Robust Multidimensional Chinese Remainder Theorem (MD-CRT) With Non-Diagonal Moduli and Multistage Framework

Guangpu Guo, *Graduate Student Member, IEEE,* and Xiang-Gen Xia, *Fellow, IEEE*

***Abstract*—The Chinese remainder theorem (CRT) provides an efficient way to reconstruct an integer from its remainders modulo several integer moduli, and has been widely applied in signal processing and information theory. Its multidimensional extension (MD-CRT) generalizes this principle to integer vectors and integer matrix moduli, enabling reconstruction in multidimensional signal processing scenarios. However, since matrices are generally non-commutative, the multidimensional extension introduces new theoretical and algorithmic challenges. When all matrix moduli are diagonal, the system is equivalent to applying the one-dimensional CRT independently along each dimension. This work first investigates whether non-diagonal (non-separable) moduli offer fundamental advantages over traditional diagonal (separable) ones. We show that under the same determinant constraint, non-diagonal matrices do not increase the maximum dynamic range but can yield more balanced and better-conditioned sampling patterns. More importantly, under the common left factor model, we show that, in the two-dimensional setting with a prime determinant constraint, a non-diagonal common left factor can generate a lattice with a longer shortest vector than any diagonal common left factor under the same constraint, leading to better robustness to vector remainder errors. To further improve the robustness, we develop a multistage robust MD-CRT framework that improves the robustness level without reducing the dynamic range. Due to the multidimensional nature of matrix moduli, extending the existing one-dimensional multistage robust CRT is nontrivial. In this paper, we obtain a condition for matrix moduli, which can be easily checked, such that a multistage robust MD-CRT exists. Both theoretical analysis and simulation results demonstrate that the proposed multistage robust MD-CRT achieves stronger error tolerance and more reliable reconstruction under erroneous vector remainders than the single-stage robust MD-CRT.**

***Index Terms*—Multidimensional Chinese remainder theorem (MD-CRT), dynamic range, robustness, multistage, non-separable sampling, shortest vectors.**

Received 4 May 2026; revised 3 September 2026; accepted 27 September 2026. Date of publication 29 September 2026; date of current version 20 October 2026. This work was supported by the National Science Foundation (NSF) under Grant CCF-2246917. The associate editor coordinating the review of this article and approving it for publication was Nicolas Tremblay. *(Corresponding author: Guangpu Guo.)*

The authors are with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: guangpu@udel.edu; xxia@ee.udel.edu).

Digital Object Identifier 10.1109/TSP.2026.3738672

I. Introduction

THE Chinese remainder theorem (CRT) [1] is a classical result in number theory. It reconstructs a large integer from its remainders modulo several smaller positive integers, called integer moduli. As a powerful tool for recovering large or high-resolution quantities from multiple smaller or folded measurements, the CRT has been widely used in signal processing, coding theory, and cryptography [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14]. However, the traditional CRT is highly sensitive to errors. A small error in one remainder may lead to a large reconstruction error. To address this issue, the robust CRT was introduced in [15], [16], [17], [18], [19]. Its main idea is to introduce redundancy among the moduli, such as a common integer factor, so that bounded remainder errors lead to bounded reconstruction errors. Similar ideas have also been extended to generalized forms of the CRT [20], [21], [22].

In many modern applications, the unknowns of interest are multidimensional vectors rather than scalars. Motivated by problems in imaging, radar, and communications, multidimensional CRT (MD-CRT) has been addressed in, for example, [23], [24], [25], [26], where integer moduli are replaced by integer matrices, called matrix moduli, and remainders become vector remainders. Similar to the one-dimensional case, the robustness issue also arises in the multidimensional setting, and the robust MD-CRT was proposed in [24], [25] by introducing redundancy among the matrix moduli.

When all matrix moduli are diagonal, the MD-CRT reduces to applying the one-dimensional CRT independently to each dimension, which is the separable case. This naturally raises an important question: can non-diagonal, or non-separable, matrices offer any fundamental advantage over diagonal, or separable, ones? Although general matrix moduli have been studied in [24], [25], [26], the existing works mainly focused on algorithmic formulations and reconstruction conditions. Whether non-diagonal matrices can bring inherent performance benefits has not been systematically investigated. In [27], we briefly discussed one potential benefit from a sampling perspective: non-diagonal matrices can yield more uniform sampling patterns across different dimensions and help avoid ill-conditioning. Moreover, as a special case of the two-dimensional CRT, the complex CRT (C-CRT) has been applied to self-reset analog-to-digital converters (SR-ADCs), achieving better performance

1053-587X © 2026 IEEE. All rights reserved, including rights for text and data mining, and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

than traditional SR-ADCs using two separate real-valued 1D CRTs [28]. These observations suggest that non-diagonal matrices may have deeper theoretical advantages beyond implementation convenience.

In this paper, we study this question from two key aspects: the dynamic range and the robustness. The dynamic range represents the total number of uniquely determinable vectors for a given set of matrix moduli, or equivalently, the volume of the uniquely determinable range. Mathematically, it equals the absolute determinant value of the least common right multiple (lcrm) of all the matrix moduli. When the MD-CRT is used in multidimensional sub-Nyquist sampling, each matrix modulus acts as a sampling matrix, and its absolute determinant value corresponds to the sampling rate. Since practical sampling rates are limited, the absolute determinant values of all matrix moduli are upper bounded. Under the same determinant constraint, non-diagonal matrices form a much larger candidate set than diagonal ones. This raises the question of whether they can achieve a larger dynamic range.

We first characterize the maximum dynamic range of the MD-CRT under a fixed determinant constraint. We show that this maximum can already be achieved by certain diagonal matrices. Thus, non-diagonal matrices do not increase the maximum dynamic range. However, such diagonal constructions lead to unbalanced sampling patterns, since their sampling rates are concentrated in one dimension. In contrast, using our previously proposed construction of pairwise co-prime non-diagonal matrices [27], [29], one can preserve the same number of moduli and the same determinant for each matrix while obtaining more balanced sampling patterns across all dimensions.

The second key measure is the robustness level. We use the vector remainder error bound denoted by τ to quantify robustness, which means that if every vector remainder error is bounded by τ, then the reconstruction error of the recovered vector is also bounded by τ. Therefore, a larger τ implies stronger robustness and higher noise tolerance. Following [25], this bound is obtained from a sufficient condition for robust multidimensional reconstruction and depends on the shortest nonzero vector of certain lattices generated by pairwise greatest common left divisors (gclds) of the moduli. Although this sufficient bound does not claim the true maximum error tolerance, our simulations indicate that it is a practical and reliable indicator for comparing robustness across different sets of matrix moduli.

To study the effect of matrix geometry on robustness, we adopt a common left factor model. Given a fixed set of pairwise co-prime integer matrices $\mathbf{\Gamma}_1, \ldots, \mathbf{\Gamma}_L$, we study $\mathbf{M}\mathbf{\Gamma}_1, \ldots, \mathbf{M}\mathbf{\Gamma}_L$, for which the sufficient bound τ is determined by the shortest nonzero vector of the lattice generated by $\mathbf{M}$. The problem then becomes whether, under the same determinant constraint $|\det(\mathbf{M})| \leq p$, a non-diagonal matrix $\mathbf{M}$ can generate a lattice whose shortest vector is longer than that of any diagonal matrix. For tractability, we focus on the two-dimensional case with prime p. We show that the best diagonal matrix achieves the shortest-vector length $\lfloor \sqrt{p} \rfloor$, while there are non-diagonal matrices that achieve strictly larger values than $\lfloor \sqrt{p} \rfloor$. We also develop a simple search procedure and verify the improvement for all prime determinants below 10^5. Therefore, under the considered left-factor model, a non-diagonal common left factor can provide a clear robustness advantage over a diagonal one. This search method has also been used for non-separable planar array design in our recent work on moving target SAR imaging over three dimensional terrain [33], where it helps choose non-diagonal matrices with larger shortest vector lengths for more robust MD-CRT based ambiguity resolution.

This difference comes from the different nature of dynamic range and robustness. The dynamic range is determined by the determinant of the lcrm of matrix moduli and reflects the algebraic structure of the integer matrix ring. In contrast, under the considered common left factor model, the robustness depends on the geometry of the lattice generated by the common left factor. Non-diagonal choices allow more lattice shapes and can therefore lead to longer shortest vectors.

In the second part of this paper, we further improve the robustness of the MD-CRT. There are two possible approaches. One is to build a multistage framework like that used for the 1D-CRT in [18], and the other is to trade dynamic range for robustness as in [19], [21]. Although these ideas can be borrowed to study the MD-CRT, they become much more challenging in the multidimensional setting due to the matrix forms of the moduli.

Based on the single-stage robust MD-CRT algorithm in [25], we propose a multistage robust MD-CRT framework. Recall that the main idea in [18] is to divide all moduli into groups, apply the single-stage algorithm to each group, and then treat the reconstructed results as new remainders for the next stage. The key difficulty in the multidimensional case is that the robustly determinable range of the robust MD-CRT is not always consistent with the uniquely determinable range of the MD-CRT for the same moduli. In fact, it cannot be represented as a fundamental parallelepiped (FPD) in general, which makes the multistage framework nontrivial.

To address this problem, we analyze the robustly determinable range of the single-stage robust MD-CRT and derive an easily checkable sufficient condition under which it becomes consistent with that of the MD-CRT. Based on this condition, the matrix moduli can be partitioned into multiple valid groups, and multistage reconstruction can be performed across these groups. The proposed multistage framework improves robustness without reducing the dynamic range. In particular, some matrix moduli that have no robustness in the single-stage case become robust in the multistage version, and for those already having robustness, the vector remainder error bound τ can be further increased. Simulation results confirm these findings.

The rest of this paper is organized as follows. Section II reviews the necessary preliminaries. Section III analyzes the dynamic ranges of diagonal and non-diagonal matrices. Section IV investigates the robustness advantage of non-diagonal common left factors. Section V presents the proposed multistage robust MD-CRT framework. Simulation results are provided in Section VI, and conclusions are given in Section VII.

II. Preliminaries

In this section, we briefly review the basic concepts and properties of integer lattices and matrices that are essential for

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

TABLE I
MAIN NOTATIONS USED IN THIS PAPER

Notation	Meaning
$\mathbf{f}$	Unknown D-dimensional integer vector
$\mathbf{M}_i$	The i-th nonsingular integer matrix modulus
$\mathbf{r}_i, \tilde{\mathbf{r}}_i$	Exact and erroneous vector remainders of $\mathbf{f}$ modulo $\mathbf{M}_i$, respectively
$\mathcal{L}(\mathbf{M})$	Integer lattice generated by $\mathbf{M}$
$\lambda_{\mathcal{L}(\mathbf{M})}$	Length of the shortest nonzero vector of $\mathcal{L}(\mathbf{M})$
$\mathcal{N}(\mathbf{M})$	Fundamental parallelepiped (FPD) generated by $\mathbf{M}$
$\mathrm{lcrm}(\cdot)$	Least common right multiple
$\mathrm{gcld}(\cdot)$	Greatest common left divisor
τ	Vector remainder error bound

analyzing the MD-CRT. For additional background on integer matrices and related results, the reader may refer to [25], [30], [31].

Throughout this paper, $\mathbb{Z}$ denotes the set of integers and $\mathbb{R}$ denotes the set of real numbers. All vectors (e.g., $\mathbf{n}$, $\mathbf{f}$, $\mathbf{r}$) are D-dimensional integer vectors, and all matrices (e.g., $\mathbf{M}$, $\mathbf{N}$, $\mathbf{P}$) are $D \times D$ integer matrices, unless stated otherwise. We write $\mathbf{I}$ for the $D \times D$ identity matrix and $\mathbf{0}$ for the zero matrix or vector. The determinant of a matrix $\mathbf{M}$ is denoted by $\det(\mathbf{M})$. The operator $\mathrm{diag}(\cdot)$ represents a diagonal matrix, and $|\mathcal{S}|$ denotes the cardinality of a set $\mathcal{S}$. Unless otherwise stated, the robustness statements and theorems in this paper hold for *any* vector norm $\|\cdot\|$. For numerical evaluations and when computing shortest vectors (e.g., $\lambda_{\mathcal{L}(\mathbf{M})}$), we take $\|\cdot\|$ to be the Euclidean norm $\|\cdot\|_2$. The notation $\lfloor \cdot \rfloor$ denotes the floor operation, applied element-wise when the argument is a vector. For convenience, Table I summarizes the main notations used throughout the paper.

1) **Lattice:** Given a nonsingular integer matrix $\mathbf{M} \in \mathbb{Z}^{D\times D}$, the lattice generated by $\mathbf{M}$ is defined as
$$\mathcal{L}(\mathbf{M}) = \{\mathbf{Mn} \mid \mathbf{n} \in \mathbb{Z}^D\}.$$
2) **Shortest vector problem (SVP):** The minimum distance of $\mathcal{L}(\mathbf{M})$ is
$$\lambda_{\mathcal{L}(\mathbf{M})} = \min_{\mathbf{v}\in\mathcal{L}(\mathbf{M})\setminus\{\mathbf{0}\}} \|\mathbf{v}\|,$$
which corresponds to the length of the shortest nonzero lattice vector.
3) **Fundamental parallelepiped (FPD):** For a nonsingular integer matrix $\mathbf{M} \in \mathbb{Z}^{D\times D}$, its FPD is defined as
$$\mathcal{N}(\mathbf{M}) = \{\mathbf{k} \in \mathbb{Z}^D \mid \mathbf{k} = \mathbf{Mx},\ \mathbf{x} \in [0,1)^D\},$$
and the number of elements in $\mathcal{N}(\mathbf{M})$ equals $|\det(\mathbf{M})|$.
4) **Division representation for integer vectors:** Any integer vector $\mathbf{f} \in \mathbb{Z}^D$ can be uniquely expressed as
$$\mathbf{f} = \mathbf{Mn} + \mathbf{r}, \quad \mathbf{r} \in \mathcal{N}(\mathbf{M}),\ \mathbf{n} \in \mathbb{Z}^D,$$
which is denoted as $\mathbf{f} \equiv \mathbf{r} \mod \mathbf{M}$, where $\mathbf{r}$ is called the *vector remainder* of $\mathbf{f}$ modulo $\mathbf{M}$.
5) **Unimodular matrix:** A square integer matrix $\mathbf{U}$ is unimodular if $|\det(\mathbf{U})| = 1$.
6) **Greatest common left divisor (gcld):** For two integer matrices $\mathbf{M}$ and $\mathbf{N}$, a nonsingular integer matrix $\mathbf{G}$ is a *common left divisor* (cld) of $\mathbf{M}$ and $\mathbf{N}$ if $\mathbf{G}^{-1}\mathbf{M}$ and $\mathbf{G}^{-1}\mathbf{N}$ are both integer matrices. Moreover, if any other cld of $\mathbf{M}$ and $\mathbf{N}$ is also a left divisor of $\mathbf{G}$, then $\mathbf{G}$ is called their *greatest common left divisor* (gcld).
7) **Least common right multiple (lcrm):** For two integer matrices $\mathbf{M}$ and $\mathbf{N}$, a matrix $\mathbf{R}$ is a *common right multiple* (crm) if there exist integer matrices $\mathbf{P}$ and $\mathbf{Q}$ such that $\mathbf{R} = \mathbf{MP} = \mathbf{NQ}$. If any other crm of $\mathbf{M}$ and $\mathbf{N}$ is also a right multiple of $\mathbf{R}$, then $\mathbf{R}$ is called their *least common right multiple* (lcrm). It is worth noting that the lcrm is not unique: if $\mathbf{R}$ is an lcrm of $\mathbf{M}$ and $\mathbf{N}$, then $\mathbf{RU}$ is also an lcrm for any unimodular matrix $\mathbf{U}$. However, the absolute determinant value of the lcrm, $|\det(\mathbf{R})|$, is unique.
8) **Smith normal form (SNF):** Any integer matrix $\mathbf{M} \in \mathbb{Z}^{D\times K}$ can be factorized as $\mathbf{UMV} = \mathbf{\Lambda}$, where $\mathbf{U} \in \mathbb{Z}^{D\times D}$ and $\mathbf{V} \in \mathbb{Z}^{K\times K}$ are unimodular matrices, and $\mathbf{\Lambda}$ is diagonal with entries $\delta_1, \ldots, \delta_{\min\{K,D\}}$ satisfying $\delta_i \mid \delta_{i+1}$, i.e., δ_i divides δ_{i+1}.
9) **Hermite normal form (HNF):** Any nonsingular integer matrix $\mathbf{M} \in \mathbb{Z}^{D\times D}$ can be uniquely decomposed as $\mathbf{M} = \mathbf{HU}$, where $\mathbf{U} \in \mathbb{Z}^{D\times D}$ is unimodular and $\mathbf{H} \in \mathbb{Z}^{D\times D}$ is a lower-triangular integer matrix satisfying $0 \le H_{i,j} < H_{i,i}$ for $j < i$.
10) **Coprimality:** Matrices $\mathbf{M}$ and $\mathbf{N}$ are said to be left co-prime if their gcld is a unimodular matrix. Equivalently, $\mathbf{M}$ and $\mathbf{N}$ are left co-prime if and only if the SNF of matrix $(\mathbf{M}\ \mathbf{N})$ equals $(\mathbf{I}\ \mathbf{0})$. Throughout this paper, "co-prime" always refers to the left co-prime case.

III. DYNAMIC RANGE ANALYSIS OF MD-CRT

In this section, we introduce the multidimensional undersampling model, and for MD-CRT, analyze the maximum dynamic range under a fixed determinant constraint. We then compare the performance of diagonal and non-diagonal matrix moduli. Our analysis shows that although non-diagonal matrices do not have a strictly larger dynamic range, they yield more balanced and better-conditioned sampling patterns than diagonal ones.

A. Multidimensional Undersampling and MD-CRT

Consider a D-dimensional harmonic signal
$$x(\mathbf{t}) = a\, e^{j2\pi \mathbf{f}^\top \mathbf{t}} + \omega(\mathbf{t}), \quad \mathbf{t} \in \mathbb{R}^D, \tag{1}$$
where a is an unknown amplitude, $\omega(\mathbf{t})$ denotes additive noise, and $\mathbf{f} \in \mathbb{Z}^D$ is a D-dimensional integer frequency vector. The goal is to determine $\mathbf{f} = [N_1, N_2, \ldots, N_D]^\top$ from several undersampled D-dimensional signals of $x(\mathbf{t})$, where each N_i is a positive integer and may be large. In practice, the true frequency vector may not be integer-valued. In that case, evaluating the multidimensional DFT (MD-DFT) on a discrete frequency grid introduces a frequency-grid quantization error, which appears as a vector remainder error in the MD-CRT reconstruction. Such errors can in principle be handled by robust MD-CRT. However,

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

for a general lattice-based MD-DFT, this quantization error is more difficult to characterize than that in the one-dimensional DFT case. This non-integer frequency case is left for future work, and this paper focuses on the integer-valued case.

Let $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$ be L nonsingular integer matrices of size $D \times D$, called *sampling matrices*. Sampling with $\mathbf{M}_i$ gives

$$x_i[\mathbf{n}] = a\, e^{j2\pi \mathbf{f}^\top \mathbf{M}_i^{-\top} \mathbf{n}} + \omega[\mathbf{M}_i^{-\top}\mathbf{n}], \quad \mathbf{n} \in \mathbb{Z}^D, \tag{2}$$

where the sampling density of $\mathbf{M}_i$ equals $|\det(\mathbf{M}_i)|$, i.e., there are $|\det(\mathbf{M}_i)|$ many sampled points per unit spatial volume of $\mathbb{R}^D$.

Applying the MD-DFT [32] to $x_i[\mathbf{n}]$ over $\mathbf{n} \in \mathcal{N}(\mathbf{M}_i^\top)$, yields

$$X_i(\mathbf{k}) = a\,|\det(\mathbf{M}_i)|\,\delta(\mathbf{k} - \mathbf{r}_i) + \Omega_i(\mathbf{k}), \quad \mathbf{k} \in \mathcal{N}(\mathbf{M}_i), \tag{3}$$

where $\mathbf{r}_i$ is the integer vector remainder of $\mathbf{f}$ modulo $\mathbf{M}_i$, and $\delta(\cdot)$ denotes the discrete delta function. Hence, each sampler provides one vector remainder $\mathbf{r}_i \equiv \mathbf{f} \bmod \mathbf{M}_i$. The MD-CRT enables reconstruction of $\mathbf{f}$ from these vector remainders.

Proposition 1 (MD-CRT [24]): Let $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_L$ be arbitrary nonsingular integer matrices of size $D \times D$, and let $\mathbf{R}$ be any lcrm of them. For any integer vector $\mathbf{f} \in \mathbb{Z}^D$, it can be uniquely determined from its vector remainders $\mathbf{r}_i \equiv \mathbf{f} \bmod \mathbf{M}_i$, $1 \le i \le L$, if and only if $\mathbf{f} \in \mathcal{N}(\mathbf{R})$.

The MD-CRT considered above is formulated with integer matrix moduli. A common known nonsingular real-valued transformation can nevertheless be incorporated. Specifically, if the matrices have the form $\mathbf{T}\mathbf{M}_i$ and the corresponding vector remainders are $\mathbf{T}\mathbf{r}_i$, applying $\mathbf{T}^{-1}$ reduces the problem to the integer MD-CRT with $\mathbf{M}_i$ and $\mathbf{r}_i$. Thus, a common real-valued transformation can be combined with the underlying integer CRT structure, while arbitrary real-valued matrices are not considered here.

From Proposition 1, the set of all uniquely determinable integer vectors is $\mathcal{N}(\mathbf{R})$, and its size $|\det(\mathbf{R})|$ defines the *dynamic range* of the system. In practice, one wants to minimize the sampling densities $|\det(\mathbf{M}_i)|$ while maximizing the dynamic range $|\det(\mathbf{R})|$. We next study the maximum dynamic range under a fixed determinant constraint, i.e., an upper bound on the sampling rates.

B. Dynamic Range Analysis

In the undersampling model introduced in the previous subsection, each matrix modulus serves as a sampling matrix whose absolute determinant value represents the sampling rate. In many practical systems, such as moving-target parameter estimation in SAR imaging [4], hardware limitations impose an upper bound on these sampling rates. This bound directly limits the possible matrix moduli, leading to a limited dynamic range.

To better understand the problem, we first recall the one-dimensional case. For the classical CRT, if all the integer moduli are upper bounded by q, i.e., all integer moduli are less than or equal to q, where q is a positive integer, then the maximum dynamic range equals the least common multiple (lcm) of $1, 2, \cdots, q$, denoted by $\mathrm{lcm}(1, 2, \cdots, q)$. This range can be achieved by choosing all integers from 1 to q as moduli, but that is clearly inefficient. A smaller subset of pairwise co-prime integers can already reach the same dynamic range, as shown below. In the following optimization, the cardinality of this subset is not fixed in advance.

Lemma 1: Let $\{q_1, q_2, \cdots, q_L\} \subseteq \{1, 2, \cdots, q\}$ be a set of pairwise co-prime positive integers that maximizes the product $\prod_{i=1}^{L} q_i$, where the cardinality L is not fixed in advance. Then, $\prod_{i=1}^{L} q_i$ is equal to $\mathrm{lcm}(1, 2, \cdots, q)$.

Proof: Because $q_1, q_2, \cdots, q_L$ are pairwise co-prime integers, $\prod_{i=1}^{L} q_i$ equals the lcm of them. Since $\{q_1, q_2, \cdots, q_L\} \subseteq \{1, 2, \cdots, q\}$, we have $\mathrm{lcm}(1, 2, \cdots, q) \ge \prod_{i=1}^{L} q_i$. We then just need to prove $\mathrm{lcm}(1, 2, \cdots, q) \le \prod_{i=1}^{L} q_i$ by proving that any integer p with $1 \le p \le q$ is a divisor of $\prod_{i=1}^{L} q_i$.

Assume that there exists a p with $1 \le p \le q$ such that p is not a divisor of $\prod_{i=1}^{L} q_i$. Since any integer can be decomposed as the product of prime integers, there must be a divisor r^n of p where r is a prime integer and n is a positive integer, such that r^n is not a divisor of $\prod_{i=1}^{L} q_i$.

If r^n is co-prime with every q_i for $1 \le i \le L$, we can construct a new set of pairwise co-prime integers $\{q_1, q_2, \cdots, q_L, r^n\} \subseteq \{1, 2, \cdots, q\}$ such that the product $r^n \prod_{i=1}^{L} q_i$ is greater than $\prod_{i=1}^{L} q_i$, which contradicts the assumption.

If r^n is not co-prime with all q_i for $1 \le i \le L$, there exists exactly one q_j such that q_j is not co-prime with r^n since all q_i for $1 \le i \le L$ are pairwise co-prime. Let r^a be the highest power of r that divides q_j. Then, $1 \le a < n$, otherwise r^n would be a divisor of q_j, which would contradict the assumption about r^n. We then construct a new set of pairwise co-prime integers $\{q_1, q_2, \cdots, q_j/r^a, \cdots, q_L, r^n\} \subset \{1, 2, \cdots, q\}$ such that their product $r^{n-a} \prod_{i=1}^{L} q_i$ is greater than $\prod_{i=1}^{L} q_i$, which contradicts the assumption.

Therefore, any integer p with $1 \le p \le q$ is a divisor of $\prod_{i=1}^{L} q_i$ and then $\mathrm{lcm}(1, 2, \cdots, q) = \prod_{i=1}^{L} q_i$. □

Now consider the multidimensional case where each matrix modulus $\mathbf{M}$ satisfies $|\det(\mathbf{M})| \le q$ for a positive integer q. In this setting, the maximum possible dynamic range is determined by the lcrm of all such matrices. However, unlike in the one-dimensional case, the number of such matrices is huge especially when the dimension D is large. As a result, it is hard to describe the maximum possible dynamic range in a direct way. Before presenting the main result, we first present two lemmas that will be used for the main result.

Lemma 2 (Lemma 1 in [27]): Let m_1 and m_2 be two non-zero integers with the greatest common divisor (gcd) k for a positive integer k. For each i with $1 \le i \le D$, we can obtain a new matrix $[k\mathbf{e}_i \quad \mathbf{0}]$ by performing elementary column transformations on matrix $[m_1\mathbf{e}_i \quad m_2\mathbf{e}_i]$, where $\mathbf{e}_i$ is the D-dimensional vector with the i-th component 1 and the other components 0.

Lemma 3 (Lemma 2 in [24]): Let $\mathbf{M}_i$ for $1 \le i \le L$ be L nonsingular and pairwise co-prime and commutative integer matrices, then their product $\mathbf{M}_1\mathbf{M}_2 \cdots \mathbf{M}_L$ is an lcrm of them.

We then proceed to present the main result.

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

Theorem 1: Assume that the absolute determinant values of all $D \times D$ matrix moduli are upper bounded by q. Let $\{q_1, q_2, \cdots, q_L\} \subseteq \{1, 2, \cdots, q\}$ be a set of pairwise co-prime integers that maximizes the product $\prod_{i=1}^{L} q_i$ among all such sets, where the cardinality L is not fixed in advance. Then, the maximum possible dynamic range of MD-CRT under the upper bound q of matrix moduli is $(q_1 q_2 \cdots q_L)^D$. The number of matrix moduli is not fixed in advance in this optimization.

Proof: We first prove that the dynamic range of MD-CRT under the upper bound q of matrix moduli is less than or equal to $(q_1 q_2 \cdots q_L)^D$ by proving the $D \times D$ diagonal matrix

$$\mathbf{R} = \text{diag}(q_1 q_2 \cdots q_L, \cdots, q_1 q_2 \cdots q_L)$$

is a crm of all the matrix moduli.

Let $\mathbf{M}$ be an integer matrix with the absolute determinant value p for $1 \le p \le q$. We then have

$$\begin{aligned}\mathbf{M}^{-1}\mathbf{R} &= \pm(1/p)\ \text{adj}\,(\mathbf{M})\ \text{diag}\,(q_1 q_2 \cdots q_L, \cdots, q_1 q_2 \cdots q_L) \\ &= \pm\ \text{adj}\,(\mathbf{M})\ \text{diag}\left(\frac{q_1 q_2 \cdots q_L}{p}, \cdots, \frac{q_1 q_2 \cdots q_L}{p}\right).\end{aligned}$$

From Lemma 1, the matrix $\text{diag}(\frac{q_1 q_2 \cdots q_L}{p}, \cdots, \frac{q_1 q_2 \cdots q_L}{p})$ is an integer matrix. Therefore, $\mathbf{M}^{-1}\mathbf{R}$ is an integer matrix and $\mathbf{R}$ is a right multiple of $\mathbf{M}$. Since $\mathbf{R}$ is a right multiple of all possible integer matrices that the absolute determinant values are less than or equal to q, $\mathbf{R}$ is a crm of all such matrices. For MD-CRT, the uniquely determinable range is an FPD of an lcrm of all the matrix moduli and the dynamic range is equal to the absolute determinant value of the lcrm of all the matrix moduli. As a result, the maximum dynamic range of MD-CRT under the upper bound q of matrix moduli is less than or equal to $|\det(\mathbf{R})|$, i.e., $(q_1 q_2 \cdots q_L)^D$.

We then prove that there is a set of integer matrices whose absolute determinant values are less than or equal to q such that the dynamic range of MD-CRT with these matrix moduli is $(q_1 q_2 \cdots q_L)^D$ by proving $\mathbf{R}$ is an lcrm of these matrices.

Let $\mathbf{D}_{i,1} = \text{diag}(q_i, 1, \cdots, 1), \mathbf{D}_{i,2} = \text{diag}(1, q_i, \cdots, 1), \cdots, \mathbf{D}_{i,D} = \text{diag}(1, 1, \cdots, q_i)$ for $1 \le i \le L$. We can easily check, according to Lemma 2, that the Smith normal form of matrix $(\mathbf{D}_{i_1,j_1}\ \mathbf{D}_{i_2,j_2})$ is $(\mathbf{I}\ \mathbf{0})$ for any two distinct pairs $(i_1, j_1) \neq (i_2, j_2)$. As a result, all matrices $\mathbf{D}_{i,j}$ for $1 \le i \le L$ and $1 \le j \le D$ are pairwise co-prime and commutative. According to Lemma 3, the product of these matrices is an lcrm of them, which is the matrix $\mathbf{R}$. As a result, if we choose $\mathbf{D}_{i,j}$ as matrix moduli, the dynamic range is equal to $(q_1 q_2 \cdots q_L)^D$.

Combining the above two parts, we have completed the proof. □

According to Lemma 1, the maximum possible dynamic range of MD-CRT under the upper bound q of matrix moduli is $\big(\text{lcm}(1, 2, \cdots, q)\big)^D$. This result is consistent with the classical CRT when $D = 1$. The proof of Theorem 1 also shows that diagonal matrices are already sufficient to achieve the maximum dynamic range. Although non-diagonal matrices provide a larger candidate set, they cannot further increase this dynamic range. Next, we explore whether non-diagonal moduli can still bring advantages in other aspects of the MD-CRT.

C. Sampling Advantage of Non-Diagonal Matrix Moduli

While diagonal matrices achieve the maximum possible dynamic range, their sampling rates are often very uneven across dimensions. For example, in $\mathbf{D}_{i,j}$, the sampling rate along the j-th dimension is q_i, and it is 1 on the others. Such an imbalance may cause poor numerical conditioning and practical hardware difficulty. A natural question is whether these diagonal sampling matrices can be replaced by non-diagonal ones that have more balanced per-dimension sampling rates, without increasing the total number of matrices or changing their determinants.

From Lemma 2, we have the following straightforward necessary and sufficient condition that two diagonal integer matrices are co-prime.

Corollary 1: Two nonsingular diagonal integer matrices $\text{diag}(a_1, \cdots, a_D)$ and $\text{diag}(b_1, \cdots, b_D)$ are co-prime if and only if a_i and b_i are co-prime integers for all $1 \le i \le D$.

Since q_i for $1 \le i \le L$ are pairwise co-prime integers, to keep the maximum dynamic range, we must have L groups of matrix moduli $\mathcal{S}_i$ for $1 \le i \le L$, such that $\text{diag}(q_i, \cdots, q_i)$ is an lcrm of the matrices in $\mathcal{S}_i$. Therefore, to analyze the replacement of diagonal matrices $\mathbf{D}_{i,j}$ with non-diagonal ones that achieve more balanced per-dimension sampling rates, it suffices to focus on a single group corresponding to a fixed q_i. The analysis for other groups is similar.

Let $q_i = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ be its prime factorization, where $k, n_1, n_2, \cdots, n_k$ are positive integers and $p_1, \cdots, p_k$ are prime integers.

Consider the special case $n_j = D$ for all $1 \le j \le k$. In this case, q_i can be written as $q_i = p_1^D p_2^D \cdots p_k^D$. To construct D-dimensional matrices from these k factors, we redefine a new set of D pairwise co-prime integers $s_1, s_2, \ldots, s_D$ as follows: if $k < D$, we append additional factors equal to 1; if $k > D$, we partition these prime power factors into D groups. After this adjustment, q_i can still be expressed as $q_i = s_1^D s_2^D \cdots s_D^D$, where $s_1, \ldots, s_D$ are pairwise co-prime integers. Among all such decompositions, we choose $s_1, \ldots, s_D$ such that $s_{\max} = \max_{1 \le j \le D} s_j$ is minimized. One can then construct D pairwise co-prime diagonal matrices whose diagonal entries are cyclic shifts of $(s_1^D, s_2^D, \ldots, s_D^D)$. For these diagonal matrices, the largest sampling rate along each dimension is $s_{\max}^D$. Moreover, by the optimality of $s_{\max}$, no other set of D pairwise co-prime diagonal matrices with determinant q_i can make the largest per-dimension sampling rate smaller than $s_{\max}^D$. However, following the construction in [27], we can have a set of D non-diagonal matrices with determinant values q_i, whose lcrm is still $\text{diag}(q_i, \ldots, q_i)$. In this case, the maximum sampling rate along each dimension is $s_1 s_2 \cdots s_D + 1$, which is much smaller than $s_{\max}^D$. This shows that the non-diagonal matrices give a more balanced sampling pattern compared with the diagonal construction. The special case $k = 1$ has been studied in detail in [27].

IV. Single-Stage Robust MD-CRT

In low-SNR scenarios, detected vector remainders are often erroneous. The MD-CRT is highly sensitive to such errors, i.e., even a small error in a single vector remainder may cause a large

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

error in the reconstructed vector. As a result, directly applying the MD-CRT under noise performs poorly. To address this issue, a robust MD-CRT for general matrix moduli was proposed in [25]. It guarantees that if each vector remainder error is bounded by a moduli-dependent threshold, then the reconstruction error of the unknown integer vector is bounded by the same threshold. A larger threshold means a higher robustness level. In this section, we briefly review the robust MD-CRT in [25] and then investigate the potential robustness advantage of a non-diagonal common left factor over a diagonal common left factor in the single-stage setting.

A. Single-Stage Robust MD-CRT

Consider the following system of congruences:

$$\mathbf{f} = \mathbf{M}_i\mathbf{n}_i + \mathbf{r}_i, \qquad 1 \le i \le L, \tag{4}$$

where $\mathbf{f}$ is an unknown integer vector to be determined, $\mathbf{M}_i$, for $1 \le i \le L$, are nonsingular integer matrices and $\mathbf{r}_i \in \mathcal{N}(\mathbf{M}_i)$, for $1 \le i \le L$, are vector remainders of $\mathbf{f}$ modulo $\mathbf{M}_i$. If all vector remainders $\mathbf{r}_i$ for $1 \le i \le L$ are error-free, then the unknown vector $\mathbf{f}$ can be uniquely determined by the MD-CRT if $\mathbf{f}$ lies within the FPD generated by an lcrm of the matrix moduli.

In practical applications, the observed vector remainders are often noisy, i.e.,

$$\tilde{\mathbf{r}}_i = \mathbf{r}_i + \Delta\mathbf{r}_i, \quad 1 \le i \le L,$$

where $\mathbf{r}_i \in \mathcal{N}(\mathbf{M}_i)$ is an error-free vector remainder and $\Delta\mathbf{r}_i \in \mathbb{Z}^D$ represents an error. If the MD-CRT is directly applied to these erroneous vector remainders $\tilde{\mathbf{r}}_i$, the resulting vector $\tilde{\mathbf{f}}$ constructed from MD-CRT may have a large error compared to the true vector $\mathbf{f}$, even when the errors $\Delta\mathbf{r}_i$ are small.

To overcome this issue, a robust MD-CRT for general matrix moduli has been proposed in [25]. The key idea is to first accurately estimate the terms $\mathbf{M}_i\mathbf{n}_i$ for all $1 \le i \le L$ in the system of congruences (4) and then reconstruct the unknown vector $\mathbf{f}$ by averaging as follows:

$$\tilde{\mathbf{f}} = \frac{1}{L}\sum_{i=1}^{L}(\mathbf{M}_i\mathbf{n}_i + \tilde{\mathbf{r}}_i).$$

In this case, the reconstruction error can be expressed as

$$\tilde{\mathbf{f}} - \mathbf{f} = \frac{1}{L}\sum_{i=1}^{L}\Delta\mathbf{r}_i.$$

If the errors in the vector remainders are bounded by a parameter τ, i.e., $\|\Delta\mathbf{r}_i\| \le \tau$, for all $1 \le i \le L$, then the reconstruction error is also bounded by the same parameter, i.e. $\|\tilde{\mathbf{f}} - \mathbf{f}\| \le \tau$. The parameter τ is called the vector remainder error bound, which is determined by the length of the shortest nonzero vector of certain lattices generated by pairwise gclds of the moduli. It also reflects the level of robustness: a larger τ indicates a stronger tolerance to vector remainder errors and thus a higher robustness level.

Let $\mathbf{G}_{i,j}$ be a gcld of $\mathbf{M}_i$ and $\mathbf{M}_j$, for all $1 \le i \ne j \le L$. A necessary and sufficient condition for accurately estimating $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$ in [25] is given as follows.

Proposition 2 (Robust MD-CRT from [25]): Let $\mathbf{M}_i$ for all $1 \le i \le L$ be L distinct, arbitrary, nonsingular integer matrices. Suppose that there exists an index $l_0 \in \{1, 2, \ldots, L\}$ satisfying

$$\min_{\substack{1\le j\le L\\ j\ne l_0}} \lambda_{\mathcal{L}(\mathbf{G}_{l_0,j})} = \max_{1\le i\le L} \min_{\substack{1\le j\le L\\ j\ne i}} \lambda_{\mathcal{L}(\mathbf{G}_{i,j})}. \tag{5}$$

For any integer vector $\mathbf{f}$ with

$$\left\lfloor \mathbf{M}_{l_0}^{-1}\mathbf{f} \right\rfloor \in \mathcal{N}\left(\mathbf{M}_{l_0}^{-1}\,\mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L)\right), \tag{6}$$

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

$$\mathbf{0} = \arg\min_{\mathbf{h}\in\mathcal{L}(\mathbf{G}_{l_0,j})} \|\mathbf{h} - (\Delta\mathbf{r}_j - \Delta\mathbf{r}_{l_0})\|, \tag{7}$$

for all $1 \le j \le L$ with $j \ne l_0$. Moreover, if the remainder errors are bounded by $\|\Delta\mathbf{r}_i\| \le \tau$ for all $1 \le i \le L$, then a sufficient condition for correct reconstruction of $\{\mathbf{M}_i\mathbf{n}_i\}_{i=1}^{L}$ is

$$\tau < \max_{1\le i\le L} \min_{\substack{1\le j\le L\\ j\ne i}} \frac{\lambda_{\mathcal{L}(\mathbf{G}_{i,j})}}{4} = \min_{\substack{1\le j\le L\\ j\ne l_0}} \frac{\lambda_{\mathcal{L}(\mathbf{G}_{l_0,j})}}{4}. \tag{8}$$

We now outline the procedure for robustly reconstructing $\mathbf{f}$ from the erroneous vector remainders $\{\tilde{\mathbf{r}}_i\}_{i=1}^{L}$.

Step 1: Compute all $\mathbf{G}_{i,j}$ and their lattice minimum distances $\lambda_{\mathcal{L}(\mathbf{G}_{i,j})}$ for $1 \le i \ne j \le L$. Select an index l_0 that satisfies the condition in (5).

Step 2: For each $j \ne l_0$, compute the vector $\mathbf{v}_j$ as

$$\mathbf{v}_j = \arg\min_{\mathbf{v}\in\mathcal{L}(\mathbf{G}_{l_0,j})} \|\mathbf{v} - (\tilde{\mathbf{r}}_j - \tilde{\mathbf{r}}_{l_0})\|.$$

Step 3: Set $\mathbf{v}_{l_0} = \mathbf{0}$. Compute $\mathbf{M}_{l_0}\mathbf{n}_{l_0} \in \mathcal{N}(\mathrm{lcrm}(\mathbf{M}_1, \ldots, \mathbf{M}_L))$ by applying the MD-CRT to

$$\mathbf{M}_{l_0}\mathbf{n}_{l_0} \equiv \mathbf{v}_j \mod \mathbf{M}_j, \qquad 1 \le j \le L.$$

Step 4: For each $1 \le j \le L$ with $j \ne l_0$, compute

$$\mathbf{M}_j\mathbf{n}_j = \mathbf{M}_{l_0}\mathbf{n}_{l_0} - \mathbf{v}_j.$$

Step 5: Estimate $\mathbf{f}$ by averaging

$$\tilde{\mathbf{f}} = \frac{1}{L}\sum_{i=1}^{L}(\mathbf{M}_i\mathbf{n}_i + \tilde{\mathbf{r}}_i).$$

Remark 1 (Choice of lattice basis in implementation): For any unimodular integer matrix $\mathbf{U}$, $\mathcal{L}(\mathbf{GU}) = \mathcal{L}(\mathbf{G})$ and hence $\lambda_{\mathcal{L}(\mathbf{GU})} = \lambda_{\mathcal{L}(\mathbf{G})}$. Therefore, in Step 2, the basis $\mathbf{G}$ may be replaced by an equivalent reduced basis $\mathbf{GU}$, for example one obtained by LLL reduction, for the closest-vector computation. Such a basis may provide better numerical properties and facilitate the closest-vector search. Since the underlying lattice is unchanged, this basis replacement does not affect the robustness condition or the reconstruction range.

The goal of the robust MD-CRT is to ensure that if the errors in the vector remainders are bounded by a parameter τ, then the error in the reconstructed vector is also bounded by the same τ. Two questions arise in the robust MD-CRT. The first concerns the dynamic range: how many integer vectors $\mathbf{f}$ can be robustly reconstructed? The second is about the robustness

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

level: how large can the vector remainder error bound τ be that still guarantees robust reconstruction?

For the first question, Proposition 2 shows that any integer vector $\mathbf{f}$ satisfying (6) can be robustly reconstructed if and only if condition (7) is satisfied. Such an $\mathbf{f}$ can be uniquely decomposed as

$$\mathbf{f} = \mathbf{M}_{l_0} \left\lfloor \mathbf{M}_{l_0}^{-1} \mathbf{f} \right\rfloor + \mathbf{r}, \tag{9}$$

where $\mathbf{r} \in \mathcal{N}(\mathbf{M}_{l_0})$. Hence, each pair $(\left\lfloor \mathbf{M}_{l_0}^{-1} \mathbf{f} \right\rfloor, \mathbf{r})$ uniquely determines an $\mathbf{f}$. According to (6), the number of possible vectors for $\left\lfloor \mathbf{M}_{l_0}^{-1} \mathbf{f} \right\rfloor$ is

$$\frac{|\det(\mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L))|}{|\det(\mathbf{M}_{l_0})|},$$

and the total number of possible such vectors $\mathbf{r}$ is $|\det(\mathbf{M}_{l_0})|$. Therefore, the total number of vectors that can be robustly reconstructed is $|\det(\mathrm{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L))|$, which coincides with the dynamic range of the MD-CRT with the same set of matrix moduli. However, this does not mean that the set of vectors that can be robustly reconstructed with the robust MD-CRT, called *robustly determinable range*, is the same as the set of vectors that can be uniquely determined by the MD-CRT, called *uniquely determinable range*[1]. In fact, the robustly determinable range of the robust MD-CRT does not, in general, form an FPD of any matrix, unlike that of MD-CRT, which is analyzed in detail in a later section.

For the second question, according to Proposition 2, a sufficient condition for robust reconstruction is given in (8). This condition shows that the robustness level is determined by the chosen matrix moduli. More specifically, the robustness level is limited by the smallest minimum distance among all the lattices generated by the gclds of the chosen matrix with the other matrices. This motivates the question: can a non-diagonal matrix yield a larger τ than the maximum achievable by diagonal matrices under the same determinant constraint? We address this next.

B. Robustness Advantage of Non-Diagonal Common Left Factors

In the previous section, comparing to diagonal matrix moduli we have shown that non-diagonal matrices do not increase the dynamic range of MD-CRT. For the robust MD-CRT, the dynamic range remains the same when the moduli are unchanged. The key performance index here is the vector remainder error bound τ, which depends on the shortest vectors of certain lattices. We first consider the two-dimensional case and then give a three-dimensional example to show that such a robustness advantage occurs as well in higher dimensions.

A direct comparison is difficult because (8) involves multiple gcld lattices. To solely investigate the robustness, we adopt a common left factor model. Given a fixed set of pairwise coprime integer matrices $\mathbf{\Gamma}_1, \mathbf{\Gamma}_2, \cdots, \mathbf{\Gamma}_L$, consider the matrix moduli $\mathbf{M\Gamma}_1, \mathbf{M\Gamma}_2, \cdots, \mathbf{M\Gamma}_L$. In this setting, $\mathbf{M}$ is a gcld of any two of the matrix moduli. Hence, by (8), the sufficient threshold for the vector remainder error bound τ is $\lambda_{\mathcal{L}(\mathbf{M})}/4$.

We also note that, within this common left factor model, requiring all the matrix moduli $\mathbf{M\Gamma}_i$ to be diagonal is a stronger restriction. If all $\mathbf{M\Gamma}_i$ are diagonal, then a gcld of any two of them can also be chosen diagonal by Lemma 2. Since $\mathbf{M}$ is also a gcld of the same two matrix moduli and any two gclds differ by a right unimodular factor, $\mathcal{L}(\mathbf{M})$ must be a rectangular lattice. The converse does not hold. A diagonal matrix $\mathbf{M}$ may still produce non-diagonal matrix moduli when some $\mathbf{\Gamma}_i$ are non-diagonal. The comparison below is therefore carried out at the level of $\mathbf{M}$, because $\mathcal{L}(\mathbf{M})$ is the gcld lattice that directly determines the robustness threshold, and requiring all the matrix moduli to be diagonal necessarily forces the lattice $\mathcal{L}(\mathbf{M})$ to be rectangular, which is already covered by the diagonal choices of $\mathbf{M}$ considered below.

Since each modulus has a determinant constraint, $|\det(\mathbf{M})|$ is also upper bounded. We first focus on the two-dimensional case and assume $|\det(\mathbf{M})| \le p$, where p is a prime integer. The question is whether there exists a non-diagonal integer matrix $\mathbf{M}$ under this constraint whose lattice has a longer shortest vector than those generated by all diagonal integer matrices under the same constraint.

The related two-dimensional integer-lattice problem has been studied previously for a general prescribed determinant. Bajić and Woods [34] considered, for a given positive integer P, finding a 2×2 integer matrix satisfying $|\det(\mathbf{M})| = P$ that maximizes the shortest-vector length. They first removed the integer constraint, for which the optimal hexagonal lattice gives an upper bound, and then searched near the hexagonal lattice for integer matrices with the prescribed determinant. With a fixed finite search region, this practical search does not, in general, guarantee the global optimum. They also noted that global optimality can be guaranteed by allowing the search region to increase without bound, at the cost of reducing the procedure to exhaustive search [34, Sec. IV-A].

For the prime determinant considered here, the HNF representation takes a simple finite and complete form. Together with the congruence relation derived below, this structure allows us to determine the maximum shortest-vector length exactly with a finite search.

We examine all 2×2 integer matrices of determinant p. Let

$$\mathbf{N}_i = \begin{pmatrix} 1 & 0 \\ i & p \end{pmatrix},$$

for $i = 0, 1, 2, \cdots, p-1$, where p is a prime integer. Each $\mathbf{N}_i$ is in Hermite normal form (HNF), and together with $\mathrm{diag}(p, 1)$ they represent all distinct HNFs of 2×2 integer matrices with determinant p. Matrices with the same HNF generate the same lattice. Hence all the possible lattices generated by all 2×2 integer matrices with determinant p are exactly those generated by $\mathbf{N}_i$ for $0 \le i < p$ and $\mathrm{diag}(p, 1)$. The diagonal matrix $\mathrm{diag}(p, 1)$ always generates a lattice whose shortest non-zero vector has length 1, offering no robustness advantage. We therefore focus on $\mathbf{N}_i$ with $0 \le i < p$.

[1]For the conventional 1D-CRT, this uniquely determinable range is the same as the dynamic range. However, for the MD-CRT in multidimensional cases, it is the set of all uniquely determinable integer vectors from the vector remainders and different from the dynamic range.

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

For the lattices generated by $\mathbf{N}_i$ with $0 \le i < p$, two natural questions arise: which lattice achieves the maximum shortest vector length, and what is the value of this maximum shortest vector length? In the following, we derive a general algorithm to compute $\max_{0\le i<p} \lambda_{\mathcal{L}(\mathbf{N}_i)}$ and the corresponding index i.

The key idea is to find the smallest integer d such that the set of integer vectors

$$\{[x,y]^\top | x^2+y^2 \le d\} \setminus \{[0,0]^\top\} \tag{10}$$

contains at least one vector from each lattice $\mathcal{L}(\mathbf{N}_i)$, $0 \le i < p$. Then, $\sqrt{d}$ equals the maximum shortest non-zero vector length over these lattices, i.e.,

$$\sqrt{d} = \max_{0\le i<p} \lambda_{\mathcal{L}(\mathbf{N}_i)}.$$

Since $[1,i]^\top \in \mathcal{L}(\mathbf{N}_i)$ for every $0 \le i \le p-1$, the shortest nonzero vector length of $\mathcal{L}(\mathbf{N}_i)$ satisfies

$$\lambda^2_{\mathcal{L}(\mathbf{N}_i)} \le \|[1,i]^\top\|_2^2 = 1+i^2 \le 1+(p-1)^2 < p^2.$$

Hence, it suffices to search for the maximum shortest vector length over $d < p^2$. Moreover, since $[0,p]^\top$ is a basis vector of $\mathcal{L}(\mathbf{N}_i)$, the shortest nonzero lattice vector $[x,y]^\top$ with $x=0$ has length p, which is greater than $\lambda_{\mathcal{L}(\mathbf{N}_i)}$. If $[x,y]^\top \in \mathcal{L}(\mathbf{N}_i)$, then so does $[-x,-y]^\top$. Therefore, it is sufficient to restrict the search to integer vectors $[x,y]^\top$ with $0 < x < p$ in the set (10).

For each lattice $\mathcal{L}(\mathbf{N}_i)$, every lattice point has the form $[m, im+np]^\top$, where m and n are integers. Equivalently, $[x,y]^\top \in \mathcal{L}(\mathbf{N}_i)$ if and only if $xi \equiv y \mod p$. When p is prime, $\mathbb{Z}_p$ is a field under modulo-p operations, so every nonzero $x \in \mathbb{Z}_p$ has a unique inverse x^{-1}. Hence, for any $[x,y]^\top$ with $0 < x < p$, there exists a unique $i \in \mathbb{Z}_p$ such that $i \equiv yx^{-1} \mod p$ and $[x,y]^\top \in \mathcal{L}(\mathbf{N}_i)$. These observations lead directly to Algorithm 1. The procedure returns the exact maximum shortest-vector length among the lattices $\mathcal{L}(\mathbf{N}_i)$. The prime assumption is used only for this exact two-dimensional search and is not required by the robust MD-CRT itself. For a non-prime determinant, the HNF representation is no longer reduced to the simple one-parameter family used above, and a nonzero integer does not always have a multiplicative inverse modulo the determinant. Therefore, Algorithm 1 cannot be directly applied to this case. For general prescribed determinants, existing integer-lattice search methods, such as that of Bajić and Woods [34], may provide more general approaches.

We briefly discuss the complexity of Algorithm 1. From the two-dimensional hexagonal-lattice upper bound [34], the squared shortest-vector length satisfies $d \le 2p/\sqrt{3}$, and hence the algorithm needs to consider only $O(p)$ values of d. For each d, at most $O(\sqrt{d})$ values of x are examined. Therefore, the worst-case computational complexity is $O(p^{3/2})$, and the set $\mathcal{S}$ requires $O(p)$ storage.

For a diagonal integer matrix $\mathbf{D} = \mathrm{diag}(a,b)$, the shortest-vector length of $\mathcal{L}(\mathbf{D})$ is $\min\{|a|,|b|\}$. Under $|\det(\mathbf{D})| = |ab| \le p$, we have $\min\{|a|,|b|\} \le \lfloor\sqrt{p}\rfloor$. This value is achieved by $\mathbf{D} = \lfloor\sqrt{p}\rfloor \mathbf{I}$. Hence, the maximum shortest-vector length among all diagonal integer matrices satisfying the determinant constraint is $\lfloor\sqrt{p}\rfloor$.

Algorithm 1: Finding the maximum shortest non-zero vector length among lattices $\mathcal{L}(\mathbf{N}_i)$, $0 \le i < p$

Input: A prime integer p
Output: The maximum shortest non-zero vector length $\sqrt{d}$ and a set of indices i achieving it
Initialize $d \leftarrow 1$, $\mathcal{S} \leftarrow \emptyset$;
while $|\mathcal{S}| < p$ **do**
  $\mathcal{S}_{\text{new}} \leftarrow \emptyset$;
  for $x \leftarrow 1$ **to** $\lfloor\sqrt{d}\rfloor$ **do**
    $y^2 \leftarrow d - x^2$;
    if $y^2 < 0$ ***or*** y^2 *is not a perfect square* **then**
      continue;
    $y \leftarrow \sqrt{y^2}$;
    foreach $y' \in \{-y, +y\}$ **do**
      $a \leftarrow (y' \cdot x^{-1}) \bmod p$;
      if $a \notin \mathcal{S}$ **then**
        $\mathcal{S}_{\text{new}} \leftarrow \mathcal{S}_{\text{new}} \cup \{a\}$;
  $\mathcal{S} \leftarrow \mathcal{S} \cup \mathcal{S}_{\text{new}}$;
  if $|\mathcal{S}| = p$ **then**
    return $\sqrt{d}, \mathcal{S}_{new}$;
  $d \leftarrow d+1$;

Based on Algorithm 1, we compute the solutions for all prime integers $p < 100{,}000$. For every tested p, the exact maximum shortest-vector length among the lattices $\mathcal{L}(\mathbf{N}_i)$, $0 \le i < p$, is strictly greater than $\lfloor\sqrt{p}\rfloor$. Therefore, for every tested p, there exists a non-diagonal integer matrix with determinant p whose shortest-vector length is larger than that of every diagonal integer matrix satisfying $|\det(\mathbf{D})| \le p$.

Example 1: Consider $p = 3257$. For diagonal matrices, the maximum shortest-vector length under the determinant constraint is $\lfloor\sqrt{p}\rfloor = 57$. In contrast, Algorithm 1 shows that one of the maximizing matrices is

$$\mathbf{N}_{971} = \begin{pmatrix} 1 & 0 \\ 971 & 3257 \end{pmatrix},$$

whose shortest-vector length is $\sqrt{3730} \approx 61.07$.

We next give a three-dimensional integer example to show that this robustness advantage is not restricted to two dimensions. Let the determinant constraint be $|\det(\mathbf{M})| \le p$ with the prime integer $p = 54001$. Consider

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}. \tag{11}$$

This integer matrix generates the face-centered cubic lattice [35], and satisfies $|\det(\mathbf{A})| = 2$ and $\lambda_{\mathcal{L}(\mathbf{A})} = \sqrt{2}$. The largest shortest-vector length among all diagonal integer matrices under the determinant constraint is 37, achieved by $37\mathbf{I}$. On the other hand, the non-diagonal choice $\mathbf{M}_{\text{nd}} = 30\mathbf{A}$ satisfies $|\det(\mathbf{M}_{\text{nd}})| = 54000 < p$ and $\lambda_{\mathcal{L}(\mathbf{M}_{\text{nd}})} = 30\sqrt{2} \approx 42.43$. Therefore, its shortest-vector length is larger than that of every diagonal choice of $\mathbf{M}$ under the same determinant constraint.

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

According to (8), this gives a larger sufficient vector remainder error bound in the corresponding robust MD-CRT. A general characterization of the best integer matrices $\mathbf{M}$ under determinant constraints in higher dimensions is left for future work.

The above optimization considers robustness under only the determinant constraint. In practical systems, additional structural constraints may also be imposed on $\mathbf{M}$. For example, non-diagonal integer matrices can arise naturally from non-separable planar sampling geometries in 3D SAR imaging [33]. In SR-ADC or modulo-ADC systems, structured constructions based on the complex CRT or Gaussian integers [10], [28] may be easier to implement than a general matrix selected only according to its shortest-vector length. In such cases, the same shortest-vector criterion can be used to compare the admissible matrices within the corresponding structured family.

These results show that, in the considered two-dimensional setting with a prime determinant constraint and in the three-dimensional example above, a non-diagonal choice of $\mathbf{M}$ can provide a larger sufficient vector remainder error bound than any diagonal choice under the same constraint. To further improve the robustness of robust MD-CRT, we next turn to the second focus of this paper: how to further enhance the robustness of the robust MD-CRT through a multistage framework similar to the robust 1D-CRT studied in [18].

V. Multistage Robust MD-CRT

In the MD-CRT, a large dynamic range is usually obtained by using many pairwise co-prime matrix moduli. However, if all moduli are pairwise co-prime, then every gcld $\mathbf{G}_{i,j}$ is unimodular and hence $\lambda_{\mathcal{L}(\mathbf{G}_{i,j})} = 1$. From (8), the vector remainder error bound satisfies $\tau < 1/4$. Since the vector remainders and their errors are integer vectors, no nonzero error can be tolerated in this case.

Therefore, robustness requires redundancy among the matrix moduli, similar to the robust 1D-CRT. For a fixed set of matrix moduli, there are two possible ways to improve robustness. One is to reduce the dynamic range in exchange for a larger vector remainder error bound, as studied for the robust 1D-CRT in [19]. The other is to use a multistage reconstruction method to improve robustness without reducing the dynamic range, as studied for the robust 1D-CRT in [18]. This section focuses on the latter. Such a multistage method may provide robustness even when the single-stage robust MD-CRT cannot tolerate any nonzero error, and may also further increase the vector remainder error bound over that from the single-stage method.

The basic idea of the multistage robust CRT in [18] is to divide the moduli into groups, perform robust reconstruction within each group, and then use the reconstructed results as remainders in the next stage. For the 1D-CRT, this procedure can be applied directly because the robustly determinable range of each group is an interval and can serve as a remainder range for the next stage. For the MD-CRT, however, the robustly determinable range of a group does not necessarily form an FPD of an lcrm of that group. Consequently, even if the first-stage reconstruction is robust, its output cannot always be directly regarded as a valid vector remainder in the next stage. This is the main difficulty in extending the multistage robust CRT to the MD-CRT.

We first use an example to illustrate this difficulty and show why directly applying the 1D multistage procedure is not sufficient. We then derive an easily checkable sufficient condition under which the robustly determinable range of a group becomes an FPD of an lcrm of that group. Based on this condition, we develop the two-stage robust MD-CRT and then extend it to the general multistage case.

A. Motivating Example

Let

$$\mathbf{\Gamma}_1 = \begin{pmatrix} 22 & -17 \\ 17 & 22 \end{pmatrix}, \quad \mathbf{A}_1 = \begin{pmatrix} 16 & 0 \\ 1 & 16 \end{pmatrix}, \quad \mathbf{A}_2 = \begin{pmatrix} 16 & 1 \\ 0 & 16 \end{pmatrix},$$
$$\mathbf{\Gamma}_2 = \begin{pmatrix} 22 & 17 \\ -17 & 22 \end{pmatrix}, \quad \mathbf{B}_1 = \begin{pmatrix} 24 & 0 \\ 1 & 24 \end{pmatrix}, \quad \mathbf{B}_2 = \begin{pmatrix} 24 & 1 \\ 0 & 24 \end{pmatrix}.$$

Consider the six matrix moduli

$$\mathbf{M}_1 = \mathbf{\Gamma}_1, \quad \mathbf{M}_2 = \mathbf{\Gamma}_1\mathbf{A}_1, \quad \mathbf{M}_3 = \mathbf{\Gamma}_1\mathbf{A}_2,$$
$$\mathbf{M}_4 = \mathbf{\Gamma}_2, \quad \mathbf{M}_5 = \mathbf{\Gamma}_2\mathbf{B}_1, \quad \mathbf{M}_6 = \mathbf{\Gamma}_2\mathbf{B}_2.$$

Since $\mathbf{\Gamma}_1$ and $\mathbf{\Gamma}_2$ are co-prime, for every $\mathbf{M}_i$, $1 \le i \le 6$, there exists another $\mathbf{M}_j$, $j \neq i$, that is co-prime with it. Thus, by Proposition 2, the single-stage robust MD-CRT has $\tau < 1/4$ and cannot tolerate any integer vector remainder error.

However, the first three moduli share the common left divisor $\mathbf{\Gamma}_1$, while the last three moduli share the common left divisor $\mathbf{\Gamma}_2$. This suggests the grouping

$$\{\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3\}, \qquad \{\mathbf{M}_4, \mathbf{M}_5, \mathbf{M}_6\}.$$

Let $\mathbf{R}_1$ and $\mathbf{R}_2$ be lcrms of the two groups, respectively. In the error-free case, the first group gives the vector remainder $\mathbf{f}_1 \in \mathcal{N}(\mathbf{R}_1)$ satisfying

$$\mathbf{f} \equiv \mathbf{f}_1 \mod \mathbf{R}_1, \tag{12}$$

and the second group gives $\mathbf{f}_2 \in \mathcal{N}(\mathbf{R}_2)$ satisfying

$$\mathbf{f} \equiv \mathbf{f}_2 \mod \mathbf{R}_2. \tag{13}$$

The second stage then reconstructs $\mathbf{f}$ from the two congruences (12) and (13). Since an lcrm of $\mathbf{R}_1$ and $\mathbf{R}_2$ is also an lcrm of all six original moduli, this grouping does not reduce the noiseless dynamic range.

The difficulty appears in the robust case. For the first group, the gcld of any two moduli is $\mathbf{\Gamma}_1$. Thus, choosing $l_0 = 1$, Proposition 2 guarantees robust reconstruction over

$$\left\lfloor \mathbf{M}_1^{-1}\mathbf{f} \right\rfloor \in \mathcal{N}\left(\mathbf{M}_1^{-1}\mathbf{R}_1\right) \tag{14}$$

whenever $\tau < \lambda_{\mathcal{L}(\mathbf{\Gamma}_1)}/4 = \sqrt{773}/4$. Similarly, for the second group, choosing $l_0 = 4$, robust reconstruction is guaranteed over

$$\left\lfloor \mathbf{M}_4^{-1}\mathbf{f} \right\rfloor \in \mathcal{N}\left(\mathbf{M}_4^{-1}\mathbf{R}_2\right) \tag{15}$$

whenever $\tau < \lambda_{\mathcal{L}(\mathbf{\Gamma}_2)}/4 = \sqrt{773}/4$.

Ideally, the first-stage outputs should be erroneous versions of the true vector remainders $\mathbf{f}_1$ and $\mathbf{f}_2$ modulo $\mathbf{R}_1$ and $\mathbf{R}_2$, so

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

that the second stage again becomes a single-stage robust MD-CRT problem. This property is automatic in the error-free MD-CRT. It is also automatic in the one-dimensional robust CRT, because the robustly determinable range is always an interval and hence a one-dimensional FPD.

In the multidimensional robust MD-CRT, however, this property is not automatic. Although $\mathcal{N}(\mathbf{M}_1^{-1}\mathbf{R}_1)$ and $\mathcal{N}(\mathbf{M}_4^{-1}\mathbf{R}_2)$ in (14) and (15) are FPDs, the corresponding robustly determinable ranges of $\mathbf{f}$ induced by these conditions may not be FPDs of any integer matrix. They are generally unions of shifted copies of $\mathcal{N}(\mathbf{M}_1)$ or $\mathcal{N}(\mathbf{M}_4)$. Then the first-stage output may fail to be an erroneous version of a true vector remainder in $\mathcal{N}(\mathbf{R}_i)$, and therefore cannot be used as a valid input for the next stage. This is the main obstacle in extending the multistage robust CRT from one dimension to multiple dimensions. We next derive a sufficient condition under which this obstacle disappears.

B. A Sufficient Condition for Multistage Robustness

For the multistage framework to be valid, each intermediate robust stage must produce a vector that can be interpreted as a vector remainder modulo the lcrm of that group. Therefore, the robustly determinable range at every intermediate stage must form an FPD of some integer matrix. We now derive a simple sufficient condition for this property.

Consider a single-stage robust MD-CRT with moduli $\mathbf{M}_1, \ldots, \mathbf{M}_L$, and choose the index l_0 as in Proposition 2. Let $\mathbf{R}$ be an lcrm of these moduli. From (6), every vector in the robustly determinable range satisfies

$$\left\lfloor \mathbf{M}_{l_0}^{-1}\mathbf{f} \right\rfloor \in \mathcal{N}(\mathbf{M}_{l_0}^{-1}\mathbf{R}).$$

Using the decomposition (9), the robustly determinable range can be written as the union of shifted FPDs

$$\bigcup_{\mathbf{k}\in\mathcal{N}(\mathbf{M}_{l_0}^{-1}\mathbf{R})} \left(\mathcal{N}(\mathbf{M}_{l_0}) + \mathbf{M}_{l_0}\mathbf{k}\right). \tag{16}$$

This union contains $\frac{|\det(\mathbf{R})|}{|\det(\mathbf{M}_{l_0})|}$ disjoint shifted copies of $\mathcal{N}(\mathbf{M}_{l_0})$. In general, such a union is not necessarily an FPD.

Example 2: Let

$$\mathbf{M}_1 = \begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}, \mathbf{M}_2 = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}.$$

An lcrm of these two matrices is $\mathbf{R} = 4\mathbf{I}$ [23, 25]. Then, we have

$$\mathcal{N}(\mathbf{M}_1^{-1}\mathbf{R}) = \{[0,0]^\top, [1,0]^\top, [0,1]^\top, [1,-1]^\top\}.$$

The corresponding robustly determinable range is shown in Fig. 1. This figure shows exactly four shifted copies of $\mathcal{N}(\mathbf{M}_1)$ and the dashed lines and hollow circles are not included in the robustly determinable range.

Since both $[0,0]^\top$ and $[2,0]^\top$ lie in the robustly determinable range in Example 2 while $[1,0]^\top$ does not, this region cannot be represented as an FPD of any integer matrix.

Example 2 shows that the robustly determinable range is not always a valid remainder set. The next lemma gives an easily checked sufficient condition under which the union in (16) is exactly an FPD.

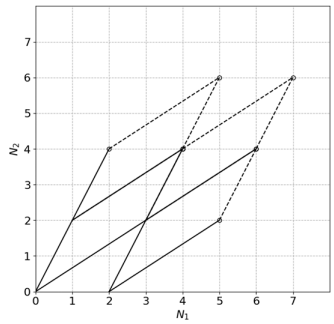


Fig. 1. The robustly determinable range in Example 2.

Lemma 4: Let $\mathbf{M}_1, \cdots, \mathbf{M}_L$ be nonsingular integer matrices. If the Hermite normal form of the matrix $\mathbf{M}_{l_0}^{-1}\operatorname{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L)$ is a diagonal matrix, denoted by $\mathbf{D}$, then the robustly determinable range in (16) can be expressed as the FPD of $\mathbf{M}_{l_0}\mathbf{D}$, when $\operatorname{lcrm}(\mathbf{M}_1, \mathbf{M}_2, \cdots, \mathbf{M}_L) = \mathbf{M}_{l_0}\mathbf{D}$.

Proof: Since all lcrms of $\mathbf{M}_1, \ldots, \mathbf{M}_L$ share the same Hermite normal form, the Hermite normal form of $\mathbf{M}_{l_0}^{-1}\operatorname{lcrm}(\mathbf{M}_1, \ldots, \mathbf{M}_L)$ is unique. Let this HNF be a diagonal matrix $\mathbf{D}$. Then there exists a unimodular matrix $\mathbf{U}$ such that $\mathbf{M}_{l_0}^{-1}\operatorname{lcrm}(\mathbf{M}_1, \ldots, \mathbf{M}_L)\mathbf{U} = \mathbf{D}$. Thus $\mathbf{R} = \mathbf{M}_{l_0}\mathbf{D}$ is also an lcrm of $\mathbf{M}_1, \ldots, \mathbf{M}_L$. With this choice of $\mathbf{R}$, the robustly determinable range in (16) becomes

$$\mathcal{S} = \bigcup_{\mathbf{k}\in\mathcal{N}(\mathbf{D})} \left(\mathcal{N}(\mathbf{M}_{l_0}) + \mathbf{M}_{l_0}\mathbf{k}\right).$$

We prove that $\mathcal{S} = \mathcal{N}(\mathbf{R})$.

For any $\mathbf{s} \in \mathcal{S}$, there exist $\mathbf{x} \in [0,1)^D$ and $\mathbf{k} \in \mathcal{N}(\mathbf{D})$ such that $\mathbf{s} = \mathbf{M}_{l_0}(\mathbf{x} + \mathbf{k})$. Let $\mathbf{D} = \operatorname{diag}(d_1, \ldots, d_D)$. Since $\mathbf{k} \in \mathcal{N}(\mathbf{D})$, we have $0 \le k_i \le d_i - 1$. Hence $\mathbf{D}^{-1}(\mathbf{x} + \mathbf{k}) \in [0,1)^D$, and $\mathbf{s} = \mathbf{M}_{l_0}\mathbf{D}\left(\mathbf{D}^{-1}(\mathbf{x} + \mathbf{k})\right) \in \mathcal{N}(\mathbf{M}_{l_0}\mathbf{D}) = \mathcal{N}(\mathbf{R})$.

Conversely, for any $\mathbf{z} \in \mathcal{N}(\mathbf{R})$, there exists $\mathbf{y} \in [0,1)^D$ such that $\mathbf{z} = \mathbf{M}_{l_0}\mathbf{D}\mathbf{y}$. Write $\mathbf{D}\mathbf{y} = \lfloor \mathbf{D}\mathbf{y} \rfloor + \mathbf{r}$, where $\lfloor \mathbf{D}\mathbf{y} \rfloor \in \mathcal{N}(\mathbf{D})$ and $\mathbf{r} \in [0,1)^D$. Then $\mathbf{z} = \mathbf{M}_{l_0}\mathbf{r} + \mathbf{M}_{l_0}\lfloor \mathbf{D}\mathbf{y} \rfloor \in \mathcal{S}$. Therefore, $\mathcal{S} = \mathcal{N}(\mathbf{R})$. □

Lemma 4 gives an easily checkable sufficient condition. When it holds, the robustly determinable range coincides with the FPD of a chosen lcrm, and the intermediate output can be used as a valid vector remainder in the next stage. The condition is sufficient but not necessary and there exist cases where the robustly determinable range can still form an FPD even when the corresponding HNF is not diagonal.

C. A Multistage Robust Reconstruction Framework

We now return to the motivating example. For the first group $\{\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3\}$, with $l_0 = 1$, there exists an lcrm $\mathbf{R}_1 = \mathbf{M}_1(256\mathbf{I})$. Thus Lemma 4 applies. By Proposition 2, if $\tau < \lambda_{\mathcal{L}(\mathbf{\Gamma}_1)}/4 = \sqrt{773}/4$, then the first group produces an estimate $\tilde{\mathbf{f}}_1$ satisfying $\|\mathbf{f}_1 - \tilde{\mathbf{f}}_1\| \le \tau$, where $\mathbf{f}_1$ is the true vector remainder modulo $\mathbf{R}_1$ in (12).

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

Similarly, for the second group $\{\mathbf{M}_4, \mathbf{M}_5, \mathbf{M}_6\}$, with $l_0 = 4$, there exists an lcrm $\mathbf{R}_2 = \mathbf{M}_4(576\mathbf{I})$, and if $\tau < \lambda_{\mathcal{L}(\mathbf{\Gamma}_2)}/4 = \sqrt{773}/4$, then the second group produces an estimate $\tilde{\mathbf{f}}_2$ satisfying $\|\mathbf{f}_2 - \tilde{\mathbf{f}}_2\| \le \tau$.

In the second stage, we treat $\mathbf{R}_1, \mathbf{R}_2$ as new moduli and $\tilde{\mathbf{f}}_1, \tilde{\mathbf{f}}_2$ as their erroneous remainders. Since the gcld of $\mathbf{R}_1$ and $\mathbf{R}_2$ is $64\mathbf{I}$, the second-stage bound is $\tau < \lambda_{\mathcal{L}(64\mathbf{I})}/4 = 16$. Combining the two stages, the overall vector remainder error bound is

$$\tau < \min\{\sqrt{773}/4, 16\} = \sqrt{773}/4.$$

Thus, although the direct single-stage robust MD-CRT applied to all six moduli has no error tolerance, the two-stage method achieves nontrivial robustness without reducing the noiseless dynamic range.

We next present the general two-stage framework. Let $\mathcal{M}$ be the full set of matrix moduli. For $1 \le i \le K$, let

$$\mathcal{M}_i = \{\mathbf{M}_{i,1}, \mathbf{M}_{i,2}, \ldots, \mathbf{M}_{i,L_i}\}$$

be K (not necessarily disjoint) subsets of $\mathcal{M}$ whose union is $\mathcal{M}$. Let $\mathbf{R}_i$ be an lcrm of the matrices in $\mathcal{M}_i$. If $L_i = 1$, set $\mathbf{R}_i = \mathbf{M}_{i,1}$. If $L_i > 1$, assume that $\mathbf{M}_{i,1}$ satisfies Lemma 4, i.e., the HNF of

$$\mathbf{M}_{i,1}^{-1} \operatorname{lcrm}(\mathbf{M}_{i,1}, \ldots, \mathbf{M}_{i,L_i})$$

is a diagonal matrix $\mathbf{D}_i$, and choose $\mathbf{R}_i = \mathbf{M}_{i,1}\mathbf{D}_i$. Let $\mathbf{f}_i \in \mathcal{N}(\mathbf{R}_i)$ be the vector remainder of $\mathbf{f}$ modulo $\mathbf{R}_i$.

The original congruence system is

$$\mathbf{f} = \mathbf{M}_{i,j}\mathbf{n}_{i,j} + \mathbf{r}_{i,j}, \qquad 1 \le i \le K, \quad 1 \le j \le L_i. \tag{17}$$

In the first stage, each group gives the subsystem

$$\mathbf{f}_i = \mathbf{M}_{i,j}\mathbf{n}'_{i,j} + \mathbf{r}_{i,j}, \qquad 1 \le j \le L_i. \tag{18}$$

After the first stage, the intermediate vector remainders $\{\mathbf{f}_i\}_{i=1}^K$ form the second-stage system

$$\mathbf{f} = \mathbf{R}_i\mathbf{n}_i + \mathbf{f}_i, \qquad 1 \le i \le K. \tag{19}$$

If there exists a unimodular matrix $\mathbf{U}$ such that $\mathbf{R}_i = \mathbf{R}_j\mathbf{U}$ for some $i \ne j$, then one of the equations in (19) is redundant and can be omitted. In the following, we assume that no such unimodular equivalence holds between any distinct pair $\mathbf{R}_i$ and $\mathbf{R}_j$.

We now turn to the case with erroneous vector remainders. Let $\tilde{\mathbf{r}}_{i,j}$ denote the erroneous vector remainder of $\mathbf{f}$ modulo $\mathbf{M}_{i,j}$ for $1 \le i \le K$ and $1 \le j \le L_i$. Based on these inputs, we present a robust reconstruction procedure for $\mathbf{f}$, referred to as the *two-stage robust MD-CRT*.

Step 1: For each subsystem (18) corresponding to $\mathcal{M}_i$:
- If $L_i > 1$, fix $l_0 = 1$ and apply Steps 2–5 of the single-stage robust MD-CRT in Section IV to obtain a robust estimate $\tilde{\mathbf{f}}_i$ of $\mathbf{f}_i$.
- If $L_i = 1$, simply set $\mathbf{R}_i = \mathbf{M}_{i,1}$ and $\tilde{\mathbf{f}}_i = \tilde{\mathbf{r}}_{i,1}$.

Step 2: Regard the estimates $\tilde{\mathbf{f}}_i$ as the erroneous remainders in the system (19), and apply Steps 1–5 of the single-stage robust MD-CRT in Section IV to obtain the final estimate $\tilde{\mathbf{f}}$ of $\mathbf{f}$.

Remark 2 (Real-valued intermediate errors): Although the original remainder errors considered in Proposition 2 are integer vectors, the intermediate estimation errors in the multistage framework may be real-valued because of the averaging in Step 5. The sufficient condition in (8) remains valid for such errors, since its derivation depends only on the error norms and the minimum distances of the corresponding gcld lattices, rather than whether the errors are integer-valued. Therefore, the same sufficient bound can be used when the intermediate estimates are treated as erroneous remainders in subsequent stages.

The correctness and robustness of this two-stage procedure are established in the following theorem.

For each $1 \le i \le K$, let τ_i be the vector remainder error bound in the i-th group, i.e.,

$$\|\Delta\mathbf{r}_{i,j}\| = \|\tilde{\mathbf{r}}_{i,j} - \mathbf{r}_{i,j}\| \le \tau_i,$$

for $1 \le j \le L_i$.

For each group $\mathcal{M}_i$ with $L_i > 1$, let $\mathbf{G}_{j_1,j_2}^{(i)}$ be a gcld of $\mathbf{M}_{i,j_1}$ and $\mathbf{M}_{i,j_2}$ for $1 \le j_1 \ne j_2 \le L_i$ and define

$$\delta_i = \min_{2 \le j \le L_i} \frac{\lambda_{\mathcal{L}(\mathbf{G}_{1,j}^{(i)})}}{4}.$$

For each group $\mathcal{M}_i$, the first matrix $\mathbf{M}_{i,1}$ is assumed to be the one satisfying Lemma 4, which plays the role of $\mathbf{M}_{l_0}$ in Proposition 2. Therefore, in computing the vector remainder error bound, we fix $l_0 = 1$ for every group. If $L_i = 1$, we conventionally set $\delta_i = +\infty$ since a single modulus imposes no restriction at this stage.

Let $\mathbf{R}$ be an lcrm of $\mathbf{R}_1, \mathbf{R}_2, \ldots, \mathbf{R}_K$ and let $\mathbf{P}_{i,j}$ be a gcld of $\mathbf{R}_i$ and $\mathbf{R}_j$ for $1 \le i \ne j \le K$. Choose an index l_0 such that

$$\min_{\substack{1 \le j \le K \\ j \ne l_0}} \lambda_{\mathcal{L}(\mathbf{P}_{l_0,j})} = \max_{1 \le i \le K} \min_{\substack{1 \le j \le K \\ j \ne i}} \lambda_{\mathcal{L}(\mathbf{P}_{i,j})},$$

and define

$$\delta = \min_{\substack{1 \le j \le K \\ j \ne l_0}} \frac{\lambda_{\mathcal{L}(\mathbf{P}_{l_0,j})}}{4}.$$

Theorem 2: Let $\mathbf{f}$ be an integer vector such that

$$\mathbf{f} \in \bigcup_{\mathbf{k} \in \mathcal{N}(\mathbf{R}_{l_0}^{-1}\mathbf{R})} \big(\mathcal{N}(\mathbf{R}_{l_0}) + \mathbf{R}_{l_0}\mathbf{k}\big).$$

If the vector remainder errors satisfy

$$\|\Delta\mathbf{r}_{i,j}\| \le \tau_i < \min\{\delta_i, \delta\}, \tag{20}$$

for all $1 \le i \le K$ and $1 \le j \le L_i$, then $\mathbf{f}$ can be robustly reconstructed. In particular, the estimate $\tilde{\mathbf{f}}$ obtained by the two-stage robust MD-CRT satisfies

$$\|\tilde{\mathbf{f}} - \mathbf{f}\| \le \frac{1}{K}\sum_{i=1}^{K} \tau_i. \tag{21}$$

Proof: For each i with $L_i > 1$, Lemma 4 ensures that, with $\mathbf{M}_{i,1}$ chosen as $\mathbf{M}_{l_0}$ in Proposition 2, the robustly determinable range equals $\mathcal{N}(\mathbf{R}_i)$.

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

Since $\mathbf{f}_i \in \mathcal{N}(\mathbf{R}_i)$ and $\|\Delta\mathbf{r}_{i,j}\| \le \tau_i < \delta_i$, Proposition 2 ensures that $\mathbf{M}_{i,j}\mathbf{n}'_{i,j}$ in (18) can be correctly determined. Thus, $\mathbf{f}_i$ can be robustly reconstructed as

$$\tilde{\mathbf{f}}_i = \frac{1}{L_i}\sum_{j=1}^{L_i}(\mathbf{M}_{i,j}\mathbf{n}'_{i,j} + \tilde{\mathbf{r}}_{i,j}).$$

Moreover, we have

$$\|\tilde{\mathbf{f}}_i - \mathbf{f}_i\| \le \|\frac{1}{L_i}\sum_{j=1}^{L_i}\Delta\mathbf{r}_{i,j}\| \le \tau_i.$$

If $L_i = 1$, then $\mathbf{R}_i = \mathbf{M}_{i,1}$ and $\tilde{\mathbf{f}}_i = \tilde{\mathbf{r}}_{i,1}$. In this case, the first stage reduces to a trivial identity and no further operation is needed.

In the second stage, the estimates $\tilde{\mathbf{f}}_i$ serve as erroneous vector remainders in the system (19). Since

$$\mathbf{f} \in \bigcup_{\mathbf{k}\in\mathcal{N}(\mathbf{R}_{l_0}^{-1}\mathbf{R})} \left(\mathcal{N}(\mathbf{R}_{l_0}) + \mathbf{R}_{l_0}\mathbf{k}\right)$$

and $\|\tilde{\mathbf{f}}_i - \mathbf{f}_i\| \le \tau_i < \delta$, Proposition 2 guarantees that $\mathbf{R}_i\mathbf{n}_i$ can be accurately obtained. Therefore, $\mathbf{f}$ can be robustly reconstructed as

$$\tilde{\mathbf{f}} = \frac{1}{K}\sum_{i=1}^{K}(\mathbf{R}_i\mathbf{n}_i + \tilde{\mathbf{f}}_i).$$

Therefore, we obtain the error bound in (21). □

The motivating example presented earlier has shown a case where the single-stage method cannot provide any robustness, while the two-stage framework successfully enables robust reconstruction. We next present another example to show that even when the single-stage method already provides a certain level of robustness, the proposed multistage framework can further improve the robustness level.

Example 3: Let

$$\mathbf{C}_1 = \begin{pmatrix} 7 & 0 \\ 1 & 7 \end{pmatrix}, \mathbf{C}_2 = \begin{pmatrix} 7 & 1 \\ 0 & 7 \end{pmatrix}, \mathbf{C}_3 = \begin{pmatrix} 11 & 1 \\ 0 & 11 \end{pmatrix}.$$

These three matrices are pairwise co-prime [27]. For any 2×2 matrix $\mathbf{M}$, consider the following four matrix moduli:

$$30\mathbf{M}, 10\mathbf{M}\mathbf{C}_1, 15\mathbf{M}\mathbf{C}_2, 42\mathbf{M}\mathbf{C}_3.$$

For the single-stage robust MD-CRT, choosing $30\mathbf{M}$ as $\mathbf{M}_{l_0}$ achieves the maximum vector remainder error bound $3\lambda_{\mathcal{L}(\mathbf{M})}/2$.

For the two-stage robust MD-CRT, since $30\mathbf{M}$, $10\mathbf{M}\mathbf{C}_1, 15\mathbf{M}\mathbf{C}_2$ satisfy Lemma 4, we divide the matrix moduli into the following two groups: $\{30\mathbf{M}, 10\mathbf{M}\mathbf{C}_1, 15\mathbf{M}\mathbf{C}_2\}$ and $\{42\mathbf{M}\mathbf{C}_3\}$. For the first group, when $30\mathbf{M}$ is chosen as $\mathbf{M}_{l_0}$, the lcrm $\mathbf{R}_1$ is $1470\mathbf{M}$ and the robustness level $\delta_1 = 5\lambda_{\mathcal{L}(\mathbf{M})}/2$. Since the second group contains only one matrix, it is directly carried into the second stage. So, the moduli in the second stage are $1470\mathbf{M}$ and $42\mathbf{M}\mathbf{C}_3$. The robustness level of the second stage is $\delta = 21\lambda_{\mathcal{L}(\mathbf{M})}/2$. As a result, the vector remainder error bound of the two-stage approach is $\min\{\delta_1, \delta\} = 5\lambda_{\mathcal{L}(\mathbf{M})}/2$, which is greater than that of the single-stage robust MD-CRT shown above.

In Theorem 2, the vector remainder errors within the i-th group must satisfy $\|\Delta\mathbf{r}_{i,j}\| \le \tau_i < \delta_i$, so the vector remainder error bound is governed by δ_i, which depends on the gclds $\{\mathbf{G}_{1,j}^{(i)}\}_{j=2}^{L_i}$. Hence, different partitions of the whole moduli set generally lead to different $\{\delta_i\}_{i=1}^{K}$. In the second stage, the vector remainder error bound is further constrained by δ, which depends on the cross-group gclds $\{\mathbf{P}_{i,j}\}_{i\neq j}$. Consequently, the overall robustness level of the two-stage procedure is $\tau_{\text{overall}} = \min\{\delta_i, \delta\}$. This shows that an appropriate grouping can increase the vector remainder error bound by enlarging some δ_i (and possibly δ).

Unlike the one-dimensional case where groups can be formed arbitrarily, in the multidimensional setting each group needs to satisfy the sufficient condition in Lemma 4 so that its robustly determinable range is an FPD and the vector remainders in Stage-2 are well-defined. Therefore, for a fixed set of matrix moduli, finding a grouping that maximizes τ_{overall} is nontrivial and is an interesting direction for future work.

The two-stage procedure can be naturally extended to multiple stages. Let $\mathcal{M}$ be the full set of matrix moduli, which is also the matrix moduli in the first stage. Let the full set of moduli be processed in $S \ge 3$ stages. At stage s, $1 \le s \le S-1$, we form K_s not necessarily disjoint groups

$$\mathcal{M}_i^{(s)} = \{\mathbf{M}_{i,1}^{(s)}, \mathbf{M}_{i,2}^{(s)}, \ldots, \mathbf{M}_{i,L_i^{(s)}}^{(s)}\}, \quad 1 \le i \le K_s,$$

whose union is the full matrix moduli of stage s. If $L_i^{(s)} = 1$, then we set $\mathbf{R}_i^{(s)} = \mathbf{M}_{i,1}^{(s)}$; otherwise, we assume there exists a matrix $\mathbf{M}_{i,1}^{(s)} \in \mathcal{M}_i^{(s)}$ such that the Hermite normal form of

$$(\mathbf{M}_{i,1}^{(s)})^{-1}\ \text{lcrm}(\mathbf{M}_{i,1}^{(s)}, \ldots, \mathbf{M}_{i,L_i^{(s)}}^{(s)})$$

is a diagonal matrix $\mathbf{D}_i^{(s)}$. We then define $\mathbf{R}_i^{(s)} = \mathbf{M}_{i,1}^{(s)}\mathbf{D}_i^{(s)}$, which is an lcrm of all matrices in $\mathcal{M}_i^{(s)}$. Thus the output matrix moduli of stage s is the collection $\{\mathbf{R}_i^{(s)}\}_{i=1}^{K_s}$, which becomes the input set of matrix moduli at stage $s+1$. Then, the matrix moduli of the final stage S are $\mathbf{R}_1^{(S-1)}, \ldots, \mathbf{R}_{K_{S-1}}^{(S-1)}$.

For each group $\mathcal{M}_i^{(s)}$ with $L_i^{(s)} > 1$, define

$$\delta_i^{(s)} = \min_{2\le j\le L_i^{(s)}} \frac{\lambda_{\mathcal{L}(\,\text{gcld}(\mathbf{M}_{i,1}^{(s)}, \mathbf{M}_{i,j}^{(s)}))}}{4}. \tag{22}$$

If $L_i^{(s)} = 1$, set $\delta_i^{(s)} := +\infty$. For the final stage S, let $\mathbf{R}^{(S)}$ denote an lcrm of $\mathbf{R}_1^{(S-1)}, \ldots, \mathbf{R}_{K_{S-1}}^{(S-1)}$, and define

$$\delta = \min_{\substack{1\le j\le K_{S-1} \\ j\neq l_0}} \frac{\lambda_{\mathcal{L}(\,\text{gcld}(\mathbf{R}_{l_0}^{(S-1)}, \mathbf{R}_j^{(S-1)}))}}{4}, \tag{23}$$

where l_0 is chosen as (5) in Proposition 2 for the set $\{\mathbf{R}_i^{(S-1)}\}_{i=1}^{K_{S-1}}$.

We then define a path sequence for each initial group. For each group $\mathcal{M}_i^{(1)}$, $1 \le i \le K_1$, let

$$\phi^{(1)}(i) := \{i\}, \qquad \phi^{(s)}(i) \subseteq \{1, \ldots, K_s\}, \quad 2 \le s \le S-1,$$

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

where $\phi^{(s)}(i)$ denotes the set of indices of the groups at stage s that can be reached from the first-stage group $\mathcal{M}_i^{(1)}$ through the preceding stages.

We first describe the exact relations among the vector remainders at different stages. For $1 \le s \le S-1$ and $1 \le i \le K_s$, let $\mathbf{f}_i^{(s)} \in \mathcal{N}(\mathbf{R}_i^{(s)})$ denote the exact vector remainder of the original vector $\mathbf{f}$ modulo $\mathbf{R}_i^{(s)}$. For convenience, for each group $\mathcal{M}_i^{(s)}$, $1 \le s \le S-1$ and $1 \le i \le K_s$, we call $\mathbf{R}_i^{(s)}$ the *output modulus* of this group, where $\mathbf{R}_i^{(s)}$ is the chosen lcrm of the matrix moduli in the group when $L_i^{(s)} > 1$, and is its only matrix modulus when $L_i^{(s)} = 1$.

For each first-stage group $\mathcal{M}_i^{(1)}$, $1 \le i \le K_1$, we define one path from this group to the final stage as follows. Let $i_1 = i$. Since the groups at stage 2 cover all the output moduli of stage 1, the output modulus $\mathbf{R}_{i_1}^{(1)}$ belongs to at least one group at stage 2. We choose one such group and denote its index by i_2. Similarly, for each $2 \le s \le S-1$, once $\mathcal{M}_{i_{s-1}}^{(s-1)}$ has been chosen, its output modulus $\mathbf{R}_{i_{s-1}}^{(s-1)}$ belongs to at least one group at stage s. We choose one such group and denote its index by i_s. Thus, $\mathbf{R}_{i_{s-1}}^{(s-1)} \in \mathcal{M}_{i_s}^{(s)}$, for $2 \le s \le S-1$. Finally, the output modulus $\mathbf{R}_{i_{S-1}}^{(S-1)}$ is one of the input moduli at the final stage S. The sequence $i_1 = i, i_2, \ldots, i_{S-1}$ therefore specifies one path from the i-th first-stage group to the final stage. If an output modulus belongs to more than one group at a subsequent stage, any one of these groups can be chosen to continue the path. In particular, $i_s \in \phi^{(s)}(i)$ for $2 \le s \le S-1$.

Along this path, for every $2 \le s \le S-1$, $\mathbf{f}_{i_{s-1}}^{(s-1)}$ is the vector remainder of $\mathbf{f}_{i_s}^{(s)}$ modulo $\mathbf{R}_{i_{s-1}}^{(s-1)}$. Hence, there exists an integer vector $\mathbf{n}_i^{(s)}$ such that

$$\mathbf{f}_{i_s}^{(s)} = \mathbf{R}_{i_{s-1}}^{(s-1)} \mathbf{n}_i^{(s)} + \mathbf{f}_{i_{s-1}}^{(s-1)}. \tag{24}$$

At the final stage, $\mathbf{f}_{i_{S-1}}^{(S-1)}$ is the vector remainder of $\mathbf{f}$ modulo $\mathbf{R}_{i_{S-1}}^{(S-1)}$, so there exists an integer vector $\mathbf{n}_i^{(S)}$ satisfying

$$\mathbf{f} = \mathbf{R}_{i_{S-1}}^{(S-1)} \mathbf{n}_i^{(S)} + \mathbf{f}_{i_{S-1}}^{(S-1)}. \tag{25}$$

Combining these relations gives

$$\mathbf{f} = \mathbf{f}_i^{(1)} + \sum_{s=2}^{S} \mathbf{R}_{i_{s-1}}^{(s-1)} \mathbf{n}_i^{(s)}. \tag{26}$$

We next describe how, for each first-stage group $\mathcal{M}_i^{(1)}$ and one selected path $i_1 = i, i_2, \ldots, i_{S-1}$ from this group to the final stage, an estimate $\tilde{\mathbf{f}}_i$ of the original vector $\mathbf{f}$ is constructed from the erroneous vector remainders. At every stage s, $1 \le s \le S-1$, the complete single-stage robust MD-CRT procedure is applied within each group containing more than one matrix modulus. A group containing only one matrix modulus is passed directly to the next stage without applying the single-stage reconstruction procedure. Recall from Proposition 2 that Steps 3 and 4 of the single-stage procedure determine the terms of the form $\mathbf{Mn}$ in the corresponding system of congruences. If the robustness condition in Proposition 2 is satisfied, these terms are determined accurately.

For the path $i_1 = i, i_2, \ldots, i_{S-1}$ associated with the i-th first-stage group, define, for $2 \le s \le S-1$,

$$\mathbf{q}_i^{(s)} := \mathbf{R}_{i_{s-1}}^{(s-1)} \mathbf{n}_i^{(s)}.$$

If $\mathcal{M}_{i_s}^{(s)}$ contains more than one matrix modulus, let $\widehat{\mathbf{q}}_i^{(s)}$ denote the corresponding estimate obtained in Steps 3 and 4 of the single-stage robust MD-CRT at stage s. These estimates are retained for the final reconstruction. Step 5 is then applied within the group to obtain $\tilde{\mathbf{f}}_{i_s}^{(s)}$, an estimate of $\mathbf{f}_{i_s}^{(s)}$, and this estimate is used as an erroneous vector remainder at stage $s+1$. If $\mathcal{M}_{i_s}^{(s)}$ contains only one matrix modulus, its only matrix modulus is $\mathbf{R}_{i_{s-1}}^{(s-1)}$. Hence, $\mathbf{R}_{i_s}^{(s)} = \mathbf{R}_{i_{s-1}}^{(s-1)}$ and $\mathbf{f}_{i_s}^{(s)} = \mathbf{f}_{i_{s-1}}^{(s-1)}$. We therefore take $\mathbf{n}_i^{(s)} = \mathbf{0}$, so that $\mathbf{q}_i^{(s)} = \mathbf{0}$, and define $\widehat{\mathbf{q}}_i^{(s)} = \mathbf{0}$. In this case, $\tilde{\mathbf{f}}_{i_s}^{(s)} = \tilde{\mathbf{f}}_{i_{s-1}}^{(s-1)}$ is passed directly to the next stage.

At the final stage, the inputs are $\tilde{\mathbf{f}}_1^{(S-1)}, \ldots, \tilde{\mathbf{f}}_{K_{S-1}}^{(S-1)}$, with matrix moduli $\mathbf{R}_1^{(S-1)}, \ldots, \mathbf{R}_{K_{S-1}}^{(S-1)}$, respectively. For the path associated with the i-th first-stage group, define

$$\mathbf{q}_i^{(S)} := \mathbf{R}_{i_{S-1}}^{(S-1)} \mathbf{n}_i^{(S)}.$$

Applying Steps 1–4 of the single-stage robust MD-CRT at the final stage gives an estimate $\widehat{\mathbf{q}}_i^{(S)}$ of this term. Step 5 is not applied at the final stage. Together with the estimates retained from the previous stages, we form

$$\tilde{\mathbf{f}}_i = \tilde{\mathbf{f}}_i^{(1)} + \sum_{s=2}^{S} \widehat{\mathbf{q}}_i^{(s)}, \tag{27}$$

which is an estimate of the original vector $\mathbf{f}$ associated with the i-th first-stage group.

For each first-stage group, if there is only one path from this group to the final stage, the above procedure gives one estimate $\tilde{\mathbf{f}}_i$ of $\mathbf{f}$. If a first-stage group has more than one path to the final stage, it is sufficient to choose any one of these paths and use the above procedure to form $\tilde{\mathbf{f}}_i$ in (27). After one such estimate is obtained from each of the K_1 first-stage groups, the final estimate is

$$\tilde{\mathbf{f}} = \frac{1}{K_1} \sum_{i=1}^{K_1} \tilde{\mathbf{f}}_i = \frac{1}{K_1} \sum_{i=1}^{K_1} \left(\tilde{\mathbf{f}}_i^{(1)} + \sum_{s=2}^{S} \widehat{\mathbf{q}}_i^{(s)} \right). \tag{28}$$

The main result is as follows.

Theorem 3: Let $\mathbf{f}$ be an integer vector such that

$$\mathbf{f} \in \bigcup_{\mathbf{k} \in \mathcal{N}((\mathbf{R}_{l_0}^{(S-1)})^{-1} \mathbf{R}^{(S)})} \left(\mathcal{N}(\mathbf{R}_{l_0}^{(S-1)}) + \mathbf{R}_{l_0}^{(S-1)} \mathbf{k} \right).$$

If the vector remainder errors satisfy

$$\|\Delta \mathbf{r}_{i,j}\| \le \tau_i < \min \left\{ \delta_i^{(1)}, \min_{\substack{2 \le s \le S-1 \\ k \in \phi^{(s)}(i)}} \delta_k^{(s)}, \delta \right\}, \tag{29}$$

for $1 \le i \le K_1$ and $1 \le j \le L_i^{(1)}$, then $\mathbf{f}$ can be robustly reconstructed. Moreover, the final estimate $\tilde{\mathbf{f}}$ in (28) satisfies

$$\|\tilde{\mathbf{f}} - \mathbf{f}\| \le \frac{1}{K_1} \sum_{i=1}^{K_1} \tau_i. \tag{30}$$

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

Proof: By (29) and Proposition 2, together with the treatment of groups containing only one matrix modulus described above, the reconstruction can be carried out successively through all intermediate stages and the final stage. At each intermediate stage, the estimation errors remain within the sufficient error bound required at the next stage. The argument is the same as that in the proof of Theorem 2, applied successively to the groups at each stage, and is omitted here. Therefore, all the required product terms along each selected path are accurately determined, i.e.,

$$\widehat{\mathbf{q}}_i^{(s)} = \mathbf{q}_i^{(s)}, \qquad 2 \le s \le S.$$

For the i-th first-stage group,

$$\|\tilde{\mathbf{f}}_i^{(1)} - \mathbf{f}_i^{(1)}\| \le \tau_i,$$

which also holds for a group containing only one matrix modulus because its erroneous remainder is passed through directly. Using (26) and (27), we therefore have

$$\tilde{\mathbf{f}}_i - \mathbf{f} = \tilde{\mathbf{f}}_i^{(1)} - \mathbf{f}_i^{(1)}.$$

Hence, from (28),

$$\|\tilde{\mathbf{f}} - \mathbf{f}\| = \left\| \frac{1}{K_1} \sum_{i=1}^{K_1} \left(\tilde{\mathbf{f}}_i^{(1)} - \mathbf{f}_i^{(1)} \right) \right\| \le \frac{1}{K_1} \sum_{i=1}^{K_1} \tau_i.$$

□

To conclude this section, we note that the multistage framework can be extended beyond two stages and may further improve the vector remainder error bound. A detailed three-stage example is shown below.

Example 4: Let

$$\mathbf{E}_{i1} = \begin{pmatrix} e_i & 1 \\ 0 & e_i \end{pmatrix}, \mathbf{E}_{i2} = \begin{pmatrix} e_i & 0 \\ 1 & e_i \end{pmatrix},$$

for $1 \le i \le 5$, where $e_1 = 8, e_2 = 16, e_3 = 36, e_4 = 9, e_5 = 27$. Let $\mathbf{\Gamma}_1$ and $\mathbf{\Gamma}_2$ be as in the motivating example and

$$\mathbf{\Gamma}_3 = \begin{pmatrix} 1 & 0 \\ 53 & 769 \end{pmatrix}, \mathbf{\Gamma}_4 = \begin{pmatrix} 26 & -11 \\ 11 & 26 \end{pmatrix}, \mathbf{\Gamma}_5 = \begin{pmatrix} 26 & 11 \\ -11 & 26 \end{pmatrix},$$

All $\mathbf{\Gamma}_j$ are pairwise co-prime and $\lambda_{\mathcal{L}(\mathbf{\Gamma_1})} = \lambda_{\mathcal{L}(\mathbf{\Gamma_2})} = \sqrt{773}$,$\lambda_{\mathcal{L}(\mathbf{\Gamma_3})} = \sqrt{842}$, $\lambda_{\mathcal{L}(\mathbf{\Gamma_4})} = \lambda_{\mathcal{L}(\mathbf{\Gamma_5})} = \sqrt{797}$.

Consider the following matrix moduli:

$$\{\mathbf{\Gamma}_k, \mathbf{\Gamma}_k\mathbf{E}_{k1}, \mathbf{\Gamma}_k\mathbf{E}_{k2} \mid 1 \le k \le 5\}.$$

Since all $\mathbf{\Gamma}_j$ are pairwise co-prime, the vector remainder error bound of single-stage robust MD-CRT is $1/4$, which means that no error can be tolerated.

We then divide them into five groups:

$$\mathcal{M}_k^{(1)} = \{\mathbf{\Gamma}_k, \mathbf{\Gamma}_k\mathbf{E}_{k1}, \mathbf{\Gamma}_k\mathbf{E}_{k2}\}, \quad \text{for } 1 \le k \le 5,$$

and let the remainder errors of each group k be bounded by τ_k. Each $\mathcal{M}_k^{(1)}$ satisfies Lemma 4 with $\mathbf{M}_{l_0} = \mathbf{\Gamma}_k$. Hence, by (22), $\delta_1^{(1)} = \delta_2^{(1)} = \sqrt{773}/4 \approx 6.95$, $\delta_3^{(1)} = \sqrt{842}/4 \approx 7.25$, $\delta_4^{(1)} = \delta_5^{(1)} = \sqrt{797}/4 \approx 7.05$. Moreover, the lcrms satisfying Lemma 4 are

$$\mathbf{R}_k^{(1)} = \mathbf{\Gamma}_k \mathrm{diag}(r_k, r_k), \quad 1 \le k \le 5,$$

TABLE II
VECTOR REMAINDER ERROR BOUNDS IN EXAMPLE 4

Groups	τ_1	τ_2	τ_3	τ_4	τ_5
Single-stage	0.25	0.25	0.25	0.25	0.25
Two-stage	4	4	4	4	4
Three-stage	4	4	4	7.05	7.05

where $r_1 = 64, r_2 = 256, r_3 = 1296, r_4 = 81, r_5 = 729$. Then, all these $\mathbf{R}_k^{(1)}$ serve as the inputs of the second stage. If we use the single-stage robust MD-CRT directly to the second stage, the vector remainder error bound is $\delta_{\text{2-stage}} = 4$.

Instead, we split the matrix moduli in the second stage into two groups: $\mathcal{M}_1^{(2)} = \{\mathbf{R}_1^{(1)}, \mathbf{R}_2^{(1)}, \mathbf{R}_3^{(1)}\}$ and $\mathcal{M}_2^{(2)} = \{\mathbf{R}_3^{(1)}, \mathbf{R}_4^{(1)}, \mathbf{R}_5^{(1)}\}$. Both groups satisfy Lemma 4 with $\mathbf{M}_{l_0} = \mathbf{R}_3^{(1)}$. Then, we can calculate the vector remainder error bound of each group by (22) and obtain $\delta_1^{(2)} = 4$, $\delta_2^{(2)} = 81/4 = 20.25$. The resulting lcrms (still satisfying Lemma 4) are

$$\mathbf{R}_k^{(2)} = \mathbf{\Gamma}_3 \mathrm{diag}(r'_k, r'_k), \quad k = 1, 2,$$

where $r'_1 = 16028928, r'_2 = 9296208$. Then, both $\mathbf{R}_k^{(2)}$ serve as the inputs of the third stage. Using single-stage robust MD-CRT on $\{\mathbf{R}_1^{(2)}, \mathbf{R}_2^{(2)}\}$, the vector remainder error bound is $\delta_{\text{3-stage}} = 324\sqrt{842} \approx 9401.6$. According to the grouping structure, the flow of remainders can be described as follows: $\phi^{(2)}(1) = \{1\}$, $\phi^{(2)}(2) = \{1\}$, $\phi^{(2)}(3) = \{1, 2\}$, $\phi^{(2)}(4) = \{2\}$, $\phi^{(2)}(5) = \{2\}$.

According to (29), we can explicitly compute the upper bounds on the remainder error τ_k for each initial group $\mathcal{M}_k^{(1)}$. These values are summarized in Table II. From the table, it is clear that while the single-stage approach allows no error, the two-stage framework improves the vector remainder error bound uniformly across all groups, and the three-stage framework further enhances the bounds for certain groups, specifically groups 4 and 5.

VI. SIMULATIONS

In this section, we present numerical simulations to verify the robustness advantage of a non-diagonal common left factor, and the proposed multistage robust MD-CRT framework developed in Theorem 2.

We first consider the four matrix moduli in Example 3, namely $30\mathbf{M}$, $10\mathbf{MC}_1$, $15\mathbf{MC}_2$, and $42\mathbf{MC}_3$. As discussed in Example 3, the vector remainder error bound of the single-stage scheme is $3\lambda_{\mathcal{L}(\mathbf{M})}/2$, while that of the two-stage scheme is $5\lambda_{\mathcal{L}(\mathbf{M})}/2$.

Assume the determinant constraint of $\mathbf{M}$ is 881. Under this constraint, one of the diagonal matrices achieving the maximum shortest vector length among diagonal integer matrices is $\mathbf{M} = 29\mathbf{I}$ with $\lambda_{\mathcal{L}(\mathbf{M})} = 29$. According to Algorithm 1, one of the non-diagonal matrices achieving the maximum shortest vector length among integer matrices with determinant 881 is

$$\mathbf{M}' = \begin{pmatrix} 1 & 0 \\ 32 & 881 \end{pmatrix},$$

with $\lambda_{\mathcal{L}(\mathbf{M}')} = \sqrt{1009} \approx 31.76$.

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

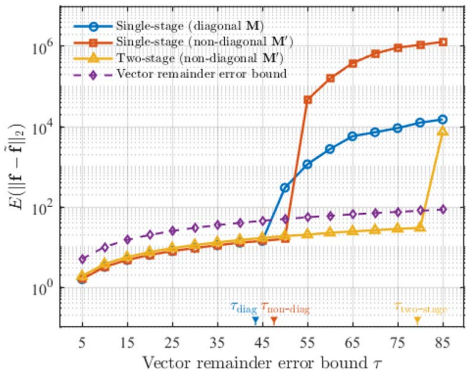


Fig. 2. Mean reconstruction error versus vector remainder error bound τ for single-stage systems with diagonal and non-diagonal common left factors and for the two-stage system.

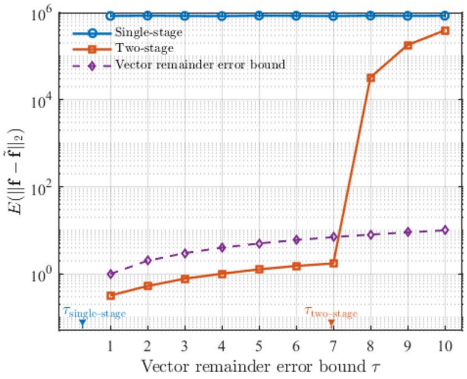


Fig. 3. Mean reconstruction error versus vector remainder error bound τ for the single-stage and two-stage systems using the six matrix moduli in Section V.

For both matrices, a fixed integer vector $\mathbf{f}$ is chosen within the robustly determinable range. For each vector remainder error bound $\tau = 5, 10, \ldots, 85$, error vectors $\Delta\mathbf{r}_i$ satisfying $\|\Delta\mathbf{r}_i\|_2 \le \tau$ are generated uniformly and independently within $\{\mathbf{e} \in \mathbb{Z}^2 : \ \|\mathbf{e}\|_2 \le \tau\}$ for $i = 1, 2, 3, 4$. Each case is averaged over 2000 independent trials, and the mean reconstruction error $\mathbb{E}[\|\mathbf{f} - \tilde{\mathbf{f}}\|_2]$ is plotted versus τ in Fig. 2. As shown in the figure, the single-stage system with the diagonal common left factor $\mathbf{M} = 29\mathbf{I}$ loses robustness when τ exceeds 45. In contrast, the system with the non-diagonal common left factor $\mathbf{M} = \mathbf{M}'$ maintains robust reconstruction for larger τ, which agrees with its larger shortest vector length and hence larger sufficient vector remainder error bound.

For the non-diagonal case, the two-stage reconstruction strategy of Example 3 is applied using the same setting. The results, also plotted in Fig. 2, show that the two-stage scheme further enlarges the robust region of the vector remainder error bound. Even when the single-stage system fails, the two-stage approach keeps the reconstruction error small, demonstrating a clear robustness improvement. The theoretical vector remainder error bounds obtained directly from (8) and (20) are $\tau_{\text{diag}} = 43.5$, $\tau_{\text{non-diag}} = 47.6$, and $\tau_{\text{two-stage}} = 79.4$, which are marked in Fig. 2. The reason why the simulation performances for the robust MD-CRTs are slightly better than the theoretical vector remainder error bounds is that these theoretical bounds are only sufficient conditions and behave as lower bounds on performance. This holds similarly in Fig. 3 below.

Overall, these results confirm that the single-stage robust MD-CRT with the non-diagonal common left factor provides a larger robustness region than that with the diagonal common left factor, while the proposed multistage framework further improves the robustness.

We next test the six matrix moduli introduced in the motivating example at the beginning of Section V. Both single-stage and two-stage reconstructions are performed to further verify the robustness improvement.

The vector remainder error bound is set as $\tau = 1, 2, \ldots, 10$. For each τ, 2000 random trials are conducted. In every trial, the remainder errors are independently drawn from a uniform distribution within $\{\mathbf{e} \in \mathbb{Z}^2 : \ \|\mathbf{e}\|_2 \le \tau\}$, and the mean reconstruction error $\mathbb{E}[\|\mathbf{f} - \tilde{\mathbf{f}}\|_2]$ is then computed.

As shown in Fig. 3, the single-stage reconstruction fails to provide robust recovery for all tested τ values. In contrast, the proposed two-stage framework remains stable for $\tau \le 7$. The theoretical vector remainder error bounds $\tau_{\text{single-stage}} = 0.25$ and $\tau_{\text{two-stage}} = 6.95$ are also shown in Fig. 3. These results clearly demonstrate that even when a single-stage robust MD-CRT has no robustness, the multistage framework can successfully achieve robust reconstruction.

Finally, we consider the multidimensional frequency estimation application introduced in Section III to provide a validation of the proposed framework in three dimensions. We set $D = 3$, $a = 1$, and $\mathbf{f} = [70, 75, 100]^\top$ in (1), and add complex white Gaussian noise to the sampled signals.

Let $\mathbf{A}$ be the three-dimensional matrix in (11), and choose the two common left factors as

$$\mathbf{M}_{\text{nd}} = 3\mathbf{A}, \qquad \mathbf{M}_{\text{d}} = \text{diag}(3, 3, 6).$$

They satisfy $|\det(\mathbf{M}_{\text{nd}})| = |\det(\mathbf{M}_{\text{d}})| = 54$, while $\lambda_{\mathcal{L}(\mathbf{M}_{\text{nd}})} = 3\sqrt{2}$ and $\lambda_{\mathcal{L}(\mathbf{M}_{\text{d}})} = 3$. Under the determinant constraint $|\det(\mathbf{M})| \le 54$, the largest shortest-vector length achievable by a diagonal integer matrix is 3, since a diagonal matrix with shortest-vector length at least 4 would have determinant at least $4^3 = 64 > 54$. Although $3\mathbf{I}$ also achieves the shortest-vector length 3, we use $\text{diag}(3, 3, 6)$ because its determinant is 54, exactly the same as that of $\mathbf{M}_{\text{nd}}$. Therefore, the diagonal and non-diagonal systems have the same sampling rate.

For $\mathbf{M} \in \{\mathbf{M}_{\text{d}}, \mathbf{M}_{\text{nd}}\}$, we use the four matrix moduli $\{3\mathbf{M}, 5\mathbf{M}, 6\mathbf{M}, 10\mathbf{M}\}$. The two single-stage systems use all of these four moduli directly. For the two-stage system with $\mathbf{M}_{\text{nd}}$, the first-stage groups are $\{3\mathbf{M}_{\text{nd}}, 6\mathbf{M}_{\text{nd}}\}$ and $\{5\mathbf{M}_{\text{nd}}, 10\mathbf{M}_{\text{nd}}\}$. The sufficient vector remainder error bounds are $\tau_{\text{d}} = \frac{3}{4}$, $\tau_{\text{nd}} = \frac{3\sqrt{2}}{4}$, and $\tau_{\text{two}} = \frac{3\sqrt{2}}{2}$, for the diagonal single-stage, non-diagonal single-stage, and non-diagonal two-stage systems, respectively.

Fig. 4 shows $\mathbb{E}[\|\mathbf{f} - \tilde{\mathbf{f}}\|_2]$ versus SNR with 10,000 Monte Carlo trials. The non-diagonal single-stage system achieves smaller reconstruction errors than the diagonal system at low SNRs, consistent with its larger vector remainder error bound.

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

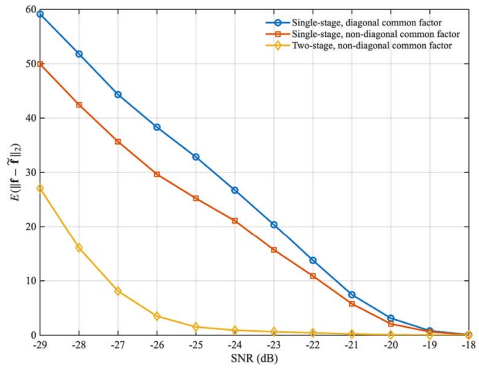


Fig. 4. Mean reconstruction error versus SNR for the three-dimensional frequency estimation example.

The two-stage method further improves the reconstruction performance. These results validate the proposed framework in the three-dimensional frequency estimation setting.

VII. Conclusion

This paper has investigated the MD-CRT for general matrix moduli from the perspectives of dynamic range and robustness. We showed that under a fixed determinant constraint, non-diagonal matrix moduli do not increase the maximum dynamic range but can lead to more balanced and better-conditioned sampling patterns. Under the common left factor model, in the considered two-dimensional setting with a prime determinant constraint, a non-diagonal choice of $\mathbf{M}$ can generate a lattice with a longer shortest vector than diagonal choices under the same constraint, leading to a larger sufficient vector remainder error bound. To further improve robustness, we developed a multistage robust MD-CRT framework that improves the robustness level without reducing the dynamic range. Both theoretical analysis and numerical simulations confirmed that the proposed approach achieves higher error tolerance and more reliable reconstruction in multidimensional settings.

References

[1] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography.* Singapore: World Scientific, 1996.

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

[3] 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.

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

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

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

[7] 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.

[8] C. 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.

[9] C. 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.

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

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

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

[13] 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.

[14] 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.

[15] 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.

[16] X. 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.

[17] W. 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.

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

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

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

[21] H. Xiao, Y. Huang, Y. Ye, and G. 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.

[22] H. Xiao, Y. Zhang, B. Zhou, and G. Xiao, "On the foundation of sparsity constrained sensing–Part I: Sampling theory and robust remainder problem," *IEEE Trans. Signal Process.*, vol. 71, pp. 1263–1276, 2023.

[23] 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, Nov. 1994.

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

[25] L. Xiao, H. Huo, and X.-G. Xia, "Robust multidimensional Chinese remainder theorem for integer vector reconstruction," *IEEE Trans. Signal Process.*, vol. 72, pp. 2364–2376, 2024.

[26] G. Guo and X.-G. Xia, "A generalized multidimensional Chinese remainder theorem (MD-CRT) for multiple integer vectors," *IEEE Trans. Signal Process.*, vol. 73, pp. 5136–5151, 2025.

[27] G. Guo and X.-G. Xia, "A construction of pairwise co-prime integer matrices of any dimension and their least common right multiple," *IEEE Trans. Signal Process.*, vol. 73, pp. 2187–2199, 2025.

[28] X. Li, S. Sun, Q. Liao, and X.-G. Xia, "Maximum likelihood estimation based complex-valued robust Chinese remainder theorem and its fast algorithm," *IEEE J. Miniaturization Air Space Syst.*, vol. 7, no. 1, pp. 64–79, Mar. 2026.

[29] X.-G. Xia and G. Guo, "Prime and co-prime integer matrices," *IEEE Signal Process. Lett.*, vol. 32, pp. 3037–3041, 2025.

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

[31] 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.

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

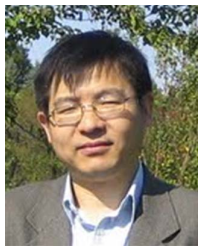
[33] G. Guo and X.-G. Xia, "Moving target SAR imaging using planar arrays and multidimensional Chinese remainder theorem (MD-CRT), Part II: Two subarray designs," 2026, *arXiv:2606.14911*.

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.

[34] I. V. Bajić and J. W. Woods, "Maximum minimal distance partitioning of the $\mathbb{Z}^2$ lattice," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 981–992, Apr. 2003.
[35] F. Pausinger, "Long shortest vectors in low dimensional lattices," *Discrete Math.*, vol. 343, no. 12, Dec. 2020, Art. no. 112138.



Guangpu Guo (Graduate Student Member, IEEE) received the B.S. and M.S degrees from Nankai University, Tianjin, China, in 2021 and 2024, respectively. He is currently working toward the Ph.D. degree in electrical and computer engineering with the University of Delaware, Newark, Delaware. His research interest includes multidimensional signal processing.



Xiang-Gen Xia (Fellow, IEEE) received the B.S. degree from Nanjing Normal University, Nanjing, China, in 1983, and the M.S. degree from Nankai University, Tianjin, China, in 1986, both in mathematics, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, 1992. He was a Senior/Research Staff Member with Hughes Research Laboratories, Malibu, California, from 1995 to 1996. In 1996, he joined the Department of Electrical and Computer Engineering, University of Delaware, Newark, Delaware, where he is the Charles Black Evans Professor. His research interests include space-time coding, MIMO and OFDM systems, digital signal processing, and SAR and ISAR imaging. He is the author of the book titled *Modulated Coding for Intersymbol Interference Channels* (Marcel Dekker, 2000), and a coauthor of the book titled *Array Beamforming Enabled Wireless Communications* (CRC Press, 2023). He received the National Science Foundation (NSF) Faculty Early Career Development (CAREER) Program Award in 1997, the Office of Naval Research (ONR) Young Investigator Award in 1998, and the Outstanding Overseas Young Investigator Award from the National Nature Science Foundation of China in 2001. He received the 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 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.

Authorized licensed use limited to: UNIVERSITY OF DELAWARE LIBRARY. Downloaded on November 03,2026 at 22:16:08 UTC from IEEE Xplore. Restrictions apply.