Signal Processing 150 (2018) 248–258

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Review

Frequency determination from truly sub-Nyquist samplers based on robust Chinese remainder theorem

Li Xiao*, Xiang-Gen Xia[1]

Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716, USA

ARTICLE INFO

Article history:
Received 14 October 2017
Revised 6 March 2018
Accepted 24 April 2018
Available online 25 April 2018

Keywords:
Compressed sensing
Discrete fourier transform
Frequency estimation
Robust Chinese remainder theorem
Undersampling

ABSTRACT

In this paper, a truly sub-Nyquist sampling method for frequency estimation of sinusoidal signals in noise is presented. Basically speaking, sinusoidal signals are first sampled at multiple sampling rates lower than the Nyquist rate, and then a robust Chinese remainder theorem (CRT) is proposed to estimate the frequencies of interest from the aliased frequencies obtained by taking the discrete Fourier transform of the collected samples in each undersampled waveform. Compared with compressed sensing, this method can be easily implemented from the hardware point of view. This paper provides a thorough overview of the existing research results on the robust CRT during the last decade, and discusses some related open problems as well.

1. Introduction

Frequency estimation of sinusoidal signals from a finite number of noisy samples is a fundamental problem in signal processing [1–3]. It has wide applications in many fields, such as radar, sonar, digital communications, and image analysis. In the past few decades, numerous frequency estimation approaches have been proposed in the literature, including maximum likelihood [4,5], nonlinear least squares [6], Prony's method [7], MUSIC and ESPRIT [8,9], just to name a few. In these methods, the signal is usually assumed to be sampled at a rate higher than the Nyquist rate, i.e., the sampling rate is higher than twice the highest frequency of the signal. However, in some applications, e.g., detecting high-speed moving targets in a synthetic aperture radar (SAR) image and estimating the wide-range carrier frequency offset in a coherent optical orthogonal frequency division multiplexing (CO-OFDM) system, the signal to be estimated has intrinsically high bandwidth, and the traditional Nyquist sampling consequently becomes infeasible due to high power consumption, great cost, and limited bit resolution of a high-rate analog-to-digital converter (ADC), or in spatial domain in, such as, SAR. Therefore, studies on frequency estimation from sub-Nyquist sampling sequences are interesting and important.

Compressed sensing (CS), also known as compressive sampling or sparse sampling, has been proposed in the recent years [10–13], which basically randomly samples signals with a much smaller number of samples than that of using the Nyquist sampling if they are sparse or sparsable in an appropriate transformation domain. However, the design of random sampling-based hardware is still a great challenge [14]. Another family of statistical frequency estimation methods based on two truly undersampled signal sequences has been proposed in [15–17], where by truly undersampled it means that regular samplers with sub-Nyquist sampling rates are used. More specifically, they use two uniform sub-Nyquist samplers/arrays with sampling periods being coprime to estimate the signal autocorrelation sequence at Nyquist rate, and from the estimated autocorrelation sequence the frequencies are estimated. However, these coprime sampler based methods may require long time observations of signals in order to achieve the same autocorrelation sequence estimation performance as before.

Unlike the above statistical methods, an efficient deterministic method based on the Chinese remainder theorem (CRT), which we will review in this paper, had been proposed in the earlier past to estimate frequencies of sinusoidal signals from multiple truly undersampled waveforms [18–21] starting from the mid 1990s. It takes the discrete Fourier transform (DFT) of the collected samples in each undersampled waveform to detect the aliased frequency, and then the frequencies are estimated from these aliased frequencies by using generalized versions of the CRT. Without loss of generality, let us consider a single harmonic signal

$$x(t) = a\exp(j2\pi Nt) + \omega(t), \tag{1}$$

* Corresponding author.
E-mail addresses: lixiao@ee.udel.edu, lxiao1@tulane.edu, lixiao@udel.edu (L. Xiao), xxia@ee.udel.edu (X.-G. Xia).

[1] Fellow, IEEE.

https://doi.org/10.1016/j.sigpro.2018.04.022
0165-1684/© 2018 Elsevier B.V. All rights reserved.

where N Hz, the frequency to be estimated, is assumed to be a positive integer for simplicity, a is an unknown complex coefficient, and $\omega(t)$ is an additive white noise. We now exploit multiple undersampled versions of $x(t)$ with several different but much low sampling rates m_1Hz, m_2Hz, $\cdots$, m_LHz, i.e.,

$$x_i[n] = a\exp(j2\pi Nn/m_i) + \omega_i(n/m_i) \tag{2}$$

for $1 \le i \le L$. Then, for each of the undersampled signals in (2), the remainder r_i of N modulo m_i is obtained as the aliased frequency by performing the m_i-point DFT, if the signal-to-noise ratio (SNR) is not too low. It is equivalent to solving a system of simultaneous linear congruences for the signal frequency N given the remainders r_i:

$$r_i \equiv N \bmod m_i \tag{3}$$

for $1 \le i \le L$, where the sampling rates m_i are called the moduli and $0 \le r_i < m_i$. Once we have collected these remainders, we can uniquely determine the signal frequency N via the CRT if N is less than the least common multiple (lcm) of all the moduli [22–24]. In this paper, we are more concerned about the robust problem. When the SNR is too low, the detected remainders are most likely subject to error contamination. It is well known that the CRT reconstruction formula is highly sensitive to errors in the remainders in the sense that a small remainder error may produce a large reconstruction error in N. In this paper, we first give an overview of a robust CRT [25–30] that can be precisely applied and provide a robust solution to (3) or the above frequency estimation problem when the remainders have errors. What the robust CRT basically says is that under some conditions on the moduli the reconstruction error is upper bounded by the remainder error bound. Two generalizations of the robust CRT are then presented: one is a robust generalized CRT for multiple integers [31] which aims to estimate more than one integer (or frequencies of a multi-harmonic signal) from the remainder sets (or sets of the detected aliased frequencies in undersampled waveforms), and the other is a robust double-remaindering CRT [32] which aims to estimate a large integer (or the radial velocity of a ground moving target in a SAR image) from the so-called double-remaindering remainders (or the detections after resolving Doppler ambiguity successively in both time domain and spatial domain). The robust CRT and its generalizations have been found to have many potential applications in other fields, such as phase unwrapping in radar signal processing [33–38] and optical interferometry [39–41], wireless sensor networks [42–44], and computational neuroscience [45,46].

The rest of this paper is organized as follows. In Section 2, we briefly introduce the CRT. In Sections 3–5, the robust CRT and its latest results are described in a self-contained manner. In Section 6, we present the two generalizations of the robust CRT and discuss some interesting open problems for future research.

2. Chinese remainder theorem

Before stating the CRT, let us review some basic concepts and notations from number theory.

i. For two or more integers m_1, m_2, $\cdots$, m_L with $L \ge 2$, their greatest common divisor (gcd), denoted by $\gcd(m_1, m_2, \cdots, m_L)$, is the largest integer that divides each of them, and their least common multiple (lcm), denoted by $\text{lcm}(m_1, m_2, \cdots, m_L)$, is the smallest integer that is divisible by each of them. Two integers are said to be coprime if their gcd is 1.

ii. Given a positive integer m, two integers a and b are said to be congruent modulo m, written mathematically as $a \equiv b \bmod m$, if their difference $a - b$ is divisible by m (i.e., $(a-b)/m$ is an integer), where the number m is called the modulus. If and only if a and m are coprime, there is exactly one solution for x to the linear congruence $ax \equiv 1 \bmod m$ with $x \in \{0, 1, \cdots, m-1\}$. We call such a solution the modular multiplicative inverse of a modulo m. For example, $-5 \equiv 9 \bmod 7$, and 4 is the modular multiplicative inverse of 2 modulo 7, i.e., $2 \cdot 4 \equiv 1 \bmod 7$.

iii. For two integers a and m with $m > 0$, there exists a unique pair of integers k and r such that $a = km + r$ and $0 \le r < m$, where the number k is called the folding number, and r is called the remainder of a modulo m. Thus, a is congruent to its remainder r modulo m, i.e., $r \equiv a \bmod m$, and moreover, if $a \equiv b \bmod m$, then a and b have the same remainder modulo m. For example, $9 \equiv 15 \bmod 6$, and the remainders of 9 and 15 modulo 6 are both 3.

The earliest congruence problem first appeared in the 3rd-century book entitled *Sunzi Suanjing*:

> *"There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, we have two left over. What will be the number?"*

Letting N denote the number of such things, the congruence problem above can be interpreted as finding N such that its remainders modulo 3, 5, 7 are 2, 3, 2, respectively, i.e.,

$$\begin{aligned} 2 &\equiv N \mod 3 \\ 3 &\equiv N \mod 5 \\ 2 &\equiv N \mod 7. \end{aligned} \tag{4}$$

In the year 1247, a Chinese mathematician *Qin Jiushao* first presented a complete solution to simultaneous linear congruences, which is later named the CRT, in his book entitled *Shushu Jiuzhang*. The CRT has now evolved into a systematic theorem that exists ubiquitously in elementary mathematical textbooks.

We next formally introduce the CRT. Let N be a nonnegative integer, $m_1 < m_2 < \cdots < m_L$ be the L moduli, $M \triangleq \text{lcm}(m_1, m_2, \cdots, m_L)$ be the lcm of all the moduli, and r_1, r_2, $\cdots$, r_L be the L remainders of N, i.e.,

$$r_i \equiv N \bmod m_i \quad \text{or} \quad N = n_i m_i + r_i \tag{5}$$

for $1 \le i \le L$, where $0 \le r_i < m_i$, and n_i are the folding numbers. Given N and the moduli m_i, the remainders r_i can be uniquely calculated from division. Conversely, given the moduli m_i and remainders r_i, N can be uniquely determined modulo M via the CRT as follows.

Theorem 1 [22] **(Chinese remainder theorem).** *Given the moduli m_i and remainders r_i in (5), there is a unique solution for N modulo M, which is given by*

$$N \equiv \sum_{i=1}^{L} r_i D_i M_i \bmod M, \tag{6}$$

where $M_i = M/\mu_i$, D_i is the modular multiplicative inverse of M_i modulo μ_i (i.e., $1 \equiv D_i M_i \bmod \mu_i$) if $\mu_i \neq 1$, else $D_i = 0$, and μ_1, μ_2, $\cdots$, μ_L are taken to be any L pairwise coprime positive integers such that $\prod_{i=1}^{L} \mu_i = M$ and μ_i divides m_i for each $1 \le i \le L$. In particular, if it is assumed that N is less than the lcm of all the moduli, i.e., $0 \le N < M$, then we can uniquely determine N from (6), which is in fact the smallest nonnegative integer solution to (5).

When the moduli are pairwise coprime, i.e., the gcd of every pair of m_i and m_j, denoted by

$$d_{ij} \triangleq \gcd(m_i, m_j) \tag{7}$$

is 1, Theorem 1 reduces to the traditional CRT wherein we have $\mu_i = m_i$ for $1 \le i \le L$ in the reconstruction formula (6). Another remark we have to make here is that to enforce the uniqueness of the solution in the CRT, we tacitly admit that N is in the range

[0, M) in the remaining of this paper, unless specifically stated otherwise.

Example 1. Let us find the solution to the simultaneous linear congruences (4) via the CRT. Since the moduli in (4) are pairwise coprime, we have $\mu_1 = 3, \mu_2 = 5, \mu_3 = 7$. Then, we calculate

1. $M = 3 \cdot 5 \cdot 7 = 105$;
2. $M_1 = 35, M_2 = 21, M_3 = 15$;
3. $D_1 = 2, D_2 = 1, D_3 = 1$;
4. $N \equiv (2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15) \bmod 105 \equiv 23 \bmod 105$.

As a result, we get $N = 23$.

Due to the carry-free property of the modular arithmetic, the CRT provides an energy-efficient and fast arithmetic operation through breaking down a large computation into a series of smaller computations that can be performed independently and in parallel. Thus, the CRT has offered widespread applications in many fields such as computing, cryptography, and coding theory, see [22–24] and references therein.

3. Robust Chinese remainder theorem

In this section, we state the robust CRT that is the focus of this paper, and compare it with the Chinese residue code.

As aforementioned in Introduction, the remainders r_i are detected from noisy data in most signal processing applications, and therefore, they are usually known inaccurately. Let $\tilde{r}_i \triangleq r_i + \triangle r_i$ denote the erroneous remainders, where $\triangle r_i$ are the remainder errors. If we apply the CRT directly to reconstruct N from the erroneous remainders $\tilde{r}_i$ instead of r_i, the reconstruction formula (6) is likely to yield a large reconstruction error even though the remainder errors $\triangle r_i$ are small enough. To illustrate this point, let us look at a simple example.

Example 2. Consider the moduli $m_1 = 16, m_2 = 24, m_3 = 40$. The lcm of all the moduli is $M = 240$. In this case, we let $\mu_1 = 16, \mu_2 = 3, \mu_3 = 5$. We then calculate $M_1 = 15, M_2 = 80, M_3 = 48$ and $D_1 = 15, D_2 = 2, D_3 = 2$. The CRT says that any integer N in the range $0 \le N < 240$ can be uniquely reconstructed from its remainders by (6). As one knows, all the remainders of $N = 1$ are equal to 1. If its remainders are subject to small errors $\triangle r_1 = \triangle r_3 = 0, \triangle r_2 = 1$, i.e., $\tilde{r}_1 = 1, \tilde{r}_2 = 2, \tilde{r}_3 = 1$, then replacing r_i with $\tilde{r}_i$ in (6), we get a reconstruction $\hat{N} = 161$, which differs significantly from the true value $N = 1$. In other words, a large reconstruction error occurs.

Indeed, a large reconstruction error indicates poor performance of applications. It is, therefore, a matter of great importance to properly resist the remainder errors, in the sense that a robust reconstruction can be obtained from the erroneous remainders, where, and throughout this paper, the term “robust” means that when the remainders are known approximately within an error bound τ, i.e.,

$$|\triangle r_i| = |\tilde{r}_i - r_i| \le \tau \text{ for } 1 \le i \le L, \tag{8}$$

the reconstruction error is upper bounded by τ, i.e., the reconstructed integer $\hat{N}$ of N satisfies

$$|\hat{N} - N| \le \tau. \tag{9}$$

We also call it a robust CRT. In either theoretical or applied researches, the robust CRT raises two fundamental problems: 1) How large can the remainder error bound τ be for the robustness to hold? The larger τ is, the weaker the condition is required or the lower SNR is needed. 2) How do we develop a fast and efficient reconstruction algorithm?

To the best of our knowledge, the robust CRT first appeared in resolving the ambiguity in radar signal processing [47,48]. Nevertheless, there was no dedicated and systematic approach proposed in [47,48] to well addressing the above two problems until two decades later the robust CRT was independently investigated in [25–30] to estimate a large frequency from multiple undersampled waveforms. Under the assumption that the remaining factors of the moduli divided by their gcd are pairwise coprime, i.e., $m_i = m\Gamma_i$ for $1 \le i \le L$, where $\Gamma_1, \Gamma_2, \cdots, \Gamma_L$ are pairwise coprime, it is basically stated in [25–27] that an integer N in the range [0, M) can be robustly reconstructed, if τ is less than a quarter of the gcd of the moduli, i.e., $\tau < m/4$. Especially, a closed-form reconstruction algorithm was proposed in [27]. More recently, by removing the coprimeness assumption made in [25–27], some improved versions of the robust CRT with a general set of moduli and the corresponding reconstruction algorithms were presented in [28–30]. Their brief descriptions will be stated in the following Sections 4 and 5, respectively.

The key idea for the robust CRT in [25–30] is to accurately determine the unknown folding numbers n_i in (5) first and then reconstruct N as

$$\hat{N} = \left[\frac{1}{L} \sum_{i=1}^{L} (n_i m_i + \tilde{r}_i) \right], \tag{10}$$

where $[x]$ stands for the rounding function such that

$$-0.5 \le x - [x] < 0.5. \tag{11}$$

It is straightforward to see that as long as the folding numbers n_i are accurately determined, (10) provides a robust reconstruction, i.e., $|\hat{N} - N| \le \tau$, because of $\hat{N} = N + \left[\sum_{i=1}^{L} \triangle r_i / L\right]$ and $|\triangle r_i| \le \tau$ for $1 \le i \le L$. Therefore, the robust CRT turns into a problem of accurately determining the folding numbers n_i from these erroneous remainders $\tilde{r}_i$.

The Chinese residue code is well known as another remainder-error-resistant technique, which is an error-correcting code and has been investigated extensively in the literature [49–52]. More precisely, given V pairwise coprime moduli $m_1 < m_2 < \cdots < m_V$ and an integer $L < V$, the Chinese residue code has a message space $\mathcal{N} = \{0, 1, \cdots, \prod_{i=1}^{L} m_i - 1\}$, and encodes a message $N \in \mathcal{N}$ as its remainder vector $(r_1, r_2, \cdots, r_V)$. In this code, the remainders form a redundant representation of N, and according to the CRT, if there are only $\lfloor (V - L)/2 \rfloor$ or fewer erroneous remainders, where $\lfloor \cdot \rfloor$ denotes the floor function, then N can be accurately reconstructed as a unique output in the minimum Hamming distance decoding algorithm. Remarkably, an alternative decoding algorithm, called list decoding, was proposed for the Chinese residue code with a large error rate in [53–55], where the number of erroneous remainders may be larger than $\lfloor (V - L)/2 \rfloor$, i.e., the number of erroneous remainders that the minimum Hamming distance decoding algorithm can handle, and the decoding algorithm outputs a small list of possibilities one of which is accurate. As a note, the robust CRT considered in this paper is quite different from the Chinese residue code: In the robust CRT, the moduli are generally not pairwise coprime, the reconstruction may be inaccurate but is robust to the remainder errors, and all the remainders are allowed to have errors that are not too large.

4. Closed-form algorithm for robust CRT

In the robust CRT setting above, we first present a condition on the remainder error bound along with a closed-form robust CRT algorithm [27,29] in this section. We then develop a multi-stage extension [29] of the proposed closed-form robust CRT algorithm to further improve the remainder error bound condition. Some illustrative examples are given to verify the results.

As the CRT in Theorem 1 says, an integer N in the range [0, M) can be uniquely reconstructed from its remainders $r_1, r_2, \cdots, r_L$ with respect to the moduli $m_1, m_2, \cdots, m_L$ in (5). This N will also give the unique folding numbers n_i as $n_i = (N - r_i)/m_i$, which satisfy $0 \le n_i < M/m_i$ for $1 \le i \le L$. In what follows, we try to directly reconstruct n_i for $1 \le i \le L$ from the remainders $r_1, r_2, \cdots, r_L$.

Letting the last $L-1$ equations in (5) subtract the first one, we get

$$n_1 m_1 - n_i m_i = r_i - r_1 \tag{12}$$

for $2 \le i \le L$. Dividing both sides of (12) by the gcd d_{1i} of m_1 and m_i, we get

$$n_1 \Gamma_{1i} - n_i \Gamma_{i1} = q_{i1}, \tag{13}$$

where $\Gamma_{1i} \triangleq m_1/d_{1i}$, $\Gamma_{i1} \triangleq m_i/d_{1i}$, and $q_{i1} \triangleq (r_i - r_1)/d_{1i}$. Next, we take both sides of (13) modulo Γ_{i1}, and then have

$$n_1 \Gamma_{1i} \equiv q_{i1} \mod \Gamma_{i1}. \tag{14}$$

Since Γ_{1i} and Γ_{i1} are coprime, the modular multiplicative inverse of Γ_{1i} modulo Γ_{i1} uniquely exists, denoted by $\overline{\Gamma}_{1i}$, and then it is not hard to see that the congruence (14) can be simplified to

$$n_1 \equiv q_{i1} \overline{\Gamma}_{1i} \mod \Gamma_{i1}. \tag{15}$$

According to (15), n_1 and $q_{i1}\overline{\Gamma}_{1i}$ have the same remainders modulo Γ_{i1} for $2 \le i \le L$. Therefore, we readily have the following simultaneous linear congruences

$$\xi_{i1} \equiv n_1 \mod \Gamma_{i1}, \tag{16}$$

where ξ_{i1} are the remainders of $q_{i1}\overline{\Gamma}_{1i}$ modulo Γ_{i1} for $2 \le i \le L$ and can be calculated in advance. Because of $\operatorname{lcm}(\Gamma_{21}, \Gamma_{31}, \cdots, \Gamma_{L1}) = M/m_1$ and $0 \le n_1 < M/m_1$, we can uniquely reconstruct n_1 by solving (16) via the CRT, and then from (13) the other folding numbers can be obtained by

$$n_i = \frac{n_1 \Gamma_{1i} - q_{i1}}{\Gamma_{i1}} \tag{17}$$

for $2 \le i \le L$. Therefore, by following the above steps, the folding numbers n_i are uniquely reconstructed from the remainders without first reconstructing N.

Since the erroneous remainders $\tilde{r}_i$ are only known in place of r_i in the robust CRT, we naturally use

$$\hat{q}_{i1} \triangleq \left[\frac{\tilde{r}_i - \tilde{r}_1}{d_{1i}} \right] \tag{18}$$

as an estimate of q_{i1}, where $[\,\cdot\,]$ is the rounding function as defined in (11). If the remainder error bound τ in (8) is less than each of $d_{1i}/4$ for $2 \le i \le L$, i.e.,

$$\tau < \min_{2 \le i \le L} \frac{d_{1i}}{4}, \tag{19}$$

it is immediate that $[(\triangle r_i - \triangle r_1)/d_{1i}] = 0$ and

$$\begin{aligned} \hat{q}_{i1} &= \left[\frac{r_i - r_1}{d_{1i}} + \frac{\triangle r_i - \triangle r_1}{d_{1i}} \right] \\ &= \frac{r_i - r_1}{d_{1i}} + \left[\frac{\triangle r_i - \triangle r_1}{d_{1i}} \right] \\ &= \frac{r_i - r_1}{d_{1i}} \\ &= q_{i1}. \end{aligned} \tag{20}$$

One can see that the rounding function used in (18) enables us to completely eliminate the effect of the remainder errors given by (19). Once $\hat{q}_{i1}$ are equal to q_{i1}, the remainders ξ_{i1} of n_1 in (16) are accurately determined, and of course we can accurately reconstruct n_1 via the CRT as well as the other n_i from (17) for $2 \le i \le L$. It then follows from (10) that a robust reconstruction $\hat{N}$ of N is ultimately obtained. Therefore, (19) gives a condition on the remainder error bound τ such that a robust reconstruction of N is obtained.

Note that the subtractions in (12) are taken with respect to the first remainder. It is suggested that n_1 is selected as a reference to be first determined. In fact, we can arbitrarily select the kth equation in (5) to be subtracted from the others analogous to (12), and thereafter, by replacing the index 1 with k in (12)–(20), we first accurately determine n_k followed by the other folding numbers, provided the remainder error bound τ satisfies

$$\tau < \min_{\substack{1 \le i \le L \\ i \ne k}} \frac{d_{ki}}{4}. \tag{21}$$

So, we are able to get the largest possible τ by selecting a reference n_{k_0} such that

$$\min_{\substack{1 \le i \le L \\ i \ne k_0}} d_{k_0 i} = \max_{1 \le k \le L} \min_{\substack{1 \le i \le L \\ i \ne k}} d_{ki}. \tag{22}$$

In the following, we summarize the closed-form robust CRT algorithm and present the corresponding theorem.

Algorithm 1 : Closed-form robust CRT [29].

```
Input: the moduli $\{m_i\}_{i=1}^{L}$ and the erroneous remainders $\{\tilde{r}_i\}_{i=1}^{L}$.
Output: a reconstruction $\hat{N}$.
Through (22), find the index $k_0$ of a proper reference.
Calculate $\hat{q}_{k_0 i}$ for $1 \le i \le L, i \ne k_0$:
    $\hat{q}_{ik_0} = \left[ \frac{\tilde{r}_i - \tilde{r}_{k_0}}{d_{k_0 i}} \right].$   (23)
Calculate the remainders of $\hat{q}_{ik_0}\overline{\Gamma}_{k_0 i}$ modulo $\Gamma_{ik_0}$ for $1 \le i \le L, i \ne k_0$:
    $\hat{\xi}_{ik_0} \equiv \hat{q}_{ik_0}\overline{\Gamma}_{k_0 i} \mod \Gamma_{ik_0},$   (24)
    where $\overline{\Gamma}_{k_0 i}$ are the modular multiplicative inverse of $\Gamma_{k_0 i}$ modulo $\Gamma_{ik_0}$.
Calculate $\hat{n}_{k_0}$ via the CRT reconstruction formula for the simultaneous linear congruences:
    $\hat{\xi}_{ik_0} \equiv \hat{n}_{k_0} \mod \Gamma_{ik_0}$   (25)
    for $1 \le i \le L, i \ne k_0$.
Calculate $\hat{n}_i$ for $1 \le i \le L, i \ne k_0$:
    $\hat{n}_i = \frac{\hat{n}_{k_0}\Gamma_{k_0 i} - \hat{q}_{ik_0}}{\Gamma_{ik_0}}.$   (26)
Calculate $\hat{N}$:
    $\hat{N} = \left[ \frac{1}{L} \sum_{i=1}^{L} (\hat{n}_i m_i + \tilde{r}_i) \right].$   (27)
```

Theorem 2 [29]**.** *If an integer N is assumed to be in the range $0 \le N < M$ and the remainder error bound τ satisfies*

$$\tau < \max_{1 \le k \le L} \min_{\substack{1 \le i \le L \\ i \ne k}} \frac{d_{ki}}{4}, \tag{28}$$

where $d_{ki} \triangleq \gcd(m_k, m_i)$, then by Algorithm 1 we can accurately determine the folding numbers n_i, i.e., $\hat{n}_i = n_i$, for $1 \le i \le L$, and hence can robustly reconstruct N as $\hat{N}$ in (27), from the erroneous remainders.

In particular, when the moduli are given by $m_i = m\Gamma_i$ for $1 \le i \le L$, where $\Gamma_1, \Gamma_2, \cdots, \Gamma_L$ are pairwise coprime, Theorem 2 coincides exactly with the result in [25–27].

Example 3. Let $m_1 = 63, m_2 = 224, m_3 = 240$. Based on Theorem 2, an unknown integer N with $0 \le N < M \triangleq \operatorname{lcm}(m_1, m_2, m_3) = 10,080$ can be robustly reconstructed from its erroneous remainders by Algorithm 1, provided the remainder error bound is less than 7/4. Without loss of generality, let $N = 7000$, then its remainders and folding numbers are calculated as $r_1 = 7, r_2 = 56, r_3 = 40$ and $n_1 = 111, n_2 = 31, n_3 = 29$. If the remainders are contaminated with errors $\triangle r_1 = 0, \triangle r_2 = -1, \triangle r_3 = -1$, i.e., $\tilde{r}_1 = 7, \tilde{r}_2 = 55, \tilde{r}_3 = 39$, the condition (28) is fulfilled and we can use Algorithm 1 to robustly reconstruct N:

1: Find the index $k_0 = 2$ such that (22) holds.
2: Calculate $\hat{q}_{12} = [(7-55)/7] = -7$ and $\hat{q}_{32} = [(39-55)/16] = -1$ from (23).
3: Calculate $\hat{\xi}_{12} = 4 = (-7 \cdot 2 \bmod 9)$ and $\hat{\xi}_{32} = 1 = (-1 \cdot 14 \bmod 15)$ from (24).
4: Calculate $\hat{n}_2 = 31$ via the CRT reconstruction formula for (25).
5: Calculate $\hat{n}_1 = 111$ and $\hat{n}_3 = 29$ from (26).
6: Calculate $\hat{N} = 6999$ from (27).

From Theorem 2, the remainder error bound is closely related to the gcd of each pair of the moduli: the larger the gcd is, the larger the remainder error bound is. Now the question of particular interest is: For a given set of moduli, can we improve the remainder error bound obtained in Theorem 2 by splitting the set of moduli into several groups so that the gcd in each group becomes larger and the system of congruences in each group is independently solved based on the above closed-form robust CRT algorithm? To answer this question, let us first review the cascade architecture of the CRT [28,29].

Suppose that the moduli $m_1, m_2, \cdots, m_L$ are split into s groups, denoted by $\{m_{i,1}, m_{i,2}, \cdots, m_{i,L_i}\}$ for $1 \le i \le s$, which are not necessarily disjoint, i.e., $\bigcup_{i=1}^{s}\{m_{i,1}, m_{i,2}, \cdots, m_{i,L_i}\} = \{m_1, m_2, \cdots, m_L\}$ and $\sum_{i=1}^{s} L_i \ge L$. Analogously, the L remainders $r_1, r_2, \cdots, r_L$ are correspondingly split into s groups, denoted by $\{r_{i,1}, r_{i,2}, \cdots, r_{i,L_i}\}$ for $1 \le i \le s$. Then, it is shown conclusively that the integer N with $0 \le N < M$ can be uniquely reconstructed from its remainders by a two-stage CRT method, where the basic idea is first to apply the CRT to each group and then to apply the CRT across all the groups. In the first stage, we can uniquely reconstruct an integer N_i with $0 \le N_i < \eta_i \triangleq \mathrm{lcm}(m_{i,1}, m_{i,2}, \cdots, m_{i,L_i})$ via the CRT for each group i, and with these obtained reconstructions N_i being the remainders and η_i being the moduli, the following new system of congruences is evident:

$$N_i \equiv N \bmod \eta_i \tag{29}$$

for $1 \le i \le s$. In the second stage, because of $\mathrm{lcm}(\eta_1, \eta_2, \cdots, \eta_s) = M$ and $0 \le N < M$, we can uniquely reconstruct N by solving (29) via the CRT again.

Motivated by this cascade architecture of the CRT, we next propose a two-stage robust CRT algorithm when the remainders have errors, as shown in Fig. 1. We first apply Algorithm 1 to obtain a robust integer $\hat{N}_i$ for each group i, if the remainder error bound τ satisfies

$$\tau < G_i \triangleq \max_{1 \le k \le L_i} \min_{\substack{1 \le p \le L_i \\ p \ne k}} \frac{\gcd(m_{i,k}, m_{i,p})}{4}, \tag{30}$$

where in case group i consists of only one modulus, let $G_i \triangleq m_{i,\,1}/4$ and $\hat{N}_i$ is just $\tilde{r}_{i,1}$. Then, regarding these robust reconstructions $\hat{N}_i$ for $1 \le i \le s$ as possibly erroneous remainders in (29), Algorithm 1 is applied again across the groups, and a robust reconstruction $\hat{N}$ of N can be obtained, if τ satisfies again

$$\tau < G \triangleq \max_{1 \le k \le s} \min_{\substack{1 \le i \le s \\ i \ne k}} \frac{\gcd(\eta_k, \eta_i)}{4}. \tag{31}$$

With this two-stage robust CRT algorithm, we may boost up the remainder error bound in Theorem 2 that is obtained by applying Algorithm 1 to the simultaneous linear congruences (5) as a whole. Therefore, we obtain an improved result as stated below.

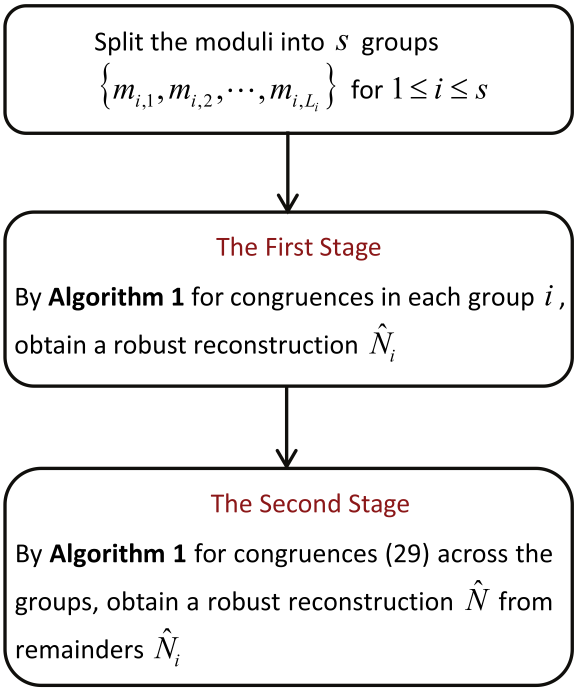
Split the moduli into s groups
$\{m_{i,1}, m_{i,2}, \cdots, m_{i,L_i}\}$ for $1 \le i \le s$
The First Stage
By **Algorithm 1** for congruences in each group i, obtain a robust reconstruction $\hat{N}_i$
The Second Stage
By **Algorithm 1** for congruences (29) across the groups, obtain a robust reconstruction $\hat{N}$ from remainders $\hat{N}_i$

Fig. 1. Flowchart of the two-stage robust CRT algorithm.

Theorem 3 *[29]. If an integer N is assumed to be in the range $0 \le N < M$ and the remainder error bound τ satisfies*

$$\tau < \min(G_1, G_2, \cdots, G_s, G), \tag{32}$$

then we can robustly reconstruct N from the erroneous remainders.

Note that Theorem 2 can be viewed as a special case of Theorem 3 with $s = 1$. It is due to the fact that when $s = 1$, we have $G_1 = \max_{1 \le k \le L} \min_{\substack{1 \le i \le L \\ i \ne k}} d_{ki}/4$, $G = M/4$, and $G_1 < G$.

Example 4. Let us reconsider Example 3 with the two-stage robust CRT algorithm. We split the three moduli into two groups $\{m_1\}$ and $\{m_2, m_3\}$. Based on Theorem 3, we can robustly reconstruct an integer N with $0 \le N < M = 10,080$, if $\tau < 16/4$. One can see that the remainder error bound $\tau < 16/4$ in Theorem 3 is more than twice that (i.e., $\tau < 7/4$) in Theorem 2 for the same moduli but with the grouping and the two-stage method. Similarly, let $N = 7000$, while the remainders have relatively large errors $\triangle r_1 = 2, \triangle r_2 = 3, \triangle r_3 = -1$, i.e., $\tilde{r}_1 = 9, \tilde{r}_2 = 59, \tilde{r}_3 = 39$. Since the condition (32) is fulfilled, we can use the two-stage robust CRT algorithm to robustly reconstruct N:

1. By Algorithm 1 for each group, we obtain $\hat{N}_1 = 9$ and $\hat{N}_2 = 281$.
2. By Algorithm 1 across the two groups again, we obtain $\hat{N} = 7001$.

The above two-stage robust CRT algorithm can be easily generalized to a multi-stage (three or more stages) robust CRT algorithm. For instance, if we further split the moduli $\eta_1, \eta_2, \cdots, \eta_s$ in the second stage into several groups, then we can develop a three-stage robust CRT algorithm in the same way as the two-stage robust CRT algorithm. Although we, by deploying a multi-stage robust CRT algorithm, may improve the remainder error bound for a given set of moduli, there are certain challenges that are especially difficult to overcome, such as how to allocate the moduli to each group and how many groups and stages we shall split in order to achieve a best remainder error bound. Interestingly, when the modulus set is the case considered in [25–27], i.e., the remaining

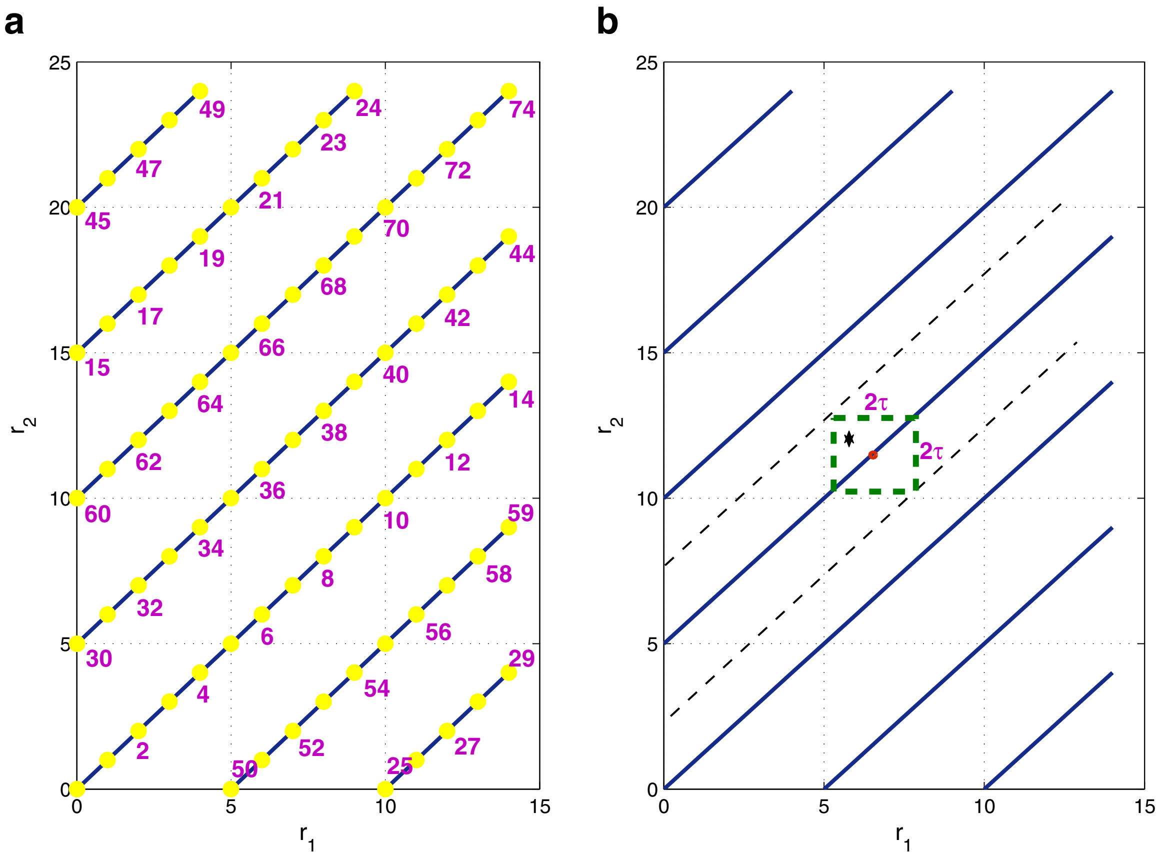

Fig. 2. (a) Integer position representation with respect to two moduli, $m_1 = 15$ and $m_2 = 25$; (b) The remainders of an integer with an error bound τ.

factors Γ_i of the moduli $m_i = m\Gamma_i$ divided by their gcd m are pairwise coprime, it is proven in [29] that the remainder error bound cannot be enlarged by the multi-stage robust CRT algorithm anymore. Apart from these challenges, one might ask what the largest remainder error bound is for a given set of moduli. We will discuss it in a geometrical manner in the next section.

5. Geometrical interpretation of robust CRT

In this section, we describe an intuitive interpretation for the robust CRT from a geometrical point of view, which helps us to develop a heuristic method and derive some more in-depth results.

Given a set of moduli m_1, m_2, $\cdots$, m_L, the CRT says that all integers in the range $[0, M)$ and their remainder vectors are in one-to-one correspondence with each other. In other words, each integer $N \in [0, M)$ is paired with exactly its own remainder vector $(r_1, r_2, \cdots, r_L)$, and vice versa. Thus, we can represent each integer $N \in [0, M)$ by a unique point with coordinates being its remainder vector $(r_1, r_2, \cdots, r_L)$ in the L-dimensional remainder space, and all integers are connected by a set of parallel line segments, denoted by $\mathcal{S}$, with direction $(1, 1, \cdots, 1)$ inside the hyperrectangle $[0, m_1 - 1] \times [0, m_2 - 1] \times \cdots \times [0, m_L - 1]$, where the integers on a line segment in $\mathcal{S}$ share the same folding number vector $(n_1, n_2, \cdots, n_L)$, and all the line segments in $\mathcal{S}$ are characterized by different folding number vectors, see, for example, Fig. 2(a).

Accordingly, we next see the robust CRT from a geometric perspective. When the remainders have errors with the error bound τ, the point $(\tilde{r}_1, \tilde{r}_2, \cdots, \tilde{r}_L)$ is inside the hypercube of side length 2τ centered on the point $(r_1, r_2, \cdots, r_L)$, but probably not lie on the line segment that passes through the point $(r_1, r_2, \cdots, r_L)$ (e.g., see Fig. 2(b)). Let d_{min} denote the minimum distance between the line segments in $\mathcal{S}$. It rapidly becomes apparent that if the remainder error bound τ satisfies

$$\tau < \frac{d_{min}}{2\sqrt{L}}, \tag{33}$$

the closest line segment in $\mathcal{S}$ to the point $(\tilde{r}_1, \tilde{r}_2, \cdots, \tilde{r}_L)$ is exactly the one that passes through the point $(r_1, r_2, \cdots, r_L)$, which equivalently means that the folding number vector is accurately determined by finding the closest line segment in $\mathcal{S}$ to the point $(\tilde{r}_1, \tilde{r}_2, \cdots, \tilde{r}_L)$, and as a consequence, a robust reconstruction of N can be obtained. It is worth mentioning here that (33) indeed gives the largest remainder error bound for the set of moduli $\{m_1, m_2, \cdots, m_L\}$. However, the direct computation of d_{min} is very cumbersome. A relatively efficient calculation is attainable via orthogonal projections. Since all the line segments in $\mathcal{S}$ are parallel, we can project these line segments orthogonally onto a hyperplane through the center $(m_1/2, m_2/2, \cdots, m_L/2)$ of the hyperrectangle, and then calculate d_{min} equivalently as the minimum distance between these projected points on the hyperplane, as seen in Fig. 3.

In addition, we observe that the minimum distance d_{min} increases as the range of N decreases. More precisely, if N is assumed to be in a smaller range $[0, R)$ than the maximum possible range $[0, M)$, i.e., $R < M$, the number of the line segments in $\mathcal{S}$ that connect all the integers from 0 to $R - 1$ becomes smaller, which implies that the minimum distance between these line segments becomes larger. An example for a three-modulus system is shown in Fig. 3. As the minimum distance increases, the remainder error bound increases according to (33). In short, there exists a tradeoff between the range of N and the remainder error bound τ.

Considering the robust CRT in a two-modulus system (i.e., $L = 2$), some rough results on the tradeoff between the range and the remainder error bound have been obtained in [56]. Inspired by

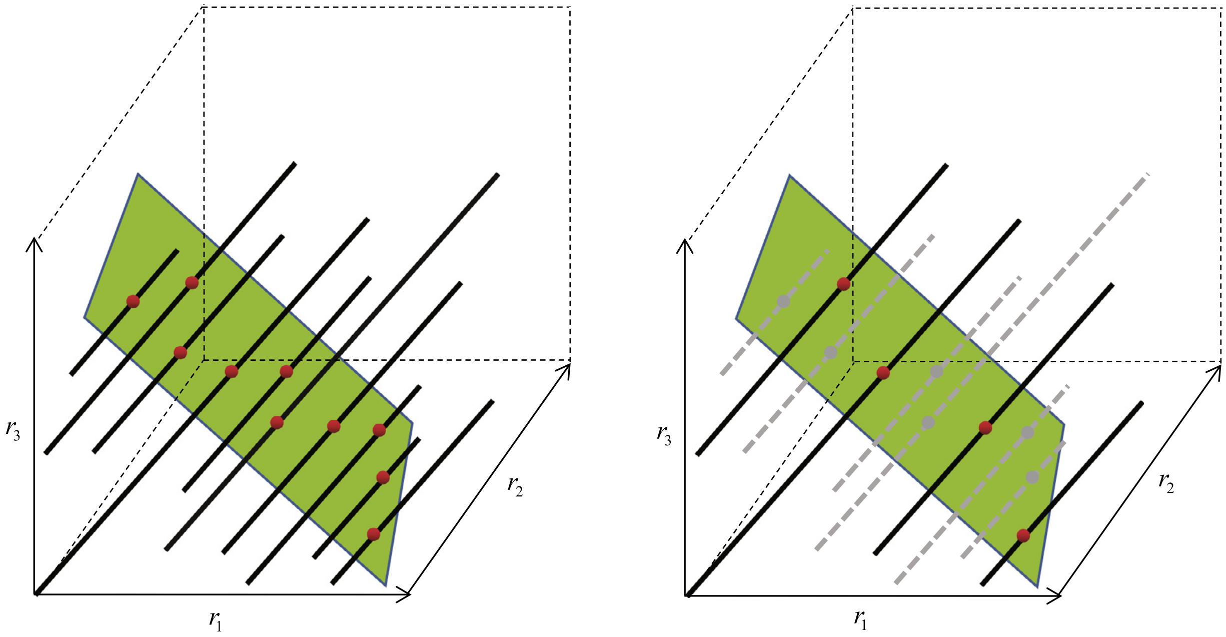

Fig. 3. Integer position representation with respect to three moduli.

Parhami [56], our recent work [30] derived the explicit closed-form expressions for the range and the remainder error bound by a hierarchical structure in a two-modulus system, as briefly stated below.

Given two moduli m_1 and m_2 with $m_1 < m_2$ and $m_1 \nmid m_2$ in a two-modulus system, write $m_1 = m\Gamma_1$ and $m_2 = m\Gamma_2$, where $m \triangleq \gcd(m_1,\ m_2)$, and the notation $a \nmid b$ means that b is not divisible by a. Let $\sigma_{-1} \triangleq \Gamma_2, \sigma_0 \triangleq \Gamma_1$, and for $i \geq 1$,

$$\sigma_i = |\sigma_{i-2}|_{\sigma_{i-1}}, \tag{34}$$

where $|a|_b$ is a shorthand notation for the remainder of a modulo b. Based on (34), there must be an index $K \geq 0$ such that $\sigma_{-1} > \cdots > \sigma_K > \sigma_{K+1} = 1$. Then, we have the following result.

Theorem 4 *[30]. If an integer N is assumed to be in the range* $0 \leq N < \min(m_2(1+\breve{n}_{2,i}), m_1(1+\breve{n}_{1,i}))$ *and the remainder error bound* τ *satisfies*

$$\tau < \frac{m\sigma_i}{4} \tag{35}$$

for some i, $1 \leq i \leq K+1$, *then we can robustly reconstruct N from the erroneous remainders, where* $\breve{n}_{2,i}$ *and* $\breve{n}_{1,i}$ *can be, respectively, calculated by the following recursive formulae:*

i) *When* $K = 0$, *we have* $\breve{n}_{2,1} = \Gamma_1 - 1, \breve{n}_{1,1} = \Gamma_2 - 1.$
ii) *When* $K \geq 1$, *we have* $\breve{n}_{2,K+1} = \Gamma_1 - 1, \breve{n}_{1,K+1} = \Gamma_2 - 1$, *and for* $1 \leq i \leq K$,

$$\breve{n}_{2,i} = \begin{cases} \left\lfloor \frac{\Gamma_1}{\sigma_1} \right\rfloor, & \text{if } i = 1; \\ \left\lfloor \frac{\Gamma_1}{\sigma_1} \right\rfloor \left\lfloor \frac{\sigma_1}{\sigma_2} \right\rfloor, & \text{if } i = 2; \\ \left\lfloor \frac{\sigma_{2p}}{\sigma_{2p+1}} \right\rfloor (\breve{n}_{2,2p}+1) + \breve{n}_{2,2p-1}, & \text{if } i = 2p+1 \text{ for } p \geq 1; \\ \left\lfloor \frac{\sigma_{2p+1}}{\sigma_{2p+2}} \right\rfloor \breve{n}_{2,2p+1} + \breve{n}_{2,2p}, & \text{if } i = 2p+2 \text{ for } p \geq 1 \end{cases} \tag{36}$$

Table 1
The tradeoff between the range and the remainder error bound in Example 5.

Level	Value of σ_i	Remainder error bound	$\breve{n}_{1,i}$	$\breve{n}_{2,i}$	Range
V	$\sigma_1 = 11$	$\tau < (13 \cdot 11)/4 = 35.75$	1	1	$0 \leq N < 468$
IV	$\sigma_2 = 7$	$\tau < (13 \cdot 7)/4 = 22.75$	3	1	$0 \leq N < 754$
III	$\sigma_3 = 4$	$\tau < (13 \cdot 4)/4 = 13$	4	3	$0 \leq N < 1170$
II	$\sigma_4 = 3$	$\tau < (13 \cdot 3)/4 = 9.75$	8	4	$0 \leq N < 1885$
I	$\sigma_5 = 1$	$\tau < (13 \cdot 1)/4 = 3.25$	28	17	$0 \leq N < 6786$

and

$$\breve{n}_{1,i} = \begin{cases} \left\lfloor \frac{\Gamma_2}{\Gamma_1} \right\rfloor \left\lfloor \frac{\Gamma_1}{\sigma_1} \right\rfloor, & \text{if } i = 1; \\ \left\lfloor \frac{\Gamma_2}{\Gamma_1} \right\rfloor \left\lfloor \frac{\Gamma_1}{\sigma_1} \right\rfloor \left\lfloor \frac{\sigma_1}{\sigma_2} \right\rfloor + \left\lfloor \frac{\sigma_1}{\sigma_2} \right\rfloor + \left\lfloor \frac{\Gamma_2}{\Gamma_1} \right\rfloor, & \text{if } i = 2; \\ \left\lfloor \frac{\sigma_{2p}}{\sigma_{2p+1}} \right\rfloor \breve{n}_{1,2p} + \breve{n}_{1,2p-1}, & \text{if } i = 2p+1 \text{ for } p \geq 1; \\ \left\lfloor \frac{\sigma_{2p+1}}{\sigma_{2p+2}} \right\rfloor (\breve{n}_{1,2p+1}+1) + \breve{n}_{1,2p}, & \text{if } i = 2p+2 \text{ for } p \geq 1. \end{cases} \tag{37}$$

Theorem 4 demonstrates that the remainder error bound decreases as the range increases for a two-modulus system. When the range increases to the maximum, i.e., $0 \leq N < \text{lcm}(m_1,\ m_2)$ or $i = K+1$ in Theorem 4, the remainder error bound decreases to the minimum, i.e., $\tau < m/4$, which is in coincidence with the result in Theorem 2 for a two-modulus system. Let us see this in an example below.

Example 5. Let $m_1 = 13 \cdot 18$ and $m_2 = 13 \cdot 29$. The lcm of the moduli is $\text{lcm}(m_1, m_2) = 6786$. Based on Theorem 4, we have the following result in Table 1, where the last row, i.e., Level I, is the known result in Theorem 2.

However, for a multi-modulus (three or more moduli) system, it is very difficult to derive the explicit expressions for the range and the remainder error bound as what is done for a two-modulus system in Theorem 4. Motivated by the two-stage CRT method introduced in the previous section, we propose a suboptimal method to quantify the tradeoff between the range and the remainder error bound for a multi-modulus system as follows. First, the moduli are split into two groups, and a robust reconstruction is obtained for

Table 2
The tradeoff between the range and the remainder error bound in Example 6.

Level	Value of σ_i	Remainder error bound	$\ddot{n}_{1,i}$	$\ddot{n}_{2,i}$	Range
III	$\sigma_1 = 9$	$\tau < 60/4 = 15$	4	2	$0 \le N < 3000$
II	$\sigma_2 = 2$	$\tau < 60/4 = 15$	22	8	$0 \le N < 13,230$
I	$\sigma_3 = 1$	$\tau < 30/4 = 7.5$	48	19	$0 \le N < 29,400$

each group according to Theorem 3. Then, with these two obtained reconstructions from the groups, Theorem 4 is applied across the two groups. Let us take a concrete example as an illustration below.

Example 6. Let $m_1 = 60 \cdot 2,\ m_2 = 60 \cdot 5,\ m_3 = 70 \cdot 3,\ m_4 = 70 \cdot 7$. The lcm of all the moduli is $M \triangleq \mathrm{lcm}(m_1, m_2, m_3, m_4) = 29,400$. We split the moduli into two groups: $\{m_1,\ m_2\}$ and $\{m_3,\ m_4\}$. Let $m^{(1)} \triangleq \gcd(m_1, m_2) = 60,\ m^{(2)} \triangleq \gcd(m_3, m_4) = 70,\ \eta_1 \triangleq \mathrm{lcm}(m_1, m_2) = 600 = 30 \cdot 20,$ and $\eta_2 \triangleq \mathrm{lcm}(m_3, m_4) = 1470 = 30 \cdot 49$. We first apply Theorems 2 or 3 to each group and obtain two reconstructions $\hat{N}_1, \hat{N}_2$. Then, regarding $\hat{N}_1, \hat{N}_2$ as the erroneous remainders and $\eta_1,\ \eta_2$ as the moduli in (29), we apply Theorem 4 across the two groups and obtain a reconstruction $\hat{N}$ as desired. Let $\eta \triangleq \gcd(\eta_1, \eta_2) = 30,$ and $\Gamma_1,\ \Gamma_2$ denote the remaining factors of $\eta_1,\ \eta_2$ divided by their gcd η, i.e., $\eta_1 = \eta\Gamma_1$ and $\eta_2 = \eta\Gamma_2$. Therefore, $\hat{N}$ is a robust reconstruction of N, if N is assumed to be in the range $0 \le N < \min(\eta_2(1 + \breve{n}_{2,i}), \eta_1(1 + \breve{n}_{1,i}))$ and the remainder error bound τ satisfies

$$\tau < \frac{\min(m^{(1)}, m^{(2)}, \eta\sigma_i)}{4} \tag{38}$$

for some $i, 1 \le i \le K + 1,$ where the values of $\sigma_i, K, \breve{n}_{2,i}, \breve{n}_{1,i}$ are determined by $\Gamma_1,\ \Gamma_2$ in (34), (36), (37). The result is shown in Table 2, where the last row, i.e., Level I, is the known result in Theorem 3. One can see that when the range of N is $0 \le N < 13,230,$ the remainder error bound can reach 60/4 that is twice as large as that obtained in Theorem 3.

6. Generalizations and open problems

In this section, we introduce two interesting generalizations of the robust CRT, i.e., robust generalized CRT for multiple integers and robust double-remaindering CRT, and their related open problems, respectively.

6.1. Robust generalized CRT for multiple integers

The above robust CRT is studied for estimating the frequency of a single harmonic signal in the signal model (1). A common practice is to estimate the multiple frequencies of a superposition of harmonic signals from multiple undersamplings. More explicitly, let us consider ρ frequencies N_i Hz for $1 \le i \le \rho$ that need to be estimated in a superpositioned signal $x(t)$:

$$x(t) = \sum_{i=1}^{\rho} a_i \exp(j2\pi N_i t), \tag{39}$$

where a_i are unknown nonzero complex coefficients. We undersample $x(t)$ with multiple sampling rates m_k Hz for $1 \le k \le L$, and the sampled signal with sampling rate m_k Hz is

$$x_k[n] = \sum_{i=1}^{\rho} a_i \exp(j2\pi N_i n / m_k). \tag{40}$$

We then take the m_k-point DFT to $x_k[n]$ and obtain

$$X_k[l] = \sum_{i=1}^{\rho} a_i \delta(l - r_{i,k}), \tag{41}$$

where $\delta(l)$ takes 1 when $l = 0$ and 0 otherwise, and $r_{i,\,k}$ are the remainders of N_i modulo m_k, i.e., $r_{i,k} \equiv N_i \bmod m_k$. Thus, what can be detected from the sampled signal with sampling rate m_k Hz is the following remainder set

$$S_k \triangleq \bigcup_{i=1}^{\rho} \{r_{i,k}\} \triangleq \{t_{i,k} : i = 1, 2, \cdots, \rho_k\}, \tag{42}$$

where $t_{i_1,k} < t_{i_2,k}$ for $1 \le i_1 < i_2 \le \rho_k$, and $\rho_k \le \rho$ is the number of distinct elements, i.e., the cardinality, of the set S_k. Note that the correspondence between the elements in a remainder set and the multiple integers is unknown. Hence, the multiple frequency estimation problem equivalently becomes the reconstruction problem of the multiple integers from their unordered remainder sets [18–21], which we call the generalized CRT for multiple integers.

As an illustrative example, let us consider the case when three integers are 5,19,192 and three moduli are 5,7,9. In this case, the three remainder sets we can detect are {0, 2, 4}, {3, 5}, {1, 3, 5}, respectively. The problem is to uniquely reconstruct the three integers from these remainder sets and moduli, where the correspondence between the three integers and their remainders in a remainder set is not specified, for example, in the second remainder set {3, 5}, we know neither whether 3 is the remainder of the first, second or third unknown integer modulo 7, nor whether 3 repeats once or twice. One can easily check that another three integers 10,12,59 have the same remainder sets as above. So, the range for the uniqueness of the reconstruction of the three integers would be much smaller than $[0, \mathrm{lcm}(5, 7, 9)) = [0, 315),$ unlike the CRT for a singe integer. Without loss of generality, assume that $m_1 < m_2 < \cdots < m_L$ are pairwise coprime. A best known range for the generalized CRT for multiple integers was proposed in [57] when $\rho < 2$. Before stating it, let us introduce some notations. Let ϖ be a γ-partition of modulus set $\mathcal{M} \triangleq \{m_1, m_2, \cdots, m_L\}$ such that $\mathcal{M}$ is decomposed into a union of its γ disjoint subsets, i.e., $\mathcal{M} = \mathcal{M}_1^{\varpi} \bigcup \mathcal{M}_2^{\varpi} \bigcup \cdots \bigcup \mathcal{M}_{\gamma}^{\varpi}$ and $\mathcal{M}_i^{\varpi} \bigcap \mathcal{M}_j^{\varpi} = \emptyset$ for any pair of i and j with $i \neq j$, where $\mathcal{M}_i^{\varpi}$ can be the empty set. Define $b_i^{\varpi} \triangleq \prod_{m_l \in \mathcal{M}_i^{\varpi}} m_l$ if $\mathcal{M}_i^{\varpi}$ is not empty, and $b_i^{\varpi} \triangleq 1$ otherwise. Then, let $b(\gamma) \triangleq \max_{\varpi \in \mathcal{P}} \min_{1 \le i \le \gamma} b_i^{\varpi}$ and $c(\gamma) \triangleq \min_{\varpi \in \mathcal{P}} \max_{1 \le i \le \gamma} b_i^{\varpi}$, where $\mathcal{P}$ denotes the set of all γ-partitions of $\mathcal{M}$. Then, we have the following result.

Theorem 5. [57] *$N_1,\ N_2,\ \cdots,\ N_\rho$ can be uniquely determined from their remainder sets, if*

$$\max\{N_1, N_2, \cdots, N_\rho\} < \max\left\{\min\{c(\rho), b(2)\}, \prod_{i=1}^{\lceil L/\rho \rceil} m_i, m_L\right\} \tag{43}$$

when $\rho > 2$, and

$$\max\{N_1, N_2, \cdots, N_\rho\} < \max\{b(2), m_L\} \tag{44}$$

when $\rho = 2$, where $\lceil \cdot \rceil$ denotes the ceiling function.

The range given in Theorem 5 is not necessarily the largest one. Let us give a simple counter example as follows. Consider the case of two integer determination (i.e., $\rho = 2$) from their four remainder sets (i.e., $L = 4$), where the four moduli are given by

$m_1 = 17, m_2 = 19, m_3 = 20, m_4 = 21$. In this case, the range from Theorem 5 is $\max\{N_1, N_2\} < 357$, whereas the largest range is easily checked to be $\max\{N_1, N_2\} < 737$. Recently, the largest range along with an efficient reconstruction algorithm for the generalized CRT for two integers, i.e., $\rho = 2$, has been studied and/or provided in [58] and [59] with the following theorem.

Theorem 6. *[59] If $m_{L-1} \geq 3$, the largest range for uniquely determining two integers N_1, N_2 from their remainder sets is*

$$\max\{N_1, N_2\} < \min_{\mathcal{I} \subseteq \mathcal{Q}} \left\{ \prod_{i \in \mathcal{I}} m_i + \prod_{i \in \overline{\mathcal{I}}} m_i \right\}, \tag{45}$$

where $\mathcal{Q} = \{1, 2, \cdots, L\}$, and the symbol $\overline{\mathcal{I}}$ denotes the complement of $\mathcal{I}$ in $\mathcal{Q}$.

So far the largest range and any simple reconstruction algorithm for the generalized CRT for multiple (larger than 2) integers are still unknown and would be interesting. Incidentally, by imposing additional conditions on the multiple integers and/or the moduli, some different results were proposed in [19, 60–62].

On the other hand, considering that the detected remainders in the remainder sets often have errors due to noise in practical applications, there is an even greater need in the future for robustly reconstructing the multiple integers from the erroneous remainders, similar to the robust CRT. Recently, the generalized robust CRT for two integers has been presented in [31], under the assumption that the remaining factors of the moduli divided by their gcd are pairwise coprime. Mathematically, let moduli $m_i = m\Gamma_i$ for $1 \leq i \leq L$, where $\Gamma_1, \Gamma_2, \cdots, \Gamma_L$ are pairwise coprime. Let τ be the remainder error bound, i.e., $|\triangle r_{i,k}| = |\tilde{r}_{i,k} - r_{i,k}| \leq \tau$ for $i = 1, 2$ and $1 \leq k \leq L$. Then, we have the generalized robust CRT for two integers in the following.

Theorem 7. *[31] If integers N_1, N_2 are assumed to be in the range*

$$\max\{N_1, N_2\} < m \cdot \min_{\mathcal{I} \subseteq \mathcal{Q}} \left\{ \prod_{i \in \mathcal{I}} \Gamma_i + \prod_{i \in \overline{\mathcal{I}}} \Gamma_i \right\} \tag{46}$$

and the remainder error bound τ satisfies

$$\tau < m/8, \tag{47}$$

where $\mathcal{Q}$ and $\overline{\mathcal{I}}$ are defined as in Theorem 6, then we can robustly reconstruct N_1, N_2, i.e., $|\hat{N}_i - N_i| \leq \tau$ for $i = 1, 2$.

For a reconstruction algorithm of Theorem 7, we refer the reader to [31]. General results for the generalized robust CRT for multiple integers as well as fast reconstruction algorithms are of great interest for further research.

Remark 1. Note that the estimation of frequencies of a multi-harmonic signal in (39) from multiple undersampled waveforms has also been considered in the more recent sparse fast Fourier transform (SFFT) [63–71]. The algorithm in [63,64] relies on the combinatorial properties of aliasing among frequencies in DFTs such that by taking enough DFTs of sub-samples with coprime sampling rates, each frequency is isolated from the others in at least half of the DFTs. Then, based on the CRT and majority rule, all the frequencies are guaranteed to be recovered. In [65,66], enough DFTs of sub-samples with coprime sampling rates are also needed such that each frequency is isolated for at least one DFT, and then by using slightly shifted samples to distinguish non-aliased frequencies from aliased ones in a DFT and determine the values of the non-aliased frequencies, a different algorithm with reduced sampling and runtime complexities was proposed. In [67–71], by using aliasing filters with coprime sub-Nyquist sampling rates, the frequency coefficients are split into buckets such that the value in each bucket is the sum of the values of only the frequency coefficients that compose the bucket. All the frequencies are then estimated by iteratively estimating the frequencies from buckets where they do not collide and subtracting them from buckets where they do collide, in which the change of the phase caused by shifted samples is used to determine the frequency and the corresponding frequency coefficient in the bucket with exactly one frequency coefficient. The robust CRT and generalized robust CRT we have discussed in this paper are different from the above mentioned SFFT based algorithms in a number of aspects:

1) The sub-Nyquist sampling rates (or moduli) are neither limited to being pairwise coprime nor require specific combinatorial structures.
2) Additional samplings at slightly shifted points are not needed. The number of DFTs or the number of samples required is significantly less.
3) All the frequencies (or large integers) are estimated in one shot based on the proposed generalized (robust) CRT from the detected aliased frequency (or remainder) sets.
4) The robustness is considered with respect to the errors in the remainders.

6.2. Robust double-remaindering CRT

Many ambiguity problems in practice can be reduced to the solution of simultaneous linear congruences. So, the CRT provides an ambiguity resolution method. We next state the (robust) double-remaindering CRT, which originally arises from estimating the radial velocity of a ground moving target by resolving the so-called time-space Doppler ambiguity in multichannel SAR [32], where the time domain Doppler ambiguity occurs first in each channel and then the spatial domain Doppler ambiguity occurs among multi-channels. We refer the reader to [32] for details.

In terms of number theory, the double-remaindering CRT opens a brand new mathematical problem, as described below. Let $M_1, M_2, \cdots, M_L$ and $N_1, N_2, \cdots, N_L$ be positive integers, where $N_i < M_i$ for $1 \leq i \leq L$. Then, a nonnegative integer N can be written as

$$N = m_i M_i + n_i N_i + r_i, \ \text{for } 1 \leq i \leq L, \tag{48}$$

where r_i with $0 \leq r_i < N_i$ are called the double-remaindering remainders for which N is first taken a modulo with a larger positive integer M_i and then its remainder is taken another modulo with a smaller positive integer N_i, i.e.,

$$r_i \equiv (N \bmod M_i) \bmod N_i. \tag{49}$$

For example, let $M_1 = 12, M_2 = 20$ and $N_1 = 5, N_2 = 9$. We can find that $N = 29$ and $N = 0$ have the same double-remaindering remainders $r_1 = r_2 = 0$. A natural question is how large the integer N can be so that it can be uniquely determined from the double-remaindering remainders r_i for $1 \leq i \leq L$. Let $d_i \triangleq \gcd(M_i, N_i)$ and $r_i = k_i d_i + |r_i|_{d_i}$ for $1 \leq i \leq L$, where $|r_i|_{d_i}$ denotes the remainder of r_i modulo d_i. We rewrite (48) as

$$N = \left(m_i \frac{M_i}{d_i} + n_i \frac{N_i}{d_i} + k_i \right) d_i + |r_i|_{d_i}, \tag{50}$$

and then we can simply regard the double-remaindering CRT as the CRT. Accordingly, N can be uniquely reconstructed from r_i if $0 \leq N < \mathrm{lcm}(d_1, d_2, \cdots, d_L)$. Obviously, the range we have above is too weak, especially when M_i and N_i are coprime. This analysis is only a first look for this problem, and further research is clearly needed. What is more is that we expect to see any development of the robust double-remaindering CRT, when the double-remaindering remainders r_i for $1 \leq i \leq L$ have errors.

7. Conclusion

In this paper, we have provided an overview on the robust CRT and its applications in frequency estimation from multiple truly sub-Nyquist samplers. It summaries some of the research results on this topic from the authors' group starting from the mid 1990s. It also provides some of the challenging open research problems on this topic. Since the robust CRT problem is a fundamental problem, we believe that it will have broader applications than what we have mentioned in this paper.

References

[1] H.L.V. Trees, Detection, Estimation and Modulation Theory: Part III. Radar–Sonar Signal Processing and Gaussian Signals in Noise, Wiley, New York, NY, USA, 1971.

[2] S.M. Kay, Modern Spectral Estimation: Theory and Application, Englewood Cliffs, NJ: Prentice-Hall, 1988.

[3] P. Stoica, R.L. Moses, Spectral Analysis of Signals, NJ: Prentice-Hall, Upper Saddle River, 2005.

[4] S. Kay, S. Saha, Mean likelihood frequency estimation, IEEE Trans. Signal Process. 48 (7) (2000) 1937–1946.

[5] H.C. So, K.W. Chan, Approximate maximum-likelihood algorithms for two dimensional frequency estimation of a complex sinusoid, IEEE Trans. Signal Process. 54 (8) (2006) 3231–3237.

[6] M.G. Christensen, S.H. Jensen, New results on perceptual distortion minimization and nonlinear least-squares frequency estimation, IEEE Trans. Audio, Speech, Lang. Process. 19 (7) (2011) 2239–2244.

[7] D. Potts, M. Tasche, Parameter estimation for exponential sums by approximate prony method, Signal Process. 90 (5) (2010) 1631–1642.

[8] O. Besson, P. Stoica, Analysis of MUSIC and ESPRIT frequency estimates for sinusoidal signals with lowpass envelopes, IEEE Trans. Signal Process. 44 (9) (1996) 2359–2364.

[9] W.J. Zeng, H.C. So, L. Huang, l_p-MUSIC: robust direction-of-arrival estimator for impulsive noise environments, IEEE Trans. Signal Process. 61 (17) (2013) 4296–4308.

[10] E.J. Candès, T. Tao, Decoding by linear programming, IEEE Trans. Inf. Theory 51 (12) (2005) 4203–4215.

[11] D.L. Donoho, Compressed sensing, IEEE Trans. Inf. Theory 52 (4) (2006) 1289–1306.

[12] E.J. Candès, M.B. Wakin, An introduction to compressive sampling, IEEE Signal Process. Mag. 25 (2) (2008) 21–30.

[13] Y. Chen, Y. Chi, Robust spectral compressed sensing via structured matrix completion, IEEE Trans. Inf. Theory 60 (10) (2014) 6576–6601.

[14] T. Strohmer, Measure what should be measured: progress and challenges in compressive sensing, IEEE Signal Process. Lett. 19 (12) (2012) 887–893.

[15] P.P. Vaidyanathan, P. Pal, Sparse sensing with co-prime samplers and arrays, IEEE Trans. Signal Process. 59 (2) (2011) 573–586.

[16] P. Pal, P.P. Vaidyanathan, Coprime sampling and the MUSIC algorithm, in: Proc. IEEE Digit. Signal Process. Workshop and IEEE Signal Process. Educ. Workshop (DSP/SPE), 2011, pp. 289–294.

[17] S. Qin, Y.D. Zhang, M.G. Amin, A.M. Zoubir, Generalized coprime sampling of toeplitz matrices for spectrum estimation, IEEE Trans. Signal Process. 65 (1) (2017) 81–94.

[18] X.G. Xia, On estimation of multiple frequencies in undersampled complex valued waveforms, IEEE Trans. Signal Process. 47 (12) (1999) 3417–3419.

[19] G. Zhou, X.G. Xia, Multiple frequency detection in undersampled complex-valued waveforms with close multiple frequencies, Electron. Lett. 33 (15) (1997) 1294–1295.

[20] X.G. Xia, An efficient frequency-determination algorithm from multiple undersampled waveforms, IEEE Signal Process. Lett. 7 (2) (2000) 34–37.

[21] X.G. Xia, K. Liu, A generalized chinese remainder theorem for residue sets with errors and its application in frequency determination from multiple sensors with low sampling rates, IEEE Signal Process. Lett. 12 (11) (2005) 768–771.

[22] N.S. Szabo, R.I. Tanaka, Residue Arithmetic and its Application to Computer Technology, McGraw-Hill, New York, 1967.

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

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

[25] X.G. Xia, G. Wang, Phase unwrapping and a robust chinese remainder theorem, IEEE Signal Process. Lett. 14 (4) (2007) 247–250.

[26] X.W. Li, H. Liang, X.G. Xia, A robust chinese remainder theorem with its applications in frequency estimation from undersampled waveforms, IEEE Trans. Signal Process. 57 (11) (2009) 4314–4322.

[27] W.J. Wang, X.G. Xia, A closed-form robust chinese remainder theorem and its performance analysis, IEEE Trans. Signal Process. 58 (11) (2010) 5655–5666.

[28] B. Yang, W.J. Wang, X.G. Xia, Q. Yin, Phase detection based range estimation with a dual-band robust chinese remainder theorem, Sci. China-Inf. Sci. 57 (2) (2014) 1–9.

[29] L. Xiao, X.G. Xia, W.J. Wang, Multi-stage robust chinese remainder theorem, IEEE Trans. Signal Process. 62 (18) (2014) 4772–4785.

[30] L. Xiao, X.G. Xia, H.Y. Huo, Towards robustness in residue number systems, IEEE Trans. Signal Process. 65 (6) (2017) 1497–1510.

[31] X.P. Li, X.G. Xia, W.J. Wang, W. Wang, A robust generalized chinese remainder theorem for two integers, IEEE Trans. Inf. Theory 62 (12) (2016) 7491–7504.

[32] J. Xu, Z.Z. Huang, Z. Wang, L. Xiao, X.G. Xia, T. Long, Radial velocity retrieval for multichannel SAR moving targets with time-space doppler de-ambiguity, IEEE Trans. Geosci. Remote Sens. 56 (1) (2018) 35–48.

[33] M. Ruegg, E. Meier, D. Nuesch, Capabilities of dual-frequency millimeter wave SAR with monopulse processing for ground moving target indication, IEEE Trans. Geosci. Remote Sens. 45 (3) (2007) 539–553.

[34] G. Li, J. Xu, Y.N. Peng, X.G. Xia, Location and imaging of moving targets using non-uniform linear antenna array, IEEE Trans. Aerosp. Electron. Syst. 43 (3) (2007) 1214–1220.

[35] Y.M. Zhang, M. Amin, MIMO radar exploiting narrowband frequency-hopping waveforms, in: Proc. 16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, 2008, pp. 25–29.

[36] X.W. Li, X.G. Xia, Location and imaging of elevated moving target using multi-frequency velocity SAR with cross-track interferometry, IEEE Trans. Aerosp. Electron. Syst. 47 (2) (2011) 1203–1212.

[37] Z. Yuan, Y. Deng, F. Li, R. Wang, G. Liu, X. Han, Multichannel inSAR DEM reconstruction through improved closed-form robust Chinese remainder theorem, IEEE Geosci. Remote Sens. Lett. 10 (6) (2013) 1314–1318.

[38] A. Akhlaq, R.G. McKilliam, R. Subramanian, Basic construction for range estimation by phase unwrapping, IEEE Signal Process. Lett. 22 (11) (2015) 2152–2156.

[39] K. Falaggis, D.P. Towers, C.E. Towers, Method of excess fractions with application to absolute distance metrology: analytical solution, Appl. Opt. 52 (23) (2013) 5758–5765.

[40] S. Tang, X. Zhang, D. Tu, Micro-phase measuring profilometry: its sensitivity analysis and phase unwrapping, Opt. Lasers Eng. 72 (2015) 47–57.

[41] T. Petković, T. Pribanić, M. Donlić, Temporal phase unwrapping using orthographic projection, Opt. Lasers Eng. 90 (2017) 34–47.

[42] G. Campobello, A. Leonardi, S. Palazzo, Improving energy saving and reliability in wireless sensor networks using a simple CRT-based packet-forwarding solution, IEEE/ACM Trans. Netw. 20 (1) (2012) 191–205.

[43] S. Chessa, P. Maestrini, Robust distributed storage of residue encoded data, IEEE Trans. Inf. Theory 58 (12) (2012) 7280–7294.

[44] Y.S. Su, Topology-transparent scheduling via the chinese remainder theorem, IEEE/ACM Trans. Netw. 23 (5) (2015) 1416–1429.

[45] I. Fiete, Y. Burak, T. Brookings, J. Neurosci, What grid cells convey about rat location, J. Neurosci. 28 (27) (2008) 6858–6871.

[46] M. Stemmler, A. Mathis, A.V.M. Herz, Connecting multiple spatial scales to decode the population activity of grid cells, Sci. Adv. 1 (11) (2015) E1500816.

[47] Z. Huang, Z. Wan, Range ambiguity resolution in multiple PRF pulse doppler radars, in: Proc. Int. Conf. Acoustics, Speech, Signal Process. (ICASSP), Dallas, TX, 1987, pp. 1786–1789.

[48] W.S.M. Cormick, J.B.Y. Tsui, V.L. Bakke, A noise insensitive solution to an ambiguity problem in spectral estimation, IEEE Trans. Aerosp. Electron. Syst. 25 (5) (1989) 729–732.

[49] H. Krishna, K.Y. Lin, J.D. Sun, A coding theory approach to error control in redundant residue number systems. part i: theory and signal error correction, IEEE Trans. Circuits Syst. 39 (1) (1992) 8–17.

[50] J.D. Sun, H. Krishna, A coding theory approach to error control in redundant residue number systems. part II: multiple error detection and correction, IEEE Trans. Circuits Syst. 39 (1) (1992) 18–34.

[51] L.L. Yang, L. Hanzo, Coding theory and performance of redundant residue number system codes. [Online]. Available: http://www-mobile.ecs.soton.ac.uk.

[52] C.H. Chang, A.S. Molahosseini, A.A.E. Zarandi, T.F. Tay, Residue number systems: a new paradigm to datapath optimization for low-power and high-performance digital signal processing applications, IEEE Circuits Syst. Mag. 15 (4) (2015) 26–44.

[53] O. Goldreich, D. Ron, M. Sudan, Chinese remaindering with errors, IEEE Trans. Inform. Theory 46 (7) (2000) 1330–1338.

[54] V. Guruswami, A. Sahai, M. Sudan, Soft-decision decoding of chinese remainder codes, in: Proc. 41st IEEE Symp. Foundations Computer Science, Redondo Beach, CA, 2000, pp. 159–168.

[55] D. Boneh, Finding smooth integers in short intervals using CRT decoding, J. Comp. and Syst. Sci. 64 (4) (2002) 768–784.

[56] B. Parhami, Digital arithmetic in nature: continuous-digit RNS, The Computer J. 58 (5) (2015) 1214–1223.

[57] H. Liao, X.G. Xia, A sharpened dynamic range of a generalized chinese remainder theorem for multiple integers, IEEE Trans. Inf. Theory 53 (1) (2007) 428–433.

[58] L. Xiao, X.G. Xia, A generalized chinese remainder theorem for two integers, IEEE Signal Process. Lett. 21 (1) (2014) 55–59.

[59] W. Wang, X.P. Li, X.G. Xia, W.J. Wang, The largest dynamic range of a generalized chinese remainder theorem for two integers, IEEE Signal Process. Lett. 22 (2) (2015) 254–258.

[60] L. Xiao, X.G. Xia, H.Y. Huo, New conditions on achieving the maximal possible dynamic range for a generalized chinese remainder theorem of multiple integers, IEEE Signal Process. Lett. 22 (12) (2015) 2199–2203.

[61] B. Arazi, A generalization of the chinese remainder theorem, Pac. J. Math. 70 (2) (1977) 289–296.

[62] H.S. Xiao, C. Cremers, H.K. Garg, Symmetric polynomial & CRT based algorithms for multiple frequency determination from undersampled waveforms, in: Signal and Information Processing (GlobalSIP), 2016 IEEE Global Conference on, Greater Washington D.C., 2016, pp. 202–206.

[63] M.A. Iwen, Combinatorial sublinear-time fourier algorithms, Found. Comput. Math. 10 (3) (2010) 303–338.

[64] M.A. Iwen, Improved approximation guarantees for sublinear-time fourier algorithms, Appl. Comput. Harmon. Anal. 34 (1) (2013) 57–82.

[65] D. Lawlor, Y. Wang, A. Christlieb, Adaptive sub-linear time fourier algorithms, Adv. Adapt. Data Anal. 5 (1) (2013).

[66] A. Christlieb, D. Lawlor, Y. Wang, A multiscale sub-linear time fourier algorithm for noisy data, Appl. Comput. Harmon. Anal. 40 (3) (2016) 553–574.

[67] H. Hassanieh, The Sparse Fourier Transform: Theory & Practice, Massachusetts Institute of Technology, 2016 Phd dissertation.

[68] H. Hassanieh, L. Shi, O. Abari, E. Hamed, D. Katabi, GHz-wide sensing and decoding using the sparse fourier transform, in: Proceedings of the IEEE International Conference on Computer Communications, INFOCOM'14, 2014, pp. 2256–2264.

[69] S. Pawar, K. Ramchandran, FFAST: An algorithm for computing an exactly k-sparse DFT in $o(k\log k)$ time, IEEE Trans. Inf. Theory 64 (1) (2018) 429–450.

[70] S. Pawar, K. Ramchandran, R-FFAST: A robust sub-linear time algorithm for computing a sparse DFT, IEEE Trans. Inf. Theory 64 (1) (2018) 451–466.

[71] D. Potts, M. Tasche, T. Volkmer, Efficient spectral estimation by MUSIC and ESPRIT with application to sparse FFT, Front. Appl. Math. Stat. 2 (1) (2016).