Exact and Robust Reconstructions of Integer Vectors Based on Multidimensional Chinese Remainder Theorem (MD-CRT)

Li Xiao, Xiang-Gen Xia, *Fellow, IEEE*, and Yu-Ping Wang, *Senior Member, IEEE*

***Abstract*—The robust Chinese remainder theorem (CRT) has been recently proposed for robustly reconstructing a large nonnegative integer from erroneous remainders. It has found many applications in signal processing, including phase unwrapping, and frequency estimation under sub-Nyquist sampling. Motivated by the applications in multidimensional (MD) signal processing, in this article we propose the MD-CRT and robust MD-CRT for integer vectors. Specifically, by rephrasing the abstract CRT for rings in number-theoretic terms, we first derive the MD-CRT for integer vectors with respect to a general set of integer matrix moduli, which provides an algorithm to uniquely reconstruct an integer vector from its remainders, if it is in the fundamental parallelepiped of the lattice generated by a least common right multiple of all the moduli. For some special forms of moduli, we present explicit reconstruction formulae. Moreover, we derive the robust MD-CRT for integer vectors when the remaining integer matrices of all the moduli left divided by their greatest common left divisor (gcld) are pairwise commutative, and coprime. Two different reconstruction algorithms are proposed, and accordingly, two different conditions on the remainder error bound for the reconstruction robustness are obtained, which are related to a quarter of the minimum distance of the lattice generated by the gcld of all the moduli or the Smith normal form of the gcld.**

***Index Terms*—Chinese remainder theorem (CRT), integer matrices, lattices, multidimensional (MD) frequency estimation, robust CRT, robust MD-CRT.**

I. INTRODUCTION

THE Chinese remainder theorem (CRT) is one of the most fundamental theorems in number theory, and has a long history going back to the 3rd–5th centuries AD [1]–[3]. Basically, the CRT allows to uniquely reconstruct a large nonnegative integer from its remainders with respect to a set of small moduli, if the large integer is less than the least common multiple (lcm) of all the moduli. To date, there has been a surge in work on applying the CRT for partitioning a large task into a number of smaller but independent subtasks, which can be performed in parallel. For example, the CRT has been intensively utilized in the signal processing community in the context of cyclic convolution [4], [5], fast Fourier transform [6], [7], coprime sensor arrays [8]–[11], to name a few. It also finds applications in various other fields, such as computer arithmetic based on modulo operations (e.g., multiplication of very large numbers), coding theory (e.g., residue number system codes), and cryptography (e.g., secret sharing); see [1]–[3] and references therein.

Motivated by the applications of the CRT in phase unwrapping and frequency estimation under sub-Nyquist sampling, a robust remaindering problem has been raised and investigated in [12]–[19]. In these applications, signals are usually subject to noise, and thereby the detected remainders may be erroneous. Two significant questions underlying the robust remaindering problem are: 1) what is the reconstruction range of the large nonnegative integer? and 2) how large can the remainder errors be to ensure the robust reconstruction? It is well-known that the CRT is not robust against remainder errors, i.e., a small error in a remainder may result in a large error in the reconstruction solution. Directly applying the CRT to these applications will thus yield poor performance. Recently, the robust CRT has been proposed in [12]–[14] and further systematically studied in [20]–[24], for solving the robust remaindering problem. The robust CRT demonstrates that even though every remainder has a small error, a large nonnegative integer can be robustly reconstructed in the sense that the reconstruction error is upper bounded by the bound of the remainder errors. Beyond these applications aforementioned, the robust CRT may have or has offered applications in multi-wavelength optical measurement [25]–[27], distance or velocity ambiguity resolution [28]–[31], fault-tolerant wireless sensor networks [32]–[34], error-control neural coding [35]–[37], signal recovery using multi-channel modulo samplers [38], etc. Note that the (robust) CRT has been generalized to (robustly) reconstruct multiple large nonnegative integers from their unordered remainder sets as well [39]–[45]. A thorough review of the robust CRT can be found in [46].

In this article, we extend the CRT and robust CRT for integers to the multidimensional (MD) case, called the MD-CRT and robust MD-CRT for integer vectors, so that they can be utilized in MD signal processing. Note that MD signal processing here refers to true (nonseparable) MD signal processing, since separable MD signal processing is straightforward by handling their

Manuscript received March 24, 2020; revised August 24, 2020; accepted September 8, 2020. Date of publication September 15, 2020; date of current version September 29, 2020. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Pascal Vallet. This work was supported in part by NIH under Grants R01GM109068, R01MH107354, and R01MH104680, and in part by NSF under Grant 1539067. *(Corresponding author: Li Xiao.)*

Li Xiao and Yu-Ping Wang are with the Department of Biomedical Engineering, Tulane University, New Orleans, LA 70118 USA (e-mail: lixiao@udel.edu; wyp@tulane.edu).

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.2020.3023584

1-dimensional counterparts separately along each dimension. First, through rephrasing the abstract CRT for rings in number-theoretic terms, we derive the MD-CRT for integer vectors with respect to a general set of moduli (namely a set of arbitrary nonsingular integer matrices). It is basically that given a set of nonsingular moduli $\{\mathbf{M}_i\}_{i=1}^L$, an integer vector $\mathbf{m} \in \mathcal{N}(\mathbf{R})$ can be uniquely reconstructed from its remainders $\mathbf{r}_i$ for $1 \leq i \leq L$, where $\mathbf{R}$ is a least common right multiple of all the moduli, and $\mathcal{N}(\mathbf{R})$ denotes the set of all integer vectors in the fundamental parallelepiped of the lattice generated by $\mathbf{R}$. A reconstruction algorithm is proposed as well. Notably, the MD-CRT for integer vectors was previously investigated in [47], [48] for a special case when the L moduli are given by $\mathbf{M}_i = \mathbf{U}\mathbf{\Lambda}_i\mathbf{U}^{-1}$ for $1 \leq i \leq L$ with $\mathbf{U}$ being a unimodular matrix and $\mathbf{\Lambda}_i$'s coprime diagonal integer matrices. For some other special forms of moduli, we further obtain explicit reconstruction formulae of the MD-CRT for integer vectors in this article.

Moreover, we derive the robust MD-CRT for integer vectors when the L nonsingular moduli are in the form of $\mathbf{M}_i = \mathbf{M}\mathbf{\Gamma}_i$ for $1 \leq i \leq L$, where $\mathbf{M}$ is an arbitrary integer matrix, and $\mathbf{\Gamma}_i$'s are pairwise commutative and coprime integer matrices. As in the robust CRT for integers [12]–[14], [20]–[24], we attempt to accurately determine all the folding vectors $\mathbf{n}_i$'s (i.e., the quotient vectors of $\mathbf{m}$ left divided by the moduli), and a robust reconstruction of $\mathbf{m}$ can be calculated as the average of the reconstructions obtained from the folding vectors, i.e., $\widetilde{\mathbf{m}} = \frac{1}{L}\sum_{i=1}^L(\mathbf{M}_i\mathbf{n}_i + \widetilde{\mathbf{r}}_i)$, where $\widetilde{\mathbf{r}}_i$ denotes the i-th erroneous remainder. We find that the size of the remainder error bound for the reconstruction robustness depends on the reconstruction algorithm. In other words, different reconstruction algorithms will lead to different conditions on the remainder error bound. We then propose two different reconstruction algorithms, and accordingly, we obtain two different conditions on the remainder error bound for the reconstruction robustness, which are related to a quarter of the minimum distance of the lattice generated by $\mathbf{M}$ or the Smith normal form of $\mathbf{M}$. At the end, we verify the robust MD-CRT for integer vectors by numerical simulations and apply it to MD frequency estimation when a complex MD sinusoidal signal is undersampled using multiple sub-Nyquist sampling matrices.

The rest of this article is organized as follows. In Section II, we recall some background knowledge needed to make this article more self-contained. In Section III, we derive the MD-CRT for integer vectors with respect to a general set of moduli, and provide explicit reconstruction formulae when the moduli are in some special forms. In Section IV, we investigate the robust MD-CRT for integer vectors, and propose two different algorithms for robust reconstruction, resulting in two different conditions on the remainder error bound for the reconstruction robustness. In Section V, we present simulation results of the robust MD-CRT for integer vectors as well as its application to MD sinusoidal frequency estimation with multiple sub-Nyquist samplings. We conclude this article in Section VI.

Notations: Capital and lowercase boldfaced letters are used to denote matrices and vectors, respectively. Let $\mathbb{R}$ and $\mathbb{Z}$ denote the sets of reals and integers, respectively. The transpose, inverse, inverse transpose, and determinant of a matrix $\mathbf{A}$ are denoted as $\mathbf{A}^T$, $\mathbf{A}^{-1}$, $\mathbf{A}^{-T}$, and $\det(\mathbf{A})$, respectively. Given a set of scalars $a_1, a_2, \ldots, a_D$, we denote by $\text{diag}(a_1, a_2, \ldots, a_D)$ the diagonal matrix with a_i being the i-th diagonal element. A D-dimensional vector $\mathbf{a} \in [c, d)^D$ means that every element of $\mathbf{a}$ is in the range of $[c, d)$ and $c, d \in \mathbb{R}$. We denote the (i, j)-th element of a matrix $\mathbf{A}$ as $A(i, j)$, and the i-th element of a vector $\mathbf{a}$ as $a(i)$. The symbols $\mathbf{I}$ and $\mathbf{0}$ denote the identity matrix and the all-zero vector/matrix, respectively, with size determined from context. The relative complement of a set $\mathcal{A}$ with respect to a set $\mathcal{B}$ is written as $\mathcal{B}\backslash\mathcal{A}$. Throughout this article, all matrices are square matrices unless otherwise stated.

II. Preliminaries

The preliminary knowledge involved in this article is mainly related to some fundamental properties in elementary number theory. In this section, we recall general concepts and notations for integer vectors and integer matrices [49]–[53].

i) *Unimodular matrix:* A matrix $\mathbf{U}$ is unimodular if it is an integer matrix and $|\det(\mathbf{U})| = 1$. For any unimodular matrix $\mathbf{U}$, its inverse $\mathbf{U}^{-1}$ is also unimodular because of $\mathbf{U}^{-1} = \text{adj}(\mathbf{U})/\det(\mathbf{U})$ and $|\det(\mathbf{U}^{-1})| = |\det(\mathbf{U})| = 1$, where adj($\mathbf{U}$) stands for the adjugate of $\mathbf{U}$ and is an integer matrix.

ii) *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. Similarly, $\mathbf{A}$ is a right divisor of $\mathbf{M}$ if $\mathbf{M}\mathbf{A}^{-1}$ is an integer matrix.

iii) *Multiple:* A nonsingular integer matrix $\mathbf{A}$ is a left multiple of an integer integer $\mathbf{M}$ if $\mathbf{A} = \mathbf{P}\mathbf{M}$ for some integer matrix $\mathbf{P}$. Similarly, $\mathbf{A}$ is a right multiple of $\mathbf{M}$ if $\mathbf{A} = \mathbf{M}\mathbf{Q}$ for some integer matrix $\mathbf{Q}$.

iv) *Greatest common divisor (gcd):* An integer matrix $\mathbf{A}$ is a common left divisor (cld) of L ($L \geq 2$) integer matrices $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$, if $\mathbf{A}^{-1}\mathbf{M}_i$ is an integer matrix for each $1 \leq i \leq L$. We call $\mathbf{B}$ a greatest common left divisor (gcld) of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$, if any other cld is a left divisor of $\mathbf{B}$. Note that among all cld's, a gcld has the greatest absolute determinant and is unique up to postmultiplication by a unimodular matrix (because if $\mathbf{B}$ is a gcld, so will be $\mathbf{B}\mathbf{U}$ for any unimodular matrix $\mathbf{U}$). Similarly, a common right divisor (crd) and a greatest common right divisor (gcrd) of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$ can be defined, respectively.

v) *Least common multiple (lcm):* A nonsingular integer matrix $\mathbf{A}$ is a common left multiple (clm) of L ($L \geq 2$) integer matrices $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$, if $\mathbf{A} = \mathbf{P}_i\mathbf{M}_i$ for some integer matrix $\mathbf{P}_i$ and each $1 \leq i \leq L$. We call $\mathbf{C}$ a least common left multiple (lclm) of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$, if any other clm is a left multiple of $\mathbf{C}$. Note that among all clm's, an lclm has the smallest absolute determinant and is unique up to premultiplication by a unimodular matrix (because if $\mathbf{C}$ is an lclm, so will be $\mathbf{U}\mathbf{C}$ for any unimodular matrix $\mathbf{U}$). Similarly, a common right multiple (crm) and a least common right multiple (lcrm) of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$ can be defined, respectively.

vi) *Coprimeness:* Two integer matrices $\mathbf{M}$ and $\mathbf{N}$ are said to be left (right) coprime if their gcld (gcrd) is unimodular. In other words, $\mathbf{M}$ and $\mathbf{N}$ are left (right) coprime if they have no cld's (crd's) other than unimodular matrices.

Note that both divisors and multiples above are always taken to be nonsingular integer matrices in this article. Given a $D \times D$ nonsingular integer matrix $\mathbf{M}$, we define $\mathcal{N}(\mathbf{M})$ by

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

The number of elements in $\mathcal{N}(\mathbf{M})$ is equal to $|\det(\mathbf{M})|$ [53]. In the 1-dimensional case (i.e., $D = 1$), letting M be a positive integer, we have $\mathcal{N}(M) = \{0, 1, \dots, M-1\}$.

Then, the integer vector division is defined as follows. A D-dimensional integer vector $\mathbf{m}$ has a unique representation with respect to a $D \times D$ nonsingular integer matrix $\mathbf{M}$ as $\mathbf{m} = \mathbf{M}\mathbf{n} + \mathbf{r}$, or equivalently

$$\mathbf{m} \equiv \mathbf{r} \mod \mathbf{M}, \quad (2)$$

with $\mathbf{r} \in \mathcal{N}(\mathbf{M})$, where $\mathbf{M}$ is viewed as a modulus, and integer vectors $\mathbf{n}$ and $\mathbf{r}$ are the folding vector and remainder of $\mathbf{m}$ with respect to the modulus $\mathbf{M}$, respectively. For simplicity, we write $\mathbf{r}$ in (2) as $\mathbf{r} = \langle \mathbf{m} \rangle_{\mathbf{M}}$. We can compute $\mathbf{r}$ by

$$\mathbf{r} = \mathbf{m} - \mathbf{M}\lfloor \mathbf{M}^{-1}\mathbf{m} \rfloor, \quad (3)$$

i.e., the folding vector $\mathbf{n}$ is computed by $\mathbf{n} = \lfloor \mathbf{M}^{-1}\mathbf{m} \rfloor$, where $\lfloor \cdot \rfloor$ denotes the floor operation that is performed on every element of the vector. Since $\mathbf{M}^{-1}$ is in general a matrix with rational elements, $\lfloor \mathbf{M}^{-1}\mathbf{m} \rfloor$ is subject to round-off errors due to finite precision arithmetic. To this end, an alternative [49] to compute $\mathbf{r}$ is given by

$$\mathbf{r} = \mathbf{M}\left(\operatorname{adj}(\mathbf{M})\mathbf{m} \mod \det(\mathbf{M})\right)/\det(\mathbf{M}), \quad (4)$$

where the modulo operation is performed on every element of $\operatorname{adj}(\mathbf{M})\mathbf{m}$.

It is well known that when the involved matrices in MD signal processing are diagonal, most results in the 1-dimensional case can be straightforwardly extended to the MD case by handling their 1-dimensional counterparts separately. For example, when $\mathbf{M}$ in (2) is diagonal, i.e., $\mathbf{M} = \operatorname{diag}(M_1, M_2, \dots, M_D)$, then (2) is equivalent to $m(i) \equiv r(i) \mod M_i$ for $1 \leq i \leq D$, where $m(i)$ and $r(i)$ denote the i-th elements of $\mathbf{m}$ and $\mathbf{r}$, respectively. The division for integer vectors is therefore reduced to that for integers. However, the involved matrices are usually nondiagonal, and extending the results of 1-dimensional signal processing to the MD case will become nontrivial. The Smith normal form, as a popular tool to diagonalize an integer matrix, has been widely used to simplify several MD signal processing problems; see, for example, [53], [54].

Proposition 1 (The Smith normal form [50]): A $D \times K$ integer matrix $\mathbf{M}$ can be decomposed as

$$\mathbf{UMV} = \begin{cases} \begin{pmatrix} \mathbf{\Lambda} & \mathbf{0} \end{pmatrix} & \text{if } K > D, \\ \mathbf{\Lambda} & \text{if } K = D, \\ \begin{pmatrix} \mathbf{\Lambda} \\ \mathbf{0} \end{pmatrix} & \text{if } K < D, \end{cases} \quad (5)$$

where $\mathbf{U}$ and $\mathbf{V}$ are $D \times D$ and $K \times K$ unimodular matrices, respectively, and $\mathbf{\Lambda}$ is a $\min(K, D) \times \min(K, D)$ diagonal integer matrix, i.e., $\mathbf{\Lambda} = \operatorname{diag}(\lambda_1, \lambda_2, \dots, \lambda_\gamma, 0, \dots, 0)$ with λ_i's being positive integers and γ being the rank of $\mathbf{M}$. Also, λ_i's satisfy $\lambda_i | \lambda_{i+1}$, i.e., λ_i divides λ_{i+1}, for each $1 \leq i \leq \gamma - 1$. Under the conditions, $\mathbf{\Lambda}$ is unique for a given matrix $\mathbf{M}$, while $\mathbf{U}$ and $\mathbf{V}$ are generally not. Moreover, λ_i's are called the invariant factors and can be computed by $\lambda_i = d_i/d_{i-1}$ for $1 \leq i \leq \gamma$, where d_i is the gcd of all $i \times i$ determinantal minors of $\mathbf{M}$ and $d_0 = 1$.

Proposition 2 (The Bezout's theorem [51]): Let $\mathbf{L}$ be a gcld of integer matrices $\mathbf{M}$ and $\mathbf{N}$. Then, there exist integer matrices $\mathbf{P}$ and $\mathbf{Q}$ such that

$$\mathbf{MP} + \mathbf{NQ} = \mathbf{L}. \quad (6)$$

Similarly, let $\mathbf{L}$ be a gcrd of $\mathbf{M}$ and $\mathbf{N}$. Then, there exist integer matrices $\mathbf{P}$ and $\mathbf{Q}$ such that

$$\mathbf{PM} + \mathbf{QN} = \mathbf{L}. \quad (7)$$

In Appendix A, we introduce how to calculate a gcld $\mathbf{L}$ of two given nonsingular $D \times D$ integer matrices $\mathbf{M}$ and $\mathbf{N}$, and the accompanying $\mathbf{P}$ and $\mathbf{Q}$ in (6) in the Bezout's theorem; see [51] for details. Similarly, we can calculate a gcrd $\mathbf{L}$ of $\mathbf{M}$ and $\mathbf{N}$, and the accompanying $\mathbf{P}$ and $\mathbf{Q}$ in (7).

Proposition 3 ([49]): Let $\mathbf{M}$ and $\mathbf{N}$ be two nonsingular integer matrices. When $\mathbf{MN} = \mathbf{NM}$, the following four statements are equivalent: 1) $\mathbf{M}$ and $\mathbf{N}$ are right coprime; 2) $\mathbf{M}$ and $\mathbf{N}$ are left coprime; 3) $\mathbf{MN}$ is an lcrm of $\mathbf{M}$ and $\mathbf{N}$; and 4) $\mathbf{MN}$ is an lclm of $\mathbf{M}$ and $\mathbf{N}$.

Remark 1: As stated in Proposition 3, when $\mathbf{M}$ and $\mathbf{N}$ are commutative, i.e., $\mathbf{MN} = \mathbf{NM}$, their left coprimeness and right coprimeness can imply each other, so we use the simpler term "*coprimeness*". Similarly, when $\mathbf{M}$ and $\mathbf{N}$ are commutative and coprime, their product $\mathbf{MN}$ is both an lcrm and an lclm, so we use the simpler term "*lcm*". For the 1-dimensional case (i.e., integer case), Propositions 2 and 3 are well-known facts.

Given a $D \times D$ nonsingular matrix $\mathbf{M}$ (which is not necessarily an integer matrix), the set of all integer linear combinations of the columns of $\mathbf{M}$, i.e.,

$$\operatorname{LAT}(\mathbf{M}) = \{\mathbf{Mn} \mid \mathbf{n} \text{ is an integer vector}\}, \quad (8)$$

is called the D-dimensional lattice generated by $\mathbf{M}$, denoted as $\operatorname{LAT}(\mathbf{M})$. The fundamental parallelepiped of $\operatorname{LAT}(\mathbf{M})$ is defined as the region:

$$\mathcal{F}_{\operatorname{LAT}(\mathbf{M})} = \left\{\mathbf{Mx} \mid \mathbf{x} \in [0,1)^D\right\}. \quad (9)$$

The shape of $\mathcal{F}_{\operatorname{LAT}(\mathbf{M})}$ defined above depends on the generating matrix $\mathbf{M}$. All lattice cells of $\operatorname{LAT}(\mathbf{M})$ have the same volume equal to $|\det(\mathbf{M})|$ [51]. One can observe that $\mathcal{F}_{\operatorname{LAT}(\mathbf{M})}$ and its shifted copies (i.e., the other lattice cells) constitute the whole real vector space $\mathbb{R}^D$. When $\mathbf{M}$ is a nonsingular integer matrix, we obtain $\mathcal{N}(\mathbf{M}) \subset \mathcal{F}_{\operatorname{LAT}(\mathbf{M})}$ and $\mathcal{N}(\mathbf{M}) = \mathcal{F}_{\operatorname{LAT}(\mathbf{M})} \cap \mathbb{Z}^D$.

Proposition 4 ([52]): Two nonsingular integer matrices $\mathbf{M}$ and $\mathbf{N}$ generate the same lattice, i.e., $\operatorname{LAT}(\mathbf{M}) = \operatorname{LAT}(\mathbf{N})$, if and only if $\mathbf{M} = \mathbf{NP}$, where $\mathbf{P}$ is a unimodular matrix.

Proposition 5 ([52]): Given two nonsingular integer matrices $\mathbf{M}$ and $\mathbf{N}$, let $\mathbf{C}$ be an lcrm of $\mathbf{M}$ and $\mathbf{N}$. Then, $\operatorname{LAT}(\mathbf{C}) = \operatorname{LAT}(\mathbf{M}) \cap \operatorname{LAT}(\mathbf{N})$.

III. MD-CRT FOR INTEGER VECTORS

The well-known CRT for integers allows the reconstruction of a large nonnegative integer from its remainders with respect to a general set of moduli (namely a set of arbitrary positive integers), and it has been successfully applied in 1-dimensional signal processing, cryptography, parallel arithmetic computing, coding theory, etc.; see [1]–[3] and references therein. In this section, as a natural extension of the CRT for integers, the MD-CRT for integer vectors is systematically studied, which provides a reconstruction algorithm for an integer vector from its remainders with respect to a general set of moduli (namely a set of arbitrary nonsingular integer matrices), and possesses potential usefulness in MD signal processing. To begin with, we briefly revisit the CRT for integers as follows.

Proposition 6 (CRT for integers [3]): Given L moduli M_i for $1 \leq i \leq L$, which are arbitrary positive integers, let R be their lcm. For an integer $m \in \mathcal{N}(R)$ (i.e., $0 \leq m < R$), we can uniquely reconstruct m from its remainders $r_i = \langle m \rangle_{M_i}$ as

$$m = \left\langle \sum_{i=1}^{L} W_i \widehat{W}_i r_i \right\rangle_R, \tag{10}$$

where $W_i = R/N_i$, $\widehat{W}_i$ is the modular multiplicative inverse of W_i modulo N_i, i.e., $W_i \widehat{W}_i \equiv 1 \mod N_i$ (or equivalently, $\widehat{W}_i$ is some integer satisfying

$$W_i \widehat{W}_i + N_i Q_i = 1 \tag{11}$$

for some integer Q_i), if $N_i \neq 1$, else $\widehat{W}_i = 0$, and $N_1, N_2, \ldots, N_L$ are taken to be any L pairwise coprime positive integers such that $R = N_1 N_2 \cdots N_L$ and N_i divides M_i for each $1 \leq i \leq L$.

It is worth noting that when the moduli $M_1, M_2, \ldots, M_L$ are pairwise coprime, we can take $N_i = M_i$ for $1 \leq i \leq L$, and then Proposition 6 reduces to the CRT for integers with respect to pairwise coprime moduli.

We next extend the CRT for integers to the integer vector reconstruction problem. We call it the MD-CRT for integer vectors. The non-commutativity of matrix multiplication prevents many results for integers from being clearly established for integer vectors and integer matrices. For this reason, it is necessary to explicitly derive the MD-CRT for integer vectors in this article. Before presenting the main results, we first give the following lemma, which will be used in the sequel.

Lemma 1: Given integer matrices $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$, if $\mathbf{B}$ is an lcrm of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_{L-1}$, and $\mathbf{R}$ is an lcrm of $\mathbf{B}$ and $\mathbf{M}_L$, then $\mathbf{R}$ is an lcrm of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$. In addition, a similar statement holds when lcrm above is replaced with lclm.

Proof: See Appendix B. ■

We then have the following result.

Theorem 1 (MD-CRT for integer vectors): Given L moduli $\mathbf{M}_i$ for $1 \leq i \leq L$, which are arbitrary nonsingular integer matrices, let $\mathbf{R}$ be anyone of their lcrm's. For an integer vector $\mathbf{m} \in \mathcal{N}(\mathbf{R})$, we can uniquely reconstruct $\mathbf{m}$ from its remainders $\mathbf{r}_i = \langle \mathbf{m} \rangle_{\mathbf{M}_i}$.

Proof: Let $\mathbf{G}_1$ and $\mathbf{R}_1$ be a gcld and an lcrm of $\mathbf{M}_1$ and $\mathbf{M}_2$, respectively. Based on the Bezout's theorem in Proposition 2, we have, for some integer matrices $\mathbf{P}_1$ and $\mathbf{P}_2$, $\mathbf{M}_1\mathbf{P}_1 + \mathbf{M}_2\mathbf{P}_2 = \mathbf{G}_1$, on both sides of which we right-multiply $\mathbf{G}_1^{-1}$ and obtain

$$\mathbf{M}_1\mathbf{P}_1\mathbf{G}_1^{-1} + \mathbf{M}_2\mathbf{P}_2\mathbf{G}_1^{-1} = \mathbf{I}. \tag{12}$$

Let

$$\mathbf{m}_1 = \mathbf{M}_2\mathbf{P}_2\mathbf{G}_1^{-1}\mathbf{r}_1 + \mathbf{M}_1\mathbf{P}_1\mathbf{G}_1^{-1}\mathbf{r}_2. \tag{13}$$

We next prove that $\mathbf{m}_1$ given in (13) is a solution of a system of congruences as follows:

$$\begin{cases} \mathbf{m} \equiv \mathbf{r_1} \mod \mathbf{M_1} \\ \mathbf{m} \equiv \mathbf{r}_2 \mod \mathbf{M_2}. \end{cases} \tag{14}$$

From (12), we can rewrite (13) as

$$\begin{aligned} \mathbf{m}_1 &= (\mathbf{I} - \mathbf{M}_1\mathbf{P}_1\mathbf{G}_1^{-1})\mathbf{r}_1 + \mathbf{M}_1\mathbf{P}_1\mathbf{G}_1^{-1}\mathbf{r}_2 \\ &= \mathbf{r}_1 + \mathbf{M}_1\mathbf{P}_1\mathbf{G}_1^{-1}(\mathbf{r}_2 - \mathbf{r}_1). \end{aligned} \tag{15}$$

One can see from (14) that $\mathbf{M}_1\mathbf{n}_1 - \mathbf{M}_2\mathbf{n}_2 = \mathbf{r}_2 - \mathbf{r}_1$ holds for some integer vectors $\mathbf{n}_1$ and $\mathbf{n}_2$, and thus we have $\mathbf{G}_1^{-1}(\mathbf{r}_2 - \mathbf{r}_1) = \mathbf{G}_1^{-1}\mathbf{M}_1\mathbf{n}_1 - \mathbf{G}_1^{-1}\mathbf{M}_2\mathbf{n}_2$. Since $\mathbf{G}_1$ is a gcld of $\mathbf{M}_1$ and $\mathbf{M}_2$, we know that $\mathbf{G}_1^{-1}\mathbf{M}_1$ and $\mathbf{G}_1^{-1}\mathbf{M}_2$ are integer matrices, and thus $\mathbf{G}_1^{-1}(\mathbf{r}_2 - \mathbf{r}_1)$ is an integer vector. Therefore, $\mathbf{m}_1$ given in (13) is an integer vector, and we have, from (15), $\mathbf{m}_1 \equiv \mathbf{r}_1 \mod \mathbf{M_1}$. Similarly, we can rewrite (13) as $\mathbf{m}_1 = \mathbf{r}_2 + \mathbf{M}_2\mathbf{P}_2\mathbf{G}_1^{-1}(\mathbf{r}_1 - \mathbf{r}_2)$, and $\mathbf{m}_1$ given in (13) satisfies $\mathbf{m}_1 \equiv \mathbf{r}_2 \mod \mathbf{M_2}$. That is to say, $\mathbf{m}_1$ given in (13) is a solution of the system of congruences in (14). Thus, we have $\mathbf{m} - \mathbf{m}_1 \in \text{LAT}(\mathbf{M}_1)$ and $\mathbf{m} - \mathbf{m}_1 \in \text{LAT}(\mathbf{M}_2)$. From Proposition 5, we have $\mathbf{m} - \mathbf{m}_1 \in \text{LAT}(\mathbf{R}_1)$, i.e., $\mathbf{m} \equiv \mathbf{m}_1 \mod \mathbf{R_1}$. Based on the cascade architecture of the congruences, we can accordingly calculate a solution $\mathbf{m}_2$ of

$$\begin{cases} \mathbf{m} \equiv \mathbf{m_1} \mod \mathbf{R_1} \\ \mathbf{m} \equiv \mathbf{r}_3 \mod \mathbf{M_3}. \end{cases} \tag{16}$$

Letting $\mathbf{R}_2$ be an lcrm of $\mathbf{R}_1$ and $\mathbf{M}_3$, we have $\mathbf{m} \equiv \mathbf{m}_2 \mod \mathbf{R_2}$. Moreover, from Lemma 1, $\mathbf{R}_2$ is an lcrm of $\mathbf{M}_1, \mathbf{M}_2$, and $\mathbf{M}_3$. Following the above procedure, we merge two congruences at a time until we calculate a solution $\mathbf{m}_{L-1}$ of

$$\begin{cases} \mathbf{m} \equiv \mathbf{m_{L-2}} \mod \mathbf{R_{L-2}} \\ \mathbf{m} \equiv \mathbf{r}_L \mod \mathbf{M_L}, \end{cases} \tag{17}$$

where $\mathbf{R}_{L-2}$ is an lcrm of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_{L-1}$. Let $\mathbf{R}_{L-1}$ be an lcrm of $\mathbf{R}_{L-2}$ and $\mathbf{M}_L$, and we have $\mathbf{m} \equiv \mathbf{m}_{L-1} \mod \mathbf{R_{L-1}}$, where we readily know from Lemma 1 that $\mathbf{R}_{L-1}$ is an lcrm of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$. Without loss of generality, we can let $\mathbf{R}_{L-1} = \mathbf{R}$. So, we can get $\mathbf{m} \in \mathcal{N}(\mathbf{R})$ as

$$\mathbf{m} = \langle \mathbf{m}_{L-1} \rangle_{\mathbf{R}}. \tag{18}$$

Finally, we prove the uniqueness of the solution for $\mathbf{m}$ modulo $\mathbf{R}$. Assume that there exists another solution $\mathbf{m}' \in \mathcal{N}(\mathbf{R})$ that satisfies $\mathbf{r}_i = \langle \mathbf{m}' \rangle_{\mathbf{M}_i}$ for $1 \leq i \leq L$. Let $\mathbf{m}'' = \mathbf{m} - \mathbf{m}'$. We know $\mathbf{m}'' \equiv \mathbf{0} \mod \mathbf{M_i}$ for $1 \leq i \leq L$, that is,

$$\mathbf{m}'' \in \text{LAT}(\mathbf{M}_1) \cap \text{LAT}(\mathbf{M}_1) \cap \cdots \cap \text{LAT}(\mathbf{M}_L) = \text{LAT}(\mathbf{R}), \tag{19}$$

where the last equality is valid due to Proposition 5 and Lemma 1. Hence, we have $\mathbf{m}'' \in \text{LAT}(\mathbf{R})$, i.e.,

$$\mathbf{m}'' = \mathbf{R}\mathbf{k} \text{ for some integer vector } \mathbf{k}. \tag{20}$$

Since $\mathbf{m}, \mathbf{m}' \in \mathcal{N}(\mathbf{R})$ and $\mathbf{m}'' = \mathbf{m} - \mathbf{m}'$, we have

$$\mathbf{m}'' \in \{\mathbf{n} \,|\, \mathbf{n} = \mathbf{R}\mathbf{x}, \mathbf{x} \in (-1, 1)^D \text{ and } \mathbf{n} \in \mathbb{Z}^D\}, \tag{21}$$

where D is the length of $\mathbf{m}''$. Since $\mathbf{R}$ is nonsingular from the definition of lcrm, this implies $\mathbf{k} = \mathbf{0}$ in (20), and thus $\mathbf{m}'' = \mathbf{0}$. The proof is completed. ■

As it can be seen in the proof of Theorem 1, a reconstruction algorithm for the MD-CRT for integer vectors is given as well, which solves the first two congruences, uses that result as the remainder with respect to an lcrm of the first two moduli, and combines this new congruence with the third congruence, and so on. We assume that there exist L pairwise commutative and coprime integer matrices, denoted by $\mathbf{N}_1, \mathbf{N}_2, \ldots, \mathbf{N}_L$, such that $\mathbf{R} = \mathbf{N}_1\mathbf{N}_2\cdots\mathbf{N}_L\mathbf{U}$ for some unimodular matrix $\mathbf{U}$ and $\mathbf{N}_i$ is a left divisor of $\mathbf{M}_i$ for each $1 \leq i \leq L$ in Theorem 1. Under this assumption, we can derive a simple reconstruction formula for the MD-CRT for integer vectors as follows.

Lemma 2: Let $\mathbf{N}_i$ for $1 \leq i \leq L$ be L nonsingular integer matrices, which are pairwise commutative and coprime, i.e., $\mathbf{N}_i\mathbf{N}_j = \mathbf{N}_j\mathbf{N}_i$, and $\mathbf{N}_i$ and $\mathbf{N}_j$ are coprime for each pair of i and j, $1 \leq i \neq j \leq L$. Then, $\mathbf{N}_{i_1}\mathbf{N}_{i_2}\cdots\mathbf{N}_{i_p}$ and $\mathbf{N}_{j_1}\mathbf{N}_{j_2}\cdots\mathbf{N}_{j_q}$ are commutative and coprime for any subsets $\{i_1, i_2, \ldots, i_p\} \subset \{1, 2, \ldots, L\}$ and $\{j_1, j_2, \ldots, j_q\} \subset \{1, 2, \ldots, L\}\backslash\{i_1, i_2, \ldots, i_p\}$. Moreover, $\mathbf{N}_{i_1}\mathbf{N}_{i_2}\cdots\mathbf{N}_{i_p}$ is an lcm of $\mathbf{N}_{i_1}, \mathbf{N}_{i_2}, \ldots, \mathbf{N}_{i_p}$ for any subset $\{i_1, i_2, \ldots, i_p\} \subset \{1, 2, \ldots, L\}$ with $p \geq 2$.

Proof: See Appendix C. ■

Corollary 1: Given L moduli $\mathbf{M}_i$ for $1 \leq i \leq L$, which are arbitrary nonsingular integer matrices, let $\mathbf{R}$ be anyone of their lcrm's. Let us assume that there exist L pairwise commutative and coprime integer matrices, denoted by $\mathbf{N}_1, \mathbf{N}_2, \ldots, \mathbf{N}_L$, such that $\mathbf{R} = \mathbf{N}_1\mathbf{N}_2\cdots\mathbf{N}_L\mathbf{U}$ for some unimodular matrix $\mathbf{U}$ and $\mathbf{N}_i$ is a left divisor of $\mathbf{M}_i$ for each $1 \leq i \leq L$. For an integer vector $\mathbf{m} \in \mathcal{N}(\mathbf{R})$, we can uniquely reconstruct $\mathbf{m}$ from its remainders $\mathbf{r}_i = \langle \mathbf{m} \rangle_{\mathbf{M}_i}$ as

$$\mathbf{m} = \left\langle \sum_{i=1}^{L} \mathbf{W}_i \widehat{\mathbf{W}}_i \mathbf{r}_i \right\rangle_{\mathbf{R}}, \tag{22}$$

where $\mathbf{W}_i = \mathbf{N}_1\cdots\mathbf{N}_{i-1}\mathbf{N}_{i+1}\cdots\mathbf{N}_L$, and if $\mathbf{N}_i$ is not unimodular, $\widehat{\mathbf{W}}_i$ is some integer matrix satisfying

$$\mathbf{W}_i\widehat{\mathbf{W}}_i + \mathbf{N}_i\mathbf{Q}_i = \mathbf{I} \tag{23}$$

for some integer matrix $\mathbf{Q}_i$, and can be calculated by following the procedure (83)–(91) in advance; otherwise $\widehat{\mathbf{W}}_i = \mathbf{0}$.

Proof: See Appendix D. ■

In what follows, let us see in detail some special cases of the MD-CRT for integer vectors, where the L nonsingular moduli are given by

$$\mathbf{M}_i = \mathbf{M}\mathbf{\Gamma}_i \quad \text{for } 1 \leq i \leq L, \tag{24}$$

and $\mathbf{M}$ and $\mathbf{\Gamma}_i$'s here are integer matrices. Clearly, the moduli given by (24) are in general not commutative. For the specific moduli in (24), we first prove the following lemma.

Lemma 3: For the moduli $\mathbf{M}_i$'s in (24), if $\mathbf{A}$ is an lcrm of $\mathbf{\Gamma}_i$ for $1 \leq i \leq L$, then $\mathbf{M}\mathbf{A}$ is an lcrm of $\mathbf{M}_i$ for $1 \leq i \leq L$.

Proof: See Appendix E. ■

Then, we present the following results.

Corollary 2: Given L nonsingular moduli $\mathbf{M}_i = \mathbf{M}\mathbf{\Gamma}_i$ for $1 \leq i \leq L$, where $\mathbf{M}, \mathbf{\Gamma}_1, \mathbf{\Gamma}_2, \ldots, \mathbf{\Gamma}_L$ are pairwise commutative and coprime integer matrices, let $\mathbf{R}$ be anyone of their lcrm's, i.e., $\mathbf{R} = \mathbf{M}\mathbf{\Gamma}_1\mathbf{\Gamma}_2\cdots\mathbf{\Gamma}_L\mathbf{U}$ for any unimodular matrix $\mathbf{U}$. For an integer vector $\mathbf{m} \in \mathcal{N}(\mathbf{R})$, we can uniquely reconstruct $\mathbf{m}$ from its remainders $\mathbf{r}_i = \langle \mathbf{m} \rangle_{\mathbf{M}_i}$ as in Corollary 1.

Proof: See Appendix F. ■

Corollary 3: Given L nonsingular moduli $\mathbf{M}_i = \mathbf{M}\mathbf{\Gamma}_i$ for $1 \leq i \leq L$, where $\mathbf{M}$ is a unimodular matrix, and $\mathbf{\Gamma}_i$'s are pairwise commutative and coprime integer matrices, let $\mathbf{R}$ be anyone of their lcrm's, i.e., $\mathbf{R} = \mathbf{M}\mathbf{\Gamma}_1\mathbf{\Gamma}_2\cdots\mathbf{\Gamma}_L\mathbf{U}$ for any unimodular matrix $\mathbf{U}$. For an integer vector $\mathbf{m} \in \mathcal{N}(\mathbf{R})$, we can uniquely reconstruct $\mathbf{m}$ from its remainders $\mathbf{r}_i = \langle \mathbf{m} \rangle_{\mathbf{M}_i}$ as

$$\mathbf{m} = \left\langle \sum_{i=1}^{L} \mathbf{W}_i \widehat{\mathbf{W}}_i \mathbf{r}_i \right\rangle_{\mathbf{R}}, \tag{25}$$

where $\mathbf{W}_i = \mathbf{M}\mathbf{\Gamma}_1\cdots\mathbf{\Gamma}_{i-1}\mathbf{\Gamma}_{i+1}\cdots\mathbf{\Gamma}_L$, and $\widehat{\mathbf{W}}_i$ is some integer matrix satisfying

$$\mathbf{W}_i\widehat{\mathbf{W}}_i + \mathbf{M}_i\mathbf{Q}_i = \mathbf{I} \tag{26}$$

for some integer matrix $\mathbf{Q}_i$ and can be calculated by following the procedure (83)–(91) in advance.

Proof: See Appendix G. ■

Particularly, when $\mathbf{M}$ is the identity matrix, i.e., $\mathbf{M} = \mathbf{I}$, Corollary 3 reduces to the MD-CRT for integer vectors with respect to pairwise commutative and coprime moduli (which is simply denoted as the CC MD-CRT for integer vectors), as stated below, in comparison with the CRT for integers with respect to pairwise coprime moduli.

Theorem 2 (CC MD-CRT for integer vectors): Given L nonsingular moduli $\mathbf{M}_i$ for $1 \leq i \leq L$, which are pairwise commutative and coprime integer matrices, let $\mathbf{R}$ be anyone of their lcrm's, i.e., $\mathbf{R} = \mathbf{M}_1\mathbf{M}_2\cdots\mathbf{M}_L\mathbf{U}$ for any unimodular matrix $\mathbf{U}$. For an integer vector $\mathbf{m} \in \mathcal{N}(\mathbf{R})$, we can uniquely reconstruct $\mathbf{m}$ from its remainders $\mathbf{r}_i = \langle \mathbf{m} \rangle_{\mathbf{M}_i}$ as in Corollary 3 with $\mathbf{M} = \mathbf{I}$.

We next see another special case of the MD-CRT for integer vectors, where the L nonsingular moduli can be simultaneously diagonalized by using two common unimodular matrices, i.e.,

$$\mathbf{M}_i = \mathbf{U}\mathbf{\Lambda}_i\mathbf{V} \in \mathbb{Z}^{D\times D} \quad \text{for } 1 \leq i \leq L \tag{27}$$

with $\mathbf{\Lambda}_i$'s being diagonal integer matrices, and $\mathbf{U}$ and $\mathbf{V}$ being unimodular matrices. For each $1 \leq i \leq L$, write $\mathbf{\Lambda}_i$ as $\mathbf{\Lambda}_i = \text{diag}(\Lambda_i(1,1), \Lambda_i(2,2), \ldots, \Lambda_i(D,D))$. Let

$$\mathbf{\Lambda} = \text{diag}(\Lambda(1,1), \Lambda(2,2), \ldots, \Lambda(D,D)), \tag{28}$$

and $\Lambda(j,j)$ be the lcm of $\Lambda_1(j,j), \Lambda_2(j,j), \ldots, \Lambda_L(j,j)$ for each $1 \leq j \leq D$. It is readily verified that $\mathbf{\Lambda}$ is an lcm of $\mathbf{\Lambda}_i$'s.

We next prove that $\mathbf{\Lambda}$ is also an lcrm of $\mathbf{\Lambda}_i\mathbf{V}$ for $1 \leq i \leq L$. Since $\mathbf{\Lambda}$ is an lcm of $\mathbf{\Lambda}_i$'s, we have $\mathbf{\Lambda} = \mathbf{\Lambda}_i\mathbf{P}_i$ for some integer matrices $\mathbf{P}_i$'s. Due to the unimodularity of $\mathbf{V}$, we have $\mathbf{\Lambda} = \mathbf{\Lambda}_i\mathbf{V}\mathbf{V}^{-1}\mathbf{P}_i$ and $\mathbf{V}^{-1}\mathbf{P}_i$ is an integer matrix for each $1 \leq i \leq L$. So, $\mathbf{\Lambda}$ is a crm of $\mathbf{\Lambda}_i\mathbf{V}$ for $1 \leq i \leq L$. For any other crm $\mathbf{Q}$ of $\mathbf{\Lambda}_i\mathbf{V}$ for $1 \leq i \leq L$, we have $\mathbf{Q} = \mathbf{\Lambda}_i\mathbf{V}\mathbf{Q}_i$ for some integer matrices $\mathbf{Q}_i$'s, which indicates that $\mathbf{Q}$ is a crm of $\mathbf{\Lambda}_i$'s. Thus, $\mathbf{Q}$ is a right multiple of $\mathbf{\Lambda}$, i.e., $\mathbf{\Lambda}$ is an lcrm of $\mathbf{\Lambda}_i\mathbf{V}$ for $1 \leq i \leq L$. Furthermore, from Lemma 3, we obtain that $\mathbf{U}\mathbf{\Lambda}$ is an lcrm of $\mathbf{M}_i$'s given by (27). Let $\mathbf{R}$ be anyone of the lcrm's of $\mathbf{M}_i$'s, i.e., $\mathbf{R} = \mathbf{U}\mathbf{\Lambda}\mathbf{B}$ for any unimodular matrix $\mathbf{B}$. For an integer vector $\mathbf{m} \in \mathcal{N}(\mathbf{R})$ and its remainders $\mathbf{r}_i = \langle \mathbf{m} \rangle_{\mathbf{M}_i}$, we have

$$\mathbf{m} = \mathbf{U}\mathbf{\Lambda}_i\mathbf{V}\mathbf{n}_i + \mathbf{r}_i \text{ and then } \mathbf{U}^{-1}\mathbf{m} = \mathbf{\Lambda}_i\mathbf{V}\mathbf{n}_i + \mathbf{U}^{-1}\mathbf{r}_i, \tag{29}$$

for $1 \le i \le L$. Due to the unimodularity of $\mathbf{U}$, $\mathbf{U}^{-1}\mathbf{m}$ and $\mathbf{U}^{-1}\mathbf{r}_i$'s are all integer vectors. Hence, we can view (29) as a system of congruences with respect to the moduli $\mathbf{\Lambda}_i$'s, i.e.,

$$\mathbf{U}^{-1}\mathbf{m} \equiv \mathbf{U}^{-1}\mathbf{r}_i \mod \mathbf{\Lambda}_i \quad \text{for } 1 \le i \le L, \tag{30}$$

and then calculate the remainders $\boldsymbol{\zeta}_i \in \mathcal{N}(\mathbf{\Lambda}_i)$ of $\mathbf{U}^{-1}\mathbf{r}_i$ modulo $\mathbf{\Lambda}_i$, i.e., $\mathbf{U}^{-1}\mathbf{r}_i \equiv \boldsymbol{\zeta}_i \mod \mathbf{\Lambda}_i$, for $1 \le i \le L$. From (30), we get

$$\mathbf{U}^{-1}\mathbf{m} \equiv \boldsymbol{\zeta}_i \mod \mathbf{\Lambda}_i \quad \text{for } 1 \le i \le L. \tag{31}$$

Since $\mathbf{U}$ is unimodular and $\mathbf{m} \in \mathcal{N}(\mathbf{U\Lambda B})$ for any unimodular matrix $\mathbf{B}$, we have $\mathbf{U}^{-1}\mathbf{m} \in \mathcal{N}(\mathbf{\Lambda B})$. Furthermore, as $\mathbf{\Lambda}_i$'s are diagonal integer matrices, it is always ready to find L pairwise commutative and coprime integer matrices (i.e., coprime diagonal integer matrices), denoted by $\mathbf{N}_1, \mathbf{N}_2, \ldots, \mathbf{N}_L$, such that $\mathbf{\Lambda} = \mathbf{N}_1\mathbf{N}_2\cdots\mathbf{N}_L$ and $\mathbf{N}_i$ is a left divisor of $\mathbf{\Lambda}_i$ for each $1 \le i \le L$. Therefore, from Corollary 1, we can uniquely reconstruct such $\mathbf{m}$. When $\mathbf{m}$ is restricted to $\mathbf{m} \in \mathcal{N}(\mathbf{U\Lambda})$, i.e., the unimodular matrix $\mathbf{B}$ is taken to be the identity matrix, the reconstruction of $\mathbf{m}$ is equivalent to that via the D independent conventional CRT for integers as follows. Let $\mathbf{a} = \mathbf{U}^{-1}\mathbf{m} \in \mathbb{Z}^D$. Because of $\mathbf{m} \in \mathcal{N}(\mathbf{U\Lambda})$, we obtain $\mathbf{a} \in \mathcal{N}(\mathbf{\Lambda})$. That is to say, every element $a(j)$ of $\mathbf{a}$ satisfies $a(j) \in \mathcal{N}(\Lambda(j,j))$ (i.e., $0 \le a(j) < \Lambda(j,j)$) for $1 \le j \le D$. Therefore, via the CRT for integers, we can uniquely reconstruct $a(j)$ for each $1 \le j \le D$ in the following system of congruences:

$$a(j) \equiv \zeta_i(j) \mod |\Lambda_i(j,j)| \quad \text{for } 1 \le i \le L. \tag{32}$$

Based on the above analysis, we have the following result.

Corollary 4: Let L nonsingular moduli $\mathbf{M}_i$ for $1 \le i \le L$ be given by (27), and $\mathbf{R}$ be anyone of their lcrm's, i.e., $\mathbf{R} = \mathbf{U\Lambda B}$ for any unimodular matrix $\mathbf{B}$, where $\mathbf{\Lambda}$ is given by (28). For an integer vector $\mathbf{m} \in \mathcal{N}(\mathbf{R})$, we can uniquely reconstruct $\mathbf{m}$ from its remainders $\mathbf{r}_i = \langle\mathbf{m}\rangle_{\mathbf{M}_i}$ as in Corollary 1. Interestingly, when $\mathbf{B}$ is the identity matrix, i.e., $\mathbf{R} = \mathbf{U\Lambda}$, the reconstruction of $\mathbf{m} \in \mathcal{N}(\mathbf{R})$ is equivalent to that via the D independent conventional CRT for integers.

In particular, when the $D \times D$ nonsingular moduli $\mathbf{M}_i$'s can be simultaneously diagonalized as

$$\mathbf{M}_i = \mathbf{U\Lambda}_i\mathbf{U}^{-1} \quad \text{for } 1 \le i \le L, \tag{33}$$

where $\mathbf{U}$ is a $D \times D$ unimodular matrix, and $\mathbf{\Lambda}_i$'s are diagonal integer matrices that are pairwise coprime, it is readily verified that the moduli are pairwise commutative and coprime. Note that $\mathbf{\Lambda}_i$ and $\mathbf{\Lambda}_j$ are coprime if and only if their corresponding diagonal elements $\Lambda_i(k,k)$ and $\Lambda_j(k,k)$ are coprime for each $1 \le k \le D$. For this case, as a direct consequence of Theorem 2 or Corollary 4, we obtain the following result, which has been presented in [47], [48].

Corollary 5 ([48]): Let L nonsingular moduli $\mathbf{M}_i$ for $1 \le i \le L$ be given by (33), and $\mathbf{R}$ be anyone of their lcrm's, i.e., $\mathbf{R} = \mathbf{U\Lambda}_1\mathbf{\Lambda}_2\cdots\mathbf{\Lambda}_L\mathbf{B}$ for any unimodular matrix $\mathbf{B}$. For an integer vector $\mathbf{m} \in \mathcal{N}(\mathbf{R})$, we can uniquely reconstruct $\mathbf{m}$ from its remainders $\mathbf{r}_i = \langle\mathbf{m}\rangle_{\mathbf{M}_i}$ as in Theorem 2.

It is worth pointing out that the results of the MD-CRT for integer vectors in this section are closely related to the already established results on the abstract CRT for rings [1]. In the context of the non-commutative ring $\mathbb{Z}^{D\times D}$ of integer matrices, let $\mathcal{M}_i = \mathbf{M}_i\mathbb{Z}^{D\times D}$ for $1 \le i \le L$ be right ideals in $\mathbb{Z}^{D\times D}$, where $\mathbf{M}_i$'s are pairwise left coprime. Let $\mathbb{Z}^{D\times D}/\mathbf{M}_i\mathbb{Z}^{D\times D}$, called the quotient ring of $\mathbb{Z}^{D\times D}$ by $\mathcal{M}_i$, be defined as the set of all cosets of $\mathcal{M}_i$ (i.e., $\mathbb{Z}^{D\times D}/\mathbf{M}_i\mathbb{Z}^{D\times D} = \{\mathbf{R} + \mathcal{M}_i \mid \mathbf{R} \in \mathbb{Z}^{D\times D}\}$). Based on the Bezout's theorem in Proposition 2, there exists a ring isomorphism

$$\mathbb{Z}^{D\times D}/\cap_i \mathcal{M}_i \cong \mathbb{Z}^{D\times D}/\mathcal{M}_1 \oplus \mathbb{Z}^{D\times D}/\mathcal{M}_2 \oplus \cdots \oplus \mathbb{Z}^{D\times D}/\mathcal{M}_L, \tag{34}$$

where $\oplus$ stands for the direct product of rings. Given $\mathbf{A}, \mathbf{B} \in \mathbb{Z}^{D\times D}$, $\mathbf{A}$ is congruent to $\mathbf{B}$ modulo $\mathbf{M}_i$ if and only if $\mathbf{A} - \mathbf{B} \in \mathcal{M}_i$. The elements in $\mathbb{Z}^{D\times D}/\mathcal{M}_i$ can be taken as remainder classes of $\mathbb{Z}^{D\times D}$ modulo $\mathbf{M}_i$. We can rephrase the isomorphism in (34) by stating that the system of congruences modulo $\mathbf{M}_i$'s can be solved uniquely. This result can be correspondingly generalized to the case with arbitrary nonsingular integer matrices $\mathbf{M}_i$'s. As the modulo operation on a matrix is carried out independently along every column of the matrix, the MD-CRT for integer vectors in this article can be regarded as a special case of the abstract CRT in the specific algebraic settings of $\mathbb{Z}^{D\times D}$.

We conclude this section by showing an example to explain how to implement the MD-CRT for integer vectors step by step. Since this example involves a family of 2×2 integer circulant matrices, let us first introduce some existing results for integer circulant matrices. An integer matrix is said to be circulant if each row can be obtained from the preceding row by a right circular shift, e.g., a 2×2 integer circulant matrix $\mathbf{P} = \left(\begin{smallmatrix} p & q \\ q & p \end{smallmatrix}\right)$. It is obvious that integer circulant matrices are commutative with one another. It has been proved in [55], [56] that any two 2×2 integer circulant matrices $\mathbf{P}_1 = \left(\begin{smallmatrix} p_1 & q_1 \\ q_1 & p_1 \end{smallmatrix}\right)$ and $\mathbf{P}_2 = \left(\begin{smallmatrix} p_2 & q_2 \\ q_2 & p_2 \end{smallmatrix}\right)$ are coprime, if and only if $p_1 + q_1$ is coprime with $p_2 + q_2$, and $p_1 - q_1$ is coprime with $p_2 - q_2$. A trivial subclass of 2×2 integer circulant matrices with all equal elements is excluded from consideration in [55], [56] and this article. We then prove that a 2×2 integer circulant matrix $\mathbf{P} = \left(\begin{smallmatrix} p & q \\ q & p \end{smallmatrix}\right)$ with $q \ne 0$ cannot be diagonalized as in (33).

Lemma 4: A 2×2 integer circulant matrix $\mathbf{P} = \left(\begin{smallmatrix} p & q \\ q & p \end{smallmatrix}\right)$ with $q \ne 0$ cannot be diagonalized as $\mathbf{P} = \mathbf{U\Lambda U}^{-1}$, where $\mathbf{U}$ is a 2×2 unimodular matrix and $\mathbf{\Lambda}$ is a diagonal integer matrix.

Proof: See Appendix H. ■

Example 1: Let $L = 3$ moduli be $\mathbf{M}_i = \mathbf{M\Gamma}_i$ for $1 \le i \le 3$, where $\mathbf{\Gamma}_i$'s are pairwise coprime integer circulant matrices, i.e., $\mathbf{\Gamma}_1 = \left(\begin{smallmatrix} 4 & -1 \\ -1 & 4 \end{smallmatrix}\right)$, $\mathbf{\Gamma}_2 = \left(\begin{smallmatrix} 7 & 4 \\ 4 & 7 \end{smallmatrix}\right)$, and $\mathbf{\Gamma}_3 = \left(\begin{smallmatrix} -2 & 6 \\ 6 & -2 \end{smallmatrix}\right)$. We then consider the following two cases that are not covered by [48] or Corollary 5 in this article.

i) $\mathbf{M}$ is commutative and coprime with each $\mathbf{\Gamma}_i$ for $1 \le i \le 3$. This case corresponds to the moduli given in Corollary 2. Without loss of generality, we take $\mathbf{M} = \left(\begin{smallmatrix} 4 & 3 \\ 3 & 4 \end{smallmatrix}\right)$, which is also an integer circulant matrix. One can see that $\mathbf{M}_i$ for $1 \le i \le 3$ in this case are 2×2 integer circulant matrices and their nondiagonal elements are non-zero. Therefore, from Lemma 4, the moduli $\mathbf{M}_i$'s cannot be diagonalized as in (33). Let $\mathbf{R} = \mathbf{M\Gamma}_1\mathbf{\Gamma}_2\mathbf{\Gamma}_3 = \left(\begin{smallmatrix} 402 & 522 \\ 522 & 402 \end{smallmatrix}\right)$ and $\mathbf{m} = \left(\begin{smallmatrix} 402 & 522 \\ 522 & 402 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1/6 \\ 1/2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 328 \\ 288 \end{smallmatrix}\right) \in \mathcal{N}(\mathbf{R})$. The remainders of $\mathbf{m}$

modulo $\mathbf{M}_i$ for $1 \leq i \leq 3$ are calculated from (4), respectively, i.e., $\mathbf{r}_1 = \binom{14}{14}$, $\mathbf{r}_2 = \binom{39}{38}$, and $\mathbf{r}_3 = \binom{14}{14}$. Conversely, we can reconstruct $\mathbf{m}$ from its remainders $\mathbf{r}_i$ for $1 \leq i \leq 3$ via the MD-CRT for integer vectors in Corollary 2. Let $\mathbf{N}_1 = \mathbf{M}\mathbf{\Gamma}_1$, $\mathbf{N}_2 = \mathbf{\Gamma}_2$, and $\mathbf{N}_3 = \mathbf{\Gamma}_3$. Let $\mathbf{W}_1 = \mathbf{N}_2\mathbf{N}_3$, $\mathbf{W}_2 = \mathbf{N}_1\mathbf{N}_3$, and $\mathbf{W}_3 = \mathbf{N}_1\mathbf{N}_2$, and then by following the procedure (83)–(91) to calculate the corresponding $\widehat{\mathbf{W}}_i$ for each $1 \leq i \leq 3$ in the Bezout's theorem such that (23) holds, we get $\widehat{\mathbf{W}}_1 = \left(\begin{smallmatrix} 9 & -3 \\ 23 & -7 \end{smallmatrix}\right)$, $\widehat{\mathbf{W}}_2 = \left(\begin{smallmatrix} 11 & -4 \\ -3 & 1 \end{smallmatrix}\right)$, and $\widehat{\mathbf{W}}_3 = \left(\begin{smallmatrix} -7 & 8 \\ 50 & -57 \end{smallmatrix}\right)$. Then, from the reconstruction formula in (22), we have

$$\begin{aligned}\mathbf{m} &= \left\langle \sum_{i=1}^{3} \mathbf{W}_i \widehat{\mathbf{W}}_i \mathbf{r}_i \right\rangle_{\mathbf{R}} \\ &= \left\langle \begin{pmatrix} 8456 \\ 5096 \end{pmatrix} + \begin{pmatrix} 1196 \\ 15436 \end{pmatrix} + \begin{pmatrix} -8862 \\ -10542 \end{pmatrix} \right\rangle_{\mathbf{R}} \\ &= \left\langle \begin{pmatrix} 790 \\ 9990 \end{pmatrix} \right\rangle_{\mathbf{R}} = \begin{pmatrix} 328 \\ 288 \end{pmatrix}.\end{aligned}$$

ii) $\mathbf{M}$ is an arbitrary nonsingular integer matrix, which is not commutative or coprime with $\mathbf{\Gamma}_i$'s. This case corresponds to the general moduli given in Theorem 1. Without loss of generality, we take $\mathbf{M} = \left(\begin{smallmatrix} 2 & 3 \\ 4 & 5 \end{smallmatrix}\right)$. Obviously, $\mathbf{M}_i$'s are not pairwise commutative, and thus they cannot be diagonalized as in (33). Let $\mathbf{R} = \mathbf{M}\mathbf{\Gamma}_1\mathbf{\Gamma}_2\mathbf{\Gamma}_3 = \left(\begin{smallmatrix} 390 & 270 \\ 654 & 534 \end{smallmatrix}\right)$ and $\mathbf{m} = \left(\begin{smallmatrix} 390 & 270 \\ 654 & 534 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1/2 \\ 1/3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 285 \\ 505 \end{smallmatrix}\right) \in \mathcal{N}(\mathbf{R})$. The remainders of $\mathbf{m}$ modulo $\mathbf{M}_i$ for $1 \leq i \leq 3$ are calculated from (4), respectively, i.e., $\mathbf{r}_1 = \binom{5}{9}$, $\mathbf{r}_2 = \binom{27}{49}$, and $\mathbf{r}_3 = \binom{3}{7}$. Conversely, we can reconstruct $\mathbf{m}$ from its remainders $\mathbf{r}_i$ for $1 \leq i \leq 3$ via the MD-CRT for integer vectors in Theorem 1. In this case, even though we do not have an explicit reconstruction formula as Case i), we can reconstruct $\mathbf{m}$ by following the algorithm exhibited in the proof of Theorem 1. One can readily verify that $\mathbf{M}$ and $\mathbf{R}_1 = \mathbf{M}\mathbf{\Gamma}_1\mathbf{\Gamma}_2$ are a gcld and an lcrm of $\mathbf{M}_1$ and $\mathbf{M}_2$, respectively. Based on the Bezout's theorem in Proposition 2, we follow the procedure (83)–(91) to get $\mathbf{P}_1 = \left(\begin{smallmatrix} 3 & 11 \\ 1 & 4 \end{smallmatrix}\right)$ and $\mathbf{P}_2 = \left(\begin{smallmatrix} -2 & -8 \\ 1 & 4 \end{smallmatrix}\right)$ such that $\mathbf{M}_1\mathbf{P}_1 + \mathbf{M}_2\mathbf{P}_2 = \mathbf{M}$. So, from (13), we obtain $\mathbf{m}_1 = \mathbf{M}_2\mathbf{P}_2\mathbf{M}^{-1}\mathbf{r}_1 + \mathbf{M}_1\mathbf{P}_1\mathbf{M}^{-1}\mathbf{r}_2 = \binom{510}{994}$, which satisfies

$$\begin{cases} \mathbf{m_1} \equiv \mathbf{r_1} \mod \mathbf{M_1} \\ \mathbf{m}_1 \equiv \mathbf{r}_2 \mod \mathbf{M_2}. \end{cases}$$

We then calculate the remainder $\boldsymbol{\nu}_1$ of $\mathbf{m}_1$ modulo $\mathbf{R}_1$, i.e., $\boldsymbol{\nu}_1 = \langle \mathbf{m}_1 \rangle_{\mathbf{R}_1} = \binom{30}{52}$. Following the above procedure, we calculate a solution of a system of congruences:

$$\begin{cases} \mathbf{m} \equiv \boldsymbol{\nu_1} \mod \mathbf{R_1} \\ \mathbf{m} \equiv \mathbf{r}_3 \mod \mathbf{M_3}. \end{cases}$$

It is also readily verified that $\mathbf{M}$ and $\mathbf{R}_2 = \mathbf{R} = \mathbf{M}\mathbf{\Gamma}_1\mathbf{\Gamma}_2\mathbf{\Gamma}_3$ are a gcld and an lcrm of $\mathbf{R}_1$ and $\mathbf{M}_3$, respectively. Based on the Bezout's theorem in Proposition 2, we follow the procedure (83)–(91) to get $\mathbf{Q}_1 = \left(\begin{smallmatrix} 8 & -21 \\ -7 & 18 \end{smallmatrix}\right)$ and $\mathbf{Q}_2 = \left(\begin{smallmatrix} 10 & -24 \\ -18 & 49 \end{smallmatrix}\right)$ such that $\mathbf{R}_1\mathbf{Q}_1 + \mathbf{M}_3\mathbf{Q}_2 = \mathbf{M}$. From (13), we get $\mathbf{m}_2 = \mathbf{M}_3\mathbf{Q}_2\mathbf{M}^{-1}\boldsymbol{\nu}_1 + \mathbf{R}_1\mathbf{Q}_1\mathbf{M}^{-1}\mathbf{r}_3 = \binom{-375}{1429}$. Therefore, we get

$$\mathbf{m} = \langle \mathbf{m}_2 \rangle_{\mathbf{R}_2} = \begin{pmatrix} 285 \\ 505 \end{pmatrix}.$$

IV. Robust MD-CRT for Integer Vectors

In practice, signals of interest are usually subject to noise, and accordingly the detected remainders may be erroneous in many signal processing applications of the CRT. To this end, the robust CRT for integers has been proposed in [12]–[14] and further dedicatedly studied in [20]–[24]. It basically says that even though every remainder has a small error, a large nonnegative integer can be robustly reconstructed in the sense that the reconstruction error is upper bounded by the remainder error bound. In this section, motivated by the applications in MD signal processing, we want to extend the robust CRT for integers to the MD case, called the robust MD-CRT for integer vectors. Before presenting that, we first review the robust CRT for integers in [14], for comparison purposes.

Proposition 7 (Robust CRT for integers [14]): Let L moduli be $M_i = M\Gamma_i$ for $1 \leq i \leq L$, where Γ_i's are pairwise coprime positive integers, and $M > 1$ is an arbitrary positive integer. Let $R \triangleq M\Gamma_1\Gamma_2 \cdots \Gamma_L$ be their lcm. For an integer $m \in \mathcal{N}(R)$ (i.e., $0 \leq m < R$), let r_i's be its remainders, i.e., $r_i = \langle m \rangle_{M_i}$ or

$$m = M_i n_i + r_i \quad \text{for } 1 \leq i \leq L, \tag{35}$$

where n_i's are its folding integers. Let $\tilde{r}_i \triangleq r_i + \triangle r_i$, $1 \leq i \leq L$, denote the erroneous remainders, where $\triangle r_i$'s are the remainder errors. From the erroneous remainders $\tilde{r}_i$'s, we can accurately determine the folding integers n_i's, if and only if

$$-\frac{M}{2} \leq \triangle r_i - \triangle r_1 < \frac{M}{2} \quad \text{for } 2 \leq i \leq L. \tag{36}$$

In addition, let τ be the remainder error bound, i.e., $|\triangle r_i| \leq \tau$ for $1 \leq i \leq L$, and a simple sufficient condition for accurately determining the folding integers n_i's is derived as

$$\tau < \frac{M}{4}. \tag{37}$$

Once the folding integers n_i's are accurately obtained, a robust reconstruction of m can be calculated by

$$\hat{m} = \left[\frac{1}{L} \sum_{i=1}^{L} (M_i n_i + \tilde{r}_i) \right], \tag{38}$$

where $[\cdot]$ denotes the rounding operation. Obviously, the reconstruction error is upper bounded by τ, i.e., $|\hat{m} - m| \leq \tau$.

In [14], a closed-form algorithm for determining the folding integers n_i's in Proposition 7 was proposed as well. For more information on the robust CRT for integers, we refer the reader to a thorough review in [46].

Motivated by Proposition 7 or [14], we propose the robust MD-CRT for integer vectors through accurately determining the folding vectors in the rest of this section. Before that, let us first state two significant definitions related to lattices.

Definition 1 (The shortest vector problem (SVP) on lattices): For a lattice $\mathrm{LAT}(\mathbf{M})$ that is generated by a nonsingular matrix

$\mathbf{M}$, the minimum distance of $\text{LAT}(\mathbf{M})$ is the smallest distance between any two lattice points:

$$\lambda_{\text{LAT}(\mathbf{M})} = \min_{\substack{\mathbf{w},\mathbf{v}\in\text{LAT}(\mathbf{M}),\\ \mathbf{w}\neq\mathbf{v}}} \|\mathbf{w}-\mathbf{v}\|. \tag{39}$$

It is obvious that lattices are closed under addition and subtraction operations. Therefore, the minimum distance of $\text{LAT}(\mathbf{M})$ is equivalently defined as the length (magnitude) of the shortest non-zero lattice point:

$$\lambda_{\text{LAT}(\mathbf{M})} = \min_{\mathbf{v}\in\text{LAT}(\mathbf{M})\backslash\{\mathbf{0}\}} \|\mathbf{v}\|. \tag{40}$$

Definition 2 (The closest vector problem (CVP) on lattices): For a lattice $\text{LAT}(\mathbf{M})$ that is generated by a nonsingular matrix $\mathbf{M}\in\mathbb{R}^{D\times D}$, given an arbitrary point $\mathbf{w}\in\mathbb{R}^D$, we find a closest lattice point of $\text{LAT}(\mathbf{M})$ to $\mathbf{w}$ by

$$\text{dist}(\text{LAT}(\mathbf{M}),\mathbf{w}) = \min_{\mathbf{v}\in\text{LAT}(\mathbf{M})} \|\mathbf{v}-\mathbf{w}\|. \tag{41}$$

The SVP and CVP are the two most important computational problems on lattices. The algorithms for solving these problems either exactly or approximately have been extensively studied [57], [58]. Note that the distance above can be measured by any norm of vectors, e.g., the Euclidean 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 $\|\mathbf{v}\|_\infty=\max_i|v(i)|$.

Let L nonsingular moduli $\mathbf{M}_i\in\mathbb{Z}^{D\times D}$ for $1\leq i\leq L$ be given by

$$\mathbf{M}_i = \mathbf{M}\mathbf{\Gamma}_i, \tag{42}$$

where $\mathbf{\Gamma}_i\in\mathbb{Z}^{D\times D}$ for $1\leq i\leq L$ are pairwise commutative and coprime, and $\mathbf{M}\in\mathbb{Z}^{D\times D}$. Define

$$\mathcal{A}_i=\{\mathbf{m}\in\mathbb{Z}^D \mid \lfloor\mathbf{M}_i^{-1}\mathbf{m}\rfloor\in\mathcal{N}(\mathbf{\Gamma}_1\cdots\mathbf{\Gamma}_{i-1}\mathbf{\Gamma}_{i+1}\cdots\mathbf{\Gamma}_L\mathbf{U}_i)\} \tag{43}$$

for $1\leq i\leq L$, where $\mathbf{U}_i\in\mathbb{Z}^{D\times D}$ is any unimodular matrix. Let $\widetilde{\mathbf{r}}_i=\mathbf{r}_i+\triangle\mathbf{r}_i\in\mathbb{Z}^D$ for $1\leq i\leq L$ be the erroneous remainders of an integer vector $\mathbf{m}$ with respect to the moduli $\mathbf{M}_i$'s, where $\mathbf{r}_i$'s and $\triangle\mathbf{r}_i$'s are the remainders and remainder errors, respectively.

Since $\mathbf{r}_i$'s are the remainders of $\mathbf{m}$ with respect to the moduli $\mathbf{M}_i$'s in (42), we have

$$\begin{cases}\mathbf{m}=\mathbf{M}\mathbf{\Gamma}_1\mathbf{n}_1+\mathbf{r}_1\\ \mathbf{m}=\mathbf{M}\mathbf{\Gamma}_2\mathbf{n}_2+\mathbf{r}_2\\ \quad\vdots\\ \mathbf{m}=\mathbf{M}\mathbf{\Gamma}_L\mathbf{n}_L+\mathbf{r}_L.\end{cases} \tag{44}$$

Without loss of generality, we assume that $\mathbf{m}\in\mathcal{A}_1$. Therefore, we treat the first equation in (44) as a reference to be subtracted from the other $L-1$ equations, and we get

$$\begin{cases}\mathbf{M}\mathbf{\Gamma}_1\mathbf{n}_1-\mathbf{M}\mathbf{\Gamma}_2\mathbf{n}_2=\mathbf{r}_2-\mathbf{r}_1\\ \mathbf{M}\mathbf{\Gamma}_1\mathbf{n}_1-\mathbf{M}\mathbf{\Gamma}_3\mathbf{n}_3=\mathbf{r}_3-\mathbf{r}_1\\ \quad\vdots\\ \mathbf{M}\mathbf{\Gamma}_1\mathbf{n}_1-\mathbf{M}\mathbf{\Gamma}_L\mathbf{n}_L=\mathbf{r}_L-\mathbf{r}_1.\end{cases} \tag{45}$$

Left-multiplying $\mathbf{M}^{-1}$ on both sides of all the equations in (45), we obtain

$$\begin{cases}\mathbf{\Gamma}_1\mathbf{n}_1-\mathbf{\Gamma}_2\mathbf{n}_2=\mathbf{M}^{-1}(\mathbf{r}_2-\mathbf{r}_1)\\ \mathbf{\Gamma}_1\mathbf{n}_1-\mathbf{\Gamma}_3\mathbf{n}_3=\mathbf{M}^{-1}(\mathbf{r}_3-\mathbf{r}_1)\\ \quad\vdots\\ \mathbf{\Gamma}_1\mathbf{n}_1-\mathbf{\Gamma}_L\mathbf{n}_L=\mathbf{M}^{-1}(\mathbf{r}_L-\mathbf{r}_1).\end{cases} \tag{46}$$

From (46), we know that $\mathbf{M}^{-1}(\mathbf{r}_i-\mathbf{r}_1)$ for $2\leq i\leq L$ are integer vectors, i.e.,

$$\mathbf{r}_i-\mathbf{r}_1\in\text{LAT}(\mathbf{M}). \tag{47}$$

We then perform the modulo-$\mathbf{\Gamma}_i$ operation on both sides of the corresponding $(i-1)$-th equation in (46) for $2\leq i\leq L$ to get

$$\begin{cases}\mathbf{\Gamma}_1\mathbf{n}_1\equiv\mathbf{0} \mod \mathbf{\Gamma}_1\\ \mathbf{\Gamma}_1\mathbf{n}_1\equiv\mathbf{M}^{-1}(\mathbf{r}_2-\mathbf{r}_1) \mod \mathbf{\Gamma}_2\\ \mathbf{\Gamma}_1\mathbf{n}_1\equiv\mathbf{M}^{-1}(\mathbf{r}_3-\mathbf{r}_1) \mod \mathbf{\Gamma}_3\\ \quad\vdots\\ \mathbf{\Gamma}_1\mathbf{n}_1\equiv\mathbf{M}^{-1}(\mathbf{r}_L-\mathbf{r}_1) \mod \mathbf{\Gamma}_L,\end{cases} \tag{48}$$

where the first equation is always available.

Since we know the erroneous remainders $\widetilde{\mathbf{r}}_i$'s rather than the remainders $\mathbf{r}_i$'s, we estimate $\mathbf{r}_i-\mathbf{r}_1$ for each $2\leq i\leq L$ by using a closest lattice point $\mathbf{v}_i$ of $\text{LAT}(\mathbf{M})$ to $\widetilde{\mathbf{r}}_i-\widetilde{\mathbf{r}}_1$, i.e.,

$$\mathbf{v}_i\triangleq\arg\min\nolimits_{\mathbf{v}\in\text{LAT}(\mathbf{M})}\|\mathbf{v}-(\widetilde{\mathbf{r}}_i-\widetilde{\mathbf{r}}_1)\|. \tag{49}$$

Let $\widetilde{\mathbf{n}}_i$ for $1\leq i\leq L$ be a set of solutions of (46) when $\mathbf{r}_i-\mathbf{r}_1$ for $2\leq i\leq L$ are replaced with $\mathbf{v}_i$. In summary, we have the following Algorithm 1 for obtaining $\widetilde{\mathbf{n}}_i$'s.

Based on Algorithm 1, we have the following result.

Algorithm 1:

1: Calculate $\mathbf{v}_i$ for $2\leq i\leq L$ in (49) from $\widetilde{\mathbf{r}}_i$ for $1\leq i\leq L$.

2: Calculate the remainder $\boldsymbol{\zeta}_i$ of $\mathbf{M}^{-1}\mathbf{v}_i$ modulo $\mathbf{\Gamma}_i$ for each $2\leq i\leq L$, i.e.,

$$\mathbf{M}^{-1}\mathbf{v}_i\equiv\boldsymbol{\zeta}_i \mod \mathbf{\Gamma}_i, \tag{50}$$

where $\boldsymbol{\zeta}_i\in\mathcal{N}(\mathbf{\Gamma}_i)$.

3: Calculate $\boldsymbol{\chi}_1\triangleq\mathbf{\Gamma}_1\widetilde{\mathbf{n}}_1\in\mathcal{N}(\mathbf{\Gamma}_1\mathbf{\Gamma}_2\cdots\mathbf{\Gamma}_L\mathbf{U}_1)$ via the CC MD-CRT for integer vectors in Theorem 2 from the following system of congruences

$$\begin{cases}\mathbf{\Gamma}_1\widetilde{\mathbf{n}}_1\equiv\mathbf{0} \mod \mathbf{\Gamma}_1\\ \mathbf{\Gamma}_1\widetilde{\mathbf{n}}_1\equiv\boldsymbol{\zeta}_2 \mod \mathbf{\Gamma}_2\\ \mathbf{\Gamma}_1\widetilde{\mathbf{n}}_1\equiv\boldsymbol{\zeta}_3 \mod \mathbf{\Gamma}_3\\ \quad\vdots\\ \mathbf{\Gamma}_1\widetilde{\mathbf{n}}_1\equiv\boldsymbol{\zeta}_L \mod \mathbf{\Gamma}_L.\end{cases} \tag{51}$$

4: Calculate $\widetilde{\mathbf{n}}_1=\mathbf{\Gamma}_1^{-1}\boldsymbol{\chi}_1\in\mathcal{N}(\mathbf{\Gamma}_2\mathbf{\Gamma}_3\cdots\mathbf{\Gamma}_L\mathbf{U}_1)$, and then

$$\widetilde{\mathbf{n}}_i=\mathbf{\Gamma}_i^{-1}(\boldsymbol{\chi}_1-\mathbf{M}^{-1}\mathbf{v}_i) \text{ for } 2\leq i\leq L. \tag{52}$$

Theorem 3 (Robust MD-CRT for integer vectors–I): Let L nonsingular moduli be given by (42). For an integer vector $\mathbf{m}\in$

$\bigcup_{i=1}^{L} \mathcal{A}_i$ (assuming without loss of generality that $\mathbf{m} \in \mathcal{A}_1$), we can accurately determine the folding vectors $\mathbf{n}_i$'s of $\mathbf{m}$ from the erroneous remainders $\widetilde{\mathbf{r}}_i$'s by Algorithm 1, if and only if

$$\boldsymbol{\theta}_i = \mathbf{0} \text{ for } 2 \leq i \leq L, \tag{53}$$

where $\boldsymbol{\theta}_i$ is defined by

$$\boldsymbol{\theta}_i \triangleq \arg\min_{\boldsymbol{\theta} \in \mathrm{LAT}(\mathbf{M})} \|\boldsymbol{\theta} - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\|. \tag{54}$$

Besides, we present two simple sufficient conditions for accurately determining the folding vectors $\mathbf{n}_i$'s as follows.

1) *Condition 1:* A sufficient condition is given by

$$\|\triangle\mathbf{r}_i - \triangle\mathbf{r}_1\| < \frac{\lambda_{\mathrm{LAT}(\mathbf{M})}}{2} \text{ for } 2 \leq i \leq L. \tag{55}$$

2) *Condition 2:* Let τ be the remainder error bound, i.e., $\|\triangle\mathbf{r}_i\| \leq \tau$ for $1 \leq i \leq L$, and then a much simpler sufficient condition is given by

$$\tau < \frac{\lambda_{\mathrm{LAT}(\mathbf{M})}}{4}. \tag{56}$$

Once the folding vectors $\mathbf{n}_i$'s are accurately obtained, a robust reconstruction of $\mathbf{m}$ can be calculated by $\widetilde{\mathbf{m}} = \frac{1}{L}\sum_{i=1}^{L}(\mathbf{M}_i\mathbf{n}_i + \widetilde{\mathbf{r}}_i)$. Obviously, the reconstruction error is upper bounded by τ, i.e.,

$$\|\widetilde{\mathbf{m}} - \mathbf{m}\| \leq \tau. \tag{57}$$

Proof: We first prove the sufficiency. From (49), we have

$$\mathbf{v}_i \triangleq \arg\min_{\mathbf{v} \in \mathrm{LAT}(\mathbf{M})} \|\mathbf{v} - (\mathbf{r}_i - \mathbf{r}_1) - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\| \tag{58}$$

for $2 \leq i \leq L$. As lattices are known to be closed under addition and subtraction operations, we take $\boldsymbol{\theta} = \mathbf{v} - (\mathbf{r}_i - \mathbf{r}_1) \in \mathrm{LAT}(\mathbf{M})$, and then (58) is equivalent to

$$\boldsymbol{\theta}_i \triangleq \arg\min_{\boldsymbol{\theta} \in \mathrm{LAT}(\mathbf{M})} \|\boldsymbol{\theta} - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\| \tag{59}$$

for $2 \leq i \leq L$. If the condition in (53), i.e., $\boldsymbol{\theta}_i = \mathbf{0}$ for $2 \leq i \leq L$, holds, we obtain $\mathbf{v}_i = \mathbf{r}_i - \mathbf{r}_1$ for $2 \leq i \leq L$. Then, from (48) and (51), $\boldsymbol{\Gamma}_1\mathbf{n}_1$ and $\boldsymbol{\Gamma}_1\widetilde{\mathbf{n}}_1$ have the same remainders $\boldsymbol{\zeta}_i$'s with respect to the moduli $\boldsymbol{\Gamma}_i$'s. Due to $\mathbf{m} \in \mathcal{A}_1$ and $\mathbf{n}_1 = \lfloor \mathbf{M}_1^{-1}\mathbf{m} \rfloor$, we obtain $\mathbf{n}_1 \in \mathcal{N}(\boldsymbol{\Gamma}_2\boldsymbol{\Gamma}_3 \cdots \boldsymbol{\Gamma}_L\mathbf{U}_1)$, where $\mathbf{U}_1$ is any unimodular matrix, and thus $\boldsymbol{\Gamma}_1\mathbf{n}_1 \in \mathcal{N}(\boldsymbol{\Gamma}_1\boldsymbol{\Gamma}_2 \cdots \boldsymbol{\Gamma}_L\mathbf{U}_1)$. From (51), $\boldsymbol{\Gamma}_1\mathbf{n}_1$ can be accurately determined by the CC MD-CRT for integer vectors in Theorem 2, so can be $\mathbf{n}_1$, i.e., $\widetilde{\mathbf{n}}_1 = \mathbf{n}_1$. After obtaining $\mathbf{n}_1$, we can accurately determine the other folding vectors $\mathbf{n}_i$ for $2 \leq i \leq L$ by substituting $\mathbf{n}_1$ into (46). Therefore, we get $\widetilde{\mathbf{n}}_i = \mathbf{n}_i$ for $1 \leq i \leq L$ in (52).

We next prove the necessity. Assume that there exists at least one remainder error that does not satisfy (53). For example, the k-th remainder error $\triangle\mathbf{r}_k$ with $2 \leq k \leq L$ satisfies

$$\boldsymbol{\theta}_k \neq \mathbf{0}. \tag{60}$$

Therefore, $\mathbf{v}_k$ in (49) does not equal $\mathbf{r}_k - \mathbf{r}_1$. We then have the following cases.

Case A: There exists one j with $2 \leq j \leq L$ such that

$$\boldsymbol{\theta}_j \notin \mathrm{LAT}(\mathbf{M}\boldsymbol{\Gamma}_j), \tag{61}$$

i.e., $\boldsymbol{\theta}_j \neq \mathbf{M}\boldsymbol{\Gamma}_j\mathbf{k}$ for any integer vector $\mathbf{k}$. We then prove that the remainders of $\mathbf{M}^{-1}\mathbf{v}_j$ and $\mathbf{M}^{-1}(\mathbf{r}_j - \mathbf{r}_1)$ modulo $\boldsymbol{\Gamma}_j$ are different. Assume that $\mathbf{M}^{-1}\mathbf{v}_j$ and $\mathbf{M}^{-1}(\mathbf{r}_j - \mathbf{r}_1)$ have the same remainder modulo $\boldsymbol{\Gamma}_j$, i.e.,

$$\mathbf{M}^{-1}\mathbf{v}_j - \mathbf{M}^{-1}(\mathbf{r}_j - \mathbf{r}_1) = \boldsymbol{\Gamma}_j\mathbf{q} \tag{62}$$

for some integer vector $\mathbf{q}$. Left-multiplying $\mathbf{M}$ on both sides of (62), we get $\mathbf{v}_j - (\mathbf{r}_j - \mathbf{r}_1) = \mathbf{M}\boldsymbol{\Gamma}_j\mathbf{q}$, i.e., $\boldsymbol{\theta}_j = \mathbf{M}\boldsymbol{\Gamma}_j\mathbf{q}$, which contradicts with (61). Therefore, the remainders of $\mathbf{M}^{-1}\mathbf{v}_j$ and $\mathbf{M}^{-1}(\mathbf{r}_j - \mathbf{r}_1)$ modulo $\boldsymbol{\Gamma}_j$ are different. As a consequence, $\boldsymbol{\chi}_1 = \boldsymbol{\Gamma}_1\widetilde{\mathbf{n}}_1$ obtained from the system of congruences in (51) does not equal $\boldsymbol{\Gamma}_1\mathbf{n}_1$ as in (48), and hence $\widetilde{\mathbf{n}}_1 \neq \mathbf{n}_1$.

Case B: For each $2 \leq i \leq L$, $\boldsymbol{\theta}_i \in \mathrm{LAT}(\mathbf{M}\boldsymbol{\Gamma}_i)$ but there exists at least one j with $2 \leq j \leq L$ such that $\boldsymbol{\theta}_j \neq \mathbf{0}$; see, for example, that the k-th remainder error makes $\boldsymbol{\theta}_k \neq \mathbf{0}$ according to (60), i.e., $\mathbf{v}_k \neq \mathbf{r}_k - \mathbf{r}_1$. Since $\mathbf{v}_i = \boldsymbol{\theta}_i + (\mathbf{r}_i - \mathbf{r}_1)$ and $\boldsymbol{\theta}_i \in \mathrm{LAT}(\mathbf{M}\boldsymbol{\Gamma}_i)$ for $2 \leq i \leq L$, we have $\mathbf{M}^{-1}\mathbf{v}_i \equiv \mathbf{M}^{-1}(\mathbf{r}_i - \mathbf{r}_1) \mod \boldsymbol{\Gamma}_i$. So, $\boldsymbol{\Gamma}_1\mathbf{n}_1$ and $\boldsymbol{\Gamma}_1\widetilde{\mathbf{n}}_1$ have the same remainders $\boldsymbol{\zeta}_i$'s with respect to the moduli $\boldsymbol{\Gamma}_i$'s, and $\mathbf{n}_1$ can be accurately determined, i.e., $\widetilde{\mathbf{n}}_1 = \mathbf{n}_1$. However, due to $\mathbf{v}_k \neq \mathbf{r}_k - \mathbf{r}_1$, we have $\widetilde{\mathbf{n}}_k \neq \mathbf{n}_k$ from (52). This proves the necessity.

We finally prove the two simple sufficient conditions in (55) and (56) for accurately determining the folding vectors $\mathbf{n}_i$'s, respectively.

1) *Condition 1:* Assume that there exists $\boldsymbol{\theta}_i \in \mathrm{LAT}(\mathbf{M})$ with $\boldsymbol{\theta}_i \neq \mathbf{0}$ satisfying

$$\boldsymbol{\theta}_i = \arg\min_{\boldsymbol{\theta} \in \mathrm{LAT}(\mathbf{M})} \|\boldsymbol{\theta} - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\| \tag{63}$$

for each $2 \leq i \leq L$. Then, we have

$$\begin{aligned} \|\boldsymbol{\theta}_i\| &= \|\boldsymbol{\theta}_i - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1) - (\mathbf{0} - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1))\| \\ &\leq \|\boldsymbol{\theta}_i - (\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\| + \|\triangle\mathbf{r}_i - \triangle\mathbf{r}_1\| \\ &\leq 2\|\triangle\mathbf{r}_i - \triangle\mathbf{r}_1\| < \lambda_{\mathrm{LAT}(\mathbf{M})}, \end{aligned} \tag{64}$$

which contradicts with $\|\boldsymbol{\theta}_i\| \geq \lambda_{\mathrm{LAT}(\mathbf{M})}$. Thus, we obtain $\boldsymbol{\theta}_i = \mathbf{0}$ for each $2 \leq i \leq L$.

2) *Condition 2:* When $\|\triangle\mathbf{r}_i\| \leq \tau$ for $1 \leq i \leq L$, we have

$$\|\triangle\mathbf{r}_l - \triangle\mathbf{r}_1\| \leq \|\triangle\mathbf{r}_l\| + \|\triangle\mathbf{r}_1\| \leq 2\tau < \frac{\lambda_{\mathrm{LAT}(\mathbf{M})}}{2} \tag{65}$$

for $2 \leq l \leq L$, which implies *Condition 1*.

This completes the proof of the theorem. ∎

Remark 2: In the 1-dimensional case when M is an arbitrary positive integer and Γ_i's are pairwise coprime positive integers, we can readily verify that $i)$ $\mathcal{A}_1 = \mathcal{A}_2 = \cdots = \mathcal{A}_L = \bigcup_{i=1}^{L}\mathcal{A}_i = \mathcal{N}(M\Gamma_1\Gamma_2\cdots\Gamma_L)$, and $ii)$ the conditions in (53) and (55) imply each other, whereas $i)$ and $ii)$ are generally not observed in the MD case. Therefore, in the 1-dimensional case, from Theorem 3, it turns out that $|\triangle r_i - \triangle r_1| < \frac{M}{2}$ for $2 \leq i \leq L$ is a necessary and sufficient condition for accurately determining the folding integers n_i for $1 \leq i \leq L$, which is very similar to the robust CRT for integers in Proposition 7. The only difference is that there is one more equality sign in the left side of (36), which is due to the fact that the rounding operation instead of a norm on $\mathbb{R}$ is used in [14].

Interestingly, we observe that the result of the robust MD-CRT for integer vectors is dependent upon its reconstruction algorithm. Different reconstruction algorithms might bring about different results of the robust MD-CRT for integer vectors. In the following, we propose another reconstruction algorithm, by which a different result of the robust MD-CRT for integer vectors is derived.

By Proposition 1, we first calculate the Smith normal form of $\mathbf{M}$ in (42) as

$$\mathbf{UMV} = \mathbf{\Lambda}, \tag{66}$$

where $\mathbf{U}$ and $\mathbf{V}$ are unimodular matrices, and $\mathbf{\Lambda}$ is a diagonal integer matrix. So, we have $\mathbf{M}^{-1} = \mathbf{V\Lambda}^{-1}\mathbf{U}$. From (46), we get

$$\begin{cases} \mathbf{\Gamma}_1\mathbf{n}_1 - \mathbf{\Gamma}_2\mathbf{n}_2 = \mathbf{V\Lambda}^{-1}\mathbf{U}(\mathbf{r}_2 - \mathbf{r}_1) \\ \mathbf{\Gamma}_1\mathbf{n}_1 - \mathbf{\Gamma}_3\mathbf{n}_3 = \mathbf{V\Lambda}^{-1}\mathbf{U}(\mathbf{r}_3 - \mathbf{r}_1) \\ \qquad\vdots \\ \mathbf{\Gamma}_1\mathbf{n}_1 - \mathbf{\Gamma}_L\mathbf{n}_L = \mathbf{V\Lambda}^{-1}\mathbf{U}(\mathbf{r}_L - \mathbf{r}_1). \end{cases} \tag{67}$$

Left-multiplying $\mathbf{V}^{-1}$ on both sides of all the equations in (67), we obtain

$$\begin{cases} \mathbf{V^{-1}\Gamma_1 n_1} - \mathbf{V^{-1}\Gamma_2 n_2} = \mathbf{\Lambda^{-1}U(r_2 - r_1)} \\ \mathbf{V}^{-1}\mathbf{\Gamma}_1\mathbf{n}_1 - \mathbf{V}^{-1}\mathbf{\Gamma}_3\mathbf{n}_3 = \mathbf{\Lambda}^{-1}\mathbf{U}(\mathbf{r}_3 - \mathbf{r}_1) \\ \qquad\vdots \\ \mathbf{V}^{-1}\mathbf{\Gamma}_1\mathbf{n}_1 - \mathbf{V}^{-1}\mathbf{\Gamma}_L\mathbf{n}_L = \mathbf{\Lambda}^{-1}\mathbf{U}(\mathbf{r}_L - \mathbf{r}_1). \end{cases} \tag{68}$$

We then perform the modulo-$\mathbf{V}^{-1}\mathbf{\Gamma}_i$ operation on both sides of the corresponding $(i-1)$-th equation in (68) for $2 \leq i \leq L$ to obtain

$$\begin{cases} \mathbf{V^{-1}\Gamma_1 n_1} \equiv \mathbf{0} \mod \mathbf{V^{-1}\Gamma_1} \\ \mathbf{V}^{-1}\mathbf{\Gamma}_1\mathbf{n}_1 \equiv \mathbf{\Lambda}^{-1}\mathbf{U}(\mathbf{r}_2 - \mathbf{r}_1) \mod \mathbf{V^{-1}\Gamma_2} \\ \mathbf{V}^{-1}\mathbf{\Gamma}_1\mathbf{n}_1 \equiv \mathbf{\Lambda}^{-1}\mathbf{U}(\mathbf{r}_3 - \mathbf{r}_1) \mod \mathbf{V^{-1}\Gamma_3} \\ \qquad\vdots \\ \mathbf{V}^{-1}\mathbf{\Gamma}_1\mathbf{n}_1 \equiv \mathbf{\Lambda}^{-1}\mathbf{U}(\mathbf{r}_L - \mathbf{r}_1) \mod \mathbf{V^{-1}\Gamma_L}, \end{cases} \tag{69}$$

where the first equation is always available. From Lemma 3, we know that $\mathbf{V}^{-1}\mathbf{\Gamma}_1\mathbf{\Gamma}_2\cdots\mathbf{\Gamma}_L$ is an lcrm of the moduli $\mathbf{V}^{-1}\mathbf{\Gamma}_i$'s in (69). Because of $\mathbf{m} \in \mathcal{A}_1$ and $\mathbf{n}_1 = \lfloor \mathbf{M}_1^{-1}\mathbf{m} \rfloor$, we obtain $\mathbf{n}_1 \in \mathcal{N}(\mathbf{\Gamma}_2\mathbf{\Gamma}_3\cdots\mathbf{\Gamma}_L\mathbf{U}_1)$, where $\mathbf{U}_1$ is any unimodular matrix, and thus $\mathbf{V}^{-1}\mathbf{\Gamma}_1\mathbf{n}_1 \in \mathcal{N}(\mathbf{V}^{-1}\mathbf{\Gamma}_1\mathbf{\Gamma}_2\cdots\mathbf{\Gamma}_L\mathbf{U}_1)$. So, according to Corollary 3, $\mathbf{V}^{-1}\mathbf{\Gamma}_1\mathbf{n}_1$ can be accurately determined by the MD-CRT for integer vectors, so can be $\mathbf{n}_1$.

We estimate $\mathbf{U}(\mathbf{r}_i - \mathbf{r}_1)$ for each $2 \leq i \leq L$ by using a closest lattice point $\mathbf{p}_i$ of LAT$(\mathbf{\Lambda})$ to $\mathbf{U}(\widetilde{\mathbf{r}}_i - \widetilde{\mathbf{r}}_1)$, i.e.,

$$\mathbf{p}_i \triangleq \text{arg min}_{\mathbf{p}\in \text{LAT}(\mathbf{\Lambda})} \|\mathbf{p} - \mathbf{U}(\widetilde{\mathbf{r}}_i - \widetilde{\mathbf{r}}_1)\|. \tag{70}$$

Due to $\mathbf{U}(\mathbf{r}_i - \mathbf{r}_1) \in \text{LAT}(\mathbf{\Lambda})$ and the closeness of addition and subtraction operations on lattices, (70) is equivalent to

$$\boldsymbol{\vartheta}_i \triangleq \text{arg min}_{\boldsymbol{\vartheta}\in \text{LAT}(\mathbf{\Lambda})} \|\boldsymbol{\vartheta} - \mathbf{U}(\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\|. \tag{71}$$

Since the erroneous remainders $\widetilde{\mathbf{r}}_i$'s are known rather than the remainders $\mathbf{r}_i$'s, let $\widetilde{\mathbf{n}}_i$ for $1 \leq i \leq L$ be a set of solutions of (68) when $\mathbf{U}(\mathbf{r}_i - \mathbf{r}_1)$ for $2 \leq i \leq L$ are replaced with $\mathbf{p}_i$. In summary, we have the following Algorithm 2 for obtaining $\widetilde{\mathbf{n}}_i$'s.

Based on Algorithm 2, we have the following result.

Algorithm 2:

1: Calculate $\mathbf{p}_i$ for $2 \leq i \leq L$ in (70) from $\widetilde{\mathbf{r}}_i$ for $1 \leq i \leq L$.

2: Calculate the remainder $\boldsymbol{\varpi}_i$ of $\mathbf{\Lambda}^{-1}\mathbf{p}_i$ modulo $\mathbf{V}^{-1}\mathbf{\Gamma}_i$ for each $2 \leq i \leq L$, i.e.,

$$\mathbf{\Lambda}^{-1}\mathbf{p}_i \equiv \boldsymbol{\varpi}_i \mod \mathbf{V^{-1}\Gamma_i}, \tag{72}$$

where $\boldsymbol{\varpi}_i \in \mathcal{N}(\mathbf{V}^{-1}\mathbf{\Gamma}_i)$.

3: Calculate $\boldsymbol{\psi}_1 \triangleq \mathbf{V}^{-1}\mathbf{\Gamma}_1\widetilde{\mathbf{n}}_1 \in \mathcal{N}(\mathbf{V}^{-1}\mathbf{\Gamma}_1\mathbf{\Gamma}_2\cdots\mathbf{\Gamma}_L\mathbf{U}_1)$ via the MD-CRT for integer vectors in Corollary 3 from the following system of congruences

$$\begin{cases} \mathbf{V^{-1}\Gamma_1\widetilde{n}_1} \equiv \mathbf{0} \mod \mathbf{V^{-1}\Gamma_1} \\ \mathbf{V}^{-1}\mathbf{\Gamma}_1\widetilde{\mathbf{n}}_1 \equiv \boldsymbol{\varpi}_2 \mod \mathbf{V^{-1}\Gamma_2} \\ \mathbf{V}^{-1}\mathbf{\Gamma}_1\widetilde{\mathbf{n}}_1 \equiv \boldsymbol{\varpi}_3 \mod \mathbf{V^{-1}\Gamma_3} \\ \qquad\vdots \\ \mathbf{V}^{-1}\mathbf{\Gamma}_1\widetilde{\mathbf{n}}_1 \equiv \boldsymbol{\varpi}_L \mod \mathbf{V^{-1}\Gamma_L}. \end{cases} \tag{73}$$

4: Calculate $\widetilde{\mathbf{n}}_1 = \mathbf{\Gamma}_1^{-1}\mathbf{V}\boldsymbol{\psi}_1 \in \mathcal{N}(\mathbf{\Gamma}_2\mathbf{\Gamma}_3\cdots\mathbf{\Gamma}_L\mathbf{U}_1)$, and then

$$\widetilde{\mathbf{n}}_i = \mathbf{\Gamma}_i^{-1}\mathbf{V}(\boldsymbol{\psi}_1 - \mathbf{\Lambda}^{-1}\mathbf{p}_i) \text{ for } 2 \leq i \leq L. \tag{74}$$

Theorem 4 (Robust MD-CRT for integer vectors–II): Let L nonsingular moduli be given by (42) and the Smith normal form of $\mathbf{M}$ be given by (66). For an integer vector $\mathbf{m} \in \bigcup_{i=1}^{L}\mathcal{A}_i$ (assuming without loss of generality that $\mathbf{m} \in \mathcal{A}_1$), we can accurately determine the folding vectors $\mathbf{n}_i$'s of $\mathbf{m}$ from the erroneous remainders $\widetilde{\mathbf{r}}_i$'s by Algorithm 2, if and only if

$$\boldsymbol{\vartheta}_i = \mathbf{0} \text{ for } 2 \leq i \leq L. \tag{75}$$

Besides, we present two simple sufficient conditions for accurately determining the folding vectors $\mathbf{n}_i$'s as follows.

1) *Condition 1:* A sufficient condition is given by

$$\|\mathbf{U}(\triangle\mathbf{r}_i - \triangle\mathbf{r}_1)\| < \frac{\lambda_{\text{LAT}(\mathbf{\Lambda})}}{2} \text{ for } 2 \leq i \leq L. \tag{76}$$

2) *Condition 2:* Let τ be the remainder error bound, i.e., $\|\triangle\mathbf{r}_i\| \leq \tau$ for $1 \leq i \leq L$, and then a much simpler sufficient condition is given by

$$\tau < \frac{\lambda_{\text{LAT}(\mathbf{\Lambda})}}{4\|\mathbf{U}\|_*}, \tag{77}$$

where $\|\mathbf{U}\|_*$ stands for the subordinate matrix norm of $\mathbf{U}$ based on the vector norm $\|\cdot\|$, i.e., $\|\mathbf{U}\|_* = \sup_{\|\mathbf{x}\|=1}\{\|\mathbf{Ux}\|\}$.

Once the folding vectors $\mathbf{n}_i$'s are accurately obtained, a robust reconstruction of $\mathbf{m}$ can be calculated by $\widetilde{\mathbf{m}} = \frac{1}{L}\sum_{i=1}^{L}(\mathbf{M}_i\mathbf{n}_i + \widetilde{\mathbf{r}}_i)$. Obviously, the reconstruction error is upper bounded by τ, i.e.,

$$\|\widetilde{\mathbf{m}} - \mathbf{m}\| \leq \tau. \tag{78}$$

On the basis of the above analysis (66)–(71), the proof of Theorem 4 is similar to that of Theorem 3 and is thus omitted here. Let us take a simple example below to show a difference between Theorem 3 and Theorem 4 (between Algorithm 1 and Algorithm 2). Their difference is caused by the non-equivalence of the conditions in (53) and (75).

Example 2: Let $\mathbf{U} = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ be a unimodular matrix, and $\mathbf{M}$ in (42) be $\mathbf{M} = \mathbf{U}^{-1}\mathbf{\Lambda}\mathbf{U}$, where $\mathbf{\Lambda} = \left(\begin{smallmatrix} 8 & 0 \\ 0 & 8 \end{smallmatrix}\right)$. According to Proposition 4, we know

$$\mathrm{LAT}(\mathbf{M}) = \mathrm{LAT}(\mathbf{U}^{-1}\mathbf{\Lambda}) = \mathrm{LAT}\left(\begin{pmatrix} 8 & -8 \\ -8 & 16 \end{pmatrix}\right).$$

Without loss of generality, we consider the first two remainder errors, i.e., $\triangle\mathbf{r}_1$ and $\triangle\mathbf{r}_2$. Let $\triangle\mathbf{r}_2 - \triangle\mathbf{r}_1 \triangleq \left(\begin{smallmatrix} \Delta_1 \\ \Delta_2 \end{smallmatrix}\right)$. Then,

$$\mathbf{U}(\triangle\mathbf{r}_2 - \triangle\mathbf{r}_1) = \begin{pmatrix} 2\Delta_1 + \Delta_2 \\ \Delta_1 + \Delta_2 \end{pmatrix}.$$

In this example, we measure the distance by the Euclidean norm of vectors in $\mathbb{R}^2$. On one hand, let $\Delta_1 = 5$ and $\Delta_2 = -8$. It is ready to verify that $\boldsymbol{\vartheta}_2 = \mathbf{0}$, i.e., the condition in (75) holds for $i = 2$. However, $\boldsymbol{\theta}_2 \neq \mathbf{0}$ in (53), since $\triangle\mathbf{r}_2 - \triangle\mathbf{r}_1$ is much closer to a non-zero lattice point, e.g., $\left(\begin{smallmatrix} 8 \\ -8 \end{smallmatrix}\right)$, of $\mathrm{LAT}(\mathbf{M})$ than to $\mathbf{0}$. On the other hand, let $\Delta_1 = 3$ and $\Delta_2 = 0$. It is ready to verify that $\boldsymbol{\theta}_2 = \mathbf{0}$, i.e., the condition in (53) holds for $i = 2$. However, $\boldsymbol{\vartheta}_2 \neq \mathbf{0}$ in (75), since $\mathbf{U}(\triangle\mathbf{r}_2 - \triangle\mathbf{r}_1)$ is much closer to a non-zero lattice point, e.g., $\left(\begin{smallmatrix} 8 \\ 0 \end{smallmatrix}\right)$, of $\mathrm{LAT}(\mathbf{\Lambda})$ than to $\mathbf{0}$.

We shall make a remark that the MD-CRT and robust MD-CRT for integer vectors studied in this article are different from the generalized CRT and robust generalized CRT for integers in [39]–[45]. In the generalized CRT and robust generalized CRT for integers, every modular is a positive integer and multiple large positive integers are reconstructed from their unordered remainder sets, where an unordered remainder set consists of the remainders of the multiple integers modulo one modular, but the correspondence between the multiple integers and their remainders in the remainder set is unknown. However, in the MD-CRT and robust MD-CRT for integer vectors, every modular is a nonsingular integer matrix and an integer vector is reconstructed from its remainders, where a remainder is an integer vector. In particular, when the moduli $\mathbf{M}_i \in \mathbb{Z}^{D\times D}$ for $1 \leq i \leq L$ are diagonal integer matrices with positive main diagonal elements, i.e., $\mathbf{M}_i = \mathrm{diag}(M_i(1,1), M_i(2,2), \ldots, M_i(D,D))$ with $M_i(j,j) > 0$ for $1 \leq j \leq D$ and $1 \leq i \leq L$, let $\mathbf{R} = \mathrm{diag}(R(1,1), R(2,2), \ldots, R(D,D))$ be their lcrm, where $R(j,j)$ is the lcm of $M_1(j,j), M_2(j,j), \ldots, M_L(j,j)$ for each $1 \leq j \leq D$. Then, reconstruction of an integer vector $\mathbf{m} = (m(1), m(2), \ldots, m(D))^T \in \mathcal{N}(\mathbf{R})$ using the MD-CRT and robust MD-CRT for integer vectors is equivalent to reconstruction of all elements of the integer vector one by one using the CRT and robust CRT for integers, and is also equivalent to reconstruction of all elements of the integer vector using the generalized CRT and robust generalized CRT for integers with ordered remainder sets.

V. Simulation Results

In this section, we first show numerical simulations to verify the robust MD-CRT for integer vectors. We moreover apply the robust MD-CRT for integer vectors to MD frequency estimation when a complex MD sinusoidal signal is undersampled by multiple sub-Nyquist sampling matrices. In all the experiments below, without loss of generality, we consider the robust MD-CRT for integer vectors in Theorem 3 (i.e., Algorithm 1), where the integer vector or frequency to be estimated falls into the range of $\mathcal{A}_1$ with $\mathbf{U}_1 = \mathbf{I}$ in (43), and the vector norm $\|\cdot\|$ is the Euclidean norm, i.e., $\|\cdot\|_2$. In the simulations, we solve the integer quadratic programming problems in (40) and (49) using enumeration [59] and MOSEK with CVX [60], respectively.

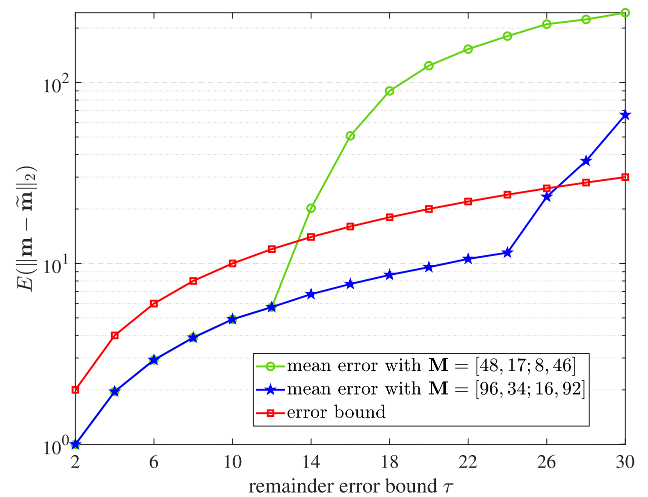

Fig. 1. Mean error and theoretical error bound for the two cases with different $\mathbf{M}$'s.

Let moduli be $\mathbf{M}_i = \mathbf{M}\mathbf{\Gamma}_i$ for $i = 1, 2$, where $\mathbf{\Gamma}_1 = \left(\begin{smallmatrix} 1 & 3 \\ 3 & 1 \end{smallmatrix}\right)$, $\mathbf{\Gamma}_2 = \left(\begin{smallmatrix} 3 & 4 \\ 4 & 3 \end{smallmatrix}\right)$, and two different $\mathbf{M}$'s are considered, given by $\mathbf{M} = \left(\begin{smallmatrix} 48 & 17 \\ 8 & 46 \end{smallmatrix}\right)$ and $\mathbf{M} = 2\left(\begin{smallmatrix} 48 & 17 \\ 8 & 46 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 96 & 34 \\ 16 & 92 \end{smallmatrix}\right)$ for simplicity. We can easily know from [55], [56] that the integer circulant matrices $\mathbf{\Gamma}_1$ and $\mathbf{\Gamma}_2$ are commutative and coprime. According to Theorem 3, the two different $\mathbf{M}$'s lead to two different remainder error bounds $\tau < 48.66/4 = 12.17$ and $\tau < 97.32/4 = 24.33$, respectively. With respect to each of $\mathbf{M}$'s, we uniformly choose the unknown integer vector $\mathbf{m} \in \mathcal{A}_1$ and two remainder errors $\|\triangle\mathbf{r}_1\|_2 \leq \tau$ and $\|\triangle\mathbf{r}_2\|_2 \leq \tau$. In this simulation, we consider the remainder error bounds $\tau = 0, 2, 4, 6, \ldots, 30$, and for each of them, 5000 trials are run. We apply Algorithm 1 to get the estimate $\widetilde{\mathbf{m}}$, and in Fig. 1, we illustrate the mean error $E(\|\mathbf{m} - \widetilde{\mathbf{m}}\|_2)$ in terms of various remainder error bounds. One can observe from Fig. 1 that for both of the two cases with different $\mathbf{M}$'s, all the reconstruction errors are much smaller than the remainder error bound τ, until τ achieves the maximal possible bound. This coincides with the theoretical result in Theorem 3.

Next, we formulate the application of the robust MD-CRT for integer vectors in MD sinusoidal frequency estimation as follows. Without loss of generality, suppose that $\mathbf{f} = \mathbf{m} \in \mathbb{Z}^D$ is an unknown integer MD frequency of interest in a complex MD sinusoidal signal $x(\mathbf{t})$ and may be very high:

$$x(\mathbf{t}) = a\exp(j2\pi\mathbf{f}^T\mathbf{t}) + \omega(\mathbf{t}),\ \mathbf{t} \in \mathbb{R}^D, \tag{79}$$

where a is an unknown non-zero constant and $\omega(\mathbf{t})$ is additive noise. Let $\mathbf{M}_i^{-T}$ for $1 \leq i \leq L$ be L different sampling matrices that have sampling densities $|\det(\mathbf{M}_i)|$, respectively, where each

$\mathbf{M}_i$ is a $D \times D$ nonsingular integer matrix. For each sampling matrix $\mathbf{M}_i^{-T}$, the undersampled sinusoidal signal is given by

$$x_i(\mathbf{n}) = a\exp(j2\pi\mathbf{f}^T\mathbf{M}_i^{-T}\mathbf{n}) + \omega_i(\mathbf{n}),\ \mathbf{n} \in \mathbb{Z}^D. \tag{80}$$

We take the MD discrete Fourier transform (DFT) with respect to $\mathbf{M}_i^T$ [61] for the above $x_i(\mathbf{n})$, $\mathbf{n} \in \mathcal{N}(\mathbf{M}_i^T)$, and we have, for $\mathbf{k} \in \mathcal{N}(\mathbf{M}_i)$,

$$\begin{aligned}
X_i(\mathbf{k}) &= a \sum_{\mathbf{n}\in\mathcal{N}(\mathbf{M}_i^T)} \exp(j2\pi\mathbf{f}^T\mathbf{M}_i^{-T}\mathbf{n})\exp(-j2\pi\mathbf{k}^T\mathbf{M}_i^{-T}\mathbf{n}) \\
&\quad + \Omega_i(\mathbf{k}) \\
&= a \sum_{\mathbf{n}\in\mathcal{N}(\mathbf{M}_i^T)} \exp(-j2\pi(\mathbf{k}-\mathbf{f})^T\mathbf{M}_i^{-T}\mathbf{n}) + \Omega_i(\mathbf{k}) \\
&= a \sum_{\mathbf{n}\in\mathcal{N}(\mathbf{M}_i^T)} \exp(-j2\pi(\mathbf{k}-\mathbf{r}_i)^T\mathbf{M}_i^{-T}\mathbf{n}) + \Omega_i(\mathbf{k}) \\
&= a|\det(\mathbf{M}_i)|\delta(\mathbf{k}-\mathbf{r}_i) + \Omega_i(\mathbf{k}),
\end{aligned} \tag{81}$$

where $\Omega_i(\mathbf{k})$ is the MD DFT of $\omega_i(\mathbf{n})$ with respect to $\mathbf{M}_i^T$, $\mathbf{r}_i$ is the remainder of $\mathbf{f}$ modulo $\mathbf{M}_i$, i.e., $\mathbf{r}_i = \langle\mathbf{f}\rangle_{\mathbf{M}_i}$, and $\delta(\mathbf{n})$ is the MD discrete delta function, i.e., $\delta(\mathbf{n}) = 1$ if $\mathbf{n} = \mathbf{0}$ and $\delta(\mathbf{n}) = 0$ otherwise. Note that the last equation in (81) holds due to the unitarity of the MD DFT [62], i.e., for any nonsingular integer matrix $\mathbf{M} \in \mathbb{Z}^{D\times D}$,

$$\sum_{\mathbf{n}\in\mathcal{N}(\mathbf{M})} \exp(-j2\pi\mathbf{k}^T\mathbf{M}^{-1}\mathbf{n}) = |\det(\mathbf{M})|\delta(\langle\mathbf{k}\rangle_{\mathbf{M}^T})$$
$$\text{for } \mathbf{k} \in \mathbb{Z}^D. \tag{82}$$

Therefore, we can detect the remainder $\mathbf{r}_i$ of $\mathbf{f}$ modulo $\mathbf{M}_i$ (also called the aliased frequency) as a peak in magnitude of the MD DFT domain of $x_i(\mathbf{n})$ in (81), if the signal-to-noise ratio (SNR) is not too low. Nevertheless, when the SNR is not too high, the detected remainder $\widetilde{\mathbf{r}}_i$ is most likely to be erroneous, i.e., $\widetilde{\mathbf{r}}_i \triangleq \mathbf{r}_i + \triangle\mathbf{r}_i \in \mathcal{N}(\mathbf{M}_i)$, where $\triangle\mathbf{r}_i$ is the remainder error. Then, the robust MD-CRT for integer vectors provides an intuitive way to estimate $\mathbf{f}$ from the erroneous remainders $\{\widetilde{\mathbf{r}}_i\}_{i=1}^L$ modulo the corresponding moduli $\{\mathbf{M}_i\}_{i=1}^L$. At this point, the sampling densities ($|\det(\mathbf{M}_i)|$ for $1 \le i \le L$) of the multiple sub-Nyquist samplings may be far less than the Nyquist sampling density that is defined by $|\det(\mathbf{R})|$, where $\mathbf{R}$ is an lcrm of $\{\mathbf{M}_i\}_{i=1}^L$.

We then illustrate the performance of the robust MD-CRT for integer vectors in the application of MD sinusoidal frequency estimation. In this simulation, we adopt the same $\mathbf{M}_i = \mathbf{M}\mathbf{\Gamma}_i$ for $i = 1, 2$ as in the first simulation (i.e., Fig. 1). Specifically, we undersample the sinusoidal signal with two sampling matrices $\mathbf{M}_i^{-T}$ for $i = 1, 2$, followed by two MD DFT's with respect to $\mathbf{M}_i^T$'s on the undersampled sinusoids, respectively, where we facilitate calculating the MD DFT's with respect to $\mathbf{M}_i^T$'s by their equivalent separable MD DFT's [47]. We set $\mathbf{f} = \begin{pmatrix}1645\\1373\end{pmatrix}$ and obviously this frequency belongs to $\mathcal{A}_1$ for both of the two sampling cases with different $\mathbf{M}$'s. The additive noise in (79) is complex white Gaussian noise, i.e., $\omega_i(\mathbf{n}) \sim \mathcal{CN}(0, 2\sigma^2)$ in (80), and the SNR is defined as $\text{SNR} = 10\log_{10}|a|^2/2\sigma^2$ dB. In Fig. 2, we present the probability of detection to illustrate the estimation performance of the robust MD-CRT for integer vectors in terms of various SNR's for the two sampling cases, where the estimated frequency $\mathbf{f}$ is said to be correctly detected if its folding vectors are accurately determined, i.e., a robust estimate of $\mathbf{f}$ is obtained, by Algorithm 1. Fig. 3 shows the mean relative error $E(\|\mathbf{f}-\widetilde{\mathbf{f}}\|_2/\|\mathbf{f}\|_2)$ between the true $\mathbf{f}$ and the reconstruction $\widetilde{\mathbf{f}}$ verse SNR's for the two sampling cases. In these two figures, the SNR is increased from -38 dB to -20 dB and 5000 trials are implemented for each SNR. From Figs. 2 and 3, the sampling case with $\mathbf{M} = \begin{pmatrix}96 & 34\\16 & 92\end{pmatrix}$ achieves better performance (higher probability of detection and lower mean relative error) than the sampling case with $\mathbf{M} = \begin{pmatrix}48 & 17\\8 & 46\end{pmatrix}$, which is in accordance with the theoretical result in Theorem 3 that the former case has a larger robustness bound than the latter case, as mentioned before.

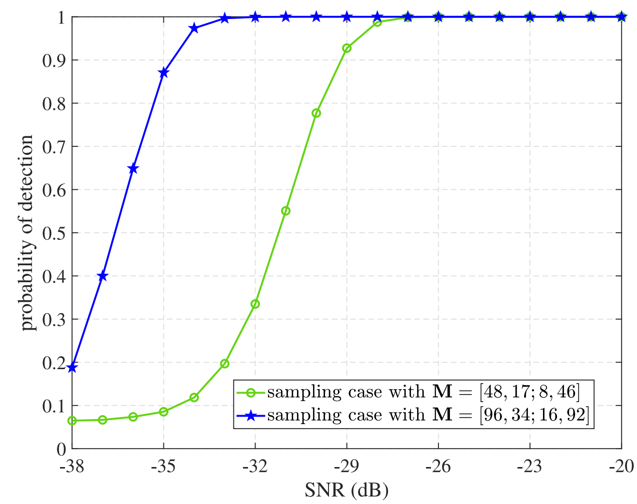

Fig. 2. The probability of detection versus various SNR's for the two sampling cases with different $\mathbf{M}$'s.

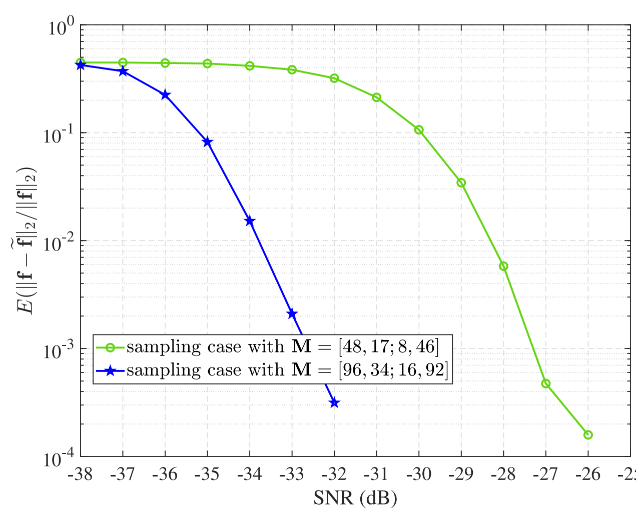

Fig. 3. Mean relative error versus various SNR's for the two sampling cases with different $\mathbf{M}$'s.

As a final comment, general non-separable sampling matrices $\{\mathbf{M}_i\}_{i=1}^L$ may lead to interesting MD signal processing properties as it has been pointed out earlier in the literature, for example, [61], [63].

VI. Conclusion

In this article, the CRT and robust CRT for integers are extended to the MD case, called the MD-CRT and robust MD-CRT for integer vectors, respectively, which are expected to have numerous applications in MD signal processing. Specifically, we first derive the MD-CRT for integer vectors with respect to a general set of moduli (namely a set of arbitrary nonsingular integer matrices), which allows to uniquely reconstruct an integer vector from its remainders, if the integer vector is in the fundamental parallelepiped of the lattice generated by an lcrm of all the moduli. When the moduli are given in some special forms, we further present explicit reconstruction formulae. Furthermore, we provide some results of the robust MD-CRT for integer vectors under the assumption that the remaining integer matrices of all the moduli left divided by their gcld are pairwise commutative and coprime. Accordingly, we propose two different reconstruction algorithms, by which two different conditions on the remainder error bound for the reconstruction robustness are separately obtained and proved to be related to a quarter of the minimum distance of the lattice generated by the gcld of all the moduli or the Smith normal form of the gcld. The robust MD-CRT for integer vectors with respect to a general set of moduli is still an open problem for future research.

Appendix

A. Matrix Computation in the Bezout's theorem

Define $\mathbf{S} = \begin{pmatrix}\mathbf{M}\ \mathbf{N}\end{pmatrix}$, which is a $D \times 2D$ integer matrix of rank D. From Proposition 1, the Smith normal form of $\mathbf{S}$ is

$$\mathbf{U}\begin{pmatrix}\mathbf{M}\ \mathbf{N}\end{pmatrix}\mathbf{V} = \begin{pmatrix}\mathbf{\Lambda}\ \mathbf{0}\end{pmatrix}, \tag{83}$$

where $\mathbf{U}$ and $\mathbf{V}$ are both unimodular matrices of sizes $D \times D$ and $2D \times 2D$, respectively, and $\mathbf{\Lambda}$ is a $D \times D$ diagonal integer matrix. Since $\mathbf{U}^{-1}$ is also unimodular, we can write (83) as

$$\begin{pmatrix}\mathbf{M}\ \mathbf{N}\end{pmatrix}\mathbf{V} = \begin{pmatrix}\mathbf{L}\ \mathbf{0}\end{pmatrix}, \tag{84}$$

where $\mathbf{L} = \mathbf{U}^{-1}\mathbf{\Lambda}$ is a $D \times D$ integer matrix. Partitioning the $2D \times 2D$ unimodular matrix $\mathbf{V}$ into $D \times D$ blocks, we have

$$\begin{pmatrix}\mathbf{M}\ \mathbf{N}\end{pmatrix}\underbrace{\begin{pmatrix}\mathbf{V_{11}} & \mathbf{V}_{12}\\ \mathbf{V}_{21} & \mathbf{V}_{22}\end{pmatrix}}_{\mathbf{V}} = \begin{pmatrix}\mathbf{L}\ \mathbf{0}\end{pmatrix}. \tag{85}$$

This implies

$$\mathbf{M}\mathbf{V}_{11} + \mathbf{N}\mathbf{V}_{21} = \mathbf{L}. \tag{86}$$

By rewriting (84) as

$$\begin{pmatrix}\mathbf{M}\ \mathbf{N}\end{pmatrix} = \begin{pmatrix}\mathbf{L}\ \mathbf{0}\end{pmatrix}\underbrace{\begin{pmatrix}\mathbf{K_{11}} & \mathbf{K}_{12}\\ \mathbf{K}_{21} & \mathbf{K}_{22}\end{pmatrix}}_{\mathbf{V}^{-1}}, \tag{87}$$

we have $\mathbf{M} = \mathbf{L}\mathbf{K}_{11}$ and $\mathbf{N} = \mathbf{L}\mathbf{K}_{12}$, where $\mathbf{K}_{ij}$ for $1 \le i, j \le 2$ are all integer matrices due to the unimodularity of $\mathbf{V}$. Therefore, $\mathbf{L}$ is a cld of $\mathbf{M}$ and $\mathbf{N}$. Then, we demonstrate that $\mathbf{L}$ is actually a gcld of $\mathbf{M}$ and $\mathbf{N}$. For any other cld $\mathbf{T}$ of $\mathbf{M}$ and $\mathbf{N}$, i.e., $\mathbf{M} = \mathbf{T}\mathbf{A}$ and $\mathbf{N} = \mathbf{T}\mathbf{B}$ for some integer matrices $\mathbf{A}$ and $\mathbf{B}$, we have, from (86), $\mathbf{T}(\mathbf{A}\mathbf{V}_{11} + \mathbf{B}\mathbf{V}_{21}) = \mathbf{L}$, which means that $\mathbf{T}$ is a left divisor of $\mathbf{L}$. Therefore, $\mathbf{L}$ is a gcld of $\mathbf{M}$ and $\mathbf{N}$, and is given by

$$\mathbf{L} = \mathbf{U}^{-1}\mathbf{\Lambda}. \tag{88}$$

From (86), the integer matrices $\mathbf{P}$ and $\mathbf{Q}$ in (6) are given by

$$\mathbf{P} = \mathbf{V}_{11} \text{ and } \mathbf{Q} = \mathbf{V}_{21}. \tag{89}$$

In particular, if $\mathbf{M}$ and $\mathbf{N}$ are left coprime, their gcld $\mathbf{L}$ must be unimodular. We right-multiply $\mathbf{L}^{-1}$ on both sides of (86), and can further get

$$\mathbf{M}\mathbf{V}_{11}\mathbf{L}^{-1} + \mathbf{N}\mathbf{V}_{21}\mathbf{L}^{-1} = \mathbf{I}. \tag{90}$$

This equation is called the Bezout's identity. In this case, $\mathbf{I}$ is viewed as a gcld of $\mathbf{M}$ and $\mathbf{N}$, and the integer matrices $\mathbf{P}$ and $\mathbf{Q}$ in (6) in the Bezout's identity are

$$\mathbf{P} = \mathbf{V}_{11}\mathbf{L}^{-1} = \mathbf{V}_{11}\mathbf{\Lambda}^{-1}\mathbf{U} \text{ and } \mathbf{Q} = \mathbf{V}_{21}\mathbf{L}^{-1} = \mathbf{V}_{21}\mathbf{\Lambda}^{-1}\mathbf{U}. \tag{91}$$

B. Proof of Lemma 1

It is obvious that $\mathbf{R}$ is a crm of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$. Then, for any other crm $\mathbf{C}$ of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$, we have $\mathbf{C} = \mathbf{M}_L\mathbf{Q}$ for some integer matrix $\mathbf{Q}$. Moreover, since $\mathbf{C}$ is a crm of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_{L-1}$, and $\mathbf{B}$ is an lcrm of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_{L-1}$, we know that $\mathbf{C}$ is a right multiple of $\mathbf{B}$, i.e., $\mathbf{C} = \mathbf{B}\mathbf{P}$ for some integer matrix $\mathbf{P}$. Thus, $\mathbf{C}$ is a crm of $\mathbf{B}$ and $\mathbf{M}_L$. Since $\mathbf{R}$ is an lcrm of $\mathbf{B}$ and $\mathbf{M}_L$, $\mathbf{C}$ is known as a right multiple of $\mathbf{R}$, i.e., $\mathbf{C} = \mathbf{R}\mathbf{A}$ for some integer matrix $\mathbf{A}$. Therefore, $\mathbf{R}$ is an lcrm of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$. Similarly, we can prove that if $\mathbf{B}$ is an lclm of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_{L-1}$, and $\mathbf{R}$ is an lclm of $\mathbf{B}$ and $\mathbf{M}_L$, then $\mathbf{R}$ is an lclm of $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$.

C. Proof of Lemma 2

As $\mathbf{N}_1, \mathbf{N}_2, \ldots, \mathbf{N}_L$ are pairwise commutative, we immediately verify the commutativity of $\mathbf{N}_{i_1}\mathbf{N}_{i_2}\cdots\mathbf{N}_{i_p}$ and $\mathbf{N}_{j_1}\mathbf{N}_{j_2}\cdots\mathbf{N}_{j_q}$. We next prove their coprimeness. For easy of presentation, we first look at a simple case when $L = 3$. In this case, we need to prove without loss of generality that $\mathbf{N}_1\mathbf{N}_2$ and $\mathbf{N}_3$ are coprime. Let $\mathbf{D}$ be a gcrd of $\mathbf{N}_1\mathbf{N}_2$ and $\mathbf{N}_3$. Since $\mathbf{N}_1$ and $\mathbf{N}_3$ are coprime, from the Bezout's theorem in Proposition 2 we have, for some integer matrices $\mathbf{P}$ and $\mathbf{Q}$, $\mathbf{P}\mathbf{N}_1 + \mathbf{Q}\mathbf{N}_3 = \mathbf{I}$, on both sides of which we right-multiply $\mathbf{N}_2\mathbf{D}^{-1}$, and then commute $\mathbf{N}_2$ and $\mathbf{N}_3$ to get $\mathbf{P}\mathbf{N}_1\mathbf{N}_2\mathbf{D}^{-1} + \mathbf{Q}\mathbf{N}_2\mathbf{N}_3\mathbf{D}^{-1} = \mathbf{N}_2\mathbf{D}^{-1}$. Since $\mathbf{D}$ is a gcrd of $\mathbf{N}_1\mathbf{N}_2$ and $\mathbf{N}_3$, we know that $\mathbf{N}_2\mathbf{D}^{-1}$ is an integer matrix. That is to say, $\mathbf{D}$ is a right divisor of $\mathbf{N}_2$. As stated above, $\mathbf{D}$ is a right divisor of $\mathbf{N}_3$, and $\mathbf{N}_2$ and $\mathbf{N}_3$ are coprime. So, $\mathbf{D}$ must be a unimodular matrix. Thus, $\mathbf{N}_1\mathbf{N}_2$ and $\mathbf{N}_3$ are right coprime (equivalently coprime from Proposition 3 and their commutativity). Accordingly, the above result can be readily generalized to the case when $L > 3$, and therefore, $\mathbf{N}_{i_1}\mathbf{N}_{i_2}\cdots\mathbf{N}_{i_p}$ and $\mathbf{N}_{j_1}\mathbf{N}_{j_2}\cdots\mathbf{N}_{j_q}$ are coprime.

In addition, based on Proposition 3 and the above result, we know that $\mathbf{R}_2 \triangleq \mathbf{N}_{i_1}\mathbf{N}_{i_2}$ is an lcm of $\mathbf{N}_{i_1}$ and $\mathbf{N}_{i_2}$, and $\mathbf{R}_2$

is commutative and coprime with $\mathbf{N}_{i_3}$. So, $\mathbf{R}_3 \triangleq \mathbf{R}_2\mathbf{N}_{i_3} = \mathbf{N}_{i_1}\mathbf{N}_{i_2}\mathbf{N}_{i_3}$ is an lcm of $\mathbf{R}_2$ and $\mathbf{N}_{i_3}$, and $\mathbf{R}_3$ is commutative and coprime with $\mathbf{N}_{i_4}$. Moreover, $\mathbf{R}_3$ is an lcrm of $\mathbf{N}_{i_1}, \mathbf{N}_{i_2}$, and $\mathbf{N}_{i_3}$ from Lemma 1. Continue this procedure until $\mathbf{R}_p \triangleq \mathbf{R}_{p-1}\mathbf{N}_{i_p} = \mathbf{N}_{i_1}\mathbf{N}_{i_2}\cdots\mathbf{N}_{i_p}$ is an lcm of $\mathbf{R}_{p-1}$ and $\mathbf{N}_{i_p}$. From Lemma 1, $\mathbf{R}_p$ is an lcrm of $\mathbf{N}_{i_1}, \mathbf{N}_{i_2}, \ldots, \mathbf{N}_{i_p}$, and similarly, we can deduce that $\mathbf{R}_p$ is also an lclm of $\mathbf{N}_{i_1}, \mathbf{N}_{i_2}, \ldots, \mathbf{N}_{i_p}$.

D. Proof of Corollary 1

Since $\mathbf{N}_i$ is a left divisor of $\mathbf{M}_i$ for each $1 \le i \le L$, there exists some integer matrix $\mathbf{P}_i$ such that $\mathbf{M}_i = \mathbf{N}_i\mathbf{P}_i$ for each $1 \le i \le L$. So, from the remainders $\mathbf{r}_i = \langle \mathbf{m} \rangle_{\mathbf{M}_i}$, we have

$$\mathbf{m} = \mathbf{N}_i\mathbf{P}_i\mathbf{n}_i + \mathbf{r}_i \quad \text{for } 1 \le i \le L, \tag{92}$$

where $\mathbf{n}_i$'s are unknown folding vectors. Regarding (92) as a system of congruences with respect to the moduli $\mathbf{N}_i$'s, we get

$$\mathbf{m} \equiv \boldsymbol{\xi}_i \mod \mathbf{N_i} \quad \text{for } \mathbf{1 \le i \le L}, \tag{93}$$

where $\boldsymbol{\xi}_i = \langle \mathbf{r}_i \rangle_{\mathbf{N}_i}$. Since $\mathbf{N}_1, \mathbf{N}_2, \ldots, \mathbf{N}_L$ are pairwise commutative and coprime, we know from Lemma 2 that $\mathbf{N}_1\mathbf{N}_2\cdots\mathbf{N}_L$ is their lcrm, so is $\mathbf{R} = \mathbf{N}_1\mathbf{N}_2\cdots\mathbf{N}_L\mathbf{U}$ for a unimodular matrix $\mathbf{U}$. Therefore, we obtain from Theorem 1 that $\mathbf{m} \in \mathcal{N}(\mathbf{R})$ can be uniquely reconstructed from its remainders $\boldsymbol{\xi}_i$'s or $\mathbf{r}_i$'s. Next, we prove that $\mathbf{m}$ in (22) is actually a solution of the system of congruences in (93). We express $\mathbf{m}$ as $\mathbf{m} = \mathbf{R}\mathbf{n} + \sum_{i=1}^{L} \mathbf{W}_i\widehat{\mathbf{W}}_i\mathbf{r}_i$ for some integer vector $\mathbf{n}$. Then, for each modulo-$\mathbf{N}_j$ operation, we calculate

$$\begin{aligned}\langle \mathbf{m} \rangle_{\mathbf{N}_j} &= \left\langle \mathbf{R}\mathbf{n} + \mathbf{W}_j\widehat{\mathbf{W}}_j\mathbf{r}_j + \sum_{i=1, i\neq j}^{L} \mathbf{W}_i\widehat{\mathbf{W}}_i\mathbf{r}_i \right\rangle_{\mathbf{N}_j} \\ &= \left\langle \mathbf{W}_j\widehat{\mathbf{W}}_j\mathbf{r}_j \right\rangle_{\mathbf{N}_j} = \langle (\mathbf{I} - \mathbf{N}_j\mathbf{Q}_j)\,\mathbf{r}_j \rangle_{\mathbf{N}_j} \\ &= \langle \mathbf{r}_j \rangle_{\mathbf{N}_j} = \boldsymbol{\xi}_j\,,\end{aligned} \tag{94}$$

where the second equality is due to the commutativity of $\mathbf{N}_i$'s, the third equality is obtained from (23), and (23) holds because $\mathbf{N}_i$ is coprime with $\mathbf{W}_i$ for each $1 \le i \le L$ from Lemma 2. This completes the proof of the corollary.

E. Proof of Lemma 3

As $\mathbf{A}$ is an lcrm of $\boldsymbol{\Gamma}_i$'s, $\mathbf{M}\mathbf{A}$ is a crm of $\mathbf{M}_i$'s. For any other crm $\mathbf{C}$ of $\mathbf{M}_i$'s, i.e., $\mathbf{C} = \mathbf{M}\boldsymbol{\Gamma}_i\mathbf{P}_i$ for some integer matrices $\mathbf{P}_i$'s, we have $\mathbf{M}^{-1}\mathbf{C} = \boldsymbol{\Gamma}_i\mathbf{P}_i$, i.e., $\mathbf{M}^{-1}\mathbf{C}$ is a crm of $\boldsymbol{\Gamma}_i$'s. So, $\mathbf{M}^{-1}\mathbf{C}$ is a right multiple of $\mathbf{A}$, i.e., $\mathbf{M}^{-1}\mathbf{C} = \mathbf{A}\mathbf{G}$ for some integer matrix $\mathbf{G}$. Hence, we have $\mathbf{C} = \mathbf{M}\mathbf{A}\mathbf{G}$. That is to say, $\mathbf{M}\mathbf{A}$ is an lcrm of $\mathbf{M}_i$'s.

F. Proof of Corollary 2

Since $\boldsymbol{\Gamma}_i$'s are pairwise commutative and coprime, we know from Lemma 2 that $\boldsymbol{\Gamma}_1\boldsymbol{\Gamma}_2\cdots\boldsymbol{\Gamma}_L$ is an lcm of $\boldsymbol{\Gamma}_i$'s. Based on Lemma 3, $\mathbf{R} = \mathbf{M}\boldsymbol{\Gamma}_1\boldsymbol{\Gamma}_2\cdots\boldsymbol{\Gamma}_L\mathbf{U}$ for any unimodular matrix $\mathbf{U}$ is an lcrm of $\mathbf{M}_i$'s. Without loss of generality, we let $\mathbf{N}_1 = \mathbf{M}\boldsymbol{\Gamma}_1, \mathbf{N}_2 = \boldsymbol{\Gamma}_2, \ldots, \mathbf{N}_L = \boldsymbol{\Gamma}_L$. As $\mathbf{M}, \boldsymbol{\Gamma}_1, \boldsymbol{\Gamma}_2, \ldots, \boldsymbol{\Gamma}_L$ are pairwise commutative and coprime, we obtain from Lemma 2 that $\mathbf{N}_i$'s are pairwise commutative and coprime. In addition, it is also readily seen that $\mathbf{R} = \mathbf{N}_1\mathbf{N}_2\cdots\mathbf{N}_L\mathbf{U}$, and $\mathbf{N}_i$ is a left divisor of $\mathbf{M}_i$ for each $1 \le i \le L$. Therefore, by Corollary 1, we can uniquely reconstruct $\mathbf{m} \in \mathcal{N}(\mathbf{R})$ from the moduli $\mathbf{M}_i$'s and its remainders $\mathbf{r}_i = \langle \mathbf{m} \rangle_{\mathbf{M}_i}$ by (22).

G. Proof of Corollary 3

Since $\boldsymbol{\Gamma}_i$'s are pairwise commutative and coprime, $\boldsymbol{\Gamma}_1\cdots\boldsymbol{\Gamma}_{i-1}\boldsymbol{\Gamma}_{i+1}\cdots\boldsymbol{\Gamma}_L$ and $\boldsymbol{\Gamma}_i$ are known to be commutative and coprime from Lemma 2. We next prove that $\mathbf{W}_i$ and $\mathbf{M}_i$ are left coprime for each $1 \le i \le L$. Let $\mathbf{D}$ be a gcld of $\mathbf{W}_i$ and $\mathbf{M}_i$. We then have $\mathbf{W}_i = \mathbf{M}\boldsymbol{\Gamma}_1\cdots\boldsymbol{\Gamma}_{i-1}\boldsymbol{\Gamma}_{i+1}\cdots\boldsymbol{\Gamma}_L = \mathbf{D}\mathbf{P}$ and $\mathbf{M}_i = \mathbf{M}\boldsymbol{\Gamma}_i = \mathbf{D}\mathbf{Q}$ for some integer matrices $\mathbf{P}$ and $\mathbf{Q}$. Hence, we have $\boldsymbol{\Gamma}_1\cdots\boldsymbol{\Gamma}_{i-1}\boldsymbol{\Gamma}_{i+1}\cdots\boldsymbol{\Gamma}_L = \mathbf{M}^{-1}\mathbf{D}\mathbf{P}$ and $\boldsymbol{\Gamma}_i = \mathbf{M}^{-1}\mathbf{D}\mathbf{Q}$. As $\mathbf{M}$ is unimodular, $\mathbf{M}^{-1}\mathbf{D}$ is an integer matrix and is a cld of $\boldsymbol{\Gamma}_1\cdots\boldsymbol{\Gamma}_{i-1}\boldsymbol{\Gamma}_{i+1}\cdots\boldsymbol{\Gamma}_L$ and $\boldsymbol{\Gamma}_i$. Since $\boldsymbol{\Gamma}_1\cdots\boldsymbol{\Gamma}_{i-1}\boldsymbol{\Gamma}_{i+1}\cdots\boldsymbol{\Gamma}_L$ and $\boldsymbol{\Gamma}_i$ are commutative and coprime, all of their cld's must be unimodular. Therefore, $\mathbf{M}^{-1}\mathbf{D}$ is a unimodular matrix, so is $\mathbf{D}$. That is to say, $\mathbf{W}_i$ and $\mathbf{M}_i$ are left coprime. Based on the Bezout's theorem in Proposition 2, there exist integer matrices, denoted by $\widehat{\mathbf{W}}_i$ and $\mathbf{Q}_i$, such that (26) holds for each $1 \le i \le L$, and we can calculate them by following the procedure (83)–(91). In addition, from Lemma 2 and Lemma 3, we know that $\mathbf{R} = \mathbf{M}\boldsymbol{\Gamma}_1\boldsymbol{\Gamma}_2\cdots\boldsymbol{\Gamma}_L\mathbf{U}$ for any unimodular matrix $\mathbf{U}$ is an lcrm of the moduli $\mathbf{M}_i$'s. The remaining proof is similar to the proof of Corollary 1 and is omitted here.

H. Proof of Lemma 4

Let $\boldsymbol{\alpha}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\boldsymbol{\alpha}_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. It is readily checked that $\boldsymbol{\alpha}_1$ and $\boldsymbol{\alpha}_2$ are two eigenvectors of $\mathbf{P}$ with the corresponding eigenvalues $p+q$ and $p-q$. Any integer vector in $\mathbb{R}^2$ can be represented by a linear combination of $\boldsymbol{\alpha}_1$ and $\boldsymbol{\alpha}_2$. Assume that $\mathbf{P}$ can be diagonalized as $\mathbf{P} = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^{-1}$, where $\mathbf{U}$ is a 2×2 unimodular matrix and $\boldsymbol{\Lambda}$ is a diagonal integer matrix. This means that $\mathbf{U}$ is an eigenmatrix of $\mathbf{P}$. Let $\mathbf{u}$ be any column vector of $\mathbf{U}$ and it can be represented by $\mathbf{u} = a\boldsymbol{\alpha}_1 + b\boldsymbol{\alpha}_2$ with $a, b \in \mathbb{R}$. Then, we get $\mathbf{P}\mathbf{u} = p\mathbf{u} + q(a\boldsymbol{\alpha}_1 - b\boldsymbol{\alpha}_2)$. Since $\mathbf{U}$ is unimodular, it is nonsingular, and its column vectors cannot be the all-zero vectors. Since $\mathbf{u}$ is a non-zero eigenvector of $\mathbf{P}$ and $q \neq 0$, we know that one and only one of a and b must be 0. Thus, $\mathbf{U}$ has to be the form of $\begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}$, $\begin{pmatrix} b_1 & b_2 \\ -b_1 & -b_2 \end{pmatrix}$, $\begin{pmatrix} a_1 & a_2 \\ a_1 & -a_2 \end{pmatrix}$, or $\begin{pmatrix} b_1 & b_2 \\ -b_1 & b_2 \end{pmatrix}$. Obviously, the determinants of $\begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}$ and $\begin{pmatrix} b_1 & b_2 \\ -b_1 & -b_2 \end{pmatrix}$ are zero, which indicates that the first two forms of matrices are not possible to be unimodular. The determinants of $\begin{pmatrix} a_1 & a_2 \\ a_1 & -a_2 \end{pmatrix}$ and $\begin{pmatrix} b_1 & b_2 \\ -b_1 & b_2 \end{pmatrix}$ are $-2a_1a_2$ and $2b_1b_2$, respectively, which are not equal to ± 1 for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. This indicates that the last two forms of matrices are also not possible to be unimodular. Therefore, $\mathbf{U}$ cannot be unimodular. That is to say, $\mathbf{P}$ cannot be diagonalized as $\mathbf{P} = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^{-1}$, where $\mathbf{U}$ is a 2×2 unimodular matrix and $\mathbf{\Lambda}$ is a diagonal integer matrix.

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, 1996.

[4] H. Krishna, K.-Y. Lin, and B. Krishna, "Rings, fields, the Chinese remainder theorem and an extension-Part II: Applications to digital signal processing," *IEEE Trans. Circuits Syst. II: Analog Digit. Signal Process.*, vol. 41, no. 10, pp. 656–668, 1994.

[5] R. C. Agarwal and C. S. Burrus, "Number theoretic transforms to implement fast digital convolution," *Proc. IEEE*, vol. 63, no. 4, pp. 550–560, 1975.

[6] C.-F. Hsiao, Y. Chen, and C.-Y. Lee, "A generalized mixed-radix algorithm for memory-based FFT processors," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 57, no. 1, pp. 26–30, Jan. 2010.

[7] A. Christlieb, D. Lawlor, and Y. Wang, "A multiscale sub-linear time Fourier algorithm for noisy data," *Appl. Comput. Harmonic Anal.*, vol. 40, no. 3, pp. 553–574, May 2016.

[8] P. P. Vaidyanathan and P. Pal, "Sparse sensing with co-prime samplers and arrays," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 573–586, Feb. 2011.

[9] S. Qin, Y. D. Zhang, and M. G. Amin, "Generalized coprime array configurations for direction-of-arrival estimation," *IEEE Trans. Signal Process.*, vol. 63, no. 6, pp. 1377–1390, Mar. 2015.

[10] C. H. Li, L. Gan, and C. Ling, "Coprime sensing via Chinese remaindering over quadratic fields—Part I: Array designs," *IEEE Trans. Signal Process.*, vol. 67, no. 11, pp. 2898–2910, Jun. 2019.

[11] C. H. Li, L. Gan, and C. Ling, "Coprime sensing via Chinese remaindering over quadratic fields—Part II: Generalizations and applications," *IEEE Trans. Signal Process.*, vol. 67, no. 11, pp. 2911–2922, Jun. 2019.

[12] 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.

[13] 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.

[14] 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.

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

[16] Y. M. Zhang and M. Amin, "MIMO radar exploiting narrowband frequency-hopping waveforms," in *Proc. 16th Eur. Signal Process. Conf.*, Lausanne, Switzerland, 2008.

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

[18] B. Silva and G. Fraidenraich, "Performance analysis of the classic and robust Chinese remainder theorems in pulsed doppler radars," *IEEE Trans. Signal Process.*, vol. 66, no. 18, pp. 4898–4903, Sep. 2018.

[19] J. Xu, Z.-Z. Huang, Z.-R. Wang, L. Xiao, X.-G. Xia, and T. Long, "Radial velocity retrieval for multichannel SAR moving targets with timespace doppler deambiguity," *IEEE Trans. Geosci. Remote Sens.*, vol. 56, no. 1, pp. 35–48, Jan. 2018.

[20] G. Xu, "On solving a generalized Chinese remainder theorem in the presence of remainder errors," in *Conference on Geometry, Algebra, Number Theory, and their Information Technology Applications (GANITA)*, Cham., Switzerland: Springer, 2016, pp. 461–476.

[21] B. Yang, W. J. Wang, X. 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, Oct. 2013.

[22] 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.

[23] 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.

[24] 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.

[25] K. Falaggis, D. P. Towers, and C. E. Towers, "Method of excess fractions with application to absolute distance metrology: Analytical solution," *Appl. Opt.*, vol. 52, no. 23, p. 5758, Aug. 2013.

[26] S. Tang, X. Zhang, and D. Tu, "Micro-phase measuring profilometry: Its sensitivity analysis and phase unwrapping," *Opt. Lasers Eng.*, vol. 72, pp. 47–57, Sep. 2015.

[27] T. Petkovi, T. Pribani, and M. onli, "Temporal phase unwrapping using orthographic projection," *Opt. Lasers Eng.*, vol. 90, pp. 34–47, Mar. 2017.

[28] W. C. Li, X. Z. Wang, and B. Moran, "Wireless signal travel distance estimation using non-coprime wavelengths," *IEEE Signal Process. Letters*, vol. 24, no. 1, pp. 27–31, Jan. 2017.

[29] A. Akhlaq, R. Mckilliam, R. Subramanian, and A. Pollok, "Selecting wavelengths for least squares range estimation," *IEEE Trans. Signal Process.*, vol. 64, no. 20, pp. 5205–5216, Oct. 2016.

[30] C. Chi, H. Vishnu, K. T. Beng, and M. Chitre, "Utilizing orthogonal coprime signals for improving broadband acoustic doppler current profilers," *IEEE J. Ocean. Eng.*, 2019, pp. 1–11.

[31] C. Chi, H. Vishnu, K. T. Beng, and M. Chitre, "Robust resolution of velocity ambiguity for multifrequency pulse-to-pulse coherent doppler sonars," *IEEE J. Ocean. Eng.*, 2019, pp. 1–10.

[32] 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.

[33] 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.

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

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

[36] M. Stemmler, A. Mathis, and A. V. M. Herz, "Connecting multiple spatial scales to decode the population activity of grid cells," *Sci. Adv.*, vol. 1, no. 11, Dec. 2015, Art. no. e1500816.

[37] Y. Yoo, O. O. Koyluoglu, S. Vishwanath, and I. Fiete, "Multi-periodic neural coding for adaptive information transfer," *Theor. Comput. Sci.*, vol. 633, pp. 37–53, Jun. 2016.

[38] L. Gan and H. Liu, "High dynamic range sensing using multi-channel modulo samplers," in *Proc. IEEE 11th Sensor Array Multichannel Signal Process. Workshop (SAM)*, ser. Hangzhou, China., Jun. 2020.

[39] X.-G. Xia, "On estimation of multiple frequencies in undersampled complex valued waveforms," *IEEE Trans. Signal Process*, vol. 47, no. 12, pp. 3417–3419, Dec. 1999.

[40] X.-G. Xia, "An efficient frequency-determination algorithm from multiple undersampled waveforms," *IEEE Signal Process. Lett.*, vol. 7, no. 2, pp. 34–37, Feb. 2000.

[41] X. P. Li, X.-G. Xia, W. J. Wang, and W. J. Wang, "A robust generalized Chinese remainder theorem for two integers," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7491–7504, Dec. 2016.

[42] H. Liao and X.-G. Xia, "A sharpened dynamic range of a generalized Chinese remainder theorem for multiple integers," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 428–433, Jan. 2007.

[43] L. Xiao, X.-G. Xia, and H. Y. Huo, "New conditions on achieving the maximal possible dynamic range for a generalized Chinese remainder theorem of multiple integers," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2199–2203, Dec. 2015.

[44] H. S. Xiao and G. S. Xiao, "On solving ambiguity resolution with robust Chinese remainder theorem for multiple numbers," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 5179–5184, May 2019.

[45] H. S. Xiao, Y. F. Huang, Y. Ye, and G. S. Xiao, "Robustness in Chinese remainder theorem for multiple numbers and remainder coding," *IEEE Trans. Signal Process.*, vol. 66, no. 16, pp. 4347–4361, Aug. 2018.

[46] 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.

[47] A. Guessoum and R. Mersereau, “Fast algorithms for the multidimensional discrete Fourier transform,” *IEEE Trans. Acoustics, Speech, Signal Process.*, vol. 34, no. 4, pp. 937–943, Aug. 1986.

[48] Y.-P. Lin, S.-M. Phoong, and P. P. Vaidyanathan, “New results on multidimensional Chinese remainder theorem,” *IEEE Signal Process. Lett*, vol. 1, no. 11, pp. 176–178, 1994.

[49] 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.

[50] H. J. S. Smith, “On systems of linear indeterminate equations and congruences,” *Philos. Trans. Roy. Soc. London*, vol. 151, pp. 293–326, Dec. 1861.

[51] 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.

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

[53] P. Pal and P. P. Vaidyanathan, “Nested arrays in two dimensions, part I: Geometrical considerations,” *IEEE Trans. Signal Process.*, vol. 60, no. 9, pp. 4694–4705, Sep. 2012.

[54] T. Hori, “Relationship between smith normal form of periodicity matrices and sampling of two-dimensional discrete frequency distributions with tiling capability,” *IEEE Trans. Circuits Syst. II: Express Briefs*, vol. 63, no. 2, pp. 191–195, Feb. 2016.

[55] P. Pal and P. P. Vaidyanathan, “Coprimality of certain families of integer matrices,” *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1481–1490, Apr. 2011.

[56] P. P. Vaidyanathan and P. Pal, “A general approach to coprime pairs of matrices, based on minors,” *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3536–3548, Aug. 2011.

[57] 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, Jan. 2013.

[58] G. Hanrot, X. Pujol, and D. Stehlé, “Algorithms for the shortest and closest lattice vector problems,” in *International Conference on Coding and Cryptology*, Berlin, Heidelberg: Springer, 2011, pp. 159–190.

[59] C. P. Schnorr and M. Euchner, “Lattice basis reduction: Improved practical algorithms and solving subset sum problems,” *Math. Program.*, vol. 66, no. 1-3, pp. 181–199, Aug. 1994.

[60] M. Grant and S. Boyd, “CVX: Matlab software for disciplined convex programming, version 2.0 beta,” Sep. 2013. [Online]. Available: https://cvxr.com/cvx

[61] D. Dudgeon and R. M. Mersereau, *Multidimensional Digital Signal Processing*, Englewood Cliffs, NJ, USA: Prentice-Hall, 1984.

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

[63] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*, Pearson Education India, 2006.

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. He is currently a Research Assistant Professor of biomedical engineering with Tulane University, New Orleans, LA, USA. His research interests include signal processing and machine learning, and their applications to biomedical data analysis.

Xiang-Gen Xia (Fellow, IEEE) received the B.S. degree in mathematics from Nanjing Normal University, Nanjing, China, in 1983, the M.S. degree in mathematics from Nankai University, Tianjin, China, in 1986, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1992.

He was a Senior/Research Staff Member with Hughes Research Laboratories, Malibu, California, during 1995–1996. In September 1996, he joined the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE, USA, where he is currently the Charles Black Evans Professor. His current 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).

Dr. Xia 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 2019 Information Theory Outstanding Overseas Chinese Scientist Award, The Information Theory Society of Chinese Institute of Electronics. He has served as an Associate Editor for numerous international journals, including the IEEE TRANSACTIONS ON SIGNAL PROCESSING, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON MOBILE COMPUTING, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He is Technical Program Chair of the Signal Processing Symposium, Globecom 2007 in Washington D.C. and the General Co-Chair of ICASSP 2005 in Philadelphia.

Yu-Ping Wang (Senior Member, IEEE) received the B.S. degree in applied mathematics from Tianjin University, Tianjin, China, in 1990, and the M.S. degree in computational mathematics and the Ph.D. degree in communications and electronic systems from Xi’an Jiaotong University, Xi’an, China, in 1993 and 1996, respectively. After graduation, he had visiting positions with the Center for Wavelets, Approximation and Information Processing, National University of Singapore, and with the Washington University School of Medicine, St. Louis. From 2000 to 2003, he was a Senior Research Engineer with Perceptive Scientific Instruments, Inc., and with Advanced Digital Imaging Research, LLC, Houston, TX, USA. In 2003, he returned to academia as an Assistant Professor of computer science and electrical engineering with the University of Missouri-Kansas City. He is currently a Professor of biomedical engineering and biostatistics and bioinformatics with the School of Science and Engineering, Tulane University, New Orleans, LA, USA, and with the School of Public Health and Tropical Medicine, New Orleans, LA, USA. He is also a member of the Tulane Center of Bioinformatics and Genomics, Tulane Cancer Center, and the Tulane Neuroscience Program. His research interests include computer vision, signal processing, and machine learning with applications to biomedical imaging and bioinformatics. He has authored or coauthored about 300 peer-reviewed articles in these areas. He has served on numerous program committees and NSF/NIH review panels. He served as an Editor for several journals, such as *Journal of Neuroscience Methods*, IEEE/ACM TRANSACTIONS ON COMPUTATIONAL BIOLOGY AND BIOINFORMATICS, and IEEE TRANSACTIONS ON MEDICAL IMAGING.