ELSEVIER

Signal Processing 40 (1994) 295–306

SIGNAL PROCESSING

Two-dimensional polynomial residue number system

Ming-Chwen Yang, Ja-Ling Wu*

Department of Computer Science and Information Engineering, National Taiwan University, Taipei, 10764, Taiwan, ROC

Received 30 September 1993; revised 5 May 1994

Abstract

The polynomial residue number system (PRNS) has been considered as a useful tool for digital signal processing (DSP) since it can support parallel, carry-free, high speed arithmetic with minimum multiplication count provided that an appropriate modular ring is chosen. In this paper, the properties of two-dimensional (2-D) PRNS are investigated in detail. It is shown that in the 2-D PRNS system, the theoretical lower bound for multiplication count of polynomial products can be achieved in some carefully chosen ring. Application of the proposed 2-D PRNS for computing 2-D circular convolution, which involves intensive multiplication operations, is also presented.

Zusammenfassung

Das Polynom-Restklassen-Zahlensystem (PRNS) wird als nützliches Werkzeug zur digitalen Signalverarbeitung angesehen, da es übertragfreie, schnelle Parallelarithmetik mit kleinstmöglicher Multiplikationszahl unterstützen kann, wenn ein geeigneter Modulo-Ring gewählt wird. In diesem Beitrag werden die Eigenschaften des zweidimensionalen (2-D-) PRNS im Einzelnen untersucht. Es wird gezeigt, daß im 2-D-PRNS die theoretische Untergrenze der Multiplikationszahl für Polynomprodukte in einem sorgfältig gewählten Ring erreichbar ist. Die Anwendung des vorgeschlagenen 2-D-PRNS zur Berechnung der 2-D-Zirkularfaltung, welche einen hohen Multiplikationsaufwand beinhaltet, wird ebenfalls vorgestellt.

Résumé

Le système à numéro de résidu polynomial (PRNS) a été considéré comme un outils utile pour le traitement des signaux digitaux (DSP) car il supporte l'arithmétique très rapide, parallèle et sans retenue avec un compteur de multiplication minimum lorsqu'un cercle modulaire approprié est choisi. Dans cet article, les propriétés des PRNS à deux dimensions (2-D) sont présentées en détails. Il est montré que dans le système PRNS 2-D, la limite théorique la plus basse pour le compteur de multiplication de produits polynomiaux peut être obtenue pour quelques cercles soigneusement choisis. Une application du 2-D PRNS proposée pour le calcul de la convolution circulaire 2-D, laquelle implique d'intensives opérations de multiplication, est également présenté.

Keywords: Polynomial residue number system; Two-dimensional convolutions; Fast Fourier transform; Quotient field

*Corresponding author.

SSDI 0165-1684(94)00083-C

1. Introduction

To date, many important digital signal processing applications involving operations like circular convolution, skew circular convolution, autocorrelation, and computation of DFT are all multiplication intensive. To efficiently perform these operations, one and maybe the most effective approach is by using the residue number system (RNS). The polynomial residue number system (PRNS) which is an extension of the quadratic residue number system (QRNS) was first proposed by Skavantzous [11]. The system enjoys all the advantages of RNS, such as parallel computing and carry-free for arithmetic operations, which results in very high throughput rates. In this paper, the properties of two-dimensional (2-D) PRNS are investigated in detail. It is shown that in the 2-D PRNS system, the theoretical lower bound for multiplication count of polynomial products can be achieved in some carefully chosen ring. Application of the proposed 2-D PRNS for computing 2-D circular convolution, which involves intensive multiplication operations, is also presented.

The organization of this paper is as follows: A brief overview of one-dimensional PRNS and a different interpretation of PRNS is presented in Section 2. The conversion of 1-D PRNS to its 2-D counterpart through the index mapping approach is then introduced. Also, the relationship between the two-dimensional convolution and the properties of 2-D PRNS are described in Section 3. It is shown that 2-D PRNS meets the theoretical lower bound of multiplication count for performing polynomial products. Concrete examples are presented in Section 4 to clarify how the system works. Finally, conclusions are addressed in Section 5.

2. One-dimensional polynomial residue number system

2.1. Preliminaries

Consider two polynomials in x, $A(x) = \sum_{i=0}^{N-1} a_i x^i$ and $B(x) = \sum_{i=0}^{N-1} b_i x^i$ also denoted as $A = (a_0, a_1, \ldots, a_{N-1})$ and $B = (b_0, b_1, \ldots, b_{N-1})$ and consider that $\langle c \rangle_m$ denotes the operation $c \bmod m$ for integers [7], while $\langle C(x) \rangle_{Q(x)}$ denotes the operation $C(x) \bmod Q(x)$ for polynomials. It was shown in [11] that if the polynomials $(x^N \pm 1)$ can be factorized in Z_m as

$$x^N \pm 1 = (x - r_0)(x - r_1)\cdots(x - r_{N-1}),$$
$$r_i \in Z_m,\ i = 0, 1, \ldots, N-1, \tag{1}$$

then there exists an isomorphic mapping between $P(m)$ and Z_m^N, where $P(m) = \{\sum_{i=0}^{N-1} p_i x^i,\ p_i \in Z_m\}$, a finite structure containing the $(N-1)$th order polynomials with coefficients in Z_m, and $Z_m^N = \bigoplus_{i=1}^{N} Z_m$, the Nth degree direct sum of Z_m, respectively. The above statement can be written in a more tracible form as

$$\langle A(x)B(x) \rangle_{x^N \pm 1} \overset{f_N}{\underset{f_N^{-1}}{\longleftrightarrow}} (\langle a_0^* b_0^* \rangle_m, \langle a_1^* b_1^* \rangle_m, \ldots, \langle a_{N-1}^* b_{N-1}^* \rangle_m), \tag{2}$$

where the forward mapping is

$$f_N : A = (a_0, a_1, \ldots, a_{N-1}) \rightarrow A^* = (a_0^*, a_1^*, \ldots, a_{N-1}^*) \tag{3}$$

with

$$a_i^* = \langle a_0 + a_1 r_i + a_2 r_i^2 + \cdots + a_{N-1} r_i^{N-1} \rangle_m, \tag{4}$$

and the inverse mapping is

$$f_N^{-1} : A^* = \langle a_0^*, a_1^*, \ldots, a_{N-1}^* \rangle \rightarrow A = (a_0, a_1, \ldots, a_{N-1}) \tag{5}$$

with

$$a_i = \langle N^{-1}(a_0^* r_0^{-i} + a_1^* r_1^{-i} + a_2^* r_2^{-i} + \cdots + a_{N-1}^* r_{N-1}^{-i}) \rangle_m, \quad i = 0, 1, \ldots, N-1, \tag{6}$$

where N^{-1} and r_j^{-i} are the multiplicative inverses of N and r_j^i in Z_m, respectively. Eqs. (4) and (6) can be written in a more compact form, respectively, as

$$a_i^* = \langle \langle A(x) \rangle_{(x - r_i)} \rangle_m = \langle A(r_i) \rangle_m, \quad i = 0, 1, \ldots, N-1 \tag{7}$$

and

$$A(x) = \sum_{i=0}^{N-1} a_i^* Q_i(x), \tag{8}$$

where

$$Q_i(x) = N^{-1}(1 + r_i^{-1}x + r_i^{-2}x^2 + \cdots + r_i^{-(N-1)}x^{N-1}). \quad (9)$$

Lemma 2.1. *The mapping f_N, defined in (3), satisfies the following:*
(i) *f_N is one-to-one and onto,*
(ii) *for $A, B \in P(m)$,*

$$f_N(A + B) = f_N(A) + f_N(B),$$
$$f_N(A \cdot B) = f_N(A) \cdot f_N(B). \quad (10)$$

Lemma 2.2. *The mapping f_N^{-1}, defined in (5), is the inverse of f_N.*

Lemma 2.3. *The necessary and sufficient condition for the existence of the factorization as shown in (1) is*

$$\begin{cases} N \mid (p_i - 1)/2 & \text{for } x^N + 1, \\ N \mid (p_i - 1) & \text{for } x^N - 1, \end{cases} \quad (11)$$

where $a|b$ means 'a divides *b' and $m = p_1^{e_1}p_2^{e_2}\cdots p_L^{e_L}$ with p_i distinct prime numbers and $N < p_i$.*

The proofs of the above lemmas can be found in [9].

2.2. A different interpretation

It is well-known that [5] if $m_1(x), m_2(x), \ldots, m_L(x)$ are polynomials which are relatively prime in pairs, then the system of congruences $R(x) = r_i(x) \bmod m_i(x)$, for $i = 1, 2, \ldots, L$, has a unique solution $R(x)$ given by

$$R(x) = \sum_{i=1}^{L} r_i(x)M_i(x)N_i(x) \bmod M(x), \quad (12)$$

where

$$M(x) = \prod_{i=1}^{L} m_i(x) = m_i(x)M_i(x) \quad (13)$$

and $N_i(x)$ uniquely satisfies the congruence

$$M_i(x)N_i(x) = 1 \bmod m_i(x). \quad (14)$$

Now consider the following congruence equation:

$$C(x) = \langle A(x) \cdot B(x) \rangle_{x^N \pm 1} \quad (15)$$

and let Z_m be chosen such that the condition (11) is satisfied. Then, based on the Chinese Remainder Theorem for polynomials (CRTP) and (1), Eq. (15) can be decomposed into the following N congruence equations:

$$c_i^* = \langle a_i^* \cdot b_i^* \rangle_m, \quad i = 0, 1, \ldots, N-1, \quad (16)$$

where $a_i^* = \langle\langle A(x)\rangle_{(x-r_i)}\rangle_m$ and $b_i^* = \langle\langle B(x)\rangle_{(x-r_i)}\rangle_m$. The polynomial $C(x)$ can be reconstructed by using the CRTP. That is,

$$M_i(x) = \prod_{j=0, j\neq i}^{N-1} (x - r_j), \quad i = 0, 1, \ldots, N-1 \quad (17)$$

$$= (x^N \pm 1)/(x - r_i)$$

$$= x^{N-1} + r_i x^{N-2} + r_i^2 x^{N-3} + \cdots + r_i^{N-2}x + r_i^{N-1}. \quad (18)$$

As a result,

$$\langle M_i(x)\rangle_{(x-r_i)} = M_i(r_i) = Nr_i^{N-1}. \quad (19)$$

Thus,

$$N_i(r_i) = (M_i(r_i))^{-1} = N^{-1}r_i^{-(N-1)} \bmod m. \quad (20)$$

It is easy to verify that

$$\langle N_i(r_i)\rangle_m \cdot M_i(x) = N^{-1}r_i^{-(N-1)}(x^{N-1} + r_i x^{N-2} + \cdots + r_i^{N-2}x + r_i^{N-1}). \quad (21)$$

Comparing Eq. (9) with Eq. (21), it follows that $\langle N_i(r_i)\rangle_m \cdot M_i(x) = Q_i(x)$. It is easy to check $\langle Q_i(x)\rangle_{(x-r_i)} = 1$ and $\langle Q_i(x)\rangle_{(x-r_j)} = 0$, for $i \neq j$. By CRTP, $C(x)$ can be obtained as

$$C(x) = \sum_{i=0}^{N-1} c_i^* \langle N_i(r_i)\rangle_m \cdot M_i(x)$$

$$= \sum_{i=0}^{N-1} c_i^* Q_i(x), \quad (22)$$

that is, the PRNS can also be interpreted by the terminology of CRTP over a finite ring.

3. Two-dimensional polynomial residue number system

3.1. Two-dimensional PRNS techniques for ring size reduction

The PRNS has one limitation: the size of the ring used for the arithmetic is proportional to the size of polynomials to be multiplied. As a result, to multiply large polynomials in a fixed-size arithmetic ring, one must involve two-dimensional PRNS techniques.

3.1.1. Survey of early works

In order to release the aforecited limitation, the one-dimensional PRNS by two-dimensional techniques was proposed by Skavantzous and Mitash [10]. Consider two polynomials in x, $A(x)=\sum_{i=0}^{N-1} a_i x^i$ and $B(x)=\sum_{i=0}^{N-1} b_i x^i$, where $N=n*m$: a composite number. Then $A(x)$ and $B(x)$ can be represented by two-variable polynomials as $A(x,y)=\sum_{i=0}^{m-1} A_i(y)x^i$ and $B(x,y)=\sum_{i=0}^{m-1} B_i(y)x^i$, where $A_i(y)$ and $B_i(y)$ are defined in (24) and (25), respectively. Now changing the variables as $y=x^m$, then similar to (15), one obtains

$$\begin{aligned} C'(x,y) &= \langle (A'(x,y))(B'(x,y))\rangle_{(x^{2m}\pm 1)(y^n\pm 1)} \\ &= \left\langle \left(\sum_{i=0}^{2m-1} A_i(y)x^i\right)\left(\sum_{i=0}^{2m-1} B_i(y)x^i\right)\right\rangle_{(x^{2m}\pm 1)(y^n\pm 1)} \\ &= \sum_{i=0}^{2m-1} C_i(y)x^i, \end{aligned} \tag{23}$$

where

$$A_i(y)=\sum_{j=0}^{n-1} a_{jm+i}y^j, \quad i=0,\ldots,m-1, \tag{24}$$

$$B_i(y)=\sum_{j=0}^{n-1} b_{jm+i}y^j, \quad i=0,\ldots,m-1, \tag{25}$$

$$C_i(y)=\sum_{j=0}^{n-1} c_{jm+i}y^j, \quad i=0,\ldots,2m-1, \tag{26}$$

and

$$A_i(y)=B_i(y)=0, \quad i=m,\ldots,2m-1.$$

Eq. (23) shows that to compute PRNS correctly, $A(x,y)$ and $B(x,y)$ must be augmented with zeros to construct $A'(x,y)$ and $B'(x,y)$, for $m\leqslant i\leqslant 2m-1$, such that aliasing of the cyclic folding along the x-dimension does not blur the correct results. Eq. (23) can be performed by applying a two-level (two-dimensional) PRNS mapping (as described in [10]); a PRNS(n) mapping followed by a PRNS($2m$) mapping provided that the mappings f_n, f_n^{-1}, f_{2m} and f_{2m}^{-1} exist in the chosen ring. To obtain the final result, Eq. (23) is converted to

$$\begin{aligned} C(x,y) &\triangleq \langle C'(x,y)\rangle_{(x^m\pm 1)(y^n\pm 1)} \\ &= \left\langle \sum_{i=0}^{m-1} C_i(y)x^i + y\cdot\sum_{i=m}^{2m-1} C_i(y)x^{i-m}\right\rangle_{(x^m\pm 1)(y^n\pm 1)}. \end{aligned} \tag{27}$$

Finally, the corresponding coefficients of $C(x)$ are obtained by substituting $y=x^m$ into Eq. (27).

3.1.2. Another approach

Index mappings for converting 1-D array to multidimensional (Multi-D) one was proposed by Agarwal [1] and Burrus [3]. The Nth degree polynomials $A(x)$ and $B(x)$ can be represented in matrix form as follows:

$$A'=\begin{bmatrix} a_0 & a_n & \cdots & a_{N-n} \\ a_1 & a_n+1 & \cdots & a_{N-n+1} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n-1} & a_{2n-1} & \cdots & a_{N-1} \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \tag{28}$$

$$B'=\begin{bmatrix} \pm b_{N-n+1} & b_1 & \cdots & b_{N-2n+1} \\ \pm b_{N-n+2} & b_2 & \cdots & b_{N-2n+2} \\ \vdots & \vdots & \cdots & \vdots \\ \pm b_{N-1} & b_{n-1} & \cdots & b_{N-n-1} \\ b_0 & b_n & \cdots & b_{N-n} \\ b_1 & b_{n+1} & \cdots & b_{N-n+1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1} & b_{2n-1} & \cdots & b_{N-1} \end{bmatrix}. \tag{29}$$

The sign of the first column in B' depends on where the PRNS was defined (i.e., positive if it is in $(x^N - 1)$, negative otherwise). Observing the above two $(2n-1)\times m$ matrices, A' is formed by columnwise sequencing the coefficients of $A(x)$ in the upper-half $n\times m$ array and appending $(n-1)$ rows of zeros to the lower-half, while B' is formed by columnwise sequencing the coefficients of $B(x)$ in the lower-half $n\times m$ array and appending the periodic extensions of each column data (with period N) to the upper-half. Matrices A' and B' can also be represented as two-variable polynomials. Each row of matrices A' and B' has the similar form as shown in Eqs. (24) and (25). Then by applying a two-level PRNS technique to obtain matrix C'. Forming an $n\times m$ matrix C'' by taking the elements of the lower $n\times m$ portion of C'. Then, it follows that the corresponding coefficients of $C(x)$ can be obtained via concatenating the columns of matrix C''. For ease of implementation with fast transform algorithms, the arrays would usually be extended one more additional row to form $2n\times m$ matrix C' rather than the $(2n-1)\times m$ one.

An interesting case occurs when n, m is coprime, the polynomial products modulo $(x^N - 1)$ has a useful mapping function to permute coefficients to form an $n\times m$ array without the necessity of extra padding $(n-1)$ rows of zeros. The mapping function of coefficient index is

$$N = mN_1 + nN_2,$$
$$0 \leqslant N_1 \leqslant n-1,\ 0 \leqslant N_2 \leqslant m-1, \tag{30}$$

or more clearly in matrix form as

$$(0,1,2,\ldots,N-1) \overset{\text{map}}{\Leftrightarrow} \begin{bmatrix} 0 & n & \cdots & (m-1)n \\ m & m+n & \cdots & m+(m+1)n \\ \vdots & \vdots & \ddots & \vdots \\ (n-1)m & (n-1)m+n & \cdots & (n-1)m+(m-1)n \end{bmatrix}. \tag{31}$$

Each element of the above matrix is evaluated modulo N. The rank of the matrix is reduced to n by m, rather than $2n$ by m. Since the computing process is performed the same as 1-D PRNS, with the reduced problem size, to obtain the results; therefore, the length limitation has been somewhat released. In the rest of this section, we will change our subject to investigate the extensibility of the PRNS, given in [11], through the computation of 2-D convolutions.

3.2. Two-variable polynomial residue number system

The two-variable polynomial residue number system (2V-PRNS) of order N by M, examines the problem of multiplying two 2-variable polynomials, with $(N-1)$th and $(M-1)$th degree in variables x and y, respectively, $\text{mod}(x^N \pm 1)\times(y^M \pm 1)$ over some modular ring Z_m and is a direct extension of one-dimensional PRNS given in [11]. Such a system performs the previously mentioned polynomial product with only MN multiplications mod m in parallel instead of M^2N^2.

The above statement can be represented by a two-variable polynomial product as $C(x,y) = \langle A(x,y)B(x,y)\rangle_{(x^N\pm1)(y^M\pm1)}$, where $A(x,y) = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} a_{i,j}x^j y^i$, $B(x,y) = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} b_{i,j}x^j y^i$ and $C(x,y) = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} c_{i,j}x^j y^i$. Here $\langle P(x,y)\rangle_{Q(x,y)}$ denotes the operation $P(x,y)$ mod $Q(x,y)$ in polynomials. It is clear that the above two-variable polynomial product is equivalent to the problem of 2-D convolutions.

3.2.1. Factorization $(y^M \pm 1)$ in Z_m

In order to factorize the polynomials $(x^N \pm 1)(y^M \pm 1)$ in NM distinct first degree factors, the factorization of $(y^M \pm 1)$ in M different roots is done first and then the factorization of $(x^N \pm 1)$ in N different roots, both in Z_m. It is clear that the above factorization is commutative. That is,

$$y^M \pm 1 = (y-r_0)(y-r_1)\cdots(y-r_{M-1}),$$
$$r_i \in Z_m,\ i = 0,1,\ldots,N-1, \tag{32}$$
$$x^N \pm 1 = (x-r'_0)(x-r'_1)\cdots(x-r'_{N-1}),$$
$$r'_i \in Z_m,\ i = 0,1,\ldots,N-1, \tag{33}$$

where r_i and r'_i are M and N distinct roots of $(y^M \pm 1)$ and $(x^N \pm 1)$, respectively, in a modular ring Z_m.

Suppose $P_1(m)$ is a finite structure containing polynomials composed of $(N-1)$th and $(M-1)$th order in variables x and y, respectively, with coefficients in Z_m. Then if polynomials $(y^M \pm 1)$ and $(x^N \pm 1)$ can be factorized in M and N distinct first degree factors in Z_m respectively, there exists an isomorphic mapping g'_M of $P_1(m)$ onto $\langle Z^N(x)\rangle_m = \bigoplus_{i=1}^{N} \langle Z(x)\rangle_m$, which is given by

$$g'_M : A(x,y) = \sum_{i=0}^{M-1} A_i(x) y^i \quad \rightarrow$$

$$A^*(x,y) = (A_0^*(x), A_1^*(x), \ldots, A_{M-1}^*(x)), \tag{34}$$

with

$$A_i^*(x) = \langle\langle A(x,y)\rangle_{(y-r_i)}\rangle_{(x^N\pm 1)} = \langle A(x,r_i)\rangle_{(x^N\pm 1)},$$
$$i = 0, 1, \ldots, M-1. \tag{35}$$

The notation $\langle Z(x)\rangle_m$ denotes that each coefficient of $Z(x)$ is defined in Z_m. And the inverse mapping is

$$g'^{-1}_M : A^*(x,y) = (A_0^*(x), A_1^*(x), \ldots, A_{M-1}^*(x)) \quad \rightarrow$$

$$A(x,y) = \sum_{i=0}^{M-1} A_i(x) y^i, \tag{36}$$

where $A(x,y)$ is defined as

$$A(x,y) = \sum_{i=0}^{M-1} A_i^*(x) Q_i^*(x,y) \tag{37}$$

and

$$Q_i^*(x,y) = M^{-1}(1 + r_i^{-1} y + r_i^{-2} y^2 + \cdots + r_i^{-(N-2)} y^{N-2} + r_i^{-(N-1)} y^{N-1}). \tag{38}$$

Combining Eqs. (37) and (38), the coefficients y^i in ring Z_m are given by

$$A_i(x) = \langle M^{-1}(A_0^*(x) + A_1^*(x) r_1^{-i} + A_2^*(x) r_2^{-i} + \cdots + A_{M-1}^*(x) r_{M-1}^{-i})\rangle_m,$$
$$i = 0, 1, \ldots, M-1, \tag{39}$$

where M^{-1} and r_i^{-j} are the multiplicative inverses of M and r_i^j in Z_m, respectively. Operations in $\langle Z^N(x)\rangle_m = \bigoplus_{i=1}^{N} \langle Z(x)\rangle_m$ are defined as follows.

Addition:

$$(A_0^*(x), A_1^*(x), \ldots, A_{M-1}^*(x)) + (B_0^*(x), B_1^*(x), \ldots, B_{M-1}^*(x)) = (\langle A_0^*(x) + B_0^*(x)\rangle_m, \langle A_1^*(x) + B_1*(x)\rangle_m, \ldots, \langle A_{M-1}^*(x) + B_{M-1}^*(x)\rangle_m). \tag{40}$$

Multiplication:

$$(A_0^*(x), A_1^*(x), \ldots, A_{M-1}^*(x)) \cdot (B_0^*(x), B_1^*(x), \ldots, B_{M-1}^*(x)) = (\langle\langle A_0^*(x)\cdot B_0^*(x)\rangle_{(x^N\pm 1)}\rangle_m, \ldots, \langle\langle A_{M-1}^*(x)\cdot B_{M-1}^*(x)\rangle_{(x^N\pm 1)}\rangle_m). \tag{41}$$

Each term of the right-hand side of Eq. (41) is a product of two single-variable polynomial defined in mod $\langle(x^N \pm 1)\rangle_m$ which can be computed by one-dimensional PRNS techniques with only N multiplications, as described in Section 2. Eq. (41) says that $\langle A(x,y)B(x,y)\rangle_{(x^N\pm 1)(y^M\pm 1)}$ only needs MN multiplications mod m performed in parallel and no additions, if the polynomial product is performed in $\langle Z^N(x)\rangle_m$. The same polynomial product requires M^2N^2 multiplications and $MN(M-1)(N-1)$ additions mod m, if directly performed in $P_1(m)$. In addition, the computation of the polynomial product in $\langle Z^N(x)\rangle_m$ requires only two levels (row and column transforms) of operations instead of the multiple levels $(M+N)$ in $P_1(m)$.

As indicated in Theorem 2 of [8], the number of MN multiplications is optimal for the aforecited 2-variable polynomial product since it achieves the theoretical minimum number of multiplications.

3.2.2. *Factorization* $(y^M \pm 1)$ *in* $Z(x)/(x^N \pm 1)$

Now let us consider another factorization method of $(x^N \pm 1)(y^M \pm 1)$ based on the ideas given in [8].

In this approach, the polynomials $(x^N \pm 1)(y^M \pm 1)$ are factorized as follows:

$$y^M \pm 1 = (y - r_0(x))(y - r_1(x))\cdots(y - r_{M-1}(x)),$$
$$r_i(x) \in Z(x)/(x^N \pm 1), \quad i = 0, 1, \ldots, M-1, \tag{42}$$

$$x^N \pm 1 = (x - r'_0)(x - r'_1)\cdots(x - r'_{N-1}),$$
$$r'_i \in Z_m, \ i = 0, 1, \ldots, N-1, \tag{43}$$

where $r_i(x)$ are M distinct roots of $(y^M \pm 1)$ in quotient ring $Z(x)/(x^N \pm 1)$ and r_i' are the N distinct roots of $x^N \pm 1$ in a modular ring Z_m.

If polynomials $(y^M \pm 1)$ and $(x^N \pm 1)$ can respectively be factorized in M and N distinct first degree factors in $Z(x)/(x^N \pm 1)$ and Z_m, there exists an isomorphic mapping g_M'' of $P_1(m)$ onto $\langle Z^N(x)\rangle_m$, which is given by

$$g_M'': A(x,y) = \sum_{i=0}^{M-1} A_i(x) y^i \quad \rightarrow$$

$$A^\circ(x,y) = (A_0^\circ(x), A_1^\circ(x), \ldots, A_{M-1}^\circ(x)), \tag{44}$$

with

$$A_i^\circ(x) = \langle\langle A(x,y)\rangle_{(y - r_i(x))}\rangle_{(x^N \pm 1)} = \langle A(x, r_i(x))\rangle_{(x^N \pm 1)}, \quad i = 0, 1, \ldots, M-1, \tag{45}$$

where $\langle Z(x)/(x^N \pm 1)\rangle_m$ denotes the operation that the coefficients of polynomial $Z(x)$ first mod$(x^N \pm 1)$ then mod m. The inverse mapping is

$$g_M''^{-1}: A^\circ(x,y) = (A_0^\circ(x), A_1^\circ(x), \ldots, A_{M-1}^\circ(x)) \quad \rightarrow$$

$$A(x,y) = \sum_{i=0}^{M-1} A_i(x) y^i, \tag{46}$$

where $A(x,y)$ is defined as

$$A(x,y) = \sum_{i=0}^{M-1} A_i^\circ(x) Q_i^\circ(x,y) \tag{47}$$

and

$$Q_i^\circ(x,y) = M^{-1}(1 + r_i^{-1}(x)y + r_i^{-2}(x)y^2 + \cdots + r_i^{-(N-2)}(x)y^{N-2} + r_i^{-(N-1)}(x)y^{N-1}). \tag{48}$$

Combining Eqs. (47) and (48), the coefficients y^i in quotient ring $\langle Z[x]/(x^N \pm 1)\rangle_m$ are given by

$$A_i(x) = \langle M^{-1}(A_0^\circ(x) + A_1^\circ(x) r_1^{-i}(x) + A_2^\circ(x) r_2^{-i}(x) + \cdots + A_{M-1}^\circ(x) r_{M-1}^{-i}(x))\rangle_m, \quad i = 0, 1, \ldots, M-1, \tag{49}$$

where M^{-1} and $r_i^{-j}(x)$ are the multiplicative inverses of M and $r_i^j(x)$ in Z_m and $Z(x)/(x^N \pm 1)$, respectively. Operations in $\langle Z^N(x)\rangle_m$ are defined as follows.

Addition:

$$(A_0^\circ(x), A_1^\circ(x), \ldots, A_{M-1}^\circ(x)) + (B_0^\circ(x), B_1^\circ(x), \ldots, B_{M-1}^\circ(x)) = (\langle\langle A_0^\circ(x) + B_0^\circ(x)\rangle_{(x^N \pm 1)}\rangle_m, \ldots, \langle\langle A_{M-1}^\circ(x) + B_{M-1}^\circ(x)\rangle_{(x^N \pm 1)}\rangle_m). \tag{50}$$

Multiplication:

$$(A_0^\circ(x), A_1^\circ(x), \ldots, A_{M-1}^\circ(x)) \cdot (B_0^\circ(x), B_1^\circ(x), \ldots, B_{M-1}^\circ(x)) = (\langle\langle A_0^\circ(x) \cdot B_0^\circ(x)\rangle_{(x^N \pm 1)}\rangle_m, \ldots, \langle\langle A_{M-1}^\circ(x) \cdot B_{M-1}^\circ(x)\rangle_{(x^N \pm 1)}\rangle_m). \tag{51}$$

Each term of the right-hand side of Eq. (51) is the product of two single-variable polynomials defined in mod $\langle x^N \pm 1\rangle_m$ which can be computed by one-dimensional PRNS techniques with only N multiplications, as described in Section 2. In other words, Eq. (51) implies that a polynomial product $\langle A(x,y)B(x,y)\rangle_{(x^N \pm 1)(y^M \pm 1)}$ only needs MN multiplications mod m performed in parallel and no additions, if the polynomial product is performed in $\langle Z^N(x)\rangle_m$.

The following theorems describe the properties of the mapping g_M'' and the simplified rules of multiplication on two-dimensional PRNS.

Theorem 3.1. *If the polynomial* $(y^M \pm 1)$ *can be factorized in* M *distinct factors in* $Z(x)/(x^N \pm 1)$, *as shown by Eq. (42), then the mapping* g_M'' *of* $P_1(m)$ *onto* $\langle Z^N(x)\rangle_m$ *satisfies the following*:

(i) g_M'' *is one-to-one and onto*,

(ii) *for* $A, B \in P_1(m)$,

$$g_M''(A + B) = g_M''(A) + g_M''(B),$$

$$g_M''(A \cdot B) = g_M''(A) \cdot g_M''(B).$$

Proof. (i): The number of elements in $P(m)$ is $m^{(N+M)}$ and so is the number of elements in $\langle Z^N(x)\rangle_m = \langle Z(x)\rangle_m \oplus \langle Z(x)\rangle_m \oplus \cdots \oplus \langle Z(x)\rangle_m$. It must now be shown that for $A, B \in P_1(m)$

$$A \neq B \Rightarrow g_M''(A) \neq g_M''(B). \tag{52}$$

Suppose that for $A = \sum_{i=0}^{M-1} A_i(x)y^i = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} a_{i,j}x^j y^i$, $B = \sum_{i=0}^{M-1} B_i(x)y^i = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} b_{i,j}x^j y^i$ with $a_{i,j}, b_{i,j} \in Z_m$ for $i = 0, \ldots, M-1$ and $j = 0, \ldots, N-1$, the following is true:

$$A \neq B \Rightarrow g''_M(A) = g''_M(B). \tag{53}$$

But

$$\begin{aligned}
&A \neq B \\
&\Leftrightarrow A_0(x) \neq \langle B_0(x)\rangle_{(x^N \pm 1)} \text{ or } \cdots \text{ or } \\
&\quad A_{M-1}(x) \neq \langle B_{M-1}(\mathbf{x})\rangle_{(x^N \pm 1)} \\
&\Leftrightarrow A_0(x) - B_0(x) \neq \langle 0\rangle_{(x^N \pm 1)} \text{ or } \cdots \text{ or } \\
&\quad A_{M-1}(x) - B_{M-1}(\mathrm{x}) \neq \langle 0\rangle_{(x^N \pm 1)} \\
&\Leftrightarrow A_0(x) - B_0(x) = k_0(x^N \pm 1) + q_0(x) \text{ and } \\
&\quad \cdots \text{ and } A_{M-1}(x) - B_{M-1}(x) \\
&\quad = k_{M-1}(x^N \pm 1) + q_{M-1}(x),
\end{aligned} \tag{54}$$

with $k_0, k_1, \ldots, k_{M-1}$ integers and $q_0(x), q_1(x), \ldots, q_{M-1}(x) \in \langle Z(x)/(x^N \pm 1)\rangle_m$ and at least one of $q_0(x), q_1(x), \ldots, q_{M-1}(x)$ is not zero.

For $g''_M(A)$ and $g''_M(B)$, Eq. (45) gives

$$\begin{aligned}
g''_M(A) &= (A_0^{\diamond}(x), A_1^{\diamond}(x), \ldots, A_{M-1}^{\diamond}(x)) \\
&\equiv \langle A(x, r_0(x)), A(x, r_1(x)), \ldots, \\
&\qquad A(x, r_{M-1}(x))\rangle_{(x^N \pm 1)}
\end{aligned} \tag{55}$$

or

$$\begin{aligned}
g''_M(A) = \Big\langle &\sum_{i=0}^{M-1} A_i(x) r_0^i(x), \sum_{i=0}^{M-1} A_i(x) r_1^i(x), \ldots, \\
&\sum_{i=0}^{M-1} A_i(x) r_{M-1}^i(x) \Big\rangle_{(x^N \pm 1)},
\end{aligned} \tag{56}$$

with a similar expression holds true for $g''_M(B)$.

For $g''_M(A) = g''_M(B)$ we have

$$\begin{aligned}
&(A_0(x) - B_0(x)) + \cdots \\
&\quad + (A_{M-1}(x) - B_{M-1}(x)) r_j^{M-1}(x) \equiv \langle 0\rangle_{(x^N \pm 1)},
\end{aligned} \tag{57}$$

Eq. (57) is true for $j = 0, 1, \ldots, M-1$.

Substituting each term $(A_i(x) - B_i(x))$ in Eq. (57) by its corresponding term defined in Eq. (54) we get

$$\begin{aligned}
&(k_0 + k_1 r_j(x) + k_2 r_j^2(x) + \cdots \\
&\quad + k_{M-1} r_j^{M-1}(x))(x^N \pm 1) \\
&\quad + (q_0(x) + q_1(x) r_j(x) + q_2(x) r_j^2(x) + \cdots \\
&\quad + q_{M-1}(x) r_j^{M-1}(x) \equiv \langle 0\rangle_{(x^N \pm 1)}
\end{aligned}$$

or

$$\begin{aligned}
&q_0(x) + q_1(x) r_j(x) + q_2(x) r_j^2(x) + \cdots \\
&\quad + q_{M-1}(x) r_j^{M-1}(x) \equiv \langle 0\rangle_{(x^N \pm 1)},
\end{aligned} \tag{58}$$

for $j = 0, 1, \ldots, M-1$.

It has been proven [9] that for $r'_0, r'_1, \ldots, r'_{N-1}$ satisfying Eq. (33) the following hold:

$$\sum_{j=0}^{N-1} r'_j = \sum_{j=0}^{N-1} r_j'^2 = \cdots = \sum_{j=0}^{N-1} r_j'^{N-1} \equiv \langle 0\rangle_m. \tag{59}$$

Similarly, it can be easily proven that for $r_0(x)$, $r_1(x), \ldots, r_{M-1}(x)$ satisfying Eq. (42), the following hold:

$$\begin{aligned}
\sum_{j=0}^{M-1} r_j(x) &= \sum_{j=0}^{M-1} r_j^2(x) = \cdots = \sum_{j=0}^{M-1} r_j^{M-1}(x) \\
&\equiv \langle 0\rangle_{(x^N \pm 1)}.
\end{aligned} \tag{60}$$

Adding all M congruences in Eq. (58) for $j = 0$ to $M-1$, we get

$$\begin{aligned}
&M q_0(x) + q_1(x) \sum_{j=0}^{M-1} r_j(x) + q_2(x) \sum_{j=0}^{M-1} r_j^2(x) + \cdots \\
&\quad + q_{M-1}(x) \sum_{j=0}^{M-1} r_j^{M-1}(x) \equiv \langle 0\rangle_{(x^N \pm 1)}
\end{aligned} \tag{61}$$

and with the aid of Eq. (60), Eq. (61) reduces to

$$M \cdot q_0(x) \equiv \langle 0\rangle_{(x^N \pm 1)} \tag{62}$$

Since $0 < M < m$ (so $M \neq \langle 0\rangle_m$), then Eq. (62) gives that $q_0(x) \equiv \langle 0\rangle_{(x^N \pm 1)}$. Now Eq. (58) becomes

$$\begin{aligned}
&r_j(x)(q_1(x) + q_2(x) r_j(x) + \cdots + q_{M-1}(x) r_j^{M-2}(x)) \\
&\quad \equiv \langle 0\rangle_{(x^N \pm 1)}, \quad j = 0, \ldots, M-1.
\end{aligned} \tag{63}$$

Adding all M congruences in Eq. (63) for $j = 0$ to $M-1$ we get $q_1(x) \equiv \langle 0 \rangle_{(x^N \pm 1)}$ (using again Eq. (60) and the fact $r_j(x) \neq \langle 0 \rangle_{(x^N \pm 1)}$). Repeating the above procedure, we obtain

$$q_0(x) \equiv q_1(x) \equiv \cdots \equiv q_{M-1}(x) \equiv \langle 0 \rangle_{(x^N \pm 1)}. \tag{64}$$

But it was stated previously that at least one of $q_0(x), q_1(x), \ldots, q_{M-1}(x)$ must be nonzero. So Eq. (64) creates a contradiction. The contradiction was a result of the wrong assumption of Eq. (53), and therefore $g''_M(A) \neq g''_M(B)$ and the proof of (i) is now completed.

(ii): Substituting $g''_M(A)$, $g''_M(B)$, $g''_M(A+B)$ and $g''_M(A \cdot B)$ into Eq. (56), the proof of (ii) can be derived easily. Since

$$A \cdot B = \sum_{i=0}^{M-1} A_i(x) y^i \cdot \sum_{i=0}^{M-1} B_i(x) y^i \bmod (x^N \pm 1)(y^M \pm 1) \tag{65}$$

and

$$\begin{aligned} g''_M(A \cdot B) &= \langle \langle AB(x, r_0(x)), AB(x, r_1(x)), \ldots, \\ &\qquad AB(x, r_{M-1}(x)) \rangle_{(x^N \pm 1)} \rangle_m \\ &= \Bigg(\sum_{i=0}^{M-1} A_i(x) r_0^i(x) \sum_{i=0}^{M-1} B_i(x) r_0^i(x), \ldots, \\ &\qquad \sum_{i=0}^{M-1} A_i(x) r_{M-1}^i(x) \sum_{i=0}^{M-1} B_i(x) r_{M-1}^i(x) \Bigg). \end{aligned} \tag{66}$$

Evaluating $g''_M(A) \cdot g''_M(B)$ and taking into account that $x^N \equiv \pm 1 \bmod (x^N \pm 1)$, it follows that $g''_M(A \cdot B) = g''_M(A) \cdot g''_M(B)$. In a similar way, it can be shown that $g''_M(A+B) = g''_M(A) + g''_M(B)$ and (ii) is proven. Therefore, g''_M is an isomorphism mapping from $P_1(m)$ onto $\langle Z^N(x) \rangle_m$. □

The theorem shows that if $(y^M \pm 1)$ can be factorized into M distinct roots, represented by powers of x, in quotient ring $Z(x)/(x^N \pm 1)$, rather than in ring Z_m, the forward mapping g''_M and inverse mapping g''^{-1}_M can simplify the hardware design, i.e., with only addition and shifting but not any multiplications. When N is a power of 2, the computation can be sped up by using an FFT-like structure.

Theorem 3.2. *The mapping g''^{-1}_M described by Eqs. (36)–(38) is the inverse of g''_M.*

Proof. Consider $A(x,y) \in P_1(m)$ with $A(x,y) = \sum_{i=0}^{M-1} A_i(x) y^i$. Then by Eqs. (32) and (35), $g''_M(A) = (A_0^\circ(x), A_1^\circ(x), \ldots, A_{M-1}^\circ(x))$ with

$$\begin{aligned} A_i^\circ(x) &= \langle \langle A_{M-1}(x) r_i^{M-1}(x) + A_{M-2}(x) r_i^{M-2}(x) \\ &\qquad + \cdots + A_0(x) \rangle_{(x^N \pm 1)} \rangle_m, \\ &\quad i = 0, 1, \ldots, M-1. \end{aligned} \tag{67}$$

Substituting $A_i^\circ(x)$ and $Q_i^\circ(x,y)$ respectively into Eq. (37) and Eq. (38), one obtains

$$\begin{aligned} A(x,y) &= \sum_{i=0}^{M-1} A_i^\circ(x) \cdot Q_i^\circ(x,y) \\ &= \sum_{i=0}^{M-1} \left(\sum_{j=0}^{M-1} A_j(x) r_i^j(x) \right) (M^{-1}(1 + r_j^{-1}(x) y \\ &\qquad + \cdots + r_j^{-(M-1)}(x) y^{M-1})) \\ &= M^{-1}(MA_0(x) + MA_1(x) y + \cdots \\ &\qquad + MA_{M-1}(x) y^{M-1}) \\ &= A_0(x) + A_1(x) y + \cdots + A_{M-1}(x) y^{M-1}. \end{aligned} \tag{68}$$

The proof is now completed since it has been shown that $g''^{-1}_M(g''_M(A(x,y))) = A(x,y)$. □

The readers can also prove that the isomorphic mapping g'_M possesses the same properties with g''_M, as described in the aforecited theorems.

Some special cases of two-dimensional PRNS are of interests especially for both M and N are powers of 2. The following lemmas show the polynomial $(y^M \pm 1)$ can be factorized in M distinct factors in $Z(x)/(x^N + 1)$ as suggested in Eq. (42)

Lemma 3.1. *$(y^M + 1)$ can be factorized into M distinct factors in quotient field $Z(x)/(x^N + 1)$ as $(y^M + 1) = \prod_{k=0}^{2^{t_2}-1} (y - (x^{N/M})^{2k+1})$ if $M = 2^{t_2}$ and $N = 2^{t_1}$, $1 \leqslant t_2 \leqslant t_1 \in Z$.*

Proof. In the following proof, we use the fact $x^N \equiv -1 \bmod Z(x)/(x^N+1)$:

$$\begin{aligned}
&\prod_{k=0}^{2^{t_2}-1}(y-(x^{N/M})^{2k+1})\\
&=\prod_{k=0}^{2^{t_2-1}-1}[y-(x^{N/M})^{2k+1}][y-(x^{N/M})^{2(k+2^{t_2-1})+1}]\\
&=\prod_{k=0}^{2^{t_2-1}-1}(y^2-(x^{2\cdot N/M})^{2k+1})\\
&=\prod_{k=0}^{2^{t_2-2}-1}[y^2-(x^{2\cdot N/M})^{2k+1}]\\
&\qquad\cdot[y^2-(x^{2\cdot N/M})^{2(k+2^{t_2-2})+1}]\\
&=\prod_{k=0}^{2^{t_2-2}-1}(y^4-(x^{4\cdot N/M})^{2k+1})\\
&\quad\vdots\\
&=\prod_{k=0}^{1}(y^{2^{t_2-1}}-(x^{2^{t_2-1}\cdot N/M})^{2k+1})\\
&=(y^{2^{t_2-1}}-x^{2^{t_2-1}\cdot N/M})(y^{2^{t_2-1}}+x^{2^{t_2-1}\cdot N/M})\\
&=y^M+1. \qquad \square
\end{aligned}$$

Lemma 3.2. *(y^M-1) can be factorized into M distinct factors in quotient field $Z(x)/(x^N+1)$ as $(y^M-1)=\prod_{k=0}^{2^{t_2-1}}(y-(x^{2N/M})^k)$ if $M=2^{t_2}$ and $N=2^{t_1}$, $1\leqslant t_2<t_1\in Z$.*

Proof. In the following proof, we use the fact $x^N \equiv -1 \bmod Z(x)/(x^N+1)$:

$$\begin{aligned}
&\prod_{k=0}^{2^{t_2}-1}(y-(x^{2N/M})^k)\\
&=\prod_{k=0}^{2^{t_2-1}-1}[y-(x^{2N/M})^k][y-(x^{2N/M})^{k+2^{t_2-1}}]\\
&=\prod_{k=0}^{2^{t_2-1}-1}(y^2-(x^{2\cdot 2N/M})^k)\\
&=\prod_{k=0}^{2^{t_2-2}-1}[y^2-(x^{2\cdot 2N/M})^k][y^2-(x^{2\cdot 2N/M})^{k+2^{t_2-2}}]\\
&=\prod_{k=0}^{2^{t_2-2}-1}(y^4-(x^{4\cdot 2N/M})^k)\\
&\quad\vdots\\
&=\prod_{k=0}^{1}(y^{2^{t_2-1}}-(x^{2^{t_2-1}\cdot 2N/M})^k)\\
&=y^{2^{t_2}}-1\\
&=y^M-1. \qquad \square
\end{aligned}$$

The 2-D circular convolution of size N by M is equivalent to the 2-D polynomial product $\bmod(x^N-1)(y^M-1)$. To factorize (y^M-1) in quotient field $Z(x)/(x^N-1)$ is not easy. By the technique presented in [2], the problem is converted to factorize (y^M-1) in quotient field $Z(x)/(x^N+1)$. Therefore, 2-D circular convolution can also be realized by 2-D PRNS techniques.

3.3. Time complexity

The complexities of the proposed approach can be analysized as follows. Without considering the forward and inverse transforms of PRNS, the row and column transforms of the input sequences can be neglected. After performing PRNS(M) and then PRNS(N), we obtain a tuple of MN transformed data. MN multiplications are required in the componentwise products between the tuples. By inverse transforming PRNS$^{-1}(M)$ and then PRNS$^{-1}(N)$, the task is completed.

In fact, based on the interpretation given in Section 2, the above processes can be executed in the MN fully decomposed distinct residue subrings modulo $(x-r_i)(y-r_j)$, $0\leqslant i<N$, $0\leqslant j<M$. In other words, only MN corresponding componentwise products and the CRTP reconstruction process are required. As a result, the product of two 2-variable polynomials can be performed by 2V-PRNS with a multiplication-complexity which meets Winograd's lower bound [6].

4. Examples

First, a concrete example of computing a 2×4 cyclic convolution is given to have a better

understanding of Section 3.2.1. Consider the following 2-D cyclic convolution:

$$\begin{bmatrix} 2 & 1 & 5 & 2 \\ 3 & 4 & 6 & 7 \end{bmatrix} (*_c) \begin{bmatrix} 2 & 4 & 2 & 3 \\ 1 & 3 & 2 & 5 \end{bmatrix}, \tag{69}$$

where '$*_c$' denotes the operation of 2-D cyclic convolution. Eq. (69) can be represented in 2-variable polynomial form as

$$C(x,y) = \langle A(x,y)\cdot B(x,y)\rangle_{(x^4-1)(y^2-1)}, \tag{70}$$

where

$$A(x,y) = (2 + 1x + 5x^2 + 2x^3) + (3 + 4x + 6x^2 + 7x^3)y,$$

$$B(x,y) = (2 + 4x + 2x^2 + 3x^3) + (1 + 3x + 2x^2 + 5x^3)y.$$

The modular ring Z_m is chosen to be integer m with $m = 173$ which satisfies $N = 4\,|\,(173 - 1)$ and $M = 2\,|\,(173 - 1)$.

Step 1. Let us factorize $(y^2 - 1)$ in Z_{173} as

$$y^2 - 1 = (y - 1)(y + 1). \tag{71}$$

Step 2.

$$A(x,y) \xrightarrow{g_2'} A^*(x,y) = (A_0^*(x), A_1^*(x))$$

$$= (5 + 5x + 11x^2 + 9x^3,\ -1 - 3x - x^2 - 5x^3),$$

$$B(x,y) \xrightarrow{g_2'} B^*(x,y) = (B_0^*(x), B_1^*(x))$$

$$= (3 + 7x + 4x^2 + 8x^3,\ 1 + 1x - 2x^3).$$

Step 3. By one-dimensional PRNS technique, we get

$$C^*(x,y) = A^*(x,y)\cdot B^*(x,y) = (162 + 174x + 160x^2 + 164x^3,\ -2x + 6x^2 - 4x^3). \tag{72}$$

Step 4. Reconstruct $C_i(x)$ from

$$C(x,y) = \sum_{i=0}^{i=1} C_i^*(x)\cdot Q_i^*(x,y) = C_0^*(x)\cdot 2^{-1}(1 + y) + C_1^*(x)(1 - y) = (81 + 86x + 83x^2 + 80x^3) + (81 + 88x + 77x^2 + 84x^3)y.$$

That is,

$$\begin{bmatrix} 2 & 1 & 5 & 2 \\ 3 & 4 & 6 & 7 \end{bmatrix} (*_c) \begin{bmatrix} 2 & 4 & 2 & 3 \\ 1 & 3 & 2 & 5 \end{bmatrix} = \begin{bmatrix} 81 & 86 & 83 & 80 \\ 81 & 88 & 77 & 84 \end{bmatrix}. \tag{73}$$

As shown in this example, the modular ring F must be chosen such that $|F| \geqslant (2\cdot\max(a_{i,j})\|b_{i,j}\| + 1)$ [4], where $|F|$ denotes the cardinality of F, $\max(a_{i,j})$ denotes the largest value of the 2-D array $a_{i,j}$ and $\|b_{i,j}\|$ is the sum of the magnitudes of all the elements of $b_{i,j}$.

Another concrete example by utilizing the full power of two-dimensional PRNS in computing 2×4 two-variable polynomial products is given to clarify the approach of Section 3.2.2. Consider the following 2-D PRNS $\bmod(x^4 + 1)(y^2 + 1)$:

$$\begin{bmatrix} 2 & 2 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} (*_+) \begin{bmatrix} 2 & 1 & 3 & 1 \\ 1 & 2 & 1 & 0 \end{bmatrix}, \tag{74}$$

where '$*_+$' denotes the operation $\bmod(x^4 + 1)\times(y^2 + 1)$. Eq. (74) can be represented in 2-variable polynomial form as

$$C(x,y) = \langle A(x,y)\cdot B(x,y)\rangle_{(x^4+1)(y^2+1)}, \tag{75}$$

where

$$A(x,y) = (2 + 2x + 0x^2 + 1x^3) + (1 + 1x + 0x^2 + 1x^3)y,$$

$$B(x,y) = (2 + 1x + 3x^2 + 1x^3) + (1 + 2x + 1x^2 + 0x^3)y.$$

The modular ring Z_m is chosen to be integer m with $m = 17$ which satisfies $N = 4\,|\,(17 - 1)$ and $M \leqslant N$.

Step 1.Let us factorize $(y^2 + 1)$ in quotient field $Z(x)/(x^4 + 1)$ as

$$y^2 + 1 = (y - x^2)(y + x^2). \tag{76}$$

Step 2.

$$A(x,y) \xrightarrow{g_2''} A^\circ(x,y) = (A_0^\circ(x), A_1^\circ(x))$$

$$= (2 + 1x + 1x^2 + 2x^3, 2 + 3x - 1x^2 + 0x^3),$$

$$B(x,y) \xrightarrow{g_2''} B^\circ(x,y) = (B_0^\circ(x), B_1^\circ(x))$$

$$= (1 + 1x + 4x^2 + 3x^3, 3 + 1x + 2x^2 - 1x^3).$$

Step 3. Let us factorize $(x^4 + 1)$ in field Z_{17} as

$$x^4 + 1 = (x - 2)(x - 4)(x - 8)(x - 16). \tag{77}$$

By 1-D PRNS technique, $C^\circ(x, y)$ can be obtained as

$$\begin{aligned} C^\circ(x, y) &= A^\circ(x, y) \cdot B^\circ(x, y) \\ &= (-7 - 8x + 4x^2 + 13x^3, \\ &\quad 11 + 10x + 4x^2 + 3x^3). \end{aligned} \tag{78}$$

Step 4. Reconstruct $C_i(x)$ from

$$\begin{aligned} C(x, y) &= \sum_{i=0}^{i=1} C_i^\circ(x) \cdot Q_i^\circ(x, y) \\ &= C_0^\circ(x) \cdot 2^{-1}(1 - x^2 y) \\ &\quad + C_1^\circ(x) \cdot 2^{-1}(1 + x^2 y) \\ &= (2 + 1x + 4x^2 + 8x^3) \\ &\quad + (0 + 5x + 9x^2 + 9x^3)y. \end{aligned}$$

That is,

$$\begin{bmatrix} 2 & 2 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} (*_+) \begin{bmatrix} 2 & 1 & 3 & 1 \\ 1 & 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 4 & 8 \\ 0 & 5 & 9 & 9 \end{bmatrix}. \tag{79}$$

5. Discussions and conclusions

In this paper, from the derivations given in Section 2, the polynomial residue number system can be interpreted by the terminology of Chinese Remainder Theorem for polynomials over a finite ring, which is more familiar with the computer and signal processing societies. The index mapping techniques is proposed to implement long length 1-D PRNS by Multi-D PRNS. 2-D PRNS system has been investigated in detail. This system provides a powerful tool for computing polynomial products $\bmod(x^N \pm 1)(y^M \pm 1)$ with a minimum multiplication complexity and full parallelism. The proposed 2-D PRNS has the advantage of better extensibility, it can be applied to define Multi-D PRNS directly.

This work is principally theoretical and strictly mathematically oriented. Applications are discussed but no complete design implementations are given. One limitation of such approach is the size of the ring used for the arithmetic is proportional to the size of polynomials to be multiplied. As a result, one must involve the expensive-cost of hardware design or table lookup implementations. Future research may focus on applications which are implemented using the PRNS to provide high-speed, low-cost, low complexity designs. The present work provides the necessary theoretical backgrounds and mathematic tools for the researchers, in this direction, for further works.

References

[1] R.C. Agarwal and C.S. Burrus, "Fast one-dimensional digital convolution by multidimensional techniques", *IEEE Trans. Acoust. Speech Signal Process.*, Vol. ASSP-22, No. 1, February 1974, pp. 1–10.

[2] B. Arambepola and P.J.W. Rayner, "Efficient transforms for multidimensional convolutions", *Electronic Lett.*, Vol. 15, No. 7, 1979, pp. 189–190.

[3] C.S. Burrus, "Index mappings for multidimensional formulation of the DFT and convolution", *IEEE Trans. Acoust. Speech Signal Process.*, Vol. ASSP-25, No. 3, June 1977, pp. 239–242.

[4] E.V. Krishnamurthy, *Error-Free Polynomial Matrix Computations*, Springer, New York, 1985, Chapter 5, pp. 74–78.

[5] J.H. McClellan and C.M. Rader, *Number Theory in Digital Signal Processing*, Prentice-Hall, Englewood Cliffs, NJ, 1979.

[6] H.J. Nussbaumer, *Fast Fourier Transform and Convolution Algorithms*, Springer, Berlin, 1981, Chapter 2, pp. 29–31.

[7] A.V. Oppenheim, *Applications of Digital Signal Processing*, Prentice-Hall, Englewood Cliffs, NJ, 1978.

[8] I. Pitas and M.G. Srintzis, "Multidimensional cyclic convolution algorithms with minimal multiplicative complexity", *IEEE Trans. Acoust. Speech Signal Process.*, Vol. ASSP-35, No. 3, March 1987, pp. 384–390.

[9] A. Skavantzos, The polynomial residue number system and its application, Ph.D. Dissertation, Univ. Florida, August 1987.

[10] A. Skavantzos and N. Mitash, "Implementation issues of 2-dimensional polynomial multipliers for signal processing using residue arithmetic", *IEE Proc.-E*, Vol. 140, No. 1, January 1993, pp. 45–53.

[11] A. Skavantzos and F.J. Taylor, "On the polynomial residue number system", *IEEE Trans. Signal Process.*, Vol. 39, No. 2, February 1991, pp. 376–382.