Robust Multidimentional Chinese Remainder Theorem for Integer Vector Reconstruction

Li Xiao, Haiye Huo, and Xiang-Gen Xia, *Fellow, IEEE*

***Abstract*—The problem of robustly reconstructing an integer vector from its erroneous remainders appears in many applications in the field of multidimensional (MD) signal processing. To address this problem, a robust MD Chinese remainder theorem (CRT) was recently proposed for a special class of moduli, where the remaining integer matrices left-divided by a greatest common left divisor (gcld) of all the moduli are pairwise commutative and coprime. The strict constraint on the moduli limits the usefulness of the robust MD-CRT in practice. In this paper, we investigate the robust MD-CRT for a general set of moduli. We first introduce a necessary and sufficient condition on the difference between paired remainder errors, followed by a simple sufficient condition on the remainder error bound, for the robust MD-CRT for general moduli, where the conditions are associated with (the minimum distances of) these lattices generated by gcld's of paired moduli, and a closed-form reconstruction algorithm is presented. We then generalize the above results of the robust MD-CRT from integer vectors/matrices to real ones. Finally, we validate the robust MD-CRT for general moduli by employing numerical simulations, and apply it to MD sinusoidal frequency estimation based on multiple sub-Nyquist samplers.**

***Index Terms*—Chinese remainder theorem (CRT), integer vectors/matrices, multidimensional frequency estimation, remainder errors, robustness.**

I. Introduction

The Chinese remainder theorem (CRT) [1] is known to offer a solution to a system of linear congruence equations, namely, reconstructing a larger nonnegative integer from its remainders modulo several smaller positive integers (called moduli). It has a broad range of applications in many areas, such as computer arithmetic, digital signal processing, and cryptography [1], [2], [3]. Nevertheless, the CRT reconstruction is extremely susceptible to errors in the remainders, which means that a very small error in any remainder might yield a large reconstruction error in the large integer of interest. This may cause failures in applications of the CRT, considering that the detected remainders are often erroneous due to environmental noise contamination. As such, during the past decades, the problem of robust reconstructions from the erroneous remainders has been continuously investigated, where "robustness" means that the reconstruction error could be bounded by the remainder error bound [4], [5], [6], [7], [8], [9], [10]. More specifically, for addressing this robust remaindering problem, a robust CRT has been introduced, of which the basic idea is to accurately determine all the quotients (called folding numbers) of the large integer divided by the moduli. An extensive review of the robust CRT and its various generalizations is presented in [11]. To distinguish from the robust multidimensional (MD) CRT for integer vector reconstruction studied in this paper, we refer to the robust CRT for integer reconstruction as the robust 1-D CRT, which has been found to have potential applications to sinusoidal frequency estimation with sub-Nyquist samplings and phase unwrapping for radar interferometry [12], [13], [14], [15], [16], [17], grid cell neural coding [18], signal reconstruction via multi-channel modulo samplers [19], and wireless sensor networks with fault tolerance [20], [21], [22].

Considering that signals found in modern applications often have a multidimensional structure, e.g., multiple input multiple output (MIMO) communication and MIMO radar systems, we recently studied exact and robust reconstructions of an integer vector from its (erroneous) remainders modulo several moduli in [23], where the moduli are nonsingular integer matrices and the remainders are integer vectors. Concretely, we first derived the MD-CRT for a general set of moduli, via which an integer vector can be accurately reconstructed from the remainders, if this integer vector is within the fundamental parallelepiped of the lattice that is generated by a least common right multiple of all the moduli. We then introduced the robust MD-CRT for a special class of moduli, where these remaining integer matrices

Manuscript received 22 November 2023; revised 2 April 2024; accepted 29 April 2024. Date of publication 3 May 2024; date of current version 14 May 2024. The work of Li Xiao was supported in part by the National Natural Science Foundation of China under Grant 62202442 and in part by the Anhui Provincial Natural Science Foundation under Grant 2208085QF188. The work of Haiye Huo was supported in part by the National Natural Science Foundation of China under Grant 12261059 and Grant 11801256 and in part by the Jiangxi Provincial Natural Science Foundation under Grant 20224BAB211001. The work of Xiang-Gen Xia was supported by the National Science Foundation (NSF) under Grant CCF-2246917. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Pascal Vallet. *(Corresponding author: Haiye Huo.)*

Li Xiao is with the MoE Key Laboratory of Brain-Inspired Intelligent Perception and Cognition, University of Science and Technology of China, Hefei 230052, China, and also with the Institute of Artificial Intelligence, Hefei Comprehensive National Science Center, Hefei 230088, China (e-mail: xiaoli11@ustc.edu.cn).

Haiye Huo is with the School of Mathematics and Computer Sciences, Nanchang University, Nanchang 330031, China (e-mail: hyhuo@ncu.edu.cn).

Xiang-Gen Xia is with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: xxia@ee.udel.edu).

Digital Object Identifier 10.1109/TSP.2024.3395898

left-divided by a greatest common left divisor of all the moduli are pairwise commutative and coprime. In this special case, the robust MD-CRT basically states that an integer vector within a certain reconstruction range can be robustly reconstructed from its erroneous remainders and the moduli, if the remainder error bound is smaller than a quarter of the minimum distance of the lattice that is generated by a greatest common left divisor (gcld) of all the moduli. One can obviously see that there is the commutativity and coprimeness constraint on the moduli for the robust MD-CRT in [23], which is very strict and therefore might limit the applications of the robust MD-CRT in practice. As an example, when applying the robust MD-CRT for animal 2-D location estimate in grid cell neural coding [18], different grid cell populations have different lattice periods (actually the moduli), which are intrinsical and in general do not satisfy the commutativity and coprimeness constraint mentioned above so that the robust MD-CRT in [23] cannot work here.

In this paper, we propose the robust MD-CRT for a general set of moduli on which the undesirable matrix commutativity and coprimeness constraint we imposed in [23] is no longer required. Instead of accurately determining the folding vectors $\{\mathbf{n}_i\}_{i=1}^L$ (namely, the quotients of an integer vector of interest $\mathbf{m}$ left-divided by moduli $\{\mathbf{M}_i\}_{i=1}^L$) in [23], we attempt to accurately determine $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^L$, and thereby obtain a robust reconstruction $\tilde{\mathbf{m}}$ of $\mathbf{m}$ by averaging the reconstructions calculated from the determined folding vectors, i.e., $\tilde{\mathbf{m}} = \frac{1}{L}\sum_{i=1}^L (\mathbf{M}_i\mathbf{n}_i + \tilde{\mathbf{r}}_i)$, in this paper, where $\{\tilde{\mathbf{r}}_i\}_{i=1}^L$ denote the erroneous remainders. Of note, this strategy actually facilitates the robust MD-CRT for a general set of moduli by avoiding the difficulties brought about by the non-commutativity of matrix multiplication. More precisely, we first present a necessary and sufficient condition on the difference between paired remainder errors, as well as a simple sufficient condition on the remainder error bound, for the robust MD-CRT for general moduli, where the conditions are related with (the minimum distances of) the lattices that are generated by greatest common left divisors of paired moduli. At the same time, a closed-form reconstruction algorithm for the derived robust MD-CRT is proposed as well. In addition, we generalize the above results of the robust MD-CRT from integer vector/matrix cases to real-valued vector/matrix cases. We finally validate the robust MD-CRT for general moduli by conducting some numerical simulations, and apply it to frequency estimation for a complex MD sinusoidal signal undersampled with multiple sub-Nyquist samplers. It demonstrates that the use of the robust MD-CRT with L properly chosen moduli $\{\mathbf{M}_i\}_{i=1}^L$ (whose inverses are referred to as sub-Nyquist sampling matrices with sampling densities $\{|\det(\mathbf{M}_i)|\}_{i=1}^L$) can result in significant sampling density reduction over the Nyquist sampling density for MD sinusoidal frequency estimation.

The rest of this paper is organized as follows. We introduce the preliminary knowledge associated with integer vectors and integer matrices in Section II, as well as our previously derived (robust) MD-CRT in Section III where the robust MD-CRT is limited to a special class of moduli. In Section IV, we propose the robust MD-CRT for a general set of moduli, together with its closed-form reconstruction algorithm. We further generalize the robust MD-CRT from integer vectors/matrices to real ones in Section V. We illustrate simulation results of the robust MD-CRT and its application to MD sinusoidal frequency estimation with multiple sub-Nyquist samplers in noise in Section VI. We conclude this paper in Section VII.

Notations: We utilize capital and lowercase boldfaced letters to denote matrices and vectors, respectively. Let $A(i, j)$ be the (i, j)-th element of a matrix $\mathbf{A}$, and $a(i)$ be the i-th element of a vector $\mathbf{a}$. Let $\mathbf{A}^T$, $\mathbf{A}^{-1}$, $\mathbf{A}^{-T}$, and $\det(\mathbf{A})$ denote the transpose, inverse, inverse transpose, and determinant of $\mathbf{A}$, respectively. We represent by $\operatorname{diag}(a_1, a_2, \cdots, a_D)$ the diagonal matrix with a scalar a_i being the i-th diagonal element. Let $\mathbb{R}$ and $\mathbb{Z}$ denote the sets of reals and integers, respectively. For a D-dimensional real vector $\mathbf{a} \in \mathbb{R}^D$, $\mathbf{a} \in [c, d)^D$ says that every element of $\mathbf{a}$ is within the range of $[c, d)$ and $c, d \in \mathbb{R}$. Let $\mathbf{I}$ and $\mathbf{0}$ respectively be the identity matrix and the all-zero vector/matrix (their sizes are determined from the context). The symbol $\lfloor\cdot\rfloor$ denotes the floor operation, and it is implemented element-wisely if acting on one vector. We let $\operatorname{adj}(\mathbf{M})$ stand for the adjugate of a square matrix $\mathbf{M}$. According to the definition, one can see that $\operatorname{adj}(\mathbf{M})$ is an integer matrix, if $\mathbf{M}$ is an integer matrix. Throughout this paper, all matrices are square matrices, unless otherwise stated.

II. Preliminaries

To make this paper self-contained, t his section reviews some of formal definitions and basic properties pertaining to lattices, integer vectors, and integer matrices [23], [24], [25], [26], [27].

1) *Lattice*: Given a $D \times D$ nonsingular matrix $\mathbf{M} \in \mathbb{R}^{D\times D}$, a lattice generated by $\mathbf{M}$ is defined as

$$\mathcal{L}(\mathbf{M}) = \left\{\mathbf{Mn} \mid \mathbf{n} \in \mathbb{Z}^D\right\}. \tag{1}$$

2) *The shortest vector problem (SVP) on lattice*: For a lattice $\mathcal{L}(\mathbf{M})$ that is generated by a nonsingular matrix $\mathbf{M} \in \mathbb{R}^{D\times D}$, its minimum distance, denoted as $\lambda_{\mathcal{L}(\mathbf{M})}$, is defined as the smallest distance between any two distinct lattice points, i.e.,

$$\lambda_{\mathcal{L}(\mathbf{M})} = \min_{\substack{\mathbf{w},\ \mathbf{v}\in\mathcal{L}(\mathbf{M}),\\ \mathbf{w}\neq\mathbf{v}}} \|\mathbf{w} - \mathbf{v}\|. \tag{2}$$

As we know, a lattice is closed under addition and subtraction. The minimum distance of $\mathcal{L}(\mathbf{M})$ is therefore equal to the length (magnitude) of the shortest non-zero lattice point, i.e., $\lambda_{\mathcal{L}(\mathbf{M})} = \min_{\mathbf{v}\in\mathcal{L}(\mathbf{M})\setminus\{\mathbf{0}\}} \|\mathbf{v}\|$.

3) *The closest vector problem (CVP) on lattice*: For a lattice $\mathcal{L}(\mathbf{M})$ that is generated by a nonsingular matrix $\mathbf{M} \in \mathbb{R}^{D\times D}$, the closest lattice point in $\mathcal{L}(\mathbf{M})$ to a given arbitrary point $\mathbf{w} \in \mathbb{R}^D$ is defined as

$$\mathbf{p} = \arg\min_{\mathbf{v}\in\mathcal{L}(\mathbf{M})} \|\mathbf{v} - \mathbf{w}\|. \tag{3}$$

Remark: There have been many algorithms for handling the SVP and CVP problems in the literature (see, e.g., [28], [29]). Here, we only discuss some classical algorithms and the complexity of exactly solving the CVP. For example, a deterministic algorithm for exactly solving the CVP was developed in [28], which runs in $\tilde{O}(2^{2D})$ time and needs $\tilde{O}(2^D)$ space. In [30], this was improved to achieve a $2^{D+o(D)}$-time and space randomized algorithm. We note that the distance above in (2) and (3) can be measured by an arbitrary vector norm, such as the ℓ_2 norm $\|\mathbf{v}\|_2 = \sqrt{\sum_i |v(i)|^2}$, the ℓ_1 norm $\|\mathbf{v}\|_1 = \sum_i |v(i)|$, and the ℓ_∞ norm $\|\mathbf{v}\|_\infty = \max_i |v(i)|$. In this paper, the SVP and CVP problems are identified as the integer quadratic programming problems, and we can solve them (i.e., (2) and (3)) utilizing enumeration [31] and MOSEK with CVX [32], respectively.

4) *Notation* $\mathcal{N}(\mathbf{M})$: Given a $D \times D$ nonsingular integer matrix $\mathbf{M} \in \mathbb{Z}^{D\times D}$, the notation $\mathcal{N}(\mathbf{M})$ is defined as

$$\mathcal{N}(\mathbf{M}) = \left\{\mathbf{k} \mid \mathbf{k} = \mathbf{M}\mathbf{x}, \mathbf{x} \in [0,1)^D \text{ and } \mathbf{k} \in \mathbb{Z}^D\right\}. \quad (4)$$

The number of elements in $\mathcal{N}(\mathbf{M})$ is equal to $|\det(\mathbf{M})|$.

5) *Division representation for integer vectors*: Given a $D \times D$ nonsingular integer matrix $\mathbf{M} \in \mathbb{Z}^{D\times D}$, any integer vector $\mathbf{m} \in \mathbb{Z}^D$ can be uniquely represented as $\mathbf{m} = \mathbf{M}\mathbf{n} + \mathbf{r}$ with $\mathbf{r} \in \mathcal{N}(\mathbf{M})$ and $\mathbf{n} \in \mathbb{Z}^D$. For modular representation, it is denoted as

$$\mathbf{m} \equiv \mathbf{r} \mod \mathbf{M}, \quad (5)$$

where $\mathbf{M}$ is a modulus, and $\mathbf{n}$ and $\mathbf{r}$ are the folding vector and remainder of $\mathbf{m}$ with respect to $\mathbf{M}$, respectively.

Remark: The folding vector and the remainder are computed as $\mathbf{n} = \lfloor \mathbf{M}^{-1}\mathbf{m} \rfloor$ and $\mathbf{r} = \mathbf{m} - \mathbf{M}\lfloor \mathbf{M}^{-1}\mathbf{m} \rfloor$. As $\mathbf{M}^{-1}$ is generally a matrix with rational elements, $\lfloor \mathbf{M}^{-1}\mathbf{m} \rfloor$ may suffer from round-off error owing to finite precision on computers, an alternative for computing $\mathbf{r}$ is given by, [26],

$$\mathbf{r} = \mathbf{M}\left(\operatorname{adj}(\mathbf{M})\mathbf{m} \mod \det(\mathbf{M})\right)/\det(\mathbf{M}), \quad (6)$$

in which the operation "mod" means that $\operatorname{adj}(\mathbf{M})\mathbf{m}$ is element-wisely modulo $\det(\mathbf{M})$. This approach is not subject to round-off error, because all arithmetic operations in (6) are performed on integers.

6) *Unimodular matrix*: A square matrix $\mathbf{U}$ is unimodular if it is an integer matrix with $|\det(\mathbf{U})| = 1$. For a unimodular matrix $\mathbf{U}$, its inverse $\mathbf{U}^{-1}$ is unimodular, due to $\mathbf{U}^{-1} = \operatorname{adj}(\mathbf{U})/\det(\mathbf{U})$.

7) *Divisor*: An integer matrix $\mathbf{A}$ is a left divisor of an integer matrix $\mathbf{M}$ if $\mathbf{A}^{-1}\mathbf{M}$ is an integer matrix. If $\mathbf{A}$ is a left divisor of each of all $L \geq 2$ integer matrices $\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L$, we call $\mathbf{A}$ a common left divisor (cld) of $\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L$. Moreover, if any other cld is a left divisor of $\mathbf{A}$, then $\mathbf{A}$ is a greatest common left divisor (gcld) of $\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L$. One can readily see that a gcld has the largest absolute determinant among all cld's, and it is unique (up to post-multiplication by a unimodular matrix).

8) *Multiple*: A nonsingular integer matrix $\mathbf{A}$ is a left multiple of an integer matrix $\mathbf{M}$, if there is a nonsingular integer matrix $\mathbf{P}$ such that $\mathbf{A} = \mathbf{P}\mathbf{M}$. We call $\mathbf{A}$ a common left multiple (clm) of $\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L$, if $\mathbf{A}$ is a left multiple of each of all $L \geq 2$ integer matrices $\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L$. In particular, $\mathbf{A}$ is termed a least common left multiple (lclm) of $\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L$, if any other clm is a left multiple of $\mathbf{A}$. Apparently, an lclm has the smallest absolute determinant among all clm's, and it is unique (up to pre-multiplication by a unimodular matrix).

Remark: Similar to 5) and 6) above, we can define right divisor/multiple, common right divisor/multiple (crd/crm), greatest common right divisor (gcrd), and least common right multiple (lcrm), respectively. Both divisors and multiples are supposed to be nonsingular integer matrices throughout this paper.

9) *Coprimeness*: A pair of integer matrices $\mathbf{M}$ and $\mathbf{N}$ are said to be right (left) coprime, if their gcrd (gcld) is a unimodular matrix. If $\mathbf{M}$ and $\mathbf{N}$ are commutative, i.e., $\mathbf{MN} = \mathbf{NM}$, the right coprimeness and left coprimeness imply each other, and so we use the one word "coprimeness". If $\mathbf{M}$ and $\mathbf{N}$ are commutative and coprime, $\mathbf{MN}$ is both an lcrm and an lclm, and so we use the one word "lcm".

10) *Bezout's theorem* [23], [27]: Let $\mathbf{L} \in \mathbb{Z}^{D\times D}$ stand for a gcld of two integer matrices $\mathbf{M}$ and $\mathbf{N} \in \mathbb{Z}^{D\times D}$. There exist integer matrices $\mathbf{P}$ and $\mathbf{Q} \in \mathbb{Z}^{D\times D}$ satisfying

$$\mathbf{MP} + \mathbf{NQ} = \mathbf{L}. \quad (7)$$

Of note, how to compute the accompanying matrices $\mathbf{P}$ and $\mathbf{Q}$ will be presented in 12) below. Similarly, if $\mathbf{L} \in \mathbb{Z}^{D\times D}$ is a gcrd of $\mathbf{M}$ and $\mathbf{N}$, there exist integer matrices $\mathbf{P}$ and $\mathbf{Q}$ satisfying $\mathbf{PM} + \mathbf{QN} = \mathbf{L}$.

11) *The Smith form* [25], [27]: A rank-γ integer matrix $\mathbf{M} \in \mathbb{Z}^{D\times K}$ can be factorized as

$$\mathbf{UMV} = \begin{cases} \begin{pmatrix} \mathbf{\Lambda} & \mathbf{0} \end{pmatrix}, & \text{if } K > D, \\ \mathbf{\Lambda}, & \text{if } K = D, \\ \begin{pmatrix} \mathbf{\Lambda} \\ \mathbf{0} \end{pmatrix}, & \text{if } K < D, \end{cases} \quad (8)$$

where $\mathbf{U} \in \mathbb{Z}^{D\times D}$ and $\mathbf{V} \in \mathbb{Z}^{K\times K}$ are unimodular matrices, and $\mathbf{\Lambda} \triangleq \operatorname{diag}(\delta_1, \delta_2, \cdots, \delta_\gamma, 0, \cdots, 0)$ is a $\min(K,D) \times \min(K,D)$ diagonal integer matrix. Assume that $\delta_1, \delta_2, \cdots, \delta_\gamma$ are positive and δ_i divides δ_{i+1} for each $1 \leq i \leq \gamma - 1$, and then $\mathbf{\Lambda}$ is unique for the given matrix $\mathbf{M}$, while $\mathbf{U}$ and $\mathbf{V}$ are in general not. In addition, $\delta_1, \delta_2, \cdots, \delta_\gamma$ are termed the invariant factors and can be obtained by $\delta_i = d_i/d_{i-1}$ for $1 \leq i \leq \gamma$, where d_i is the gcd of all $i \times i$ determinantal minors of $\mathbf{M}$ and $d_0 = 1$.

12) *Calculation of gcld*: To compute a gcld of two nonsingular integer matrices $\mathbf{M}$ and $\mathbf{N} \in \mathbb{Z}^{D\times D}$, we let $\mathbf{H} = \begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix} \in \mathbb{Z}^{D\times 2D}$ and obtain the Smith form $\mathbf{U}\begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix}\mathbf{V} = \begin{pmatrix} \mathbf{\Lambda} & \mathbf{0} \end{pmatrix}$, where $\mathbf{U} \in \mathbb{Z}^{D\times D}$ and $\mathbf{V} \in \mathbb{Z}^{2D\times 2D}$ are unimodular matrices, and $\mathbf{\Lambda} \in \mathbb{Z}^{D\times D}$ is a diagonal integer matrix (which is also nonsingular due to $\operatorname{rank}(\mathbf{H}) = D$). After simple computations, we obtain $\begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix} = \begin{pmatrix} \mathbf{L} & \mathbf{0} \end{pmatrix}\mathbf{V}^{-1}$, where $\mathbf{L} = \mathbf{U}^{-1}\mathbf{\Lambda}$. Since $\mathbf{U}^{-1}$ is unimodular, $\mathbf{L}$ is a nonsingular integer matrix, i.e., $\mathbf{L} \in \mathbb{Z}^{D\times D}$. Since $\mathbf{V}^{-1}$ is unimodular, we can partition $\mathbf{V}^{-1}$ into four $D \times D$ integer matrix blocks $\mathbf{K}_{ij} \in \mathbb{Z}^{D\times D}$ for $1 \leq i, j \leq 2$, and obtain

$$\begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix} = \begin{pmatrix} \mathbf{L} & \mathbf{0} \end{pmatrix}\begin{pmatrix} \mathbf{K}_{11} & \mathbf{K}_{12} \\ \mathbf{K}_{21} & \mathbf{K}_{22} \end{pmatrix}. \quad (9)$$

We therefore have $\mathbf{M} = \mathbf{L}\mathbf{K}_{11}$ and $\mathbf{N} = \mathbf{L}\mathbf{K}_{12}$. It is proved that such $\mathbf{L}$ is in fact a gcld of $\mathbf{M}$ and $\mathbf{N}$ (see [23] for the proof).

Remark: We then provide a way to compute the accompanying matrices $\mathbf{P}$ and $\mathbf{Q}$ in (7) for the Bezout's theorem. From the Smith form of $\mathbf{H}$ above, we get $\begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix}\mathbf{V} = \begin{pmatrix} \mathbf{L} & \mathbf{0} \end{pmatrix}$. We partition $\mathbf{V}$ into four $D \times D$ integer matrix blocks $\mathbf{V}_{ij} \in \mathbb{Z}^{D\times D}$ for $1 \leq i, j \leq 2$, and have

$$\begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix}\begin{pmatrix} \mathbf{V}_{11} & \mathbf{V}_{12} \\ \mathbf{V}_{21} & \mathbf{V}_{22} \end{pmatrix} = \begin{pmatrix} \mathbf{L} & \mathbf{0} \end{pmatrix}. \quad (10)$$

It implies the Bezout's theorem, expressed by $\mathbf{M}\mathbf{V}_{11}+\mathbf{N}\mathbf{V}_{21}=\mathbf{L}$, i.e., $\mathbf{P}=\mathbf{V}_{11}$ and $\mathbf{Q}=\mathbf{V}_{21}$ in (7).

13) *Calculation of lcrm*: To calculate an lcrm of two nonsingular integer matrices $\mathbf{M}$ and $\mathbf{N}\in\mathbb{Z}^{D\times D}$, we let $\mathbf{H}=\mathbf{M}^{-1}\mathbf{N}$. Because of $\mathbf{M}^{-1}=\text{adj}(\mathbf{M})/\det(\mathbf{M})$, $\mathbf{M}^{-1}$ has all elements being rational numbers, and so does $\mathbf{H}$. Letting d be the lcm of the denominators of all elements in $\mathbf{H}$, we know that $d\mathbf{H}$ is a $D\times D$ nonsingular integer matrix. We compute the Smith form of $d\mathbf{H}$ as $\mathbf{U}d\mathbf{H}\mathbf{V}=\boldsymbol{\Lambda}$, i.e.,

$$\mathbf{M}^{-1}\mathbf{N}=\mathbf{U}^{-1}\text{diag}(\delta_1/d,\delta_2/d,\cdots,\delta_D/d)\mathbf{V}^{-1}, \tag{11}$$

where $\mathbf{U}$ and $\mathbf{V}$ are $D\times D$ unimodular matrices (i.e., $\mathbf{U},\mathbf{V}\in\mathbb{Z}^{D\times D}$), and $\boldsymbol{\Lambda}=\text{diag}(\delta_1,\delta_2,\cdots,\delta_D)\in\mathbb{Z}^{D\times D}$ as derived in (8). All the rational numbers $\delta_1/d,\delta_2/d,\cdots,\delta_D/d$ are represented by their irreducible forms; that is to say, for $1\leq i\leq D$, $\delta_i/d=\alpha_i/\beta_i$ where α_i and β_i are coprime positive integers. Let $\boldsymbol{\Lambda}_\alpha=\text{diag}(\alpha_1,\alpha_2,\cdots,\alpha_D)$ and $\boldsymbol{\Lambda}_\beta=\text{diag}(\beta_1,\beta_2,\cdots,\beta_D)$. Based on (11), we obtain $\mathbf{M}^{-1}\mathbf{N}=\mathbf{U}^{-1}\boldsymbol{\Lambda}_\alpha\boldsymbol{\Lambda}_\beta^{-1}\mathbf{V}^{-1}$. Let $\mathbf{P}=\mathbf{U}^{-1}\boldsymbol{\Lambda}_\alpha$ and $\mathbf{Q}=\mathbf{V}\boldsymbol{\Lambda}_\beta$, which are clearly nonsingular integer matrices and right coprime. We hence have $\mathbf{M}^{-1}\mathbf{N}=\mathbf{P}\mathbf{Q}^{-1}$, i.e., $\mathbf{M}\mathbf{P}=\mathbf{N}\mathbf{Q}$. It is proved that $\mathbf{R}\triangleq\mathbf{M}\mathbf{P}=\mathbf{N}\mathbf{Q}$ is actually an lcrm of $\mathbf{M}$ and $\mathbf{N}$ (see [25] for the proof).

Remark: For $L\geq 3$ nonsingular integer matrices $\{\mathbf{M}_i\}_{i=1}^L$, we can compute an lcrm of $\{\mathbf{M}_i\}_{i=1}^L$ via computing an lcrm of two matrices iteratively, due to the fact that lcrm $(\mathbf{M}_1,\mathbf{M}_2,\cdots,\mathbf{M}_L)=$ lcrm (lcrm $(\mathbf{M}_1,\mathbf{M}_2,\cdots,\mathbf{M}_{L-1})$, $\mathbf{M}_L)$ holds, which has been proved in [23]. Besides, similar to the calculations of gcld and lcrm above, the calculations of gcrd and lclm can be obtained. For more details, we refer the reader to [23], [25].

III. Previous Results on (Robust) MD-CRT

Consider a system of congruences

$$\begin{cases}\mathbf{m}\equiv\mathbf{r}_1 \mod \mathbf{M}_1\\ \mathbf{m}\equiv\mathbf{r}_2 \mod \mathbf{M}_2\\ \quad\vdots\\ \mathbf{m}\equiv\mathbf{r}_L \mod \mathbf{M}_L,\end{cases} \tag{12}$$

where moduli $\{\mathbf{M}_i\}_{i=1}^L\in\mathbb{Z}^{D\times D}$ are nonsingular integer matrices, and $\mathbf{R}\in\mathbb{Z}^{D\times D}$ is anyone of their lcrm's. With respect to (12), let us recall the results about the (robust) MD-CRT we recently proposed in [23] as follows. For simplicity of notation, we will use $\mathbf{r}=\langle\mathbf{m}\rangle_{\mathbf{M}}$ to denote the remainder $\mathbf{r}$ of $\mathbf{m}$ modulo $\mathbf{M}$.

A. MD-CRT

Proposition 1 ([23]): Let moduli $\{\mathbf{M}_i\}_{i=1}^L$ in (12) be arbitrary nonsingular integer matrices. An integer vector $\mathbf{m}\in\mathcal{N}(\mathbf{R})$ can be accurately reconstructed from its remainders $\{\mathbf{r}_i\}_{i=1}^L$.

Notice that a cascaded reconstruction algorithm for the MD-CRT in Proposition 1 is introduced in [23]. For $2\leq i\leq L$, let $\mathbf{R}_i$ be an lcrm of $\{\mathbf{M}_k\}_{k=1}^{i-1}$, $\mathbf{G}_i$ be a gcld of $\mathbf{M}_i$ and $\mathbf{R}_i$, and $\mathbf{P}_i$ and $\mathbf{Q}_i$ be the accompanying matrices in the Bezout's theorem with $\mathbf{R}_i\mathbf{P}_i+\mathbf{M}_i\mathbf{Q}_i=\mathbf{G}_i$. On the basis of 12) and 13) in Sec. II, all these involved matrices can be computed in advance. Here, we briefly summarize the core steps of the cascaded reconstruction algorithm for the MD-CRT.

- A solution (denoted as $\mathbf{m}_1\in\mathcal{N}(\mathbf{R}_3)$) to
$$\begin{cases}\mathbf{m}\equiv\mathbf{r}_1 \mod \mathbf{M}_1\\ \mathbf{m}\equiv\mathbf{r}_2 \mod \mathbf{M}_2\end{cases} \tag{13}$$
is obtained as $\mathbf{m}_1=\left\langle\mathbf{r}_1+\mathbf{M}_1\mathbf{P}_2\ \mathbf{G}_2^{-1}(\mathbf{r}_2-\mathbf{r}_1)\right\rangle_{\mathbf{R}_3}$.
- Based on the cascade architecture of the congruences, we next obtain a solution (denoted as $\mathbf{m}_2\in\mathcal{N}(\mathbf{R}_4)$) to
$$\begin{cases}\mathbf{m}\equiv\mathbf{m}_1 \mod \mathbf{R}_3\\ \mathbf{m}\equiv\mathbf{r}_3 \mod \mathbf{M}_3\end{cases} \tag{14}$$
as $\mathbf{m}_2=\left\langle\mathbf{m}_1+\mathbf{R}_3\mathbf{P}_3\ \mathbf{G}_3^{-1}(\mathbf{r}_3-\mathbf{m}_1)\right\rangle_{\mathbf{R}_4}$.
- Following the above steps, we assemble two congruences at a time, until a solution (denoted as $\mathbf{m}_{L-1}\in\mathcal{N}(\mathbf{R})$) to
$$\begin{cases}\mathbf{m}\equiv\mathbf{m}_{L-2} \mod \mathbf{R}_L\\ \mathbf{m}\equiv\mathbf{r}_L \mod \mathbf{M}_L\end{cases} \tag{15}$$
is calculated as $\mathbf{m}_{L-1}=\big\langle\mathbf{m}_{L-2}+\mathbf{R}_L\mathbf{P}_L\mathbf{G}_L^{-1}(\mathbf{r}_L-\mathbf{m}_{L-2})\rangle_{\mathbf{R}}$. As verified in [23], the lcrm (i.e., $\mathbf{R}$) of $\{\mathbf{M}_i\}_{i=1}^L$ is an lcrm of $\mathbf{R}_L$ and $\mathbf{M}_L$, and $\mathbf{m}_{L-1}$ is a unique solution to (12) from the MD-CRT if $\mathbf{m}\in\mathcal{N}(\mathbf{R})$, i.e., $\mathbf{m}=\mathbf{m}_{L-1}$.

Remark: If the moduli $\{\mathbf{M}_i\}_{i=1}^L\in\mathbb{Z}^{D\times D}$ are pairwise commutative and coprime, it is clear that $\mathbf{R}=\mathbf{M}_1\mathbf{M}_2\cdots\mathbf{M}_L\mathbf{U}\in\mathbb{Z}^{D\times D}$ is an lcrm of all the moduli for any unimodular matrix $\mathbf{U}$, and the MD-CRT in Proposition 1 has a closed-form solution as

$$\mathbf{m}=\left\langle\sum_{i=1}^{L}\mathbf{W}_i\widehat{\mathbf{W}}_i\mathbf{r}_i\right\rangle_{\mathbf{R}}, \tag{16}$$

where $\mathbf{W}_i=\mathbf{M}_1\cdots\mathbf{M}_{i-1}\mathbf{M}_{i+1}\cdots\mathbf{M}_L$, and $\widehat{\mathbf{W}}_i$ is the accompanying matrix in the Bezout's theorem ($\mathbf{W}_i\widehat{\mathbf{W}}_i+\mathbf{M}_i\mathbf{Q}_i=\mathbf{I}$ with $\mathbf{Q}_i\in\mathbb{Z}^{D\times D}$) and can be calculated in advance.

B. Robust MD-CRT for a Special Class of Moduli

In [23], the robust MD-CRT was first proposed for a special class of moduli, i.e., moduli $\{\mathbf{M}_i\}_{i=1}^L$ in (12) are given by

$$\mathbf{M}_i=\mathbf{M}\boldsymbol{\Gamma}_i \text{ for } 1\leq i\leq L, \tag{17}$$

where $\{\boldsymbol{\Gamma}_i\}_{i=1}^L\in\mathbb{Z}^{D\times D}$ are pairwise commutative and coprime, and $\mathbf{M}\in\mathbb{Z}^{D\times D}$. In this special case, $\mathbf{R}=\mathbf{M}\boldsymbol{\Gamma}_1\boldsymbol{\Gamma}_2\cdots\boldsymbol{\Gamma}_L\mathbf{U}$ for any unimodular matrix $\mathbf{U}$ is an lcrm of $\{\mathbf{M}_i\}_{i=1}^L$, and the basic idea of the robust MD-CRT in [23] is to accurately determine the folding vectors $\{\mathbf{n}_i\}_{i=1}^L$ from the erroneous remainders

$$\tilde{\mathbf{r}}_i\triangleq\mathbf{r}_i+\triangle\mathbf{r}_i\in\mathcal{N}(\mathbf{M}_i) \text{ for } 1\leq i\leq L, \tag{18}$$

and afterwards obtain a robust reconstruction of $\mathbf{m}$ as

$$\tilde{\mathbf{m}}=\frac{1}{L}\sum_{i=1}^{L}(\mathbf{M}_i\mathbf{n}_i+\tilde{\mathbf{r}}_i), \tag{19}$$

where $\{\triangle\mathbf{r}_i\}_{i=1}^L\in\mathbb{Z}^D$ are the remainder errors. Define

$$\mathcal{A}_i\triangleq\left\{\mathbf{m}\in\mathbb{Z}^D \mid \lfloor\mathbf{M}_i^{-1}\mathbf{m}\rfloor\in\mathcal{N}(\boldsymbol{\Gamma}_1\cdots\boldsymbol{\Gamma}_{i-1}\boldsymbol{\Gamma}_{i+1}\cdots\boldsymbol{\Gamma}_L\mathbf{U}_i)\right\} \tag{20}$$

for $1 \le i \le L$, where $\{\mathbf{U}_i\}_{i=1}^{L}$ are any unimodular matrices. The robust MD-CRT for this special class of moduli expressed in (17) was obtained in [23], as stated below.

Proposition 2 ([23]): Let moduli $\{\mathbf{M}_i\}_{i=1}^{L}$ in (12) be given by (17). We can accurately determine the folding vectors $\{\mathbf{n}_i\}_{i=1}^{L}$ of an integer vector $\mathbf{m} \in \bigcup_{i=1}^{L} \mathcal{A}_i$ (without loss of generality, we suppose that $\mathbf{m} \in \mathcal{A}_1$) from the erroneous remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^{L}$, if and only if

$$\mathbf{0} = \arg\min_{\mathbf{h} \in \mathcal{L}(\mathbf{M})} \|\mathbf{h} - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\| \text{ for } 2 \le i \le L. \tag{21}$$

Moreover, letting τ be the remainder error bound, i.e., $\|\triangle\mathbf{r}_i\| \le \tau$ for $1 \le i \le L$, a simple sufficient condition is

$$\tau < \frac{\lambda_{\mathcal{L}(\mathbf{M})}}{4}. \tag{22}$$

Once $\{\mathbf{n}_i\}_{i=1}^{L}$ are accurately determined, we can obtain a robust reconstruction $\tilde{\mathbf{m}}$ of $\mathbf{m}$ by (19) such that $\|\tilde{\mathbf{m}} - \mathbf{m}\| \le \tau$.

The necessary and sufficient condition (21) means that the lattice point $\mathbf{0}$ in $\mathcal{L}(\mathbf{M})$ is the only closest lattice point to the difference of the remainder errors $\triangle\mathbf{r}_i$ and $\triangle\mathbf{r}_1$ for every i, $2 \le i \le L$.

Remark: In [23], a closed-form reconstruction algorithm for the robust MD-CRT in Proposition 2 was also provided.

IV. Robust MD-CRT for General Moduli

When moduli do not satisfy the constraint in (17), the results (i.e., Proposition 2 above) and reconstruction algorithm in [23] cannot be directly applied, which might limit the applications of the robust MD-CRT in practice. In this section, we consider the robust MD-CRT for a general set of moduli on which the constraint imposed in [23] is no longer required.

We can equivalently write (12) as

$$\begin{cases} \mathbf{m} = \mathbf{M}_1\mathbf{n}_1 + \mathbf{r}_1 \\ \mathbf{m} = \mathbf{M}_2\mathbf{n}_2 + \mathbf{r}_2 \\ \quad\vdots \\ \mathbf{m} = \mathbf{M}_L\mathbf{n}_L + \mathbf{r}_L, \end{cases} \tag{23}$$

where $\{\mathbf{n}_i\}_{i=1}^{L}$ are the folding vectors. Without loss of generality, letting the first equation in (23) be a reference, we subtract it from the last $L-1$ equations, i.e.,

$$\begin{cases} \mathbf{M}_1\mathbf{n}_1 - \mathbf{M}_2\mathbf{n}_2 = \mathbf{r}_2 - \mathbf{r}_1 \\ \mathbf{M}_1\mathbf{n}_1 - \mathbf{M}_3\mathbf{n}_3 = \mathbf{r}_3 - \mathbf{r}_1 \\ \qquad\qquad\vdots \\ \mathbf{M}_1\mathbf{n}_1 - \mathbf{M}_L\mathbf{n}_L = \mathbf{r}_L - \mathbf{r}_1. \end{cases} \tag{24}$$

Define $\mathbf{M}_{1i} = \text{gcld}(\mathbf{M}_1, \mathbf{M}_i)$, $\mathbf{\Gamma}_{1i} = \mathbf{M}_{1i}^{-1}\mathbf{M}_1$, and $\mathbf{\Gamma}_{i1} = \mathbf{M}_{1i}^{-1}\mathbf{M}_i$ for $2 \le i \le L$. Then, left-multiplying $\mathbf{M}_{1i}^{-1}$ on both sides of the $(i-1)$-th equation in (24) for $2 \le i \le L$, we get

$$\begin{cases} \mathbf{\Gamma}_{12}\mathbf{n}_1 - \mathbf{\Gamma}_{21}\mathbf{n}_2 = \mathbf{M}_{12}^{-1}(\mathbf{r}_2 - \mathbf{r}_1) \\ \mathbf{\Gamma}_{13}\mathbf{n}_1 - \mathbf{\Gamma}_{31}\mathbf{n}_3 = \mathbf{M}_{13}^{-1}(\mathbf{r}_3 - \mathbf{r}_1) \\ \qquad\qquad\vdots \\ \mathbf{\Gamma}_{1L}\mathbf{n}_1 - \mathbf{\Gamma}_{L1}\mathbf{n}_L = \mathbf{M}_{1L}^{-1}(\mathbf{r}_L - \mathbf{r}_1). \end{cases} \tag{25}$$

According to (25), it is easy to know that $\left\{\mathbf{M}_{1i}^{-1}(\mathbf{r}_i - \mathbf{r}_1)\right\}_{i=2}^{L}$ are integer vectors, i.e., for $2 \le i \le L$,

$$\mathbf{r}_i - \mathbf{r}_1 \in \mathcal{L}(\mathbf{M}_{1i}). \tag{26}$$

In the same way as that used in [23], for each $2 \le i \le L$, we estimate $\mathbf{r}_i - \mathbf{r}_1$ from the erroneous remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^{L}$ through finding a closest lattice point $\mathbf{v}_i$ in $\mathcal{L}(\mathbf{M}_{1i})$ to $\tilde{\mathbf{r}}_i - \tilde{\mathbf{r}}_1$, i.e.,

$$\mathbf{v}_i = \arg\min_{\mathbf{v} \in \mathcal{L}(\mathbf{M}_{1i})} \|\mathbf{v} - (\tilde{\mathbf{r}}_i - \tilde{\mathbf{r}}_1)\|. \tag{27}$$

Instead of accurately determining the folding vectors $\{\mathbf{n}_i\}_{i=1}^{L}$ in [23], we intend to accurately determine $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$. Specifically, by taking the modulo-$\mathbf{M}_i$ on both sides of the $(i-1)$-th equation in (24) for $2 \le i \le L$, we have

$$\begin{cases} \mathbf{M}_1\mathbf{n}_1 \equiv \mathbf{0} \mod \mathbf{M}_1 \\ \mathbf{M}_1\mathbf{n}_1 \equiv \mathbf{r}_2 - \mathbf{r}_1 \mod \mathbf{M}_2 \\ \mathbf{M}_1\mathbf{n}_1 \equiv \mathbf{r}_3 - \mathbf{r}_1 \mod \mathbf{M}_3 \\ \qquad\quad\vdots \\ \mathbf{M}_1\mathbf{n}_1 \equiv \mathbf{r}_L - \mathbf{r}_1 \mod \mathbf{M}_L, \end{cases} \tag{28}$$

where the first equation spontaneously holds. Once $\{\mathbf{r}_i - \mathbf{r}_1\}_{i=2}^{L}$ are accurately estimated from (27), i.e., $\mathbf{v}_i = \mathbf{r}_i - \mathbf{r}_1$ for $2 \le i \le L$, we can accurately determine $\mathbf{M}_1\mathbf{n}_1$ from (28) according to the MD-CRT (see Proposition 1 above), provided that $\mathbf{M}_1\mathbf{n}_1 \in \mathcal{N}(\text{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L))$, equivalently written as $\lfloor \mathbf{M}_1^{-1}\mathbf{m} \rfloor \in \mathcal{N}\left(\mathbf{M}_1^{-1}\text{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L)\right)$. Then, $\mathbf{M}_i\mathbf{n}_i$ can be accurately determined as $\mathbf{M}_1\mathbf{n}_1 - \mathbf{v}_i$ for each $2 \le i \le L$. In this end, we derive the following lemma, which can be proved similarly to Theorem 3 in [23].

Lemma 1: Let moduli $\{\mathbf{M}_i\}_{i=1}^{L}$ in (12) be L distinct arbitrary nonsingular integer matrices, and an integer vector $\mathbf{m}$ be within the range

$$\lfloor \mathbf{M}_1^{-1}\mathbf{m} \rfloor \in \mathcal{N}\left(\mathbf{M}_1^{-1}\text{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L)\right). \tag{29}$$

We can accurately determine $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$ from the erroneous remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^{L}$, if and only if

$$\mathbf{0} = \arg\min_{\mathbf{h} \in \mathcal{L}(\mathbf{M}_{1i})} \|\mathbf{h} - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\| \text{ for } 2 \le i \le L. \tag{30}$$

Moreover, letting τ be the remainder error bound, i.e., $\|\triangle\mathbf{r}_i\| \le \tau$ for $1 \le i \le L$, a simple sufficient condition is

$$\tau < \min_{2 \le i \le L} \frac{\lambda_{\mathcal{L}(\mathbf{M}_{1i})}}{4}. \tag{31}$$

After $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$ are accurately determined, a robust reconstruction $\tilde{\mathbf{m}}$ of $\mathbf{m}$ can be obtained by (19) with $\|\tilde{\mathbf{m}} - \mathbf{m}\| \le \tau$.

Proof: From (27), we have, for $2 \le i \le L$,

$$\mathbf{v}_i = \arg\min_{\mathbf{v} \in \mathcal{L}(\mathbf{M}_{1i})} \|\mathbf{v} - (\mathbf{r}_i - \mathbf{r}_1) - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\|. \tag{32}$$

Due to $\mathbf{v} \in \mathcal{L}(\mathbf{M}_{1i})$ and $\mathbf{r}_i - \mathbf{r}_1 \in \mathcal{L}(\mathbf{M}_{1i})$, we have $\mathbf{v} - (\mathbf{r}_i - \mathbf{r}_1) \in \mathcal{L}(\mathbf{M}_{1i})$, and (32) can be equivalently written as

$$\mathbf{h}_i = \arg\min_{\mathbf{h} \in \mathcal{L}(\mathbf{M}_{1i})} \|\mathbf{h} - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\| \tag{33}$$

by taking $\mathbf{h} = \mathbf{v} - (\mathbf{r}_i - \mathbf{r}_1)$.

We first prove the sufficiency of (30). If $\mathbf{h}_i = \mathbf{0}$ for $2 \le i \le L$, we get $\mathbf{v}_i = \mathbf{r}_i - \mathbf{r}_1$, i.e., $\{\mathbf{r}_i - \mathbf{r}_1\}_{i=2}^{L}$ are accurately obtained from (27). Hence, as mentioned before, $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$ can be accurately determined, when (29) satisfies.

We next prove the necessity of (30). Assume that there exists at least one $\mathbf{h}_{k_0}$ that does not satisfy (30), i.e., $\mathbf{h}_{k_0} \neq \mathbf{0}$, for some k_0 with $2 \le k_0 \le L$. Furthermore, due to $\mathbf{v}_{k_0} = \mathbf{h}_{k_0} + (\mathbf{r}_{k_0} - \mathbf{r}_1)$, we know $\mathbf{v}_{k_0} \neq \mathbf{r}_{k_0} - \mathbf{r}_1$. We then have the following two cases.

Case A: $\mathbf{h}_{l_0} \notin \mathcal{L}(\mathbf{M}_{l_0})$ for some l_0 with $2 \le l_0 \le L$ (where l_0 is not necessarily equal to k_0), i.e., $\mathbf{h}_{l_0} \neq \mathbf{M}_{l_0}\mathbf{n}$ for any $\mathbf{n} \in \mathbb{Z}^D$. In this case, it is ready to see that $\mathbf{v}_{l_0}$ and $\mathbf{r}_{l_0} - \mathbf{r}_1$ have different remainders modulo $\mathbf{M}_{l_0}$. Thus, according to the uniqueness of the reconstruction in the MD-CRT, $\mathbf{M}_1\mathbf{n}_1$ cannot be accurately determined from $\{\mathbf{v}_i\}_{i=1}^{L}$ in (28).

Case B: For each $2 \le i \le L$, $\mathbf{h}_i \in \mathcal{L}(\mathbf{M}_i)$, i.e., $\mathbf{h}_i = \mathbf{M}_i\mathbf{n}$ for some $\mathbf{n} \in \mathbb{Z}^D$. In this case, considering that $\mathbf{v}_i = \mathbf{h}_i + (\mathbf{r}_i - \mathbf{r}_1)$, we know that $\mathbf{v}_i$ and $\mathbf{r}_i - \mathbf{r}_1$ have the same remainders modulo $\mathbf{M}_i$ for each $2 \le i \le L$, and therefore, $\mathbf{M}_1\mathbf{n}_1$ can be accurately determined from $\{\mathbf{v}_i\}_{i=1}^{L}$ in (28) using the MD-CRT. However, since $\mathbf{v}_{k_0} \neq \mathbf{r}_{k_0} - \mathbf{r}_1$, the reconstruction of $\mathbf{M}_{k_0}\mathbf{n}_{k_0}$ as $\mathbf{M}_1\mathbf{n}_1 - \mathbf{v}_{k_0}$ is not accurate. This completes the proof of the necessity part.

Ultimately, we prove the simple sufficient condition in (31) for accurately determining $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$. Assume that there exists one $\mathbf{h}_{q_0}$ in (33) satisfying $\mathbf{h}_{q_0} \neq \mathbf{0}$ for some q_0 with $2 \le q_0 \le L$. We have

$$\begin{aligned}\|\mathbf{h}_{q_0}\| &= \|\mathbf{h}_{q_0} - (\triangle\mathbf{r}_{q_0} - \triangle\mathbf{r}_1) - (\mathbf{0} - (\triangle\mathbf{r}_{q_0} - \triangle\mathbf{r}_1))\| \\ &\le \|\mathbf{h}_{q_0} - (\triangle\mathbf{r}_{q_0} - \triangle\mathbf{r}_1)\| + \|\triangle\mathbf{r}_{q_0} - \triangle\mathbf{r}_1\| \\ &\le 2\|\triangle\mathbf{r}_{q_0} - \triangle\mathbf{r}_1\| \\ &\le 4\tau < \lambda_{\mathcal{L}(\mathbf{M}_{1q_0})}\,, \end{aligned} \tag{34}$$

in which the second inequality follows from the fact that $\mathbf{h}_{q_0}$ is one closest lattice point in $\mathcal{L}(\mathbf{M}_{1q_0})$ to $\triangle\mathbf{r}_{q_0} - \triangle\mathbf{r}_1$, and the last inequality holds since $4\tau < \min_{2 \le i \le L} \lambda_{\mathcal{L}(\mathbf{M}_{1i})} \le \lambda_{\mathcal{L}(\mathbf{M}_{1q_0})}$. Hence, it contradicts with $\mathbf{h}_{q_0} \in \mathcal{L}(\mathbf{M}_{1q_0})$, i.e., $\|\mathbf{h}_{q_0}\| \ge \lambda_{\mathcal{L}(\mathbf{M}_{1q_0})}$, which indicates that the condition in (31) implies (30).

Once $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$ are accurately determined, we have a robust reconstruction $\tilde{\mathbf{m}}$ of $\mathbf{m}$ as $\tilde{\mathbf{m}} = \frac{1}{L}\sum_{i=1}^{L}(\mathbf{M}_i\mathbf{n}_i + \tilde{\mathbf{r}}_i)$, i.e.,

$$\begin{aligned}\|\tilde{\mathbf{m}} - \mathbf{m}\| &= \left\| \frac{1}{L}\sum_{i=1}^{L}(\mathbf{M}_i\ \mathbf{n}_i + \mathbf{r}_i + \triangle\mathbf{r}_i) - \mathbf{m} \right\| \\ &= \left\| \frac{1}{L}\sum_{i=1}^{L}\triangle\mathbf{r}_i \right\| \le \frac{1}{L}\sum_{i=1}^{L}\|\triangle\mathbf{r}_i\| \le \tau. \end{aligned} \tag{35}$$

This completes the proof of the lemma. ■

Note that in the aforementioned analysis, we just arbitrarily select the first equation (or the first remainder $\mathbf{r}_1$) in (23) as a reference to be subtracted from the other equations to acquire (24), followed by Lemma 1. In fact, we can further improve the reconstruction robustness of the robust MD-CRT via selecting a proper reference equation in (23). Define $\mathbf{M}_{ij} = \mathrm{gcld}(\mathbf{M}_i, \mathbf{M}_j)$ for $1 \le i \neq j \le L$. Find the index l_0 with $1 \le l_0 \le L$ such that

$$\min_{\substack{1 \le j \le L \\ j \neq l_0}} \lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})} = \max_{1 \le i \le L} \min_{\substack{1 \le j \le L \\ j \neq i}} \lambda_{\mathcal{L}(\mathbf{M}_{ij})}. \tag{36}$$

Algorithm 1

```
According to 12) in Sec. II, calculate $\mathbf{M}_{l_0 j} = \mathrm{gcld}(\mathbf{M}_{l_0}, \mathbf{M}_j)$ for $1 \le j \le L$ and $j \neq l_0$.
According to 13) in Sec. II, calculate $\mathbf{R}_3 = \mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2)$, $\mathbf{R}_4 = \mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3) = \mathrm{lcrm}(\mathbf{R}_3, \mathbf{M}_3)$, $\mathbf{R}_5 = \mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3, \mathbf{M}_4) = \mathrm{lcrm}(\mathbf{R}_4, \mathbf{M}_4)$, $\cdots\cdots$, $\mathbf{R} = \mathbf{R}_{L+1} = \mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L) = \mathrm{lcrm}(\mathbf{R}_L, \mathbf{M}_L)$.
According to 3) in Sec. II, from the given $\{\tilde{\mathbf{r}}_i\}_{i=1}^{L}$, calculate $\mathbf{v}_j$ for $1 \le j \le L$ and $j \neq l_0$ as
    $$\mathbf{v}_j = \arg\min_{\mathbf{v} \in \mathcal{L}(\mathbf{M}_{l_0 j})} \|\mathbf{v} - (\tilde{\mathbf{r}}_j - \tilde{\mathbf{r}}_{l_0})\|. \tag{40}$$
Calculate $\mathbf{M}_{l_0}\tilde{\mathbf{n}}_{l_0} \in \mathcal{N}(\mathbf{R}) = \mathcal{N}(\mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L))$ via the cascaded reconstruction algorithm for the MD-CRT in Proposition 1 from the following system of congruences
    $$\begin{cases} \mathbf{M}_{l_0}\tilde{\mathbf{n}}_{l_0} \equiv \mathbf{v}_1 \mod \mathbf{M}_1 \\ \quad\vdots \\ \mathbf{M}_{l_0}\tilde{\mathbf{n}}_{l_0} \equiv \mathbf{v}_{l_0-1} \mod \mathbf{M}_{l_0-1} \\ \mathbf{M}_{l_0}\tilde{\mathbf{n}}_{l_0} \equiv \mathbf{0} \mod \mathbf{M}_{l_0} \\ \mathbf{M}_{l_0}\tilde{\mathbf{n}}_{l_0} \equiv \mathbf{v}_{l_0+1} \mod \mathbf{M}_{l_0+1} \\ \quad\vdots \\ \mathbf{M}_{l_0}\tilde{\mathbf{n}}_{l_0} \equiv \mathbf{v}_L \mod \mathbf{M}_L. \end{cases} \tag{41}$$
Calculate $\mathbf{M}_j\tilde{\mathbf{n}}_j = \mathbf{M}_{l_0}\tilde{\mathbf{n}}_{l_0} - \mathbf{v}_j$ for $1 \le j \le L$ and $j \neq l_0$. Then, a reconstruction of $\mathbf{m}$ is $\tilde{\mathbf{m}} = \frac{1}{L}\sum_{i=1}^{L}(\mathbf{M}_i\tilde{\mathbf{n}}_i + \tilde{\mathbf{r}}_i)$.
```

By treating the l_0-th remainder as the reference and following the above procedures utilized in Lemma 1, we obtain the result below straightforwardly, along with a closed-form reconstruction algorithm (see **Algorithm 1**) for the robust MD-CRT.

Theorem 1: Let moduli $\{\mathbf{M}_i\}_{i=1}^{L}$ in (12) be L different arbitrary nonsingular integer matrices. Suppose that the index l_0 with $1 \le l_0 \le L$ satisfies (36). For an integer vector $\mathbf{m}$ with

$$\lfloor \mathbf{M}_{l_0}^{-1}\mathbf{m} \rfloor \in \mathcal{N}\left(\mathbf{M}_{l_0}^{-1}\mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L)\right), \tag{37}$$

we can accurately determine $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$ from the erroneous remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^{L}$ by **Algorithm 1**, if and only if

$$\mathbf{0} = \arg\min_{\mathbf{h} \in \mathcal{L}(\mathbf{M}_{l_0 j})} \|\mathbf{h} - (\triangle\mathbf{r}_j - \triangle\mathbf{r}_{l_0})\| \ \text{ for } 1 \le j \le L \text{ and } j \neq l_0. \tag{38}$$

Moreover, letting τ be the remainder error bound, i.e., $\|\triangle\mathbf{r}_i\| \le \tau$ for $1 \le i \le L$, a simple sufficient condition is

$$\tau < \max_{1 \le i \le L} \min_{\substack{1 \le j \le L \\ j \neq i}} \frac{\lambda_{\mathcal{L}(\mathbf{M}_{ij})}}{4} = \min_{\substack{1 \le j \le L \\ j \neq l_0}} \frac{\lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})}}{4}. \tag{39}$$

After $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$ are accurately determined, a robust reconstruction $\tilde{\mathbf{m}}$ of $\mathbf{m}$ can be obtained by (19) with $\|\tilde{\mathbf{m}} - \mathbf{m}\| \le \tau$.

Let us briefly analyze the complexity of **Algorithm 1**. From 12) and 13) in Sec. II, each of the computations of gcld and lcrm needs the Smith form once. To solve (41) via the cascaded reconstruction algorithm for the MD-CRT, one can readily see from (13)-(15) that it requires the Smith form $2L - 2$ times, since we have to calculate $\mathbf{R}_3, \mathbf{R}_4, \cdots, \mathbf{R}_L, \mathbf{R}$ (i.e., $L - 1$ lcrm's) and $\mathbf{G}_2, \mathbf{G}_3, \cdots, \mathbf{G}_L$ (i.e., $L - 1$ gcld's). Suppose that the index

l_0 is known. Calculating $\{\mathbf{M}_{l_0 j}\}_{j=1; j\neq l_0}^{L}$ requires the Smith form $L-1$ times. Therefore, the Smith form is implemented $3L-3$ times in total. Moreover, we need to solve the CVP $L-1$ times for (40), and the computational complexity of exactly solving the CVP is discussed in Sec. II.

Remark: When the moduli $\{\mathbf{M}_i\}_{i=1}^{L}$ in Theorem 1 satisfy the constraint (i.e., (17)) imposed in [23], Theorem 1 reduces to Proposition 2. It should also be pointed out that the MD-CRT reconstruction range $\mathbf{m} \in \mathcal{N}\,(\mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L))$ and the robust MD-CRT reconstruction range in (37) do not imply each other, unless for the (robust) 1-D CRT and the (robust) MD-CRT with moduli being nonsingular diagonal integer matrices. We take an example as follows. Let $\mathbf{M}_1 = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$ and $\mathbf{M}_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, whose product $\mathbf{R} = \mathbf{M}_1\mathbf{M}_2 = \begin{pmatrix} 7 & 5 \\ 5 & 7 \end{pmatrix}$ is their lcrm. When $\mathbf{m} = \begin{pmatrix} 5 \\ 4 \end{pmatrix} = \mathbf{R}\begin{pmatrix} 5/8 \\ 1/8 \end{pmatrix} \in \mathcal{N}(\mathbf{R})$, we obtain $\mathbf{n}_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \mathbf{M}_2\begin{pmatrix} 2/3 \\ -1/3 \end{pmatrix}$, indicating $\mathbf{n}_1 \notin \mathcal{N}(\mathbf{M}_1^{-1}\mathbf{R}) = \mathcal{N}(\mathbf{M}_2)$. On the other hand, when $\mathbf{m} = \begin{pmatrix} 10 \\ 9 \end{pmatrix} = \mathbf{R}\begin{pmatrix} 25/24 \\ 13/24 \end{pmatrix} \notin \mathcal{N}(\mathbf{R})$, we get $\mathbf{n}_1 = \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \mathbf{M}_2\begin{pmatrix} 2/3 \\ 2/3 \end{pmatrix}$, implying $\mathbf{n}_1 \in \mathcal{N}(\mathbf{M}_1^{-1}\mathbf{R}) = \mathcal{N}(\mathbf{M}_2)$. Owing to this reconstruction range inequivalence, we cannot obtain a further improved variant of the robust MD-CRT as in [8], where a multi-stage (e.g., second-stage) robust 1-D CRT was generalized by first splitting the congruences into several groups, then applying the robust 1-D CRT to each group independently, and finally applying the robust 1-D CRT again to a new system of congruences with the reconstructions and lcm's in all the groups being the remainders and moduli, respectively.

For a better understanding of Theorem 1, we next present an example to explain our implementation of the robust MD-CRT through the step-by-step procedures in **Algorithm 1**.

Example 1: Consider $L = 3$ moduli $\mathbf{M}_1 = \begin{pmatrix} 5850 & 9000 \\ 2580 & 2940 \end{pmatrix}$, $\mathbf{M}_2 = \begin{pmatrix} 28950 & 24150 \\ 14140 & 11680 \end{pmatrix}$, and $\mathbf{M}_3 = \begin{pmatrix} 3440 & 3460 \\ 1540 & 1160 \end{pmatrix}$. Let $\mathbf{m} = \begin{pmatrix} -5365350 \\ -2402280 \end{pmatrix}$, then the remainders of $\mathbf{m}$ modulo $\{\mathbf{M}_i\}_{i=1}^{3}$ can be calculated from (6) as $\mathbf{r}_1 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\mathbf{r}_2 = \begin{pmatrix} 37650 \\ 18320 \end{pmatrix}$, and $\mathbf{r}_3 = \begin{pmatrix} 4490 \\ 1660 \end{pmatrix}$. Correspondingly, the folding vectors are given by $\mathbf{n}_1 = \begin{pmatrix} -971 \\ 35 \end{pmatrix}$, $\mathbf{n}_2 = \begin{pmatrix} 1390 \\ -1890 \end{pmatrix}$, and $\mathbf{n}_3 = \begin{pmatrix} -1561 \\ 0 \end{pmatrix}$. Let the erroneous remainders be $\tilde{\mathbf{r}}_1 = \begin{pmatrix} 52 \\ 36 \end{pmatrix}$, $\tilde{\mathbf{r}}_2 = \begin{pmatrix} 37673 \\ 18243 \end{pmatrix}$, and $\tilde{\mathbf{r}}_3 = \begin{pmatrix} 4446 \\ 1610 \end{pmatrix}$, with their respective remainder errors $\triangle\mathbf{r}_1 = \begin{pmatrix} 52 \\ 36 \end{pmatrix}$, $\triangle\mathbf{r}_2 = \begin{pmatrix} 23 \\ -77 \end{pmatrix}$, and $\triangle\mathbf{r}_3 = \begin{pmatrix} -44 \\ -50 \end{pmatrix}$. In the following, we elaborate how to robustly reconstruct $\mathbf{m}$ from the erroneous remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^{3}$ by **Algorithm 1**.

i) First, calculate $\mathbf{M}_{12} = \begin{pmatrix} -2272650 & -2274600 \\ -1002640 & -1003500 \end{pmatrix}$, $\mathbf{M}_{13} = \begin{pmatrix} -604610 & -454920 \\ -266740 & -200700 \end{pmatrix}$, $\mathbf{M}_{23} = \begin{pmatrix} -3632710 & -3661660 \\ -1774320 & -1788460 \end{pmatrix}$, according to 12) in Sec. II. Under the ℓ_2 norm, we then obtain $\lambda_{\mathcal{L}(\mathbf{M}_{12})} = 637.89$, $\lambda_{\mathcal{L}(\mathbf{M}_{13})} = 352.28$, $\lambda_{\mathcal{L}(\mathbf{M}_{23})} = 178.04$. Finally, from (36), we regard the first remainder as the reference, and the reconstruction robustness bound is $352.28/4 = 88.07$. One can easily see that the remainder error bound τ satisfies $\|\triangle\mathbf{r}_i\| \leq \tau < 88.07$ for $1 \leq i \leq 3$.

ii) According to 13) in Sec. II, calculate $\mathbf{R}_3 = \mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2) = \begin{pmatrix} 86850 & -101250 \\ 42420 & -49800 \end{pmatrix}$, followed by $\mathbf{R} = \mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3) = \mathrm{lcrm}(\mathbf{R}_3, \mathbf{M}_3) = \begin{pmatrix} 774000 & -6133500 \\ 346500 & -2746200 \end{pmatrix}$. In addition, based on 12) in Sec. II, we calculate the accompanying matrices $\mathbf{P}_2 = \begin{pmatrix} -10 & -12 \\ -69 & -69 \end{pmatrix}$ and $\mathbf{Q}_2 = \begin{pmatrix} -25 & -28 \\ -36 & -32 \end{pmatrix}$ satisfying $\mathbf{M}_1\mathbf{P}_2 + \mathbf{M}_2\mathbf{Q}_2 = \mathbf{M}_{12}$, and calculate the accompanying matrices $\mathbf{P}_3 = \begin{pmatrix} -108 & -65 \\ 85 & 51 \end{pmatrix}$ and $\mathbf{Q}_3 = \begin{pmatrix} -40 & -24 \\ -45 & -27 \end{pmatrix}$ satisfying $\mathbf{R}_3\mathbf{P}_3 + \mathbf{M}_3\mathbf{Q}_3 = \mathbf{G}_3 \triangleq \mathrm{gcld}(\mathbf{R}_3, \mathbf{M}_3) = \begin{pmatrix} -18279350 & -10984980 \\ -8928160 & -5365380 \end{pmatrix}$.

iii) According to 3) in Sec. II, calculate $\mathbf{v}_2$ and $\mathbf{v}_3$ from (40) as $\mathbf{v}_2 = \begin{pmatrix} 37650 \\ 18320 \end{pmatrix}$ and $\mathbf{v}_3 = \begin{pmatrix} 4490 \\ 1660 \end{pmatrix}$. One can easily confirm that $\lfloor \mathbf{M}_1^{-1}\mathbf{m} \rfloor = \mathbf{n}_1 \in \mathcal{N}\left(\mathbf{M}_1^{-1}\mathbf{R}\right) = \mathcal{N}\left(\begin{pmatrix} 140 & -1110 \\ -5 & 40 \end{pmatrix}\right)$, i.e., $\begin{pmatrix} -971 \\ 35 \end{pmatrix} = \begin{pmatrix} 140 & -1110 \\ -5 & 40 \end{pmatrix}\begin{pmatrix} 0.2 \\ 0.9 \end{pmatrix}$, and $\|\triangle\mathbf{r}_i\| \leq \tau < 88.07$ for $1 \leq i \leq 3$. Therefore, Theorem 1 holds.

iv) Via the cascaded reconstruction algorithm for the MD-CRT in Proposition 1, calculate $\boldsymbol{\zeta} \triangleq \mathbf{M}_1\tilde{\mathbf{n}}_1$ from

$$\begin{cases} \boldsymbol{\zeta} \equiv \mathbf{0} \mod \mathbf{M}_1 \\ \boldsymbol{\zeta} \equiv \mathbf{v}_2 \mod \mathbf{M}_2 \\ \boldsymbol{\zeta} \equiv \mathbf{v}_3 \mod \mathbf{M}_3. \end{cases} \tag{42}$$

- From (13), we acquire $\boldsymbol{\zeta}_1 = \langle \mathbf{0} + \mathbf{M}_1\mathbf{P}_2\mathbf{M}_{12}^{-1}(\mathbf{v}_2 - \mathbf{0})\rangle_{\mathbf{R}_3} = \begin{pmatrix} -20250 \\ -9960 \end{pmatrix}$.
- From (14), we get $\boldsymbol{\zeta} = \boldsymbol{\zeta}_2 = \langle \boldsymbol{\zeta}_1 + \mathbf{R}_3\mathbf{P}_3\mathbf{G}_3^{-1}(\mathbf{v}_3 - \boldsymbol{\zeta}_1)\rangle_{\mathbf{R}} = \begin{pmatrix} -5365350 \\ -2402280 \end{pmatrix}$.

We so have $\tilde{\mathbf{n}}_1 = \begin{pmatrix} -971 \\ 35 \end{pmatrix}$, which is equal to $\mathbf{n}_1$.

v) Calculate $\mathbf{M}_2\tilde{\mathbf{n}}_2 = \mathbf{M}_1\tilde{\mathbf{n}}_1 - \mathbf{v}_2 = \begin{pmatrix} -5403000 \\ -2420600 \end{pmatrix}$ as well as $\mathbf{M}_3\tilde{\mathbf{n}}_3 = \mathbf{M}_1\tilde{\mathbf{n}}_1 - \mathbf{v}_3 = \begin{pmatrix} -5369840 \\ -2403940 \end{pmatrix}$. It also implies that $\tilde{\mathbf{n}}_2 = \begin{pmatrix} 1390 \\ -1890 \end{pmatrix}$ and $\tilde{\mathbf{n}}_3 = \begin{pmatrix} -1561 \\ 0 \end{pmatrix}$, which are equal to $\mathbf{n}_2$ and $\mathbf{n}_3$, respectively. Therefore, $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{3}$ (i.e., $\{\mathbf{n}_i\}_{i=1}^{3}$) are accurately determined from the erroneous remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^{3}$, and a robust reconstruction of $\mathbf{m}$ can be obtained as $\tilde{\mathbf{m}} = \frac{1}{3}\sum_{i=1}^{3}(\mathbf{M}_i\tilde{\mathbf{n}}_i + \tilde{\mathbf{r}}_i) = \begin{pmatrix} -5365339.67 \\ -2402310.33 \end{pmatrix}$, i.e., $\|\tilde{\mathbf{m}} - \mathbf{m}\|_2 = 32.05 \leq \tau < 88.07$. ■

Since in the above new results in Theorem 1 there is no any constraint on moduli $\{\mathbf{M}_i\}_{i=1}^{L}$ (i.e., moduli $\{\mathbf{M}_i\}_{i=1}^{L}$ are arbitrary nonsingular integer matrices), some of these moduli might be redundant with respect to the reconstruction robustness bound (i.e., (39)), while retaining the reconstruction range (i.e., (37)). We investigate the case when there exists a pair of moduli $\mathbf{M}_{i_1}$ and $\mathbf{M}_{i_2}$ such that $\mathbf{M}_{i_1} = \mathbf{M}_{i_2}\mathbf{P}$ for $\mathbf{P} \in \mathbb{Z}^{D\times D}$, i.e., $\mathbf{M}_{i_1}$ is a right multiple of $\mathbf{M}_{i_2}$. For this, we have the following corollary.

Corollary 1: If there are two moduli $\mathbf{M}_{i_1}$ and $\mathbf{M}_{i_2}$ in $\{\mathbf{M}_i\}_{i=1}^{L}$ in Theorem 1 such that $\mathbf{M}_{i_1} = \mathbf{M}_{i_2}\mathbf{P}$ for $\mathbf{P} \in \mathbb{Z}^{D\times D}$, the modulus $\mathbf{M}_{i_2}$ is redundant, in the sense that the appearance of $\mathbf{M}_{i_2}$ does not help increase (and might even decrease) the reconstruction robustness bound, meanwhile keeping the reconstruction range unchanged. As such, $\mathbf{M}_{i_2}$ can be deleted from the set of moduli in this case.

Proof: Without loss of generality, let us assume that $\mathbf{M}_1 = \mathbf{M}_L\mathbf{P}$ for $\mathbf{P} \in \mathbb{Z}^{D\times D}$. We first prove $\lambda_{\mathcal{L}(\mathbf{M}_{1j})} \geq \lambda_{\mathcal{L}(\mathbf{M}_{Lj})}$ for any $2 \leq j \leq L-1$. Since $\mathbf{M}_{Lj} = \mathrm{gcld}(\mathbf{M}_L, \mathbf{M}_j)$ and $\mathbf{M}_1 = \mathbf{M}_L\mathbf{P}$ for any $2 \leq j \leq L-1$, it is ready to confirm that $\mathbf{M}_{Lj}$ is a cld of $\mathbf{M}_1$ and $\mathbf{M}_j$. Therefore, $\mathbf{M}_{Lj}$ is a left divisor of $\mathbf{M}_{1j}$ from the definition of gcld, i.e., $\mathbf{M}_{1j} = \mathbf{M}_{Lj}\mathbf{Q}_j$ for $\mathbf{Q}_j \in \mathbb{Z}^{D\times D}$. That is to say, $\mathcal{L}(\mathbf{M}_{1j}) \subseteq \mathcal{L}(\mathbf{M}_{Lj})$, and so $\lambda_{\mathcal{L}(\mathbf{M}_{1j})} \geq \lambda_{\mathcal{L}(\mathbf{M}_{Lj})}$.

For the set of moduli $\{\mathbf{M}_i\}_{i=1}^{L-1}$, let s denote the reconstruction robustness bound, i.e., $s = \max_{1\leq i\leq L-1} \min_{\substack{1\leq j\leq L-1\\ j\neq i}} \lambda_{\mathcal{L}(\mathbf{M}_{ij})}/4$. For the set of moduli $\{\mathbf{M}_i\}_{i=1}^{L}$, the reconstruction robustness bound can be expressed as

$$\begin{aligned}&\max_{1\leq i\leq L}\min_{\substack{1\leq j\leq L\\ j\neq i}} \frac{\lambda_{\mathcal{L}(\mathbf{M}_{ij})}}{4}\\ &= \max\Bigg\{\underbrace{\max_{1\leq i\leq L-1}\min_{\substack{1\leq j\leq L\\ j\neq i}} \frac{\lambda_{\mathcal{L}(\mathbf{M}_{ij})}}{4}}_{(a)}, \underbrace{\min_{1\leq j\leq L-1} \frac{\lambda_{\mathcal{L}(\mathbf{M}_{Lj})}}{4}}_{(b)}\Bigg\}. \end{aligned} \quad (43)$$

As for (a), due to $\min_{\substack{1\leq j\leq L\\ j\neq i}} \lambda_{\mathcal{L}(\mathbf{M}_{ij})}/4 \leq \min_{\substack{1\leq j\leq L-1\\ j\neq i}} \lambda_{\mathcal{L}(\mathbf{M}_{ij})}/4$, we have $\max_{1\leq i\leq L-1} \min_{\substack{1\leq j\leq L\\ j\neq i}} \lambda_{\mathcal{L}(\mathbf{M}_{ij})}/4 \leq s$. As for (b), since it has been proved above that $\lambda_{\mathcal{L}(\mathbf{M}_{1j})} \geq \lambda_{\mathcal{L}(\mathbf{M}_{Lj})}$ for any $2 \leq j \leq L-1$, we have

$$\min_{1\leq j\leq L-1} \frac{\lambda_{\mathcal{L}(\mathbf{M}_{Lj})}}{4} \leq \min_{2\leq j\leq L-1} \frac{\lambda_{\mathcal{L}(\mathbf{M}_{Lj})}}{4} \leq \min_{2\leq j\leq L-1} \frac{\lambda_{\mathcal{L}(\mathbf{M}_{1j})}}{4} \leq s. \quad (44)$$

Thus, from (43), we get $\max_{1\leq i\leq L} \min_{\substack{1\leq j\leq L\\ j\neq i}} \lambda_{\mathcal{L}(\mathbf{M}_{ij})}/4 \leq s$, which suggests that the appearance of $\mathbf{M}_L$ does not help increase the reconstruction robustness bound and might even worsen it.

For the set of moduli $\{\mathbf{M}_i\}_{i=1}^{L}$, it is straightforward that $\mathbf{M}_L$ is impossible to be a reference modulus (i.e., $l_0 \neq L$ in Theorem 1), on account of $\lambda_{\mathcal{L}(\mathbf{M}_{1j})} \geq \lambda_{\mathcal{L}(\mathbf{M}_{Lj})}$ for any $2 \leq j \leq L-1$. So, for the set of moduli $\{\mathbf{M}_i\}_{i=1}^{L-1}$, we can choose the same $\mathbf{M}_{l_0}$ as the reference modulus. Furthermore, owing to $\mathbf{M}_1 = \mathbf{M}_L\mathbf{P}$, we get $\mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L) = \mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_{L-1})$, which implies from (37) that the reconstruction range remains uncha- nged after deleting $\mathbf{M}_L$ from moduli $\{\mathbf{M}_i\}_{i=1}^{L}$. ■

Going back to the necessary and sufficient condition in (38) for the robust MD-CRT in Theorem 1, one can readily see that the remainder error difference bound depends on $\lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})}$, i.e.,

$$\|\triangle\mathbf{r}_j - \triangle\mathbf{r}_{l_0}\| < \frac{\lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})}}{2}, \quad (45)$$

for $1 \leq j \leq L$ and $j \neq l_0$. It means that if we let τ_i denote the remainder error bound for the i-th remainder, i.e., $\|\triangle\mathbf{r}_i\| \leq \tau_i$, for $1 \leq i \leq L$, then $\{\tau_i\}_{i=1}^{L}$ will have different requirements for the robust reconstruction of $\mathbf{m}$ in (37), as stated below.

Corollary 2: Let moduli $\{\mathbf{M}_i\}_{i=1}^{L}$ in (12) be L different arbitrary nonsingular integer matrices, the index l_0 with $1 \leq l_0 \leq L$ satisfy (36), and an integer vector $\mathbf{m}$ be with (37), as the same as those in Theorem 1. Let τ_i denote the remainder error bound for the i-th remainder, i.e., $\|\triangle\mathbf{r}_i\| \leq \tau_i$, for $1 \leq i \leq L$, among which the remainder error bound τ_{l_0} for the reference modulus $\mathbf{M}_{l_0}$ is given by $\tau_{l_0} < \min_{\substack{1\leq j\leq L\\ j\neq l_0}} \lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})}/4$. If the remainder error bound τ_i for $1 \leq i \leq L$ and $i \neq l_0$ satisfies

$$\|\triangle\mathbf{r}_i\| \leq \tau_i \leq \frac{\lambda_{\mathcal{L}(\mathbf{M}_{l_0 i})}}{2} - \min_{\substack{1\leq j\leq L\\ j\neq l_0}} \frac{\lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})}}{4}, \quad (46)$$

we can accurately determine $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$ from the erroneous remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^{L}$ by **Algorithm 1**, and therefore, a robust reconstruction $\tilde{\mathbf{m}}$ of $\mathbf{m}$ is obtained by (19), i.e., $\|\tilde{\mathbf{m}} - \mathbf{m}\| \leq \sum_{i=1}^{L} \tau_i/L$.

Proof: As $\|\triangle\mathbf{r}_{l_0}\| \leq \tau_{l_0} < \min_{\substack{1\leq j\leq L\\ j\neq l_0}} \lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})}/4$ and $\|\triangle\mathbf{r}_i\| \leq \tau_i \leq \lambda_{\mathcal{L}(\mathbf{M}_{l_0 i})}/2 - \min_{\substack{1\leq j\leq L\\ j\neq l_0}} \lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})}/4$ for $1 \leq i \leq L$ and $i \neq l_0$, we have

$$\|\triangle\mathbf{r}_j - \triangle\mathbf{r}_{l_0}\| \leq \|\triangle\mathbf{r}_j\| + \|\triangle\mathbf{r}_{l_0}\| \leq \tau_{l_0} + \tau_i < \frac{\lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})}}{2}, \quad (47)$$

which indicates (38) in Theorem 1. As a result, $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$ can be accurately determined from the erroneous remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^{L}$ by **Algorithm 1**, and we can obtain a robust reconstruction $\tilde{\mathbf{m}}$ of $\mathbf{m}$ as $\tilde{\mathbf{m}} = \frac{1}{L}\sum_{i=1}^{L}(\mathbf{M}_i\mathbf{n}_i + \tilde{\mathbf{r}}_i)$, i.e.,

$$\|\tilde{\mathbf{m}} - \mathbf{m}\| = \left\|\frac{1}{L}\sum_{i=1}^{L}\triangle\mathbf{r}_i\right\| \leq \frac{1}{L}\sum_{i=1}^{L}\|\triangle\mathbf{r}_i\| \leq \frac{1}{L}\sum_{i=1}^{L}\tau_i. \quad (48)$$

Therefore, Corollary 2 is proved. ■

Remark: Of note, owing to $\lambda_{\mathcal{L}(\mathbf{M}_{l_0 i})}/2 - \min_{\substack{1\leq j\leq L\\ j\neq l_0}} \lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})}/4 \geq \min_{\substack{1\leq j\leq L\\ j\neq l_0}} \lambda_{\mathcal{L}(\mathbf{M}_{l_0 j})}/4$ for $1 \leq i \leq L$ and $i \neq l_0$, the allowed remainder error bounds we derived by approaching them individually as above are larger than or equal to that in (39) for all the remainder errors in Theorem 1, while the reconstruction range (i.e., (37)) remains unchanged. In addition, note that the counterpart results of Corollary 1 and Corollary 2 were also obtained for the robust 1-D CRT in [8].

Example 2: Let us consider the $L = 3$ moduli as in Example 1. According to Corollary 2, for the robust MD-CRT, we obtain the remainder error bounds as $\tau_1 < 352.28/4$, $\tau_2 \le 923.5/4, \tau_3 \le 352.28/4$. One can obviously see that the allowed remainder error bounds here are larger than or equal to $352.28/4$ obtained in Theorem 1. Moreover, the reconstruction range in Corollary 2 is the same as that (i.e., (37)) in Theorem 1. ■

V. Generalization of Robust MD-CRT from Integer Vectors/Matrices to Real Ones

The above studies are all for integer vectors/matrices. Considering that in practical applications, an unknown vector (e.g., the phase of interest in multi-dimensional phase unwrapping in MIMO radar systems) is real-valued in general, we next generalize the robust MD-CRT results in Theorem 1 from integer vectors/matrices to real ones in this section. Note that we adopt boldfaced Sans-Serif letters to denote real vectors/matrices for distinguishing them from integer vectors/matrices.

Let $\mathbf{m}$ be a D-dimensional real vector (i.e., $\mathbf{m} \in \mathbb{R}^D$), which can be uniquely expressed as

$$\mathbf{m} = \mathbf{M}\mathbf{\Psi}_i\mathbf{n}_i + \mathbf{r}_i \ \text{ for } 1 \le i \le L, \tag{49}$$

where $\{\mathbf{\Psi}_i\}_{i=1}^L \in \mathbb{Z}^{D\times D}$ are known nonsingular integer matrices, $\mathbf{M} \in \mathbb{R}^{D\times D}$ is a known nonsingular real matrix, and $\{\mathbf{n}_i\}_{i=1}^L \in \mathbb{Z}^D$ are unknown integer vectors (or folding vectors). In particular, $\{\mathbf{r}_i\}_{i=1}^L \in \mathbb{R}^D$ are real vectors with $\mathbf{r}_i \in \mathcal{F}(\mathbf{M}\mathbf{\Psi}_i)$ for each $1 \le i \le L$, which are real-valued versions of the previously mentioned integer remainders $\{\mathbf{r}_i\}_{i=1}^L$ in (23). Here, $\mathcal{F}(\mathbf{M}\mathbf{\Psi}_i)$ is termed the fundamental parallelepiped of $\mathcal{L}(\mathbf{M}\mathbf{\Psi}_i)$, defined as

$$\mathcal{F}(\mathbf{M}\mathbf{\Psi}_i) = \left\{\mathbf{M}\mathbf{\Psi}_i\mathbf{x} \,|\, \mathbf{x} \in [0,1)^D\right\}. \tag{50}$$

The volume of $\mathcal{F}(\mathbf{M}\mathbf{\Psi}_i)$ equals $|\det(\mathbf{M}\mathbf{\Psi}_i)|$[27]. $\mathcal{F}(\mathbf{M}\mathbf{\Psi}_i)$ does not comprise any other lattice points in $\mathcal{L}(\mathbf{M}\mathbf{\Psi}_i)$, except for the origin $\mathbf{0}$. One can easily see that $\mathcal{F}(\mathbf{M}\mathbf{\Psi}_i)$ and its shifted copies (i.e., $\mathcal{F}(\mathbf{M}\mathbf{\Psi}_i) + \mathbf{v}$ for any nonzero $\mathbf{v} \in \mathcal{L}(\mathbf{M}\mathbf{\Psi}_i)$) constitute the whole real vector space $\mathbb{R}^D$.

Let us define $\mathbf{\Psi}_{ij} = \text{gcld}(\mathbf{\Psi}_i, \mathbf{\Psi}_j)$ for $1 \le i \ne j \le L$. Without loss of generality, we assume that $\mathbf{\Psi}_1$ satisfies

$$\min_{2\le j\le L} \lambda_{\mathcal{L}(\mathbf{M}\mathbf{\Psi}_{1j})} = \max_{1\le i\le L} \min_{\substack{1\le j\le L\\ j\ne i}} \lambda_{\mathcal{L}(\mathbf{M}\mathbf{\Psi}_{ij})}. \tag{51}$$

By treating $\mathbf{M}\mathbf{\Psi}_1$ as the reference and following the operations used in (24) and (25), we have, from (49),

$$\begin{cases} \mathbf{\Psi}_1\mathbf{n}_1 - \mathbf{\Psi}_2\mathbf{n}_2 = \mathbf{M}^{-1}(\mathbf{r}_2 - \mathbf{r}_1) \\ \mathbf{\Psi}_1\mathbf{n}_1 - \mathbf{\Psi}_3\mathbf{n}_3 = \mathbf{M}^{-1}(\mathbf{r}_3 - \mathbf{r}_1) \\ \qquad\qquad \vdots \\ \mathbf{\Psi}_1\mathbf{n}_1 - \mathbf{\Psi}_L\mathbf{n}_L = \mathbf{M}^{-1}(\mathbf{r}_L - \mathbf{r}_1) \end{cases} \tag{52}$$

and

$$\begin{cases} \mathbf{K}_{12}\mathbf{n}_1 - \mathbf{K}_{21}\mathbf{n}_2 = (\mathbf{M}\mathbf{\Psi}_{12})^{-1}(\mathbf{r}_2 - \mathbf{r}_1) \\ \mathbf{K}_{13}\mathbf{n}_1 - \mathbf{K}_{31}\mathbf{n}_3 = (\mathbf{M}\mathbf{\Psi}_{13})^{-1}(\mathbf{r}_3 - \mathbf{r}_1) \\ \qquad\qquad \vdots \\ \mathbf{K}_{1L}\mathbf{n}_1 - \mathbf{K}_{L1}\mathbf{n}_L = (\mathbf{M}\mathbf{\Psi}_{1L})^{-1}(\mathbf{r}_L - \mathbf{r}_1), \end{cases} \tag{53}$$

in which $\mathbf{K}_{1j} = \mathbf{\Psi}_{1j}^{-1}\mathbf{\Psi}_1$ and $\mathbf{K}_{j1} = \mathbf{\Psi}_{1j}^{-1}\mathbf{\Psi}_j$ for $2 \le j \le L$. From (52) and (53), $\left\{\mathbf{M}^{-1}(\mathbf{r}_i - \mathbf{r}_1)\right\}_{i=2}^L$ and $\left\{(\mathbf{M}\mathbf{\Psi}_{1i})^{-1}(\mathbf{r}_i - \mathbf{r}_1)\right\}_{i=2}^L$ are all integer vectors; that is,

$$\mathbf{r}_i - \mathbf{r}_1 \in \mathcal{L}(\mathbf{M}\mathbf{\Psi}_{1i}) \ \text{ for } 2 \le i \le L. \tag{54}$$

For every $2 \le i \le L$, we then estimate $\mathbf{r}_i - \mathbf{r}_1$ from the known erroneous remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^L$ via finding a closest lattice point $\mathbf{v}_i$ in $\mathcal{L}(\mathbf{M}\mathbf{\Psi}_{1i})$ to $\tilde{\mathbf{r}}_i - \tilde{\mathbf{r}}_1$, i.e.,

$$\mathbf{v}_i = \operatorname*{arg\,min}_{\mathbf{v}\in\mathcal{L}(\mathbf{M}\mathbf{\Psi}_{1i})} \|\mathbf{v} - (\tilde{\mathbf{r}}_i - \tilde{\mathbf{r}}_1)\|, \tag{55}$$

where $\tilde{\mathbf{r}}_j \triangleq \mathbf{r}_j + \triangle\mathbf{r}_j \in \mathcal{F}(\mathbf{M}\mathbf{\Psi}_j)$ for each $1 \le j \le L$ is defined, and $\{\triangle\mathbf{r}_i\}_{i=1}^L \in \mathbb{R}^D$ are the remainder errors. We try to accurately determine $\{\mathbf{\Psi}_i\mathbf{n}_i\}_{i=1}^L$. Specifically, we take the modulo-$\mathbf{\Psi}_i$ on both sides of the $(i-1)$-th equation in (52) for $2 \le i \le L$, and we have

$$\begin{cases} \mathbf{\Psi}_1\mathbf{n}_1 \equiv \mathbf{0} \mod \mathbf{\Psi}_1 \\ \mathbf{\Psi}_1\mathbf{n}_1 \equiv \mathbf{M}^{-1}(\mathbf{r}_2 - \mathbf{r}_1) \mod \mathbf{\Psi}_2 \\ \mathbf{\Psi}_1\mathbf{n}_1 \equiv \mathbf{M}^{-1}(\mathbf{r}_3 - \mathbf{r}_1) \mod \mathbf{\Psi}_3 \\ \qquad\qquad \vdots \\ \mathbf{\Psi}_1\mathbf{n}_1 \equiv \mathbf{M}^{-1}(\mathbf{r}_L - \mathbf{r}_1) \mod \mathbf{\Psi}_L, \end{cases} \tag{56}$$

where the first equation spontaneously holds. Once $\{\mathbf{r}_i - \mathbf{r}_1\}_{i=2}^L$ are accurately estimated from (55), i.e., $\mathbf{v}_i = \mathbf{r}_i - \mathbf{r}_1$ for $2 \le i \le L$, we can accurately determine $\mathbf{\Psi}_1\mathbf{n}_1$ from (56) according to the MD-CRT (see Proposition 1 above), provided that $\mathbf{\Psi}_1\mathbf{n}_1 \in \mathcal{N}(\text{lcrm}(\mathbf{\Psi}_1, \mathbf{\Psi}_2, \cdots, \mathbf{\Psi}_L))$, equivalently written as $\mathbf{M}\mathbf{\Psi}_1\mathbf{n}_1 \in \mathcal{F}(\mathbf{M}\,\text{lcrm}(\mathbf{\Psi}_1, \mathbf{\Psi}_2, \cdots, \mathbf{\Psi}_L))$, and also as

$$\lfloor \mathbf{\Psi}_1^{-1}\mathbf{M}^{-1}\mathbf{m} \rfloor \in \mathcal{N}\left(\mathbf{\Psi}_1^{-1}\text{lcrm}(\mathbf{\Psi}_1, \mathbf{\Psi}_2, \cdots, \mathbf{\Psi}_L)\right). \tag{57}$$

Next, $\mathbf{\Psi}_i\mathbf{n}_i$ can be accurately determined from (52) as $\mathbf{\Psi}_1\mathbf{n}_1 - \mathbf{M}^{-1}\mathbf{v}_i$ for each $2 \le i \le L$. One can see that the proposed robust MD-CRT for integer vectors/matrices (i.e., Theorem 1) and its closed-form reconstruction algorithm (i.e., **Algorithm 1**) can be directly applied to (52) (or (56)). Thus, the following result is straightforwardly obtained.

Corollary 3: Let $\{\mathbf{\Psi}_i\}_{i=1}^L$ and $\mathbf{M}$ in (49) be L different arbitrary nonsingular integer matrices and an arbitrary nonsingular real matrix, respectively. Without loss of generality, we assume that the index l_0 with $1 \le l_0 \le L$ satisfies

$$\min_{\substack{1\le j\le L\\ j\ne l_0}} \lambda_{\mathcal{L}(\mathbf{M}\mathbf{\Psi}_{l_0 j})} = \max_{1\le i\le L} \min_{\substack{1\le j\le L\\ j\ne i}} \lambda_{\mathcal{L}(\mathbf{M}\mathbf{\Psi}_{ij})}. \tag{58}$$

For a real vector $\mathbf{m}$ with

$$\lfloor \mathbf{\Psi}_{l_0}^{-1}\mathbf{M}^{-1}\mathbf{m} \rfloor \in \mathcal{N}\left(\mathbf{\Psi}_{l_0}^{-1}\text{lcrm}(\mathbf{\Psi}_1, \mathbf{\Psi}_2, \cdots, \mathbf{\Psi}_L)\right), \tag{59}$$

we can accurately determine $\{\mathbf{\Psi}_i\mathbf{n}_i\}_{i=1}^L$ from the erroneous remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^L$, if and only if

$$\mathbf{0} = \operatorname*{arg\,min}_{\mathbf{h}\in\mathcal{L}(\mathbf{M}\mathbf{\Psi}_{l_0 j})} \|\mathbf{h} - (\triangle\mathbf{r}_j - \triangle\mathbf{r}_{l_0})\| \ \text{ for } 1 \le j \le L \text{ and } j \ne l_0. \tag{60}$$

Moreover, letting τ be the remainder error bound, i.e., $\|\triangle \mathbf{r}_i\| \leq \tau$ for $1 \leq i \leq L$, a simple sufficient condition is

$$\tau < \max_{1\leq i\leq L} \min_{\substack{1\leq j\leq L\\ j\neq i}} \frac{\lambda_{\mathcal{L}(\mathbf{M}\boldsymbol{\Psi}_{ij})}}{4} = \min_{\substack{1\leq j\leq L\\ j\neq l_0}} \frac{\lambda_{\mathcal{L}(\mathbf{M}\boldsymbol{\Psi}_{l_0 j})}}{4}. \tag{61}$$

After $\{\boldsymbol{\Psi}_i \mathbf{n}_i\}_{i=1}^{L}$ are accurately determined, a robust reconstruction $\tilde{\mathbf{m}}$ of $\mathbf{m}$ can be obtained by $\tilde{\mathbf{m}} = \frac{1}{L}\sum_{i=1}^{L}(\mathbf{M}\boldsymbol{\Psi}_i \mathbf{n}_i + \tilde{\mathbf{r}}_i)$ with $\|\tilde{\mathbf{m}} - \mathbf{m}\| \leq \tau$.

VI. Simulations

In this section, we first conduct some numerical simulations to verify the theoretical results of the robust MD-CRT in Theorem 1 (see Sec. III above), and then illustrate the performance of the robust MD-CRT in frequency estimation for a complex MD sinusoidal signal based on multiple sub-Nyquist samplers. For all experiments below, without loss of generality, we focus on the two-dimensional case, i.e., $D = 2$, and the vector norm $\|\cdot\|$ involved is assumed to be the ℓ_2 norm, i.e., $\|\cdot\|_2$.

We consider three moduli as $\mathbf{M}_1 = \begin{pmatrix} 1360 & 1788 \\ 960 & 1728 \end{pmatrix}$, $\mathbf{M}_2 = \begin{pmatrix} 656 & 488 \\ 256 & 448 \end{pmatrix}$, and $\mathbf{M}_3 = \begin{pmatrix} 1532 & 1576 \\ 1392 & 1656 \end{pmatrix}$, which clearly do not satisfy the constraint (i.e., (17)) used in [23]. We calculate an lcrm of $\{\mathbf{M}_i\}_{i=1}^{3}$ as $\mathbf{R} = \begin{pmatrix} 733248 & 540744 \\ 655488 & 483264 \end{pmatrix}$, and the minimum distance of the lattice that is generated by a gcld of any pair of moduli as $\lambda_{\mathcal{L}(\mathbf{M}_{12})} = 85.0412$, $\lambda_{\mathcal{L}(\mathbf{M}_{13})} = 127.5617$, and $\lambda_{\mathcal{L}(\mathbf{M}_{23})} = 42.5206$. According to Theorem 1, we should choose $\mathbf{M}_1$ as the reference moduli, i.e., $l_0 = 1$, and the reconstruction robustness bound is $85.0412/4 = 21.2603$. For comparison, we also choose $\mathbf{M}_2$ as the reference moduli, and the reconstruction robustness bound is $42.5206/4 = 10.6302$. For these two cases, they have different reconstruction ranges. Let $\mathbf{m} = \begin{pmatrix} 515545 \\ 460771 \end{pmatrix}$ be an integer vector we need to estimate, which obviously falls into the reconstruction ranges of the two cases. Therefore, with respect to each case, we investigate the remainder error bounds $\tau = 0, 2, 4, \cdots, 30$, and for each of them, we uniformly select the remainder errors $\|\triangle \mathbf{r}_i\|_2 \leq \tau, 1 \leq i \leq 3$, and run 2000 trails. For every trail, we utilize **Algorithm 1** to obtain one estimate $\tilde{\mathbf{m}}$. In Fig. 1, we illustrate the mean error $E(\|\mathbf{m} - \tilde{\mathbf{m}}\|_2)$ in terms of different remainder error bounds for each of the two cases. One can see from Fig. 1 that the performance is completely in line with the results of our proposed robust MD-CRT. That is to say, the mean error curve always lies beneath the remainder error bound curve when the remainder error bound is less than the reconstruction robustness bound, and then is about to break through the remainder error bound curve (i.e., robust reconstruction fails). Moreover, Fig. 1 shows that choosing a proper modulus as the reference in **Algorithm 1** is beneficial to improved robustness performance for the robust MD-CRT.

We next show a direct application of the robust MD-CRT to MD sinusoidal frequency estimation with multiple sub-Nyquist samplers in noise. To do so, let us first recall multidimensional sampling. Sampling of a 1-D signal is performed on a line with samples located at equally spaced points of the line (generated or periodically extended by a sampling interval), whereas for an MD signal $x(\mathbf{t})$ with $\mathbf{t} \in \mathbb{R}^D$ to be considered in this paper, its samples are taken at a series of vertex points of a sampling lattice (generated by a sampling matrix) and have more degrees of freedom. For example, a sampled signal $x_s(\mathbf{t})$ of $x(\mathbf{t})$ over a sampling lattice $\mathcal{L}(\mathbf{M})$ that is generated by a $D \times D$ nonsingular matrix $\mathbf{M} \in \mathbb{R}^{D\times D}$ is defined as

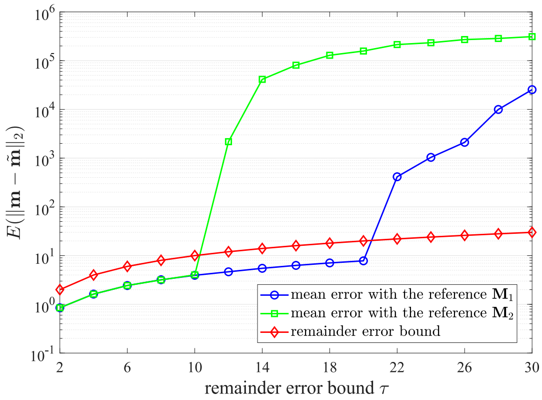

Fig. 1. Mean error and theoretical error bound for the two cases using different reference moduli in **Algorithm 1**.

$$x_s(\mathbf{t}) = \sum_{\mathbf{n}\in\mathbb{Z}^D} x(\mathbf{t})\delta(\mathbf{t} - \mathbf{M}\mathbf{n}),\ \mathbf{t} \in \mathbb{R}^D, \tag{62}$$

where $\delta(\mathbf{t})$ is the unit impulse function, and $\mathbf{M}$ is the sampling matrix with the sampling density $1/|\det(\mathbf{M})|$. Sampling density, also called sampling rate, is the density of sampling points per unit spatial volume in $\mathbb{R}^D$, and therefore, the cost of an analog-to-digital converter increases with increasing sampling density.

Assume without loss of generality that $\mathbf{f} \in \mathbb{Z}^D$ is an unknown D-dimensional integer frequency of interest in a complex MD sinusoidal signal $x(\mathbf{t})$ with noise $\omega(\mathbf{t})$, i.e.,

$$x(\mathbf{t}) = e^{j2\pi\mathbf{f}^T\mathbf{t}} + \omega(\mathbf{t}),\ \mathbf{t}\ \in \mathbb{R}^D. \tag{63}$$

Let $\mathbf{M}_1^{-T}, \mathbf{M}_2^{-T}, \cdots, \mathbf{M}_L^{-T}$ be L different sampling matrices with the sampling densities $\{|\det(\mathbf{M}_i)|\}_{i=1}^{L}$, where $\{\mathbf{M}_i\}_{i=1}^{L} \in \mathbb{Z}^{D\times D}$ are nonsingular integer matrices. We obtain the sampled sinusoidal signal of $x(\mathbf{t})$ with the sampling matrix $\mathbf{M}_i^{-T}$ as

$$x_i[\mathbf{n}] = e^{j2\pi\mathbf{f}^T\mathbf{M}_i^{-T}\mathbf{n}} + \omega_i[\mathbf{n}],\ \mathbf{n} \in \mathbb{Z}^D. \tag{64}$$

The MD discrete Fourier transform (DFT) with respect to $\mathbf{M}_i^T$ is then implemented on $x_i[\mathbf{n}], \mathbf{n} \in \mathcal{N}(\mathbf{M}_i^T)$ [33], and we have

$$\begin{aligned} X_i[\mathbf{k}] &= \sum_{\mathbf{n}\in\mathcal{N}(\mathbf{M}_i^T)} e^{j2\pi\mathbf{f}^T\mathbf{M}_i^{-T}\mathbf{n}} e^{-j2\pi\mathbf{k}^T\mathbf{M}_i^{-T}\mathbf{n}} + \Omega_i[\mathbf{k}] \\ &= \sum_{\mathbf{n}\in\mathcal{N}(\mathbf{M}_i^T)} e^{-j2\pi(\mathbf{k}-\mathbf{f})^T\mathbf{M}_i^{-T}\mathbf{n}} + \Omega_i[\mathbf{k}] \\ &= |\det(\mathbf{M}_i)|\,\varrho[\mathbf{k} - \mathbf{r}_i] + \Omega_i[\mathbf{k}] \end{aligned} \tag{65}$$

for $\mathbf{k} \in \mathcal{N}(\mathbf{M}_i)$, where $\mathbf{r}_i$ is the remainder of $\mathbf{f}$ modulo $\mathbf{M}_i$, i.e., $\mathbf{r}_i = \langle \mathbf{f} \rangle_{\mathbf{M}_i}$, $\Omega_i[\mathbf{k}]$ is the MD DFT of $\omega_i[\mathbf{n}]$ with respect to $\mathbf{M}_i^T$, and the last equation holds due to the unitarity property of the MD DFT [34]. Note that $\varrho[\mathbf{n}]$ stands for the MD discrete delta function, which equals 1 if $\mathbf{n} = \mathbf{0}$ and 0 otherwise. Hence, the

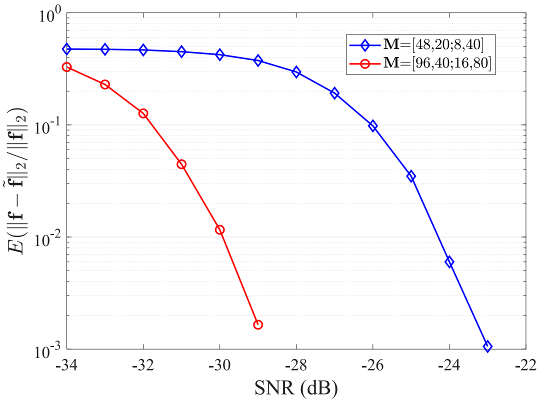

Fig. 2. Mean relative error in terms of various SNR's for the two different **M**'s.

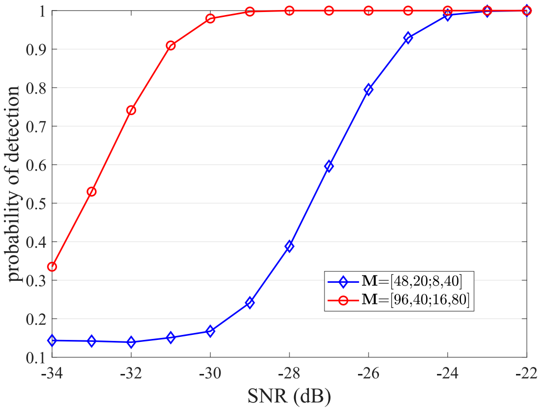

Fig. 3. Probability of detection in terms of various SNR's for the two different **M**'s.

remainder $\mathbf{r}_i$ can be accurately detected as the peak in the MD DFT magnitude of $x_i[\mathbf{n}]$ in (65), when the signal-to-noise ratio (SNR, quantified as $\text{SNR} = -10\log_{10}(2\sigma^2)$ dB where $\omega_i[\mathbf{n}]$ in (64) is zero-mean complex white Gaussian noise with variance $2\sigma^2$) is not too low. Accordingly, $\mathbf{f}$ can be accurately obtained from the detected remainders $\{\mathbf{r}_i\}_{i=1}^{L}$ based on the MD-CRT in Proposition 1, if $\mathbf{f} \in \mathcal{N}(\mathbf{R})$, where $\mathbf{R}$ is an lcrm of $\{\mathbf{M}_i\}_{i=1}^{L}$. At this point, the Nyquist sampling density defined by $|\det(\mathbf{R})|$ is considerably greater than the sampling densities $\{|\det(\mathbf{M}_i)|\}_{i=1}^{L}$. More interestingly, when the SNR is not too high, the detected remainders are likely to have errors, and thereby our proposed robust MD-CRT in Theorem 1 offers an efficient approach for robustly estimating $\mathbf{f}$ from the erroneous remainders.

To illustrate the performance of the robust MD-CRT in MD sinusoidal frequency estimation, we consider two sampling matrices $\left\{\mathbf{M}_i^{-T}\right\}_{i=1}^{2}$ for simplicity, where $\mathbf{M}_i = \mathbf{M}\boldsymbol{\Gamma}_i, i = 1, 2$, with $\boldsymbol{\Gamma}_1 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and $\boldsymbol{\Gamma}_2 = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$. It is easily known that $\boldsymbol{\Gamma}_1$ and $\boldsymbol{\Gamma}_2$ are left coprime but not commutative. Hence, $\mathbf{M}_1$ and $\mathbf{M}_2$ do not satisfy the constraint (i.e., (17)) placed in [23], and $\mathbf{M}$ is their gcld. In these simulations, we investigate two cases of $\mathbf{M}$, i.e., $\mathbf{M} = \begin{pmatrix} 48 & 20 \\ 8 & 40 \end{pmatrix}$ and $\mathbf{M} = \begin{pmatrix} 96 & 40 \\ 16 & 80 \end{pmatrix}$. Based on the robust MD-CRT for the moduli $\mathbf{M}_1$ and $\mathbf{M}_2$, we reconstruct an MD frequency $\mathbf{f} \in \mathbb{Z}^2$ from the detected remainders in the MD DFT domains of undersampled waveforms in (65). From Theorem 1, the two different $\mathbf{M}$'s yield different reconstruction robustness bounds 10.6302 and 21.2603, respectively. We take $\mathbf{f} = \begin{pmatrix} 443 \\ 388 \end{pmatrix}$, which is clearly within the reconstruction ranges of the two cases. In Fig. 2, we present the mean relative error $E(\|\mathbf{f}-\tilde{\mathbf{f}}\|_2/\|\mathbf{f}\|_2)$ between $\mathbf{f}$ and the reconstruction $\tilde{\mathbf{f}}$ verse various SNR's for the two cases. Moreover, Fig. 3 shows the probability of detection verse different SNR's to indicate the estimation accuracy for the two cases. In the experiments, we implement 2000 trails for every SNR. From Figs. 2 and 3, the second case with a larger reconstruction robustness bound results in better performance (i.e., lower mean relative error and higher probability of detection) than the first case with a smaller reconstruction robustness bound.

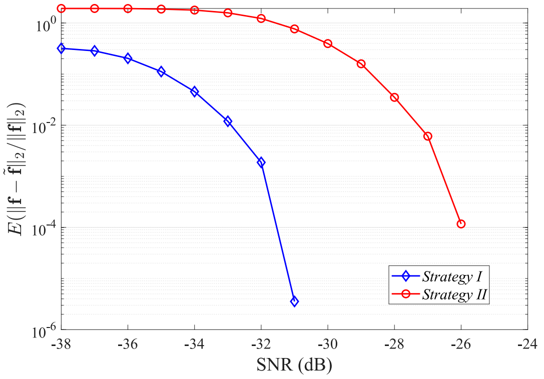

Fig. 4. Mean relative error in terms of various SNR's for the two different sampling strategies.

Furthermore, we compare two different sampling strategies with sampling matrices $\left\{\mathbf{M}_i^{-T}\right\}_{i=1}^{2}$, where $\mathbf{M}_1 = \mathbf{M}\boldsymbol{\Gamma}_1$ and $\mathbf{M}_2 = \mathbf{M}\boldsymbol{\Gamma}_2$ are given as follows. *Strategy I*: $\mathbf{M} = \begin{pmatrix} 96 & 30 \\ 12 & 90 \end{pmatrix}$, $\boldsymbol{\Gamma}_1 = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$, $\boldsymbol{\Gamma}_2 = \begin{pmatrix} 5 & 2 \\ 5 & 3 \end{pmatrix}$; and *Strategy II*: $\mathbf{M} = \begin{pmatrix} 10 & 32 \\ 30 & 4 \end{pmatrix}$, $\boldsymbol{\Gamma}_1 = \begin{pmatrix} 7 & 5 \\ 5 & 7 \end{pmatrix}$, $\boldsymbol{\Gamma}_2 = \begin{pmatrix} 5 & 1 \\ 5 & 4 \end{pmatrix}$. It is easy to see that in each of the two strategies, the moduli do not satisfy the constraint (i.e., (17)) enforced in [23], and $\mathbf{M} = \text{gcld}(\mathbf{M}_1, \mathbf{M}_2)$. In addition, the two strategies possess the same Nyquist sampling density, i.e., share an identical lcrm $\mathbf{R} = \begin{pmatrix} -4782 & 5712 \\ -6894 & 8304 \end{pmatrix}$ with $|\det(\mathbf{R})| = 331200$. According to Theorem 1, the two strategies have reconstruction robustness bounds 23.7171 and 7.9057, respectively. Let $\mathbf{f} = \begin{pmatrix} 810 \\ 1181 \end{pmatrix}$, which simultaneously satisfies $\mathbf{f} \in \mathcal{N}(\mathbf{R})$ and falls into the reconstruction ranges of these two strategies. Figs. 4 and 5 illustrate the performance of the mean relative error and the probability of detection versus various SNR's for the two strategies, respectively, where 2000 trails are implemented for every SNR. As a consequence, *Strategy I* achieves better performance than *Strategy II*, while the sub-Nyquist sampling

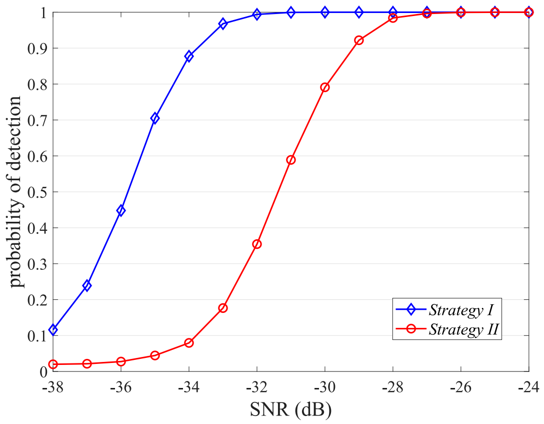

Fig. 5. Probability of detection in terms of various SNR's for the two different sampling strategies.

densities in *Strategy I* are larger than those in *Strategy II*, but far less than the Nyquist sampling density.

As a final comment, the release of the matrix commutativity and coprimeness constraint (used in [23]) on the moduli makes our proposed robust MD-CRT in this paper much more flexible for designing the optimal sampling matrices/lattices to achieve the best undersampling efficiency (e.g., the minimum sampling density as well as maximum robustness against noise). This is of great interest and will be studied in our future work.

VII. Conclusion

In this paper, we investigated the problem of robust reconstructions of an integer vector from the erroneous remainders. We introduced a theoretically well-founded solution to this problem by developing the robust MD-CRT for a general set of moduli that do not necessarily satisfy the strict constraint (i.e., the remaining integer matrices left-divided by a gcld of all the moduli are pairwise commutative and coprime) needed in the previous robust MD-CRT in [23]. Specifically, we first proved a necessary and sufficient condition on the difference between paired remainder errors, as well as a simple sufficient condition on the remainder error bound, for the robust MD-CRT for general moduli, where a closed-form reconstruction algorithm was presented. We then generalized the proposed robust MD-CRT from integer vectors/matrices to real ones. We finally validated the robust MD-CRT for general moduli by conducting numerical simulations, and showed its performance in MD sinusoidal frequency estimation using multiple sub-Nyquist samplers. We believe that beyond MD sinusoidal frequency estimation from undersampled waveforms, the robust MD-CRT will have many other potential applications.

References

[1] D. S. Dummit and R. M. Foote, *Abstract Algebra*. Hoboken, NJ, USA: Wiley, 2004.

[2] H. Krishna, B. Krishna, K.-Y. Lin, and J.-D. Sun, *Computational Number Theory and Digital Signal Processing: Fast Algorithms and Error Control Techniques*. Boca Raton, FL, USA: CRC Press, 1994.

[3] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. Singapore: World Scientific, 1999.

[4] X.-G. Xia and G. Wang, "Phase unwrapping and a robust Chinese remainder theorem," *IEEE Signal Process. Lett.*, vol. 14, no. 4, pp. 247–250, Apr. 2007.

[5] X. W. Li, H. Liang, and X.-G. Xia, "A robust Chinese remainder theorem with its applications in frequency estimation from undersampled waveforms," *IEEE Trans. Signal Process.*, vol. 57, no. 11, pp. 4314–4322, Nov. 2009.

[6] W. J. Wang and X.-G. Xia, "A closed-form robust Chinese remainder theorem and its performance analysis," *IEEE Trans. Signal Process.*, vol. 58, no. 11, pp. 5655–5666, Nov. 2010.

[7] B. Yang, W. J. Wang, X.-G. Xia, and Q. Yin, "Phase detection based range estimation with a dual-band robust Chinese remainder theorem," *Sci. China Inf. Sci.*, vol. 57, no. 2, pp. 1–9, Feb. 2014.

[8] L. Xiao, X.-G. Xia, and W. J. Wang, "Multi-stage robust Chinese remainder theorem," *IEEE Trans. Signal Process.*, vol. 62, no. 18, pp. 4772–4785, Sep. 2014.

[9] W. J. Wang, X. P. Li, W. Wang, and X.-G. Xia, "Maximum likelihood estimation based robust Chinese remainder theorem for real numbers and its fast algorithm," *IEEE Trans. Signal Process.*, vol. 63, no. 13, pp. 3317–3331, Jul. 2015.

[10] L. Xiao, X.-G. Xia, and H. Y. Huo, "Towards robustness in residue number systems," *IEEE Trans. Signal Process.*, vol. 65, no. 6, pp. 1497–1510, Mar. 2017.

[11] L. Xiao and X.-G. Xia, "Frequency determination from truly sub-Nyquist samplers based on robust Chinese remainder theorem," *Signal Process.*, vol. 150, pp. 248–258, Sep. 2018.

[12] M. Ruegg, E. Meier, and D. Nuesch, "Capabilities of dual-frequency millimeter wave SAR with monopulse processing for ground moving target indication," *IEEE Trans. Geosci. Remote Sens.*, vol. 45, no. 3, pp. 539–553, Mar. 2007.

[13] G. Li, J. Xu, Y.-N. Peng, and X.-G. Xia, "Location and imaging of moving targets using nonuniform linear antenna array SAR," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 43, no. 3, pp. 1214–1220, Jul. 2007.

[14] Y. M. Zhang and M. Amin, "MIMO radar exploiting narrowband frequency-hopping waveforms," in *Proc. 16th Eur. Signal Process. Conf. (EUSIPCO)*, Lausanne, Switzerland, 2008, pp. 1–5.

[15] X. W. Li and X.-G. Xia, "Location and imaging of elevated moving target using multi-frequency velocity SAR with cross-track interferometry," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 47, no. 2, pp. 1203–1212, Apr. 2011.

[16] Z. Yuan, Y. Deng, F. Li, R. Wang, G. Liu, and X. Han, "Multichannel InSAR DEM reconstruction through improved closed-form robust Chinese remainder theorem," *IEEE Geosci. Remote Sens. Lett.*, vol. 10, no. 6, pp. 1314–1318, Nov. 2013.

[17] A. Akhlaq, R. G. McKilliam, and R. Subramanian, "Basic construction for range estimation by phase unwrapping," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 2152–2156, Nov. 2015.

[18] I. Fiete, Y. Burak, and T. Brookings, "What grid cells convey about rat location," *J. Neurosci.*, vol. 28, no. 27, pp. 6858–6871, Jul. 2008.

[19] Y. Gong, L. Gan, and H. Liu, "Multi-channel modulo samplers constructed from Gaussian integers," *IEEE Signal Process. Lett.*, vol. 28, pp. 1828–1832, Aug. 2021.

[20] G. Campobello, A. Leonardi, and S. Palazzo, "Improving energy saving and reliability in wireless sensor networks using a simple CRT-based packet-forwarding solution," *IEEE/ACM Trans. Netw.*, vol. 20, no. 1, pp. 191–205, Feb. 2012.

[21] S. Chessa and P. Maestrini, "Robust distributed storage of residue encoded data," *IEEE Trans. Inf. Theory*, vol. 58, no. 12, pp. 7280–7294, Dec. 2012.

[22] Y.-S. Su, "Topology-transparent scheduling via the Chinese remainder theorem," *IEEE/ACM Trans. Netw.*, vol. 23, no. 5, pp. 1416–1429, Oct. 2015.

[23] L. Xiao, X.-G. Xia, and Y.-P. Wang, "Exact and robust reconstructions of integer vectors based on multidimensional Chinese remainder theorem (MD-CRT)," *IEEE Trans. Signal Process.*, vol. 68, pp. 5349–5364, Sep. 2020.

[24] C. C. MacDuffee, *The Theory of Matrices*. New York, NY, USA: Chelsea, 1946.

[25] T. Chen and P. P. Vaidyanathan, "The role of integer matrices in multidimensional multirate systems," *IEEE Trans. Signal Process.*, vol. 41, no. 3, pp. 1035–1047, Mar. 1993.

[26] T. Chen and P. P. Vaidyanathan, "Recent developments in multidimensional multirate systems," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 3, no. 2, pp. 116–137, Apr. 1993.

[27] P. P. Vaidyanathan and P. Pal, "Theory of sparse coprime sensing in multiple dimensions," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3592–3608, Aug. 2011.

[28] D. Micciancio and P. Voulgaris, "A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations," *SIAM J. Comput.*, vol. 42, no. 3, pp. 1364–1391, 2013.

[29] G. Hanrot, X. Pujol, and D. Stehlé, "Algorithms for the shortest and closest lattice vector problems," in *Coding Cryptology* (Lecture Notes in Computer Science 6639), Berlin, Heidelberg: Springer-Verlag, 2011, pp. 159–190.

[30] D. Aggarwal, D. Dadush, and N. Stephens-Davidowitz, "Solving the closest vector problem in 2^n time: The discrete Gaussian strikes again!." in *Proc. IEEE 56th Annu. Symp. Found. Comput. Sci.*, Washington, DC, 2015, pp. 563–582.

[31] C. P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," *Math. Program.*, vol. 66, pp. 181–199, Aug. 1994.

[32] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.0 beta." [Online]. Available: http://cvxr.com/cvx.

[33] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1993.

[34] P. Angeletti, "Proof of unitarity of multidimensional discrete Fourier transform," *Electron. Lett.*, vol. 49, no. 7, pp. 501–503, Mar. 2013.

Li Xiao received the B.S. degree in mathematics from Wuhan University, Wuhan, China, in 2009, the M.S. degree in mathematics from Nankai University, Tianjin, China, in 2012, and the Ph.D. degree in electrical engineering from the University of Delaware, Newark, DE, USA, in 2017. After graduation, he successively held Postdoctoral Fellow and Research Assistant Professor positions in biomedical engineering with Tulane University, New Orleans, USA. In 2021, he joined the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, China, where he is currently a Professor. His research interests include signal processing and machine learning, and their applications to biomedical data analysis.

Haiye Huo received the B.S. degree in mathematics from Xidian University, Xian, China, in 2010, and the M.S. and Ph.D. degrees in mathematics from Nankai University, Tianjin, China, in 2013 and 2016. She is currently an Associate Professor with the School of Mathematics and Computer Sciences, Nanchang University, Nanchang, China. Her research interests include mathematical signal processing.

Xiang-Gen Xia (Fellow, IEEE) received the B.S. degree in mathematics from Nanjing Normal University, Nanjing, China, and the M.S. degree in mathematics from Nankai University, Tianjin, China, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1983, 1986, and 1992, respectively. He was a Senior/Research Staff Member with the Hughes Research Laboratories, Malibu, California, during 1995 to1996. In 1996, he joined with the Department of Electrical and Computer Engineering, University of Delaware, Newark, Delaware, where he is the Charles Black Evans Professor. His research interests include space-time coding, MIMO and OFDM systems, digital signal processing, and SAR and ISAR imaging. He is the author of the book *Modulated Coding for Intersymbol Interference Channels* (New York, Marcel Dekker, 2000), and a co-author of the book *Array Beamforming Enabled Wireless Communications* (New York, CRC Press, 2023). He received the National Science Foundation (NSF) Faculty Early Career Development (CAREER) Program Award in 1997, the Office of Naval Research (ONR) Young Investigator Award in 1998, and the Outstanding Overseas Young Investigator Award from the National Nature Science Foundation of China in 2001. He received the 2019Information Theory Outstanding Overseas Chinese Scientist Award, The Information Theory Society of Chinese Institute of Electronics. He served as an Associate Editor for numerous international journals including IEEE TRANSACTIONS ON SIGNAL PROCESSING, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON MOBILE COMPUTING, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He is a Technical Program Chair of the Signal Processing Symp., Globecom 2007 in Washington DC and the General Co-Chair of ICASSP 2005 in Philadelphia.