Comput. Math. Applic. Vol. 15, No. 9, pp. 757–768, 1988
Printed in Great Britain.

0097-4943/88 $3.00 + 0.00

EXACT DECONVOLUTION USING NUMBER-THEORETIC TRANSFORMS

G. DRAUSCHKE and M. TASCHE
Wilhelm-Pieck-Universität Rostock, Sektion Mathematik, Universitätsplatz 1,
DDR-2500 Rostock, G.D.R.

(*Received* 5 *October* 1987)

Communicated by E. Y. Rodin

Abstract—Using residue arithmetic and number-theoretic transforms, new algorithms of the one- and two-dimensional deconvolution are described. These algorithms work without round-off errors and yield the exact solution under natural conditions. By the same method, the exact value of the determinant of a circulant integer matrix is computed, too.

1. DECONVOLUTION PROBLEMS

Let us denote by $\mathbb{Z}$ the ring of integers, by $\mathbb{N}$ the set of positive integers and by $\mathbb{Q}$ the field of rational numbers. Let $n \in \mathbb{N}$, $n > 2$. For given n-dimensional integer vectors $\mathbf{a} = [a(0), \ldots, a(n-1)]^T \in \mathbb{Z}^n$ and $\mathbf{b} = [b(0), \ldots, b(n-1)]^T \in \mathbb{Z}^n$, $\mathbf{b} \neq \mathbf{o} := [0, \ldots, 0]^T$, we want to solve numerically without round-off errors the following special system of n linear equations:

$$(\text{circ } \mathbf{a})\, \mathbf{x} = \mathbf{b}, \tag{1}$$

where

$$\text{circ } \mathbf{a} := \begin{bmatrix} a(0) & a(n-1) & \ldots & a(1) \\ a(1) & a(0) & \ldots & a(2) \\ \vdots & \vdots & & \vdots \\ a(n-1) & a(n-2) & \ldots & a(0) \end{bmatrix} \in \mathbb{Z}^{n \times n}$$

is a nonsingular circulant matrix and $\mathbf{x} = [x(0), \ldots, x(n-1)]^T \in \mathbb{Q}^n$ is an unknown vector. We remark that the one-dimensional deconvolution problem (1) can be written as

$$\mathbf{a} * \mathbf{x} = \mathbf{b}, \tag{2}$$

where $*$ denotes the one-dimensional cyclic convolution, i.e.

$$b(k) := \sum_{i=0}^{n-1} a(k-i)\, x(i), \quad k = 0, \ldots, n-1.$$

Note that the difference $k - i$ must be calculated modulo n.

The two-dimensional deconvolution problem considered in Section 6 reads as follows. Let two $n \times n$ integer matrices $\mathbf{A} = [a(i,j)]_{i,j=0}^{n-1} \in \mathbb{Z}^{n \times n}$ and $\mathbf{B} = [b(i,j)]_{i,j=0}^{n-1} \in \mathbb{Z}^{n \times n}$, $\mathbf{B} \neq \mathbf{O} := [0]_{i,j=0}^{n-1}$ be given. Find the exact solution $\mathbf{X} = [x(i,j)]_{i,j=0}^{n-1} \in \mathbb{Q}^{n \times n}$ of the relation

$$\mathbf{A} * \mathbf{X} = \mathbf{B}, \tag{3}$$

where $*$ denotes the two-dimensional cyclic convolution, i.e.

$$b(k,l) := \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a(k-i, l-j)\, x(i,j), \quad k, l = 0, \ldots, n-1.$$

Here, both $k - i$ and $l - j$ must be calculated modulo n. Of course, we assume that (3) is uniquely solvable.

Sampling an integer matrix $\mathbf{X} \in \mathbb{Z}^{n \times n}$ by rows, we obtain the n^2-dimensional vector

$$\text{row } \mathbf{X} := [x(0,0), \ldots, x(0,n-1), \ldots, x(n-1,0), \ldots, x(n-1,n-1)]^T \in \mathbb{Z}^{n^2}.$$

Note that $\mathbf{x} = [x(0), \ldots, x(n^2-1)]^T = \text{row } \mathbf{X}$ if and only if $x(ni+j) = x(i,j)$, $i,j = 0, \ldots, n-1$. For $\mathbf{A} \in \mathbb{Z}^{n \times n}$, let

$$\text{circ } \mathbf{A} := \begin{bmatrix} \mathbf{A}_0 & \mathbf{A}_{n-1} & \cdots & \mathbf{A}_1 \\ \mathbf{A}_1 & \mathbf{A}_0 & \cdots & \mathbf{A}_2 \\ \vdots & \vdots & & \vdots \\ \mathbf{A}_{n-1} & \mathbf{A}_{n-2} & \cdots & \mathbf{A}_0 \end{bmatrix} \in \mathbb{Z}^{n^2 \times n^2}$$

denote a circulant block matrix consisting of circulant blocks $\mathbf{A}_i := \text{circ}[a(i,0), \ldots, a(i,n-1)]^T \in \mathbb{Z}^{n \times n}$. Then (3) is equivalent to the special system of n^2 linear equations

$$(\text{circ } \mathbf{A})\, \text{row } \mathbf{X} = \text{row } \mathbf{B}. \tag{4}$$

We see that (3) is uniquely solvable if and only if circ $\mathbf{A}$ is a nonsingular matrix.

Using residue arithmetic and number-theoretic transforms, we treat the above deconvolution problems. For the more general problem, the computation of the exact solution of an integer system of linear equations using residue arithmetic, see [1] and [2].

2. RESIDUE ARITHMETIC

Let $m \in \mathbb{N}$, $m > 1$ be an odd integer. Given any $x \in \mathbb{Z}$, if $x \equiv r \pmod m$ and if $|r| \leqslant (m-1)/2$, then we write $r = /x/_m$ and we say that $/x/_m$ is the *symmetric residue of* $x \in \mathbb{Z}$ *modulo* m [3, p. 113]. For arbitrary $x, y \in \mathbb{Z}$, we have

$$/x \pm y/_m = //x/_m \pm /y/_m/_m,$$

$$/x \cdot y/_m = //x/_m \cdot /y/_m/_m.$$

Further, if $\gcd(x,m) = 1$, then there exists a unique integer x' with $/x\,x'/_m = 1$, $|x'| \leqslant (m-1)/2$. This integer x' is called *multiplicative inverse of* $x \in \mathbb{Z}$ *modulo* m and x' is denoted by

$$\left/\frac{1}{x}\right/_m.$$

The multiplicative inverse modulo m can be computed via the extended Euclidean algorithm [1].

The symmetric residue of an integer vector $\mathbf{x} = [x(0), \ldots, x(n-1)]^T \in \mathbb{Z}^n$ modulo m is defined by

$$/\mathbf{x}/_m := [/x(0)/_m, \ldots, /x(n-1)/_m]^T \in \mathbb{Z}^n.$$

Analogously, we explain the symmetric residue of an integer matrix modulo m. For arbitrary $\mathbf{x} = [x(0), \ldots, x(n-1)]^T \in \mathbb{Z}^n$ and $\mathbf{y} = [y(0), \ldots, y(n-1)]^T \in \mathbb{Z}^n$, we have

$$/\mathbf{x} \pm \mathbf{y}/_m = //\mathbf{x}/_m \pm /\mathbf{y}/_m/_m,$$

$$/\mathbf{x} * \mathbf{y}/_m = //\mathbf{x}/_m * /\mathbf{y}/_m/_m,$$

$$/\mathbf{x} \circ \mathbf{y}/_m = //\mathbf{x}/_m \circ /\mathbf{y}/_m/_m,$$

where $\circ$ signifies the *Hadamard product*

$$\mathbf{x} \circ \mathbf{y} := [x(0)\,y(0), \ldots, x(n-1)\,y(n-1)]^T.$$

Further, if $\gcd(x(j), m) = 1$ for all $j = 0, \ldots, n-1$, then there exists a unique vector $\mathbf{x}' \in \mathbb{Z}^n$ with $/\mathbf{x} \circ \mathbf{x}'/_m = [1, \ldots, 1]^T$, $\mathbf{x}' = /\mathbf{x}'/_m$. We have

$$\mathbf{x}' = \left[\left/\frac{1}{x(0)}\right/_m, \ldots, \left/\frac{1}{x(n-1)}\right/_m\right]^T.$$

This vector $\mathbf{x}'$ is called *Hadamard inverse of* $\mathbf{x} \in \mathbb{Z}^n$ *modulo* m.

If $\mathbf{X} = [x(i,j)]_{i,j=0}^{n-1} \in \mathbb{Z}^{n\times n}$, $\mathbf{Y} = [y(i,j)]_{i,j=0}^{n-1} \in \mathbb{Z}^{n\times n}$ and $\mathbf{x} \in \mathbb{Z}^n$, then it holds

$$/\mathbf{X}\,\mathbf{x}/_m = //\mathbf{X}/_m/\mathbf{x}/_m/_m,$$
$$/\mathbf{X} \pm \mathbf{Y}/_m = //\mathbf{X}/_m \pm /\mathbf{Y}/_m/_m,$$
$$/\mathbf{X}\cdot\mathbf{Y}/_m = //\mathbf{X}/_m\cdot/\mathbf{Y}/_m/_m,$$
$$/\mathbf{X} * \mathbf{Y}/_m = //\mathbf{X}/_m * /\mathbf{Y}/_m/_m,$$
$$/\mathbf{X} \circ \mathbf{Y}/_m = //\mathbf{X}/_m \circ /\mathbf{Y}/_m/_m,$$
$$/\mathbf{X} \otimes \mathbf{Y}/_m = //\mathbf{X}/_m \otimes /\mathbf{Y}/_m/_m,$$

where $\circ$ signifies the *Hadamard product*

$$\mathbf{X} \circ \mathbf{Y} := [x(i,j)\,y(i,j)]_{i,j=0}^{n-1},$$

and where $\otimes$ denotes the Kronecker product. Further, if $\gcd(x(i,j), m) = 1$ for all $i,j = 0,\ldots,n-1$, then there exists a unique matrix $\mathbf{X}' \in \mathbb{Z}^{n\times n}$ with $/\mathbf{X} \circ \mathbf{X}'/_m = [1]_{i,j=0}^{n-1}$, $\mathbf{X}' = /\mathbf{X}'/_m$. We have

$$\mathbf{X}' = \left[\left/\frac{1}{x(i,j)}\right/_m\right]_{i,j=0}^{n-1}.$$

This matrix $\mathbf{X}'$ is called *Hadamard inverse of* $\mathbf{X} \in \mathbb{Z}^{n\times n}$ *modulo* m.

Now we consider a finite number of pairwise relatively prime, odd moduli $m_i \in \mathbb{N}$, $m_i > 1$, $i = 1,\ldots,s$. Very often, these moduli are different odd primes. Let $m = m_1 \ldots m_s$. Using the Chinese Remainder Theorem (see [4]), we can reconstruct uniquely an integer x with $|x| \leqslant (m-1)/2$ from its symmetric residues $x_i := /x/_{m_i}$, $i = 1,\ldots,s$.

Theorem 2.1

Under above assumptions, any $x \in \mathbb{Z}$ with $|x| \leqslant (m-1)/2$ and with given symmetric residues x_i, $i = 1,\ldots,s$ can be expressed uniquely in the form

$$x = [x_1] + [x_1\,x_2]\,m_1 + [x_1\,x_2\,x_3]\,m_1 m_2 + \cdots + [x_1 \ldots x_s]\,m_1 \ldots m_{s-1} \tag{5}$$

with *modular divided differences* $[x_i] := x_i$, $i = 1,\ldots,s$,

$$[x_i x_j] := \left/\frac{[x_j] - [x_i]}{m_i}\right/_{m_j}, \quad 1 \leqslant i < j \leqslant s, \quad [x_{i_1} \ldots x_{i_{r-1}} x_{i_r}] := \left/\frac{[x_{i_1} \ldots x_{i_{r-2}} x_{i_r}] - [x_{i_1} \ldots x_{i_{r-1}}]}{m_{i_{r-1}}}\right/_{m_{i_r}}, \tag{6}$$

where $1 \leqslant i_1 < \ldots < i_r \leqslant s$.

Proof. It is known (see [4]) that every $x \in \mathbb{Z}$ with $|x| \leqslant (m-1)/2$ can be represented uniquely in the form

$$x = x^{(1)} + x^{(2)} m_1 + x^{(3)} m_1 m_2 + \cdots + x^{(s)} m_1 \ldots m_{s-1} \tag{7}$$

with $x^{(i)} \in \mathbb{Z}$, $|x^{(i)}| \leqslant (m_i - 1)/2$, $i = 1,\ldots,s$. By the Chinese Remainder Theorem, the residue-class ring $\mathbb{Z}/m\mathbb{Z}$ and the direct product $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}$ are isomorphic. Hence, $x \in \mathbb{Z}$ with $|x| \leqslant (m-1)/2$ is uniquely determined by its symmetric residues x_i, $i = 1,\ldots,s$.

Now let $x \in \mathbb{Z}$ with $|x| \leqslant (m-1)/2$ be given by its symmetric residues x_i, $i = 1,\ldots,s$. We have to show that $x^{(i)} = [x_1 x_2 \ldots x_i]$, $i = 1,\ldots,s$. We employ induction on s. The case $s = 1$ is trivial. Assume that the assertion is true for $s-1$. Setting

$$y := [x_1] + [x_1\,x_2]\,m_1 + \cdots + [x_1 \ldots x_{s-2}]\,m_1 \ldots m_{s-3} + [x_1 \ldots x_{s-1}]\,m_1 \ldots m_{s-2},$$
$$z := [x_1] + [x_1\,x_2]\,m_1 + \cdots + [x_1 \ldots x_{s-2}]\,m_1 \ldots m_{s-3} + [x_1 \ldots x_{s-2}\,x_s]\,m_1 \ldots m_{s-2}, \tag{8}$$

we have by the induction hypothesis that

$$/y/_{m_i} = x_i, \quad i = 1,\ldots,s-1,$$
$$/z/_{m_i} = x_i, \quad i = 1,\ldots,s-2,s. \tag{9}$$

Then we conclude from (8) and (9) that

$$w := y + \left/ \frac{1}{m_{s-1}} \right/_{m_s} (z - y) m_{s-1}$$
$$= y + \left/ \frac{1}{m_{s-1}} \right/_{m_s} ([x_1 \dots x_{s-2} x_s] - [x_1 \dots x_{s-1}]) m_1 \dots m_{s-1}$$

satisfies $/w/_{m_i} = x_i$, $i = 1, \dots, s-1$. Hence, $w \equiv x \pmod m$ by the Chinese Remainder Theorem. From $|x| \leqslant (m-1)/2$ and (7), we conclude that

$$x = y + \left/ \frac{[x_1 \dots x_{s-2} x_s] - [x_1 \dots x_{s-1}]}{m_{s-1}} \right/_{m_s} m_1 \dots m_{s-1}.$$

By (6)–(8), it follows that $x^{(i)} = [x_1 \dots x_i]$, $i = 1, \dots, s$. This completes the proof. □

It is convenient to exhibit the modular divided differences in the form of a triangular array called a modular divided difference table. This will look for $s = 4$ as follows:

m_1	m_2	m_3	m_4
$[x_1]$	$[x_2]$	$[x_3]$	$[x_4]$
	$[x_1 x_2]$	$[x_1 x_3]$	$[x_1 x_4]$
		$[x_1 x_2 x_3]$	$[x_1 x_2 x_4]$
			$[x_1 x_2 x_3 x_4]$

In this way, we can reconstruct also integer vectors or integer matrices from the corresponding symmetric residues.

Corollary 2.2

Let $m_i \in \mathbb{N}$, $m_i > 1$, $i = 1, \dots, s$, be pairwise relatively prime, odd moduli. Further let $m = m_1 \dots m_s$.

(i) Then any $\mathbf{x} = [x(0), \dots, x(n-1)]^T \in \mathbb{Z}^n$ with $|x(i)| \leqslant (m-1)/2$, $i = 0, \dots, n-1$, and with given $\mathbf{x}_i := /\mathbf{x}/_{m_i}$, $i = 1, \dots, s$, can be represented uniquely in the form

$$\mathbf{x} = [\mathbf{x}_1] + [\mathbf{x}_1 \mathbf{x}_2] m_1 + \cdots + [\mathbf{x}_1 \dots \mathbf{x}_s] m_1 \dots m_{s-1}$$

with $[\mathbf{x}_i] := \mathbf{x}_i$, $i = 1, \dots, s$,

$$[\mathbf{x}_i \mathbf{x}_j] := \left/ \frac{[\mathbf{x}_j] - [\mathbf{x}_i]}{m_i} \right/_{m_j}, \quad 1 \leqslant i < j \leqslant s,$$

$$[\mathbf{x}_{i_1} \dots \mathbf{x}_{i_{r-1}} \mathbf{x}_{i_r}] := \left/ \frac{[\mathbf{x}_{i_1} \dots \mathbf{x}_{i_{r-2}} \mathbf{x}_{i_r}] - [\mathbf{x}_{i_1} \dots \mathbf{x}_{i_{r-1}}]}{m_{i_{r-1}}} \right/_{m_{i_r}},$$

where $1 \leqslant i_1 < \cdots < i_r \leqslant s$.

(ii) Any $\mathbf{X} = [x(i,j)]_{i,j=0}^{n-1} \in \mathbb{Z}^{n \times n}$ with $|x(i,j)| \leqslant (m-1)/2$, $i, j = 0, \dots, n-1$, and with given $\mathbf{X}_i := /\mathbf{X}/_{m_i}$, $i = 1, \dots, s$, can be expressed uniquely in the form

$$\mathbf{X} = [\mathbf{X}_1] + [\mathbf{X}_1 \mathbf{X}_2] m_1 + \cdots + [\mathbf{X}_1 \dots \mathbf{X}_s] m_1 \dots m_{s-1}$$

with $[\mathbf{X}_i] := \mathbf{X}_i$, $i = 1, \dots, s$,

$$[\mathbf{X}_i \mathbf{X}_j] := \left/ \frac{[\mathbf{X}_j] - [\mathbf{X}_i]}{m_i} \right/_{m_j}, \quad 1 \leqslant i < j \leqslant s,$$

$$[\mathbf{X}_{i_1} \dots \mathbf{X}_{i_{r-1}} \mathbf{X}_{i_r}] := \left/ \frac{[\mathbf{X}_{i_1} \dots \mathbf{X}_{i_{r-2}} \mathbf{X}_{i_r}] - [\mathbf{X}_{i_1} \dots \mathbf{X}_{i_{r-1}}]}{m_{i_{r-1}}} \right/_{m_{i_r}},$$

where $1 \leqslant i_1 < \cdots < i_r \leqslant s$.

3. NUMBER-THEORETIC TRANSFORMS

Let $n \in \mathbb{N}$, $n > 2$, and let $m \in \mathbb{N}$, $m > 1$, be an odd modulus in the residue arithmetic. Then $e \in \mathbb{Z}$, $2 \leqslant |e| \leqslant (m-1)/2$, is called a *primitive* n*th root of unity modulo* m, if $e^n \equiv 1 \pmod m$ and

$\gcd(e^k - 1, m) = 1$, $k = 1, \ldots, n-1$. Then one can prove the following result:

Theorem 3.1 [5]

Let $n \in \mathbb{N}$, $n > 2$, and let $m \in \mathbb{N}$, $m > 1$, be an odd integer. A number $e \in \mathbb{Z}$, $2 \leqslant |e| \leqslant (m-1)/2$, is a primitive nth root of unity modulo m if and only if $\Phi_n(e) \equiv 0 \pmod{m}$ and $\gcd(n, m) = 1$, where Φ_n is the nth cyclotomic polynomial.

The concept of a primitive nth root of unity modulo m is fundamental in the following context. Note that the equality of two integer vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$ is defined in the residue arithmetic by $/\mathbf{x}/_m = /\mathbf{y}/_m$. Analogously, the equality of integer matrices is explained in the residue arithmetic. The *one-dimensional number-theoretic transform* (NTT) $\mathcal{F}$ of *length* n with e as primitive nth root of unity modulo m, and its inverse $\mathcal{F}^{-1}$, are defined for $\mathbf{x} \in \mathbb{Z}^n$ by

$$\mathcal{F}\mathbf{x} = \hat{\mathbf{x}} = [\hat{x}(0), \ldots, \hat{x}(n-1)]^{\mathrm{T}},$$

$$\mathcal{F}^{-1}\mathbf{x} = \mathbf{y} = [y(0), \ldots, y(n-1)]^{\mathrm{T}}$$

with

$$\hat{x}(k) := \left/ \sum_{i=0}^{n-1} x(i)\, e^{ik} \right/_m, \quad k = 0, \ldots, n-1,$$

$$y(i) := \left/ \left/ \frac{1}{n} \right/_m \sum_{k=0}^{n-1} x(k)\, e^{-ik} \right/_m, \quad i = 0, \ldots, n-1.$$

Note that there exists such an integer

$$\left/ \frac{1}{n} \right/_m$$

by $\gcd(n, m) = 1$ (see Theorem 3.1). For arbitrary $\mathbf{x} \in \mathbb{Z}^n$, we have $\mathcal{F}^{-1}\mathcal{F}\mathbf{x} = \mathcal{F}\,\mathcal{F}^{-1}\mathbf{x} = /\mathbf{x}/_m$. Introducing the integer matrices $\mathbf{F} = [/e^{ik}/_m]_{i,k=0}^{n-1}$ and

$$\mathbf{F}^{-1} = \left/ \left/ \frac{1}{n} \right/_m [/e^{-ik}/_m]_{i,k=0}^{n-1} \right/_m,$$

we get $\mathcal{F}\mathbf{x} = /\mathbf{F}\mathbf{x}/_m$ and $\mathcal{F}^{-1}\mathbf{x} = /\mathbf{F}^{-1}\mathbf{x}/_m$ for all $\mathbf{x} \in \mathbb{Z}^n$. In the case $n = 2^{t+1}$, $t \in \mathbb{N}$, and $e = 2$, we obtain the so-called *Fermat number transform*. By Theorem 3.1, we can choose as possible moduli $m \in \mathbb{N}$ only divisors >1 of $\Phi_{2^{t+1}}(2) = 2^{2^t} + 1$.

The NTT was introduced in [6] and [7] as a natural generalization of the discrete Fourier transform (DFT) in order to perform fast cyclic convolutions without round-off errors. The NTT possesses properties resembling those of the DFT [8, pp. 211–216], particularly the *cyclic convolution property*

$$\mathcal{F}(\mathbf{x} * \mathbf{y}) = /\hat{\mathbf{x}} \circ \hat{\mathbf{y}}/_m \tag{10}$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$.

Lemma 3.2

Let $\mathbf{x} \in \mathbb{Z}^n$. Then we have

$$/\mathbf{F}(\operatorname{circ} \mathbf{x})\, \mathbf{F}^{-1}/_m = \operatorname{diag} \hat{\mathbf{x}}, \tag{11}$$

$$/\det(\operatorname{circ} \mathbf{x})/_m = \left/ \prod_{k=0}^{n-1} \hat{x}(k) \right/_m. \tag{12}$$

Proof. Let $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$. By (10) and $\mathbf{x} * \mathbf{y} = (\operatorname{circ} \mathbf{x})\, \mathbf{y}$, it follows that

$$\mathcal{F}(\operatorname{circ} \mathbf{x})\, \mathbf{y} = \mathcal{F}(\mathbf{x} * \mathbf{y}) = /\hat{\mathbf{x}} \circ \hat{\mathbf{y}}/_m.$$

Setting $\mathbf{z} := \hat{\mathbf{y}}$, i.e. $\mathcal{F}^{-1}\mathbf{z} = /\mathbf{y}/_m$, this yields

$$\mathcal{F}(\operatorname{circ} \mathbf{x})\, \mathcal{F}^{-1}\mathbf{z} = /\hat{\mathbf{x}} \circ \mathbf{z}/_m = /(\operatorname{diag} \hat{\mathbf{x}})\, \mathbf{z}/_m$$

for all $\mathbf{z} \in \mathbb{Z}^n$. Then we obtain (11). Hence we have for the determinant of a circulant matrix

$$/\det(\operatorname{circ} \mathbf{x})/_m = /\det(\operatorname{diag} \hat{\mathbf{x}})/_m = \left/ \prod_{k=0}^{n-1} \hat{x}(k) \right/_m .$$

This completes the proof. □

From numerical point of view, the following three essential conditions on NTTs are required: (1) the length n has to be large enough and highly factorizable in order to implement fast algorithms (see [8, pp. 85–94, 116–120, and 125–144]); (2) the primitive nth root e of unity modulo m should have a simple binary representation such that the arithmetic modulo m is easy to perform; (3) the modulus m has to be large enough to avoid overflow, but on the other hand small enough such that the machine word length is not exceeded; furthermore, m should have a simple binary representation.

For instance, the *pseudo-Fermat number transform* with $n = 2^{t+1}$, $t \in \mathbb{N}$, $e = 2^q$, $q \in \mathbb{N}$, and $m \in \mathbb{N}$, $m > 1$, $m \mid 2^{q2^t} + 1$, is a compromise between these various conditions. By Theorem 3.1, we can determine all possible moduli $m \in \mathbb{N}$, $m > 1$ for given length $n \in \mathbb{N}$, $n > 2$, and given $e \in \mathbb{Z}$, $|e| \geqslant 2$, such that e is a primitive nth root of unity modulo m (see [5]).

The *two-dimensional number-theoretic transform* $\mathscr{F}_2$ of size $n \times n$ with e as primitive nth root of unity modulo m, and its *inverse* $\mathscr{F}_2^{-1}$ are defined for all $\mathbf{X} = [x(i,j)]_{i,j=0}^{n-1} \in \mathbb{Z}^{n \times n}$ by

$$\mathscr{F}_2 \mathbf{X} = \hat{\mathbf{X}} := /\mathbf{F}\mathbf{X}\mathbf{F}/_m ,$$

$$\mathscr{F}_2^{-1} \mathbf{X} = \mathbf{Y} := /\mathbf{F}^{-1}\mathbf{X}\mathbf{F}^{-1}/_m .$$

More precisely, we have $\hat{\mathbf{X}} = [\hat{x}(k,l)]_{k,l=0}^{n-1} \in \mathbb{Z}^{n \times n}$ and $\mathbf{Y} = [y(i,j)]_{i,j=0}^{n-1} \in \mathbb{Z}^{n \times n}$ with

$$\hat{x}(k,l) := \left/ \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} x(i,j)\, e^{ik+jl} \right/_m ,$$

$$y(i,j) := \left/ \left/ \frac{1}{n^2} \right/_m \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} x(k,l)\, e^{-(ik+jl)} \right/_m .$$

For arbitrary $\mathbf{X} \in \mathbb{Z}^{n \times n}$, we get $\mathscr{F}_2^{-1} \mathscr{F}_2 \mathbf{X} = \mathscr{F}_2 \mathscr{F}_2^{-1} \mathbf{X} = /\mathbf{X}/_m$. Introducing the Kronecker product $\mathbf{F} \otimes \mathbf{F}$, we have the known relation between the two-dimensional NTT of size $n \times n$ and a one-dimensional transform of length n^2

$$\operatorname{row} \hat{\mathbf{X}} = /(\mathbf{F} \otimes \mathbf{F}) \operatorname{row} \mathbf{X}/_m \tag{13}$$

for all $\mathbf{X} \in \mathbb{Z}^{n \times n}$. The two-dimensional NTT has properties resembling those of the two-dimensional DFT, particularly the *cyclic convolution property*

$$/\mathbf{F}(\mathbf{X} * \mathbf{Y})\mathbf{F}/_m = /(\mathbf{F}\mathbf{X}\mathbf{F}) \circ (\mathbf{F}\mathbf{Y}\mathbf{F})/_m = /\hat{\mathbf{X}} \circ \hat{\mathbf{Y}}/_m \tag{14}$$

for all $\mathbf{X}, \mathbf{Y} \in \mathbb{Z}^{n \times n}$.

Lemma 3.3

Let $\mathbf{X} \in \mathbb{Z}^{n \times n}$. Then we have

$$/(\mathbf{F} \otimes \mathbf{F})(\operatorname{circ} \mathbf{X})(\mathbf{F}^{-1} \otimes \mathbf{F}^{-1})/_m = \operatorname{diag}(\operatorname{row} \hat{\mathbf{X}}), \tag{15}$$

$$/\det(\operatorname{circ} \mathbf{X})/_m = \left/ \prod_{k=0}^{n-1} \prod_{l=0}^{n-1} \hat{x}(k,l) \right/_m . \tag{16}$$

Proof. Let $\mathbf{X}, \mathbf{Y} \in \mathbb{Z}^{n \times n}$. By (4) we see that $\operatorname{row}(\mathbf{X} * \mathbf{Y}) = (\operatorname{circ} \mathbf{X}) \operatorname{row} \mathbf{Y}$. Using (13) and (14), we have then

$$/(\mathbf{F} \otimes \mathbf{F})(\operatorname{circ} \mathbf{X}) \operatorname{row} \mathbf{Y}/_m = /(\mathbf{F} \otimes \mathbf{F}) \operatorname{row} (\mathbf{X} * \mathbf{Y})/_m = /\operatorname{row} \mathbf{F}(\mathbf{X} * \mathbf{Y})\mathbf{F}/_m = /(\operatorname{row} \hat{\mathbf{X}}) \circ (\operatorname{row} \hat{\mathbf{Y}})/_m .$$

Setting $\mathbf{Z} := \hat{\mathbf{Y}}$, this yields $\operatorname{row} \mathbf{Z} = /(\mathbf{F} \otimes \mathbf{F}) \operatorname{row} \mathbf{Y}/_m$ by (13). Hence, we obtain by $/\operatorname{row} \mathbf{Y}/_m = /(\mathbf{F}^{-1} \otimes \mathbf{F}^{-1}) \operatorname{row} \mathbf{Z}/_m$ the relation

$$/(\mathbf{F} \otimes \mathbf{F})(\operatorname{circ} \mathbf{X})(\mathbf{F}^{-1} \otimes \mathbf{F}^{-1}) \operatorname{row} \mathbf{Z}/_m = /(\operatorname{row} \hat{\mathbf{X}}) \circ (\operatorname{row} \mathbf{Z})/_m = /(\operatorname{diag}(\operatorname{row} \hat{\mathbf{X}})) \operatorname{row} \mathbf{Z}/_m$$

for all $\mathbf{Z} \in \mathbb{Z}^{n \times n}$. Thus it follows (15). Calculating the determinants on both sides of (15), we get the equation (16). This completes the proof. □

4. ALGORITHM FOR ONE-DIMENSIONAL DECONVOLUTION

Let $n \in \mathbb{N}$, $n > 2$. For given integer vectors $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^n$, we consider the one-dimensional deconvolution problem (1) and (2), respectively. Assume that $\mathbf{A} := \operatorname{circ} \mathbf{a} \in \mathbb{Z}^{n \times n}$ is nonsingular. Let $d := \det \mathbf{A} \neq 0$ denote the determinant of $\mathbf{A}$. By the well-known Hadamard's inequality, it holds

$$|d| \leqslant c_1 := \left(\sum_{k=0}^{n-1} a(k)^2 \right)^{n/2} \tag{17}$$

The formal solution $\mathbf{x} \in \mathbb{Q}^n$ of (1) reads

$$\mathbf{x} := \mathbf{A}^{-1}\mathbf{b} = \frac{1}{d}\mathbf{y} \tag{18}$$

with $\mathbf{y} = [y(0), \ldots, y(n-1)]^{\mathrm{T}} := \mathbf{A}^{\mathrm{adj}}\mathbf{b}$. For $\mathbf{A}^{\mathrm{adj}} := [a^{\mathrm{adj}}(i,j)]_{i,j=0}^{n-1} \in \mathbb{Z}^{n \times n}$, it follows again by Hadamard's inequality that

$$\max_{i,j} |a^{\mathrm{adj}}(i,j)| \leqslant \left(\sum_{k=0}^{n-1} a(k)^2 \right)^{(n-1)/2}$$

Consequently, we obtain that

$$\max_i |y(i)| \leqslant c_2 := \left(\sum_{j=0}^{n-1} |b(j)| \right) \left(\sum_{k=0}^{n-1} a(k)^2 \right)^{(n-1)/2} \tag{19}$$

Applying Theorem 3.1, we choose a finite number of NTTs $\mathscr{F}_i$, $i = 1, \ldots, s$, with $e_i \in \mathbb{Z}$, $|e_i| \geqslant 2$, as primitive nth root of unity modulo $m_i \in \mathbb{N}$, $m_i > 1$. Denote the corresponding transformed vector of arbitrary $\mathbf{w} \in \mathbb{Z}^n$ by $\hat{\mathbf{w}}_i = [\hat{w}_i(0), \ldots, \hat{w}_i(n-1)]^{\mathrm{T}} := \mathscr{F}_i \mathbf{w}$, $i = 1, \ldots, s$. We assume that the moduli m_i, $i = 1, \ldots, s$, are pairwise relatively prime and that $m = m_1 \ldots m_s$ fulfils the condition

$$\max\{c_1, c_2\} \leqslant (m-1)/2. \tag{20}$$

Further we suppose that

$$\gcd(d, m) = 1. \tag{21}$$

By (12) we obtain that

$$d_i := /d/_{m_i} = \left/ \prod_{k=0}^{n-1} \hat{a}_i(k) \right/_{m_i}, \quad i = 1, \ldots, s. \tag{22}$$

Then one can see by (22) that (21) is equivalent to

$$\gcd(\hat{a}_i(j), m_i) = 1, \quad j = 0, \ldots, n-1; \quad i = 1, \ldots, s. \tag{23}$$

From (17) and (20) it follows that $|d| \leqslant (m-1)/2$. Using Theorem 2.1, we get the exact value

$$d = [d_1] + [d_1 d_2]\, m_1 + \cdots + [d_1 \ldots d_s]\, m_1 \ldots m_{s-1} \tag{24}$$

of the determinant of the circulant matrix $\mathbf{A}$.

Applying the NTTs $\mathscr{F}_i$, $i = 1, \ldots, s$, to (2), we obtain by the cyclic convolution property (10) that

$$/\hat{\mathbf{a}}_i \circ \hat{\mathbf{x}}_i/_{m_i} = \hat{\mathbf{b}}_i, \quad i = 1, \ldots, s. \tag{25}$$

By (23) there exist the Hadamard inverses $(\hat{\mathbf{a}}_i)'$ of $\hat{\mathbf{a}}_i$ modulo m_i, $i = 1, \ldots, s$, which can be computed via the extended Euclidean algorithm. Then from (25) it follows that

$$\hat{\mathbf{x}}_i = /(\hat{\mathbf{a}}_i)' \circ \hat{\mathbf{b}}_i/_{m_i}, \quad i = 1, \ldots, s. \tag{26}$$

Using the inverse NTTs $\mathscr{F}_i^{-1}$, $i = 1, \ldots, s$, we obtain

$$/\mathbf{x}/_{m_i} = /\mathbf{F}_i^{-1}\hat{\mathbf{x}}_i/_{m_i}, \quad i = 1, \ldots, s. \tag{27}$$

Then by (18) we know the symmetric residues $\mathbf{y}_i := /\mathbf{y}/_{m_i}$ of $\mathbf{y} = d\mathbf{x} \in \mathbb{Z}^n$ modulo m_i, $i = 1, \ldots, s$. By (19) and (20) it follows from Corollary 2.2 that

$$\mathbf{y} = [\mathbf{y}_1] + [\mathbf{y}_1 \mathbf{y}_2]\, m_1 + \cdots + [\mathbf{y}_1 \ldots \mathbf{y}_s]\, m_1 \ldots m_{s-1}. \tag{28}$$

Finally, by (21) the unique solution of (1) and (2), respectively reads

$$\mathbf{x} = \frac{1}{d}\,\mathbf{y} \in \mathbb{Q}^n.$$

We summarize this deconvolution algorithm to compute the exact solution $\mathbf{x} \in \mathbb{Q}^n$ of (1) and (2), respectively. Under above mentioned assumptions, the *algorithm of one-dimensional deconvolution* can be expressed as follows:

1. Calculate $\hat{\mathbf{a}}_i$, $i = 1, \ldots, s$.
2. Calculate $d_i = /d/_{m_i}$, $i = 1, \ldots, s$ by (22).
3. Determine d by (24). Prove that (21) is fulfilled.
4. Determine the Hadamard inverses $(\hat{\mathbf{a}}_i)'$ of $\hat{\mathbf{a}}_i$ modulo m_i, $i = 1, \ldots, s$, via the extended Euclidean algorithm.
5. Compute $\hat{\mathbf{b}}_i$, $i = 1, \ldots, s$.
6. Compute $\hat{\mathbf{x}}_i$, $i = 1, \ldots, s$ by (26).
7. Form $/\mathbf{x}/_{m_i}$, $i = 1, \ldots, s$ by (27).
8. Calculate $\mathbf{y}_i = /d\mathbf{x}/_{m_i}$, $i = 1, \ldots, s$.
9. Form $\mathbf{y}$ by (28).
10. Set

$$\mathbf{x} = \frac{1}{d}\,\mathbf{y}.$$

Note that all operations of steps 1, 2 and 4–8 can be implemented in parallel manner.

5. DECONVOLUTION ALGORITHM WITH KNOWN DETERMINANT

Recently, in [9] a precise deconvolution algorithm using the Fermat number transform was described. Now we generalize this method. We use the same notations as before.

Let $n \in \mathbb{N}$, $n > 2$, not necessarily a 2-radix. Let us consider the convolution equation (2) under the assumption that $d = \det \mathbf{A} \neq 0$ is known. Further, let $\mathscr{F}$ be a NTT of length n with $e \in \mathbb{Z}$, $2 \leqslant |e| \leqslant (m-1)/2$, as primitive nth root of unity modulo an odd integer $m > 1$. Suppose that $\gcd(d, m) = 1$.

From (2) and (18) we conclude that $\mathbf{a} * \mathbf{y} = d\mathbf{b}$. Using the symmetric m-radix representation of $\mathbf{y} \in \mathbb{Z}^n$,

$$\mathbf{y} = \mathbf{y}^{(0)} + \mathbf{y}^{(1)} m + \cdots + \mathbf{y}^{(t)} m^t$$

with some $t \in \mathbb{N}$ and $\mathbf{y}^{(j)} = /\mathbf{y}^{(j)}/_m \in \mathbb{Z}^n$, $\mathbf{y}^{(t)} \neq \mathbf{o}$, $j = 0, \ldots, t$, we obtain

$$(\mathbf{a} * \mathbf{y}^{(0)}) + (\mathbf{a} * \mathbf{y}^{(1)})\, m + \cdots + (\mathbf{a} * \mathbf{y}^{(t)})\, m^t = d\mathbf{b}. \tag{29}$$

Introducing the remainder vectors $\mathbf{r}^{(0)} := d\mathbf{b} \in \mathbb{Z}^n$, $\mathbf{r}^{(0)} \neq \mathbf{o}$,

$$\mathbf{r}^{(j+1)} := \frac{1}{m}\,(\mathbf{r}^{(j)} - (\mathbf{a} * \mathbf{y}^{(j)})) \in \mathbb{Z}^n, \quad j = 0, \ldots, t, \tag{30}$$

we observe that $\mathbf{r}^{(t+1)} = \mathbf{o}$. This indicates the end of the calculation.

By (29) and (30), the unknown vectors $\mathbf{y}^{(j)}$, $j = 0, \ldots, t$, can be calculated on line from

$$/\mathbf{a} * \mathbf{y}^{(j)}/_m = /\mathbf{r}^{(j)}/_m, \quad j = 0, \ldots, t. \tag{31}$$

Then we solve (31) step by step by the known procedure

$$\mathbf{y}^{(j)} = /\mathbf{y}^{(j)}/_m = /\mathbf{F}^{-1}((\hat{\mathbf{a}})' \circ \widehat{\mathbf{r}^{(j)}})/_m, \quad j = 0, \ldots, t. \tag{32}$$

Summarizing this method, we obtain following *deconvolution algorithm:*

1. Calculate $\hat{\mathbf{a}}$.
2. Determine the Hadamard inverse $(\hat{\mathbf{a}})'$ of $\hat{\mathbf{a}}$ modulo m via the extended Euclidean algorithm.
3. Set $j = 0$.

4. Calculate $\mathbf{r}^{(j)}$ by (30). If $\mathbf{r}^{(j)} = \mathbf{o}$, then set $t := j - 1$ and go to the step 9. If $\mathbf{r}^{(j)} \neq \mathbf{o}$, then go to the next step.
5. Calculate $\widehat{\mathbf{r}^{(j)}} := /\mathbf{F}\,\mathbf{r}^{(j)}/_m$.
6. Compute $/(\hat{\mathbf{a}})' \circ \widehat{\mathbf{r}^{(j)}}/_m$.
7. Form $\mathbf{y}^{(j)}$ by (32).
8. Increment j and repeat from step 4 on.
9. Set

$$\mathbf{x} = \frac{1}{d}(\mathbf{y}^{(0)} + \mathbf{y}^{(1)}m + \cdots + \mathbf{y}^{(t)}m^t).$$

An essential assumption of this deconvolution algorithm is that the value of d is known. We have seen that d can be calculated via the first three steps of our algorithm described in Section 4. By the following Lemma, we can easily determine the sign of d.

Lemma 5.1 [10, p. 76]

Let $n \in \mathbb{N}$, $n > 2$ and let $\mathbf{a} = [a(0), \ldots, a(n-1)]^T \in \mathbb{Z}^n$. Then we have:
(i) If n is odd, then $d \geqslant 0$ if and only if

$$\sum_{i=0}^{n-1} a(i) \geqslant 0.$$

(ii) If $n = 2r$, $r > 1$, then $d \geqslant 0$ if and only if

$$\left|\sum_{i=1}^{r} a(2i-1)\right| \geqslant \left|\sum_{i=0}^{r-1} a(2i)\right|.$$

If we want to calculate only the value of d, where the sign of d is known, via the first three steps of the algorithm in Section 4, then it is sufficient to choose a finite number of NTTs with pairwise relatively prime moduli $m_i \in \mathbb{N}$, $m_i > 1$, $i = 1, \ldots, s$, such that $m_1 \ldots m_s \geqslant c_1 + 1$ is satisfied instead of (20).

6. ALGORITHM FOR TWO-DIMENSIONAL DECONVOLUTION

Now we extend the first algorithm for the one-dimensional deconvolution problem to the two-dimensional case.

Let $n \in \mathbb{N}$, $n > 2$. For given integer matrices $\mathbf{A}, \mathbf{B} \in \mathbb{Z}^{n \times n}$, we consider the two-dimensional deconvolution problem (3) and (4), respectively. Assume that $\mathbf{C} := \operatorname{circ} \mathbf{A} \in \mathbb{Z}^{n^2 \times n^2}$ is nonsingular, i.e. $d := \det \mathbf{C} \neq 0$. By Hadamard's inequality, it holds

$$|d| \leqslant c_3 := \left(\sum_{k=0}^{n-1}\sum_{l=0}^{n-1} a(k,l)^2\right)^{n^2/2}. \tag{33}$$

The formal solution $\mathbf{x} = \operatorname{row} \mathbf{X} \in \mathbb{Z}^{n^2}$ of (4) reads as follows:

$$\mathbf{x} = \mathbf{C}^{-1}\mathbf{b} = \frac{1}{d}\mathbf{y} \tag{34}$$

with $\mathbf{b} = \operatorname{row} \mathbf{B} \in \mathbb{Z}^{n^2}$ and $\mathbf{y} = [y(0), \ldots, y(n^2-1)]^T := \mathbf{C}^{\mathrm{adj}}\mathbf{b}$. For $\mathbf{C}^{\mathrm{adj}} := [c^{\mathrm{adj}}(i,j)]_{i,j=0}^{n^2-1} \in \mathbb{Z}^{n^2 \times n^2}$, it follows by Hadamard's inequality that

$$\max_{i,j} |c^{\mathrm{adj}}(i,j)| \leqslant \left(\sum_{k=0}^{n-1}\sum_{l=0}^{n-1} a(k,l)^2\right)^{(n^2-1)/2}.$$

Consequently, we obtain that

$$\max_i |y(i)| \leqslant c_4 := \left(\sum_{k=0}^{n-1}\sum_{l=0}^{n-1} |b(k,l)|\right)\left(\sum_{k=0}^{n-1}\sum_{l=0}^{n-1} a(k,l)^2\right)^{(n^2-1)/2}. \tag{35}$$

Now we choose a finite number of NTTs $\mathscr{F}_i$, $i = 1, \ldots, s$, of the length n with $e_i \in \mathbb{Z}$, $2 \leqslant |e_i| \leqslant (m_i - 1)/2$, as primitive nth root of unity modulo an odd integer $m_i > 1$. Denote the corresponding transformed matrix of $\mathbf{W} \in \mathbb{Z}^{n \times n}$ by $\hat{\mathbf{W}}_i = [\hat{w}_i(k,l)]_{k,l=0}^{n-1} := /\mathbf{F}_i \mathbf{W}\,\mathbf{F}_i/_{m_i}$, $i = 1, \ldots, s$.

Assume that $m_i, i = 1, \ldots, s$, are pairwise relatively prime and that $m = m_1 \ldots m_s$ fulfils the condition

$$\max\{c_3, c_4\} \leqslant (m-1)/2. \tag{36}$$

Further, we suppose that

$$\gcd(d, m) = 1. \tag{37}$$

By (16) we obtain that

$$d_i := /d/_{m_i} = \left/ \prod_{k=0}^{n-1} \prod_{l=0}^{n-1} \hat{a}_i(k,l) \right/_{m_i}, \quad i = 1, \ldots, s. \tag{38}$$

One can see by (38) that (37) is equivalent to

$$\gcd(\hat{a}_i(k,l), m_i) = 1, \quad k, l = 0, \ldots, n-1; \quad i = 1, \ldots, s. \tag{39}$$

From (33) and (36) it follows that $|d| \leqslant (m-1)/2$. Using (24), we get the exact value of the determinant of $\mathbf{C} = \operatorname{circ} \mathbf{A}$.

Applying two-dimensional NTTs to (3), we obtain by the cyclic convolution property (14) that

$$/\mathbf{F}_i(\mathbf{A} * \mathbf{X})\,\mathbf{F}_i/_{m_i} = /\hat{\mathbf{A}}_i \circ \hat{\mathbf{X}}_i/_{m_i} = /\hat{\mathbf{B}}_i/_{m_i}, \quad i = 1, \ldots, s. \tag{40}$$

By (39) there exist the Hadamard inverses $(\hat{\mathbf{A}}_i)'$ of $\hat{\mathbf{A}}_i$ modulo m_i, $i = 1, \ldots, s$. Then from (40) we conclude that

$$\hat{\mathbf{X}}_i = /(\hat{\mathbf{A}}_i)' \circ \hat{\mathbf{B}}_i/_{m_i}, \quad i = 1, \ldots, s. \tag{41}$$

Using the two-dimensional inverse NTTs, we obtain

$$/\mathbf{X}/_{m_i} = /\mathbf{F}_i^{-1}\,\hat{\mathbf{X}}_i\,\mathbf{F}_i^{-1}/_{m_i}, \quad i = 1, \ldots, s. \tag{42}$$

Then by (34) we know the symmetric residues $\mathbf{Y}_i := /\mathbf{Y}/_{m_i}$ of $\mathbf{Y} = d\mathbf{X} \in \mathbb{Z}^{n \times n}$ modulo m_i, $i = 1, \ldots, s$. Note that $\mathbf{y} = \operatorname{row} \mathbf{Y} \in \mathbb{Z}^{n^2}$. By (35) and (36) it follows from the Corollary 2.2 that

$$\mathbf{Y} = [\mathbf{Y}_1] + [\mathbf{Y}_1\,\mathbf{Y}_2]\,m_1 + \cdots + [\mathbf{Y}_1 \ldots \mathbf{Y}_s]\,m_1 \ldots m_{s-1}. \tag{43}$$

Finally, by (37) the unique solution of (3) reads

$$\mathbf{X} = \frac{1}{d}\,\mathbf{Y} \in \mathbb{Q}^{n \times n}.$$

We summarize the *algorithm of two-dimensional deconvolution*. Under above mentioned assumptions, this algorithm can be expressed as follows:

1. Calculate $\hat{\mathbf{A}}_i$, $i = 1, \ldots, s$.
2. Calculate $d_i = /d/_{m_i}$, $i = 1, \ldots, s$ by (38).
3. Determine d by (24). Prove that (37) is fulfilled.
4. Determine the Hadamard inverses $(\hat{\mathbf{A}}_i)'$ of $\hat{\mathbf{A}}_i$ modulo m_i, $i = 1, \ldots, s$, via the extended Euclidean algorithm.
5. Compute $\hat{\mathbf{B}}_i$, $i = 1, \ldots, s$.
6. Compute $\hat{\mathbf{X}}_i$, $i = 1, \ldots, s$ by (41).
7. Form $/\mathbf{X}/_{m_i}$, $i = 1, \ldots, s$ by (42).
8. Calculate $\mathbf{Y}_i = /d\mathbf{X}/_{m_i}$, $i = 1, \ldots, s$.
9. Form $\mathbf{Y}$ by (43).
10. Set

$$\mathbf{X} = \frac{1}{d}\,\mathbf{Y}.$$

Finally, we note that the second deconvolution algorithm described in Section 5 can be extended in obvious manner to the two-dimensional case, too.

7. EXAMPLE

We illustrate the above algorithm by a simple example. Let $n = 3$,

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & -1 & 0 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 1 & -1 & -2 \\ 0 & 0 & 1 \\ 2 & 0 & -1 \end{bmatrix}.$$

We want to solve (3) without round-off errors. By (33) and (35) we estimate that $|d| \leqslant 512$ and

$$\max_i |y(i)| \leqslant 2048.$$

Thus we have to choose $m \geqslant 4097$ by (36). Let $\mathscr{F}_1$ be the NTT of the length 3 with $e_1 = 2$ as primitive third root of unity modulo $m_1 = 7$. Then the corresponding integer matrices of this NTT and its inverse read as follows:

$$\mathbf{F}_1 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & -3 \\ 1 & -3 & 2 \end{bmatrix}, \quad \mathbf{F}_1^{-1} = /-2 \begin{bmatrix} 1 & 1 & 1 \\ 1 & -3 & 2 \\ 1 & 2 & -3 \end{bmatrix} /_7.$$

Let $\mathscr{F}_2$ be the NTT of the length 3 with $e_2 = 3$ as primitive third root of unity modulo $m_2 = 13$. Thus we have

$$\mathbf{F}_2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 3 & -4 \\ 1 & -4 & 3 \end{bmatrix}, \quad \mathbf{F}_2^{-1} = /-4 \begin{bmatrix} 1 & 1 & 1 \\ 1 & -4 & 3 \\ 1 & 3 & -4 \end{bmatrix} /_{13}.$$

Further let $\mathscr{F}_3$ be the NTT of the length 3 with $e_3 = 8$ as primitive third root of unity modulo $m_3 = 73$. Hence it holds

$$\mathbf{F}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 8 & -9 \\ 1 & -9 & 8 \end{bmatrix}, \quad \mathbf{F}_3^{-1} = /-24 \begin{bmatrix} 1 & 1 & 1 \\ 1 & -9 & 8 \\ 1 & 8 & -9 \end{bmatrix} /_{73}.$$

Note that m_1, m_2, m_3 are pairwise relatively prime and that $m = m_1 m_2 m_3 = 6643 > 4097$. Then we obtain the exact solution $\mathbf{X} \in \mathbb{Q}^{3\times 3}$ of (3) by following steps:

1. $\hat{\mathbf{A}}_1 = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & -1 \\ -3 & 2 & -3 \end{bmatrix}$, $\hat{\mathbf{A}}_2 = \begin{bmatrix} 1 & 1 & 1 \\ 3 & 3 & -3 \\ -4 & 2 & -4 \end{bmatrix}$, $\hat{\mathbf{A}}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 8 & 8 & -13 \\ -9 & 21 & -9 \end{bmatrix}$.

2. $d_1 = /d/_7 = -2$, $d_2 = /d/_{13} = 6$, $d_3 = /d/_{73} = 19$.

3. $[d_1] = -2$, $[d_1 d_2] = [d_1 d_3] = 3$, $[d_1 d_2 d_3] = 0$, $d = 19$.

4. $(\hat{\mathbf{A}}_1)' = \begin{bmatrix} 1 & 1 & 1 \\ -3 & -3 & -1 \\ 2 & -3 & 2 \end{bmatrix}$, $(\hat{\mathbf{A}}_2)' = \begin{bmatrix} 1 & 1 & 1 \\ -4 & -4 & 4 \\ 3 & 6 & 3 \end{bmatrix}$, $(\hat{\mathbf{A}}_3)' = \begin{bmatrix} 1 & 1 & 1 \\ -9 & -9 & 28 \\ 8 & 7 & 8 \end{bmatrix}$.

5. $\hat{\mathbf{B}}_1 = \begin{bmatrix} 0 & 0 & 2 \\ -3 & -2 & -3 \\ -3 & 3 & 1 \end{bmatrix}$, $\hat{\mathbf{B}}_2 = \begin{bmatrix} 0 & 8 & 1 \\ -3 & -4 & -1 \\ -3 & 1 & -3 \end{bmatrix}$, $\hat{\mathbf{B}}_3 = \begin{bmatrix} 0 & 13 & -4 \\ -3 & -14 & -34 \\ -3 & 34 & 20 \end{bmatrix}$.

6. $\hat{\mathbf{X}}_1 = \begin{bmatrix} 0 & 0 & 2 \\ 2 & -1 & 3 \\ 1 & -2 & 2 \end{bmatrix}$, $\hat{\mathbf{X}}_2 = \begin{bmatrix} 0 & 8 & 1 \\ -3 & -4 & -1 \\ -3 & 1 & -3 \end{bmatrix}$, $\hat{\mathbf{X}}_3 = \begin{bmatrix} 0 & 13 & -4 \\ 27 & -20 & -3 \\ -24 & 19 & 14 \end{bmatrix}$.

7. $$/\mathbf{X}/_7 = \begin{bmatrix} 0 & -1 & 2 \\ 3 & 0 & -2 \\ 0 & 0 & -2 \end{bmatrix}, \quad /\mathbf{X}/_{13} = \begin{bmatrix} -2 & -4 & -6 \\ -5 & -2 & -5 \\ -3 & 5 & -4 \end{bmatrix}, \quad /\mathbf{X}/_{73} = \begin{bmatrix} -30 & 27 & 4 \\ 5 & -30 & 26 \\ 28 & 2 & -32 \end{bmatrix}.$$

8. $$\mathbf{Y}_1 = \begin{bmatrix} 0 & 2 & 3 \\ 1 & 0 & -3 \\ 0 & 0 & -3 \end{bmatrix}, \quad \mathbf{Y}_2 = \begin{bmatrix} 1 & 2 & 3 \\ -4 & 1 & -4 \\ -5 & 4 & 2 \end{bmatrix}, \quad \mathbf{Y}_3 = \begin{bmatrix} 14 & 2 & 3 \\ 22 & 14 & -17 \\ 21 & -35 & -24 \end{bmatrix}.$$

9. $$[\mathbf{Y}_1] = \mathbf{Y}_1, \quad [\mathbf{Y}_1\mathbf{Y}_2] = [\mathbf{Y}_1\mathbf{Y}_3] = \begin{bmatrix} 2 & 0 & 0 \\ 3 & 2 & -2 \\ 3 & -5 & -3 \end{bmatrix}, \quad [\mathbf{Y}_1\mathbf{Y}_2\mathbf{Y}_3] = \mathbf{O}, \quad \mathbf{Y} = \mathbf{Y}_3.$$

10. $$\mathbf{X} = \frac{1}{19}\begin{bmatrix} 14 & 2 & 3 \\ 22 & 14 & -17 \\ 21 & -35 & -24 \end{bmatrix}$$

8. CONCLUSION

The considered deconvolution problems are typical inverse problems. It is known that using the DFT, the solution of a deconvolution problem is very sensitive to round-off errors.

The described deconvolution algorithms using residue arithmetic and NTTs eliminate the influence of round-off errors and yield the exact solution of the one- and two-dimensional deconvolution problem, respectively. These algorithms are new. The first algorithm works mainly parallel and affords parallel processor architectures for real time applications. Further, the exact value of the determinant of a circulant integer matrix can be computed by the first steps of this algorithm.

By generalization of a recent result [9], we obtain the second deconvolution algorithm, which works on line. Unlike [9], we show that it is not necessary to consider only 2-radix lengths and Fermat number transforms. Furthermore, we improve known results concerning the Chinese Remainder Theorem by introduction of new modular divided differences.

REFERENCES

1. J. A. Howell, Exact solution of linear equations using residue arithmetic. Algorithm 406. *Commun. ACM* **14,** 180–184 (1971).
2. S. Cabay and T. P. L. Lam, Algorithm 522 ESOLVE, Congruence techniques for the exact solution of integer systems of linear equations. *ACM Trans. math. Software* **3,** 404–410 (1977).
3. N. S. Szabó and R. I. Tanaka, *Residue Arithmetic and Its Applications to Computer Technology*. McGraw-Hill, New York (1967).
4. J. A. Howell and R. T. Gregory, An algorithm for solving linear algebraic equations using residue arithmetic. I, II. *BIT* **9,** 200–224, 324–337 (1969).
5. R. Creutzburg and M. Tasche, Number-theoretic transforms of prescribed length. *Math. Comput.* **47,** 693–701 (1986).
6. P. J. Nicholson, Algebraic theory of finite Fourier transforms. *J. Comput. System Sci.* **5,** 524–547 (1971).
7. J. M. Pollard, The fast Fourier transform in a finite field. *Math. Comput.* **25,** 365–374 (1971).
8. H. J. Nussbaumer, *Fast Fourier Transform and Convolution Algorithms*. Springer, Berlin (1981).
9. M. Morháč, Precise deconvolution using the Fermat number transform. *Comput. Math. Applic.* **12A,** 319–329 (1986).
10. P. J. Davis, *Circulant Matrices*. Wiley, New York (1979).