV = \begin{bmatrix} T_2 & T_1 & T_0 \\ T_3 & T_2 & T_1 \\ T_4 & T_3 & T_2 \end{bmatrix} \begin{bmatrix} V_0 \\ V_1 \\ V_2 \end{bmatrix} = \begin{bmatrix} P_0 + P_3 + P_4 \\ P_1 + P_3 + P_5 \\ P_2 + P_4 + P_5 \end{bmatrix}$,
$P_0 = (T_0 + T_1)V_1$,	$P_0 = (T_0 + T_1 + T_2)V_2$, $P_3 = T_1(V_1 + V_2)$,
$P_1 = (T_1 + T_2)V_0$,	$P_1 = (T_1 + T_2 + T_3)V_1$, $P_4 = T_2(V_0 + V_2)$,
$P_2 = T_1(V_0 + V_1)$	$P_2 = (T_2 + T_3 + T_4)V_0$, $P_5 = T_3(V_0 + V_1)$

$\sum_{u=1}^{k} T_u V_u$ of size $2^i 3^j$ and give the explicit complexity formula for its computation in Section 4. The obtained results are used in a hybrid scheme for a TMVP in Section 5.

In general, subquadratic approach induces smaller space complexity but larger time complexity compared with its quadratic counterparts. Therefore, a hybrid approach which mixes quadratic and subquadratic approaches may provide a trade-off between the time and space complexities. For example, the references [4–6] take hybrid approaches for multipliers which are performed by implementing a few subquadratic iterations and then a quadratic scheme on small input operands. In Section 5, we propose a hybrid approach for a TMVP of size $n = k \cdot 2^i 3^j$ using k-TMVPs-and-add architectures of size $2^i 3^j$, where $k \geq 1$ and $i, j \geq 0$. We first apply a quadratic approach and then subquadratic scheme. It is possible to make trade-offs between time and space complexities for a TMVP by choosing values k, i, and j properly. In Section 6, against one's expectations, we show that the multiplier based on the proposed hybrid TMVP approach has lower space as well as time complexities than other subquadratic space complexity multipliers in practical applications. This result comes from more flexible form of $n = k \cdot 2^i 3^j$ than forms $2^i 3^j$ in [1] or [3].

Finally, we remark that the hybrid approach for TMVP over $\mathbb{F}_2$ can be extended into TMVP over any field (see Remark 1).

2. Review of l-way split formula and its block decomposition for TMVP with $l \in \{2, 3\}$

Let $l = 2$ or 3. The l-way split formula for a TMVP TV in [1] are summarized in Table 1. A TMVP TV of size l^i is computed using the l-way split formula recursively. The recursive l-way split formula for TV is decomposed into four blocks in [3]: the component matrix formation (CMF_l), the component vector formation (CVF_l), the component multiplication (CM), and the reconstruction (R_l) (see Fig. 1). Their definitions are reported in Table 2, where T_i's and V_i's are given in Table 1, $\widetilde{\times}$ denotes a component multiplication of two vectors, and $\hat{W}_i$'s are subvectors of $\hat{W}$ with the same vector size. We describe the TMVP TV simply by

$$TV = R_l(CMF_l(T) \widetilde{\times} CVF_l(V)).$$

The complexities for each blocks of a TMVP with size $m = l^i$ are evaluated in [3]. We report those complexities in Table 3. We use the notations $S_{\oplus}^{CMF}(m)$, $S_{\oplus}^{CVF}(m)$, and $S_{\oplus}^{R}(m)$ to denote the number of XOR gates to implement CMF, CVF, and R of size m, respectively, and $S_{\otimes}^{CM}(m)$ the number of AND gates to implement CM of size m.

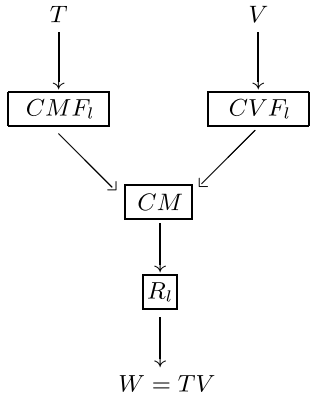

Fig. 1. Block decomposition for a TMVP TV of size l^i.

A TMVP TV of size $m = 2^i 3^j$ $(i, j \geq 0)$ is computed by applying the 2-way split formula i times and then the 3-way split formula j times since such method is more efficient than other split methods according to [1, Section 2.3]. In this case, the delay for a TMVP of size $m = 2^i 3^j$ equals to

$$T_A + (2i + 3j)T_X \tag{1}$$

by [1, Section 2], where T_A and T_X are delays due to one XOR and AND gate, respectively.

3. Block decomposition for TMVP of size $m = 2^i 3^j$

In this section, we propose a block decomposition for TMVP of size $m = 2^i 3^j$ $(i, j \geq 0)$ which is implemented by the 2-way split formula i times and then the 3-way split formula j times. We define the blocks $CMF(T)$ and $CVF(V)$ as follows:

$$CMF(T) = \begin{cases} (CMF(T_0 + T_1), CMF(T_1 + T_2), CMF(T_1)) \\ \qquad \text{if } 2|m, \\ CMF_3(T) \quad \text{otherwise}, \end{cases}$$

$$CVF(V) = \begin{cases} (CVF(V_1), CVF(V_0), CVF(V_0 + V_1)) \\ \qquad \text{if } 2|m, \\ CVF_3(V) \quad \text{otherwise}, \end{cases} \tag{2}$$

where T_i's and V_i's are given in the 2-way split formula of Table 1. Then $CMF(T)$ and $CVF(V)$ are vectors with $3^i 6^j$ components (which is easily proved by induction on i). The