A Robust Generalized Chinese Remainder Theorem for Two Integers

Xiaoping Li, Xiang-Gen Xia, *Fellow, IEEE*, Wenjie Wang, *Member, IEEE*, and Wei Wang

***Abstract*— A generalized Chinese remainder theorem (CRT) for multiple integers from residue sets has been studied recently, where the correspondence between the remainders and the integers in each residue set modulo several moduli is not known. A robust CRT has also been proposed lately to robustly reconstruct a single integer from its erroneous remainders. In this paper, we consider the reconstruction problem of two integers from their residue sets, where the remainders not only are out of order but also may have errors. We prove that two integers can be robustly reconstructed if their remainder errors are less than $M/8$, where M is the greatest common divisor of all the moduli. We also propose an efficient reconstruction algorithm. Finally, we present some simulations to verify the efficiency of the proposed algorithm. This paper is motivated from and has applications in the determination of multiple frequencies from multiple undersampled waveforms.**

***Index Terms*— Chinese remainder theorem (CRT), robust CRT, dynamic range, residue sets, remainder errors, frequency determination from undersampled waveforms.**

I. Introduction

THE traditional Chinese remainder theorem (CRT) is to reconstruct a single nonnegative integer from its remainders modulo several smaller positive integers (called moduli) and it has tremendous applications in various areas [1]–[4]. There are various generalizations of CRT, see, for example, [5] for some of them. One of the generalizations, generalized CRT, is to determine multiple integers from their residue sets where each residue set is the set of remainders of the multiple integers modulo a modulus and the correspondence between the remainders and the multiple integers is not known, i.e., each residue set is not ordered. This problem was first studied in [6]. It was later independently studied in [7]–[13], motivated from multiple frequency determination in multiple undersampled waveforms. It exists in many engineering applications, such as phase unwrapping in signal processing [14]–[20], multiwavelength optical interferometry [21], [22], radar signal processing [23]–[27], mechanical engineering [28], and wireless sensor networks [29], [30].

Usually the moduli in CRT or the generalized CRT mentioned above are required to be pairwisely co-prime, which causes the reconstruction not robust in the sense that a small error in its remainders may cause a large reconstruction error. Robust reconstruction methods, i.e., robust CRT, for a single integer from its erroneous remainders have been studied and obtained in [31]–[39]. The basic idea for these robust CRT is to include a common factor among all the moduli and then as long as the remainder errors are less than the quarter of the greatest common divisor (gcd) of all the moduli, a reconstruction error of the integer will be less than the maximum remainder error. Several robust reconstruction methods have been proposed, for example, searching based robust CRT [33]–[35], closed-form robust CRT [36], multi-stage robust CRT [38], [39], where in [39] the upper bound, i.e., the quarter of the gcd, has been improved, when the remaining integers of the moduli factorized by the gcd are not necessarily co-prime. All these studies are only for the traditional CRT for single integer. There is no attempt in the literature to robustly reconstruct multiple integers from their erroneous residue sets, i.e., robust generalized CRT, although [12] studies the case when most of the residue sets are error-free but only a few remainder sets include erroneous remainders and is not in the sense of the robustness in the literature. The main goal of this paper is on a robust generalized CRT for two integers.

For the case of more than one integer estimation from their residue sets, i.e., the generalized CRT, the reconstruction is more complicated. As mentioned in [8], the main difficulty for the case of no less than two integers comes from the fact that the correspondence between the integer and its remainder is not known, which happens when the remainders are obtained by detecting the peaks of the discrete Fourier transforms (DFT) of an undersampled waveform as described in [8]. Moreover, the number of the remainders in a residue set may be less than the number of the integers to determine, since there may be two or more integers sharing the same remainder for some moduli. While all the distinct elements in a residue set are known, the number of repetitions of any remainder

Manuscript received October 28, 2015; revised August 17, 2016; accepted September 8, 2016. Date of publication September 28, 2016; date of current version November 18, 2016. This work was supported in part by the 973 Program under Grant 2013CB329404, in part by NSFC under Grant 61172092, Grant 61370147, and Grant 11561058, in part by the Research Fund for the Doctoral Programs of Higher Education of China under Grant 20130201110014, and in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2013Z005.

X. Li is with the MOE Key Laboratory for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China, and also with the School of Mathematical Science, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: lixiaoping@stu.xjtu.edu.cn).

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

W. Wang is with the MOE Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: wjwang@xjtu.edu.cn).

W. Wang is with College of Information Engineering, Tarim University, Alar 843300, China (e-mail: wangwei.math@gmail.com).

Communicated by C. Wang, Associate Editor for Coding Techniques.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2016.2614322

is not known in general unless there are only two integers to determine. As mentioned earlier, for the robustness of reconstructing a single integer from its erroneous remainders, it is critical to have a gcd larger than 1 among all the moduli. This has to hold for the above generalized CRT for multiple integers. However, the generalized CRT methods studied before are only when all the moduli are pairwisely co-prime. Therefore, in order to study a robust generalized CRT, we first need to study the generalized CRT when all the moduli have a gcd larger than 1 and all the remainders are error-free. A basic problem then is to determine the dynamic range for a given set of moduli, i.e., the largest range within which multiple nonnegative integers can be uniquely determined from their residue sets modulo the given moduli. For this problem and when all the moduli are pairwisely co-prime, several lower bounds for the dynamic range were obtained in [7]–[10]. A most recent tight bound was obtained in [13] for two integers where a closed-form and a simple determination algorithm were also obtained.

In this paper, we first present the largest dynamic range for two integers when all the moduli have a gcd larger than 1 and the remaining integers factorized by the gcd of the moduli are pairwisely co-prime. For the generalized CRT with erroneous remainders, we obtain a remainder error bound of the eighth of the gcd of all the moduli that leads to a robust estimation of two integers. An efficient reconstruction algorithm is also presented when two integers are within the largest dynamic range. Note that, for the robustness, the remainder error bound, the eighth of the gcd for two integers, seems not surprising, when the remainder error bound, the quarter of the gcd, for a single integer in CRT is known. However, as we shall see later, the proof is not trivial at all.

This paper is organized as follows. In Section II, we briefly describe the mathematical problem and introduce some notations. In Section III, we present the largest dynamic range and a closed-form determination algorithm for two integers from their error free residue sets, where the moduli are no longer pairwisely co-prime. In Section IV, we present a robust generalized CRT for two integers. In Section V, we present an application of the proposed robust generalized CRT in frequency estimation from multiple undersampled waveforms. In Section VI, we conclude this paper.

II. Problem Description

We begin with the multiple frequency determination problem from multiple undersampled waveforms [8]. For simplicity, a complex-valued waveform is given as

$$x(t) = \sum_{l=1}^{L} A_l e^{2\pi j f_l t} + w(t) \tag{1}$$

where $w(t)$ is the additive noise, A_l and f_l are nonzero coefficients and frequencies, respectively. Suppose that these frequencies are distinct non-negative integers, i.e., $f_l = N_l$, where $N_l \in \mathbb{N}$ and $\mathbb{N}$ denotes the set of natural numbers, $N_i \neq N_j$ for $i \neq j$, in Hz. Let $K \geq 2$ and $m_1, \ldots, m_K$ be K positive integers with $1 < m_1 < \cdots < m_K$. For each subscript $k \in \{1, \ldots, K\}$, the sampled signal with sampling frequency m_k Hz is

$$x_{m_k}[n] = x\Big(\frac{n}{m_k}\Big) = \sum_{l=1}^{L} A_l e^{2\pi j N_l n/m_k} + w\Big(\frac{n}{m_k}\Big),\ n \in \mathbb{Z} \tag{2}$$

where $\mathbb{Z}$ denotes the set of integers. Then we take the m_k-point DFT to $x_{m_k}[n]$ in (2), and obtain

$$\mathrm{DFT}_{m_k}\big(x_{m_k}[n]\big)[r] = \sum_{l=1}^{L} A_l \delta[r - r_{l,k}] + W[r] \tag{3}$$

where $\delta[n]$ is the the Kronecker delta function, i.e., $\delta[n]$ equals one when $n = 0$ and zero elsewhere. Without considering the influence of noise, remainders $r_{l,k} \equiv N_l \bmod m_k$ can be detected from the m_k-point DFT without the order information. Then we have the K error-free residue sets

$$R_k(N_1, \ldots, N_L) = \big\{r_{1,k}, \ldots, r_{L,k}\big\},\ k = 1, \ldots, K \tag{4}$$

from the K DFTs. In practice, signals are usually corrupted by noises and thus the obtained remainders $r_{l,k}$ may have errors. Let the erroneous remainders be $\tilde{r}_{l,k}$:

$$\tilde{r}_{l,k} = r_{l,k} + \Delta r_{l,k},\ l = 1, \ldots, L;\ k = 1, \ldots, K \tag{5}$$

where $\Delta r_{l,k}$ denote the errors. Then the erroneous residue sets are

$$\tilde{R}_k(N_1, \ldots, N_L) = \big\{\tilde{r}_{1,k}, \ldots, \tilde{r}_{L,k}\big\},\ k = 1, \ldots, K. \tag{6}$$

The problem is to determine the L frequencies $\{N_1, \ldots, N_L\}$ from these erroneous residue sets.

Under the condition of all the remainders are error-free, $L = 2$, and all the K moduli $m_1, \ldots, m_K$ are pairwisely co-prime, in [13] we obtained the largest dynamic range within which two frequencies (integers), $\{N_1, N_2\}$, can be uniquely determined from their residue sets $R_k(N_1, N_2)$, where an efficient reconstruction algorithm was also proposed. In this paper, we first generalize the largest dynamic range result obtained in [13] from pairwisely co-prime moduli $\mathcal{M}' = \{m_1, \ldots, m_K\}$ to non-pairwisely co-prime moduli $\mathcal{M} = \{M_1, \ldots, M_K\}$ with $M_k = Mm_k$ for $k = 1, \ldots, K$, where $0 < m_1 < \cdots < m_K$ are pairwisely co-prime moduli and M is a positive integer. We then study the reconstruction problem of two integers $\{N_1, N_2\}$ from the erroneous residue sets $\tilde{R}_1(N_1, N_2), \ldots, \tilde{R}_K(N_1, N_2)$ modulo $M_1, \ldots, M_K$, respectively. This question has two parts: 1) the bound of errors, i.e., to what extent of errors we can have a robust estimation of $\{N_1, N_2\}$? 2) how to efficiently and robustly reconstruct $\{N_1, N_2\}$? In what follows, we always denote $\mathcal{M}' = \{m_1, \ldots, m_K\}$ a set of moduli, $\Gamma = \prod_{k=1}^{K} m_k$, and $\mathcal{M} = \{M_1, \ldots, M_K\}$ a set of moduli. A set of moduli, such as $\mathcal{M}$, is called a modulus set.

III. Generalized CRT for Two Integers With Error-Free Residue Sets

In this section, we first recall the basics of dynamic range with modulus set $\mathcal{M}'$ obtained in [13]. Then we obtain the largest dynamic range with a modulus set $\mathcal{M}$ and an efficient method to determine two integers from their error-free residue sets.

We first introduce some notations. The remainder of x modulo y is denoted as $\langle x\rangle_y$. For integer $n > 0$, let $\mathbb{Z}_n$ denote the set $\{0, 1, \ldots, n-1\}$. A set of n elements is called an n-set. If we let $\mathcal{N} = \{N_1, \ldots, N_L\}$ with $N_l \in \mathbb{N}$, $R_k(N_1, \ldots, N_L)$ is also denoted by $R_k(\mathcal{N})$.

Definition 1: The dynamic range of a modulus set $\mathcal{M} = \{m_1, \ldots, m_K\}$ is the minimal positive integer D such that there are two different L-sets $\mathcal{A}$ and $\mathcal{B}$ with $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_{D+1}$ satisfying $R_k(\mathcal{A}) = R_k(\mathcal{B})$ for each modulus m_k. It is denoted by $D_L(m_1, \ldots, m_K)$, or simply $D_L(\mathcal{M})$.

According to Definition 1, if any set of L integers in $\mathbb{Z}_{D'}$ can be uniquely determined by their remainders modulo $m_1, \ldots, m_K$, then we have $D_L(\mathcal{M}) \geq D'$. On the other hand, if L integers are in $\mathbb{Z}_{D_L(\mathcal{M})}$, then they can be uniquely determined from their residue sets modulo $m_1, \ldots, m_K$. Hence, the dynamic range $D_L(\mathcal{M})$ in Definition 1 is the largest dynamic range within which any L integers can be uniquely determined by their residue sets. For $L = 2$ and a given modulus set $\mathcal{M}'$, the largest dynamic range $D_2(\mathcal{M}')$ is obtained as follows.

Lemma 1 [13]: If $m_{K-1} \geq 3$, then $D_2(\mathcal{M}') = d$, where

$$d = \min_{I \subseteq \{1,\ldots,K\}} \left\{ \prod_{i \in I} m_i + \prod_{i \in \overline{I}} m_i \right\}. \tag{7}$$

In other words, if $\mathcal{M}' \neq \{2, 2n+1\}$ for any positive integer n, then $D_2(\mathcal{M}') = d$.

As an example, we consider the case of $\mathcal{M}' = \{3, 5, 7\}$. According to Lemma 1, we know that the largest dynamic is $d = 3 \times 5 + 7 = 22$, i.e., $D_2(\mathcal{M}') = 22$. For the largest dynamic range with modulus set $\mathcal{M}$, we have the following result.

Theorem 1: If $m_1 \geq 3$ and $K > 2$, then $D_2(\mathcal{M}) = Md$.

The proof of this theorem is similar to [13, Th. 1] and therefore it is omitted.

Let us continue the above example. Let $M = 100$, then the largest dynamic range with modulus set $\mathcal{M}$ for two integers is $Md = 2200$, i.e., $D_2(\mathcal{M}) = 2200$. Next, we give the basic idea of reconstructing the two integers $\{N_1, N_2\}$ from their error-free residue sets $R_k(N_1, N_2)$ with modulus set $\mathcal{M}$, where the two integers are within the largest dynamic range.

We begin with the reconstruction of one integer N with modulus set $\mathcal{M}$. Let N be an integer to be reconstructed, and r_k be the remainders of N modulo M_k, i.e.,

$$r_k \equiv N \bmod M_k, \ \ k = 1, \ldots, K \tag{8}$$

where $0 \leq r_k < M_k$. From (8), we have

$$r_k \equiv N \bmod M, \ \ k = 1, \ldots, K. \tag{9}$$

That is, all remainders r_k modulo M have the same value, named common remainder [40], denoted as r^c. It follows from (8) that both $r_k - r^c$ and $N - r^c$ have the same factor M. Let

$$Q = \frac{N - r^c}{M} \tag{10}$$

and

$$q_k = \frac{r_k - r^c}{M}. \tag{11}$$

Then, congruence (8) is equivalent to

$$q_k \equiv Q \bmod m_k, \quad k = 1, \ldots, K.$$

According to the traditional CRT, Q can be uniquely reconstructed as

$$Q \equiv \sum_{k=1}^{K} \Gamma_k \overline{\Gamma}_k q_k \bmod \Gamma \tag{12}$$

if and only if $Q < \Gamma$, where $\Gamma_k = \Gamma/m_k$, and $\overline{\Gamma}_k$ is the multiplicative inverse of Γ_k modulo m_k, i.e.,

$$\Gamma_k \overline{\Gamma}_k \equiv 1 \bmod m_k.$$

Therefore, N can be uniquely reconstructed by

$$N = MQ + r^c. \tag{13}$$

Similar to the reconstruction of one integer, the common remainders are significant to the reconstruction of $\{N_1, N_2\}$ from the residue sets $R_k(N_1, N_2)$ with modulus set $\mathcal{M}$. First, from the residue sets, obtain the two common remainders modulo all the remainders by M.

Let $\{r_1^c, r_2^c\}$ be the two common remainders. When the two common remainders are not equal, i.e., $r_1^c \neq r_2^c$, we have $R_k(N_1, N_2) = \{r_{1,k}, r_{2,k}\}$ with $r_{1,k} \neq r_{2,k}$. Note that

$$\{r_1^c, r_2^c\} = \{\langle r_{1,k}\rangle_M, \langle r_{2,k}\rangle_M\}$$

holds for each $k \in \{1, \ldots, K\}$. On the other hand,

$$\{r_1^c, r_2^c\} = \{\langle N_1\rangle_M, \langle N_2\rangle_M\}.$$

Hence, all the remainders in $R_k(N_1, N_2)$ can be split into two sets, $\{r_{1,1}, \ldots, r_{1,K}\}$ and $\{r_{2,1}, \ldots, r_{2,K}\}$, according to r_1^c and r_2^c. Using the traditional CRT, N_1 and N_2 can be uniquely determined by their remainders $\{r_{1,1}, \ldots, r_{1,K}\}$ and $\{r_{2,1}, \ldots, r_{2,K}\}$, respectively. This also means that $\{N_1, N_2\}$ can be uniquely determined if and only if $0 \leq N_1, N_2 < M\Gamma$.

When the two common remainders are the same, i.e., $r_1^c = r_2^c = r^c$, we let

$$q_{l,k} = \frac{r_{l,k} - r^c}{M}, \ \ l = 1, 2; \ \ k = 1, \ldots, K.$$

Then, (8) is equivalent to

$$q_{l,k} \equiv \frac{N_l - r^c}{M} \bmod m_k. \tag{14}$$

Denote $R_k(Q_1, Q_2) = \{q_{1,k}, q_{2,k}\}$ for $k = 1, \ldots, K$, where $Q_l = (N_l - r^c)/M$ for $l = 1, 2$. Since $N_l < Md$, we have $Q_l < d$. By the definition of dynamic range, we know that $\{Q_1, Q_2\}$ can be uniquely determined by their residue sets $R_k(Q_1, Q_2)$. Consequently, $\{N_1, N_2\}$ can be uniquely reconstructed by using (13).

In summary, we have the following corollary.

Corollary 1: Assume that $m_1 \geq 3$ and $K > 2$. Let $\{r_1^c, r_2^c\}$ be the common remainders defined as above. Then we have the following results. 1) If $r_1^c \neq r_2^c$ and $0 \leq N_1, N_2 < M\Gamma$, then $\{N_1, N_2\}$ can be uniquely determined from the above algorithm; 2) If $r_1^c = r_2^c$ and $0 \leq N_1, N_2 < Md$, then $\{N_1, N_2\}$ can be uniquely determined from the above algorithm.

Example 1: Let $M = 100, \mathcal{M}' = \{3, 5, 7\}$. According to the above discussion, we know that $D_2(\mathcal{M}) = 2200$.

Suppose that the residue sets are $R_1(N_1, N_2) = \{69, 195\}$, $R_2(N_1, N_2) = \{95, 169\}$, and $R_3(N_1, N_2) = \{69, 395\}$. Then the two common remainders are $\{r_1^c, r_2^c\} = \{69, 95\}$. Hence, the remainder in the residue sequences can be split into $\{69, 169, 69\}$ and $\{195, 95, 395\}$ corresponding to $r_1^c = 69$ and $r_2^c = 95$, respectively. By using the traditional CRT, we have $\{N_1, N_2\} = \{2169, 1095\}$.

Example 2: Consider the example above. Suppose that the residue sets are $R_1(N_1, N_2) = \{98, 198\}$, $R_2(N_1, N_2) = \{98, 398\}$, and $R_3(N_1, N_2) = \{398, 498\}$ modulo 300, 500, and 700, respectively. In this case, the two common remainders are the same: $r_1^c = r_2^c = 98$. By (11), we have $R_1(Q_1, Q_2) = \{0, 1\}$, $R_2(Q_1, Q_2) = \{0, 3\}$, $R_3(Q_1, Q_2) = \{3, 4\}$ modulo 3, 5, and 7, respectively. By using the reconstruction algorithm obtained in [13], we have $\{Q_1, Q_2\} = \{10, 18\}$. By (13), we can reconstruct the two integers $\{N_1, N_2\}$ as $\{1098, 1898\}$.

IV. A Robust Generalized CRT for Two Integers

In this section, we discuss a robust generalized CRT for two integers when the residue sets have errors.

A. Remainders With Errors

As discussed above, the two common remainders, $\{r_1^c, r_2^c\}$, are the key of the reconstruction of integers $\{N_1, N_2\}$. When remainders are error-free, the two common remainders can be directly determined by any residue set of $\{N_1, N_2\}$. However, this may not be true when residue sets have errors. Take Example 2 for example. Suppose that the erroneous residue sets are $\tilde{R}_1(N_1, N_2) = \{108, 209\}$, $\tilde{R}_2(N_1, N_2) = \{92, 399\}$, and $\tilde{R}_3(N_1, N_2) = \{397, 507\}$. Then the residue sets modulo M are $\{8, 9\}$, $\{92, 99\}$, and $\{7, 97\}$, respectively. Clearly, the erroneous residue sets $\tilde{R}_k(N_1, N_2)$ modulo M are different from each other and we can not directly determine the common remainders $\{r_1^c, r_2^c\}$ from $\tilde{R}_k(N_1, N_2)$.

Let $\tilde{r}_{l,k}^c$ be the remainder of $\tilde{r}_{l,k}$ modulo M, i.e.,

$$\tilde{r}_{l,k}^c = \langle \tilde{r}_{l,k} \rangle_M, \ l = 1, 2; \ k = 1, \ldots, K. \tag{15}$$

In case $\tilde{S}_k(N_1, N_2)$ has only one element, i.e., $\tilde{r}_{1,k} = \tilde{r}_{2,k}$, we have $\tilde{r}_{1,k}^c = \tilde{r}_{2,k}^c$ counted twice (repeated once) in the above sequence. This provides total $2K$ common remainders and some of them may be the same. In order to estimate two common remainders from these $2K$ common remainders $\tilde{r}_{1,1}^c, \ldots, \tilde{r}_{1,K}^c$, $\tilde{r}_{2,1}^c, \ldots, \tilde{r}_{2,K}^c$, two appropriate clusters, each of which contains K remainders, are formed first. Intuitively the deviation of two clusters should be large. Now, we determine two clusters from these erroneous residue sets. For convenience, we denote these $2K$ common remainders as $\tilde{r}_1^c, \ldots, \tilde{r}_{2K}^c$, and then sort them in the increasing order as follows

$$\tilde{r}_{\varsigma(1)}^c \leq \cdots \leq \tilde{r}_{\varsigma(2K)}^c \tag{16}$$

where ς is a permutation of the set $\{1, \ldots, 2K\}$.

For any two adjacent common remainders $\tilde{r}_{\varsigma(k)}^c$ and $\tilde{r}_{\varsigma(k+1)}^c$, we define the distance D_k as

$$D_k = \begin{cases} \tilde{r}_{\varsigma(k+1)}^c - \tilde{r}_{\varsigma(k)}^c, & \text{if } k = 1, \ldots, 2K-1 \\ \tilde{r}_{\varsigma(1)}^c - \tilde{r}_{\varsigma(2K)}^c + M, & \text{if } k = 2K. \end{cases} \tag{17}$$

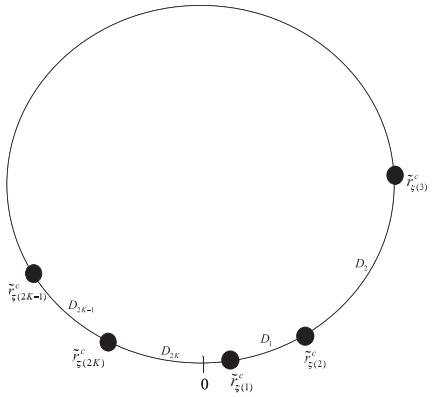

Fig. 1. Illustration of D_k.

Fig. 1 gives the illustration of the defined distance D_k. It is clear that the nonnegative distances D_k satisfy the following equation

$$\sum_{k=1}^{2K} D_k = M. \tag{18}$$

Moreover, we have the following results.

Lemma 2: Let $\tau = \max\left\{\left|\Delta r_{l,k}\right|, l = 1, 2; \ k = 1, \ldots, K\right\}$, where $\Delta r_{l,k}$ are the remainder errors as defined in (5). If $\tau < M/8$, then there exists one and only one subscript $k_0 \in \{1, \ldots, K\}$ satisfies

$$D_{k_0} + D_{k_0+K} > M/2. \tag{19}$$

Moreover, if we let

$$\begin{aligned} \Omega_1 &\triangleq \{\omega_1, \ldots, \omega_K\} = \left\{\tilde{r}_{\varsigma(k_0+1)}^c, \ldots, \tilde{r}_{\varsigma(k_0+K)}^c\right\}, \\ \Omega_2 &\triangleq \{v_1, \ldots, v_K\} \\ &= \begin{cases} \{\tilde{r}_{\varsigma(1)}^c, \ldots, \tilde{r}_{\varsigma(K)}^c\}, & \text{if } k_0 = K \\ \{\tilde{r}_{\varsigma(k_0+1+K)}^c - M, \ldots, \tilde{r}_{\varsigma(2K)}^c \\ \quad - M, \tilde{r}_{\varsigma(1)}^c, \ldots, \tilde{r}_{\varsigma(k_0)}^c\}, & \text{if } k_0 \neq K \end{cases} \end{aligned} \tag{20}$$

with $\omega_i \leq \omega_j$, $v_i \leq v_j$ for $1 \leq i < j \leq K$, then

$$\omega_K - \omega_1 \leq 2\tau, \ v_K - v_1 \leq 2\tau. \tag{21}$$

This Lemma is proved in Appendix A.

Example 3: Let us consider the example proposed at the beginning of this section. By (16), we obtain the remainder sequence $\{\tilde{r}_1^c, \ldots, \tilde{r}_{2K}^c\} = \{8, 9, 92, 99, 97, 7\}$ and its sorted sequence $\{\tilde{r}_{\varsigma(1)}^c, \ldots, \tilde{r}_{\varsigma(2K)}^c\}$ in (16) as

$$0 < 7 < 8 < 9 < 92 < 97 < 99 < M = 100.$$

Since $D_3 + D_6 = (92 - 9) + (7 - 99 + 100) = 83 + 8 > M/2$, we know that $k_0 = 3$ and obtain from (20) that the two clusters are

$$\Omega_1 = \{92, 97, 99\}, \ \Omega_2 = \{7, 8, 9\}. \tag{22}$$

Fig. 2(a) and (b) show the sketches of two clusters Ω_1 and Ω_2 when the two common remainders satisfy

$$0 \leq \left|d_M(r_1^c, r_2^c)\right| < M/4 \tag{23}$$

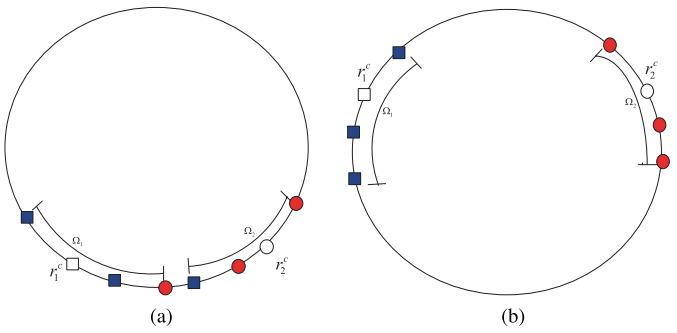

Fig. 2. (a) Two common remainders satisfy (23); (b) Two common remainders satisfy (24).

and

$$M/4 \le \left|d_M(r_1^c, r_2^c)\right| \le M/2 \tag{24}$$

respectively. In the figures, the remainder error bound is τ, and the common remainders of r_1^c (or N_1) and r_2^c (or N_2) are denoted by "□" and "◯", respectively. In the case of (23), two clusters $\mathbf{\Omega}_1$ and $\mathbf{\Omega}_2$ may not be properly grouped from the sequence $\left\{\tilde{r}^c_{\varsigma(1)}, \ldots, \tilde{r}^c_{\varsigma(2K)}\right\}$, as shown in Fig. 2(a). To be specific, both of $\mathbf{\Omega}_1$ and $\mathbf{\Omega}_2$ may contain erroneous common remainders of r_1^c and r_2^c. In the case of (24), two clusters $\mathbf{\Omega}_1$ and $\mathbf{\Omega}_2$ can be grouped without any overlaps from the sequence, as shown in Fig. 2(b).

Before reconstructing $\{N_1, N_2\}$, we introduce a kind of circular distance below.

Definition 2: For real numbers x and y, the circular distance of x to y for a non-zero positive number C is defined as

$$d_C(x, y) \triangleq x - y - \left[\frac{x-y}{C}\right]C \tag{25}$$

where $[\cdot]$ stands for the rounding integer, i.e., for any $x \in \mathbb{R}$, where $\mathbb{R}$ denotes the set of all reals, $[x]$ is an integer and subject to

$$-1/2 \le x - [x] < 1/2. \tag{26}$$

The main processes of determining two integers $\{N_1, N_2\}$ are divided into three steps. Firstly, estimate two common remainders $\{r_1^c, r_2^c\}$ from the obtained two clusters $\mathbf{\Omega}_1$ and $\mathbf{\Omega}_2$. Then reconstruct two integers $\{Q_1, Q_2\}$ after the residue sets $\{q_{1,k}, q_{2,k}\}$ are properly determined. Finally, reconstruct two integers $\{N_1, N_2\}$ by using the traditional CRT after two common remainders are modified.

Let

$$\omega_k' = \begin{cases} \omega_k, & \text{if } \omega_K - \upsilon_1 \le M/2 \\ \omega_k - M, & \text{if } \omega_K - \upsilon_1 > M/2 \end{cases} \tag{27}$$

for all $k = 1, \ldots, K$. Then, the two common remainders $\left\{r_1^c, r_2^c\right\}$ can be estimated as $\{\overline{\omega}_1, \overline{\omega}_2\}$:

$$\overline{\omega}_1 \triangleq \frac{\omega_1' + \cdots + \omega_K'}{K}, \quad \overline{\omega}_2 \triangleq \frac{\upsilon_1 + \cdots + \upsilon_K}{K}. \tag{28}$$

Note that $\overline{\omega}_1$ and $\overline{\omega}_2$ defined in (28) may be negative values. After cancelling the appropriate estimate of common remainder from the erroneous remainders $\tilde{r}_{l,k}$, we can obtain the estimates of integers $q_{l,k}$ in (14), denoted as $\hat{q}_{l,k}$:

$$\hat{q}_{l,k} = \left[\frac{\tilde{r}_{l,k} - \overline{\omega}_t}{M}\right], \ l = 1, 2; \ k = 1, \ldots, K \tag{29}$$

where

$$t = \begin{cases} 1, & \text{if } d_M(\tilde{r}^c_{l,k}, \omega_{k_1}) = 0 \text{ for some } k_1 \\ 2, & \text{if } d_M(\tilde{r}^c_{l,k}, \upsilon_{k_2}) = 0 \text{ for some } k_2 \end{cases} \tag{30}$$

with $k_1, k_2 \in \{1, \ldots, K\}$. Let

$$R_k(\hat{Q}_1, \hat{Q}_2) = \left\{\hat{q}_{1,k}, \hat{q}_{2,k}\right\}, \ k = 1, \ldots, K. \tag{31}$$

Then the two estimates $\{\hat{Q}_1, \hat{Q}_2\}$ of the integers $\{Q_1, Q_2\}$ can be reconstructed from the residue sets $R_k(\hat{Q}_1, \hat{Q}_2)$ modulo $\mathcal{M}'$ by using the generalized CRT for two integers obtained in [13].

Example 4: Let us consider Example 3. Since $\omega_3 - \upsilon_1 = 99 - 7 = 92 > M/2$, we obtain

$$\omega_1' = -8, \ \omega_2' = -3, \ \omega_3' = -1.$$

Recall that $\upsilon_1 = 7$, $\upsilon_2 = 8$, and $\upsilon_3 = 9$. According to the definitions of $\overline{\omega}_1$ and $\overline{\omega}_2$ in (28), we have

$$\overline{\omega}_1 = -4, \ \overline{\omega}_2 = 8.$$

By (29) and (31), we obtain $R_1(\hat{Q}_1, \hat{Q}_2) = \{1, 2\}$, $R_2(\hat{Q}_1, \hat{Q}_2) = \{1, 4\}$, and $R_3(\hat{Q}_1, \hat{Q}_2) = \{4, 5\}$. By using the generalized CRT for two integers obtained in [13], we have

$$\{\hat{Q}_1, \hat{Q}_2\} = \{11, 19\}.$$

Now, we estimate the two integers $\{N_1, N_2\}$ after the estimates $\{\overline{\omega}_1, \overline{\omega}_2\}$ of the two common remainders and $\{\hat{Q}_1, \hat{Q}_2\}$ are obtained. The estimates of $\{N_1, N_2\}$ are denoted as $\{\hat{N}_1, \hat{N}_2\}$ in the following.

1) $\hat{Q}_1 = \hat{Q}_2 = \hat{Q}$.

In this case, the estimates $\{\hat{N}_1, \hat{N}_2\}$ can be reconstructed as

$$\left\{\hat{N}_1, \hat{N}_2\right\} = \left\{M\hat{Q} + \overline{\omega}_1, M\hat{Q} + \overline{\omega}_2\right\}. \tag{32}$$

2) $\hat{Q}_1 \ne \hat{Q}_2$.

In this case, we can not determine $\{\hat{N}_1, \hat{N}_2\}$ from $\{\overline{\omega}_1, \overline{\omega}_2\}$ and $\{\hat{Q}_1, \hat{Q}_2\}$, which is because the correspondence between the elements in two sets $\{\overline{\omega}_1, \overline{\omega}_2\}$ and $\{\hat{Q}_1, \hat{Q}_2\}$ is not known. To be specific, we cannot determine whether $\{\hat{N}_1, \hat{N}_2\}$ are $\{M\hat{Q}_1 + \overline{\omega}_1, M\hat{Q}_2 + \overline{\omega}_2\}$ or $\{M\hat{Q}_1 + \overline{\omega}_2, M\hat{Q}_2 + \overline{\omega}_1\}$. Next, we modify the two estimates $\{\overline{\omega}_1, \overline{\omega}_2\}$ of the common remainders $\{r_1^c, r_2^c\}$ so that the modified estimates $\hat{r}_1^c$ and $\hat{r}_2^c$ correspond to $\hat{Q}_1$ and $\hat{Q}_2$, respectively. The main processes are two: Firstly, we select the elements from $\{\omega_1', \ldots, \omega_K'\}$ and $\{\upsilon_1, \ldots, \upsilon_K\}$ to form two groups, where all the elements in one group correspond to $\hat{Q}_1$ and the other correspond to $\hat{Q}_2$. Then, $\hat{r}_1^c$ and $\hat{r}_2^c$ are determined by averaging the groups corresponding to $\hat{Q}_1$ and $\hat{Q}_2$, respectively.

Let

$$\mathbf{\Omega}' \triangleq \left\{\omega_1', \ldots, \omega_K', \upsilon_1, \ldots, \upsilon_K\right\}. \tag{33}$$

By (20) and (27), we know that the elements in $\mathbf{\Omega}'$ are either $\tilde{r}^c_{\varsigma(i)}$ or $\tilde{r}^c_{\varsigma(i)} - M$ for all $i = 1, \ldots, 2K$. From the definitions of $\tilde{r}^c_{\varsigma(i)}$ in (16), we know that $\{\tilde{r}^c_{\varsigma(1)}, \ldots, \tilde{r}^c_{\varsigma(2K)}\}$ are the $2K$ sorted common remainders

from $\{\tilde{r}^c_{1,1},\ldots,\tilde{r}^c_{1,K},\tilde{r}^c_{2,1},\ldots,\tilde{r}^c_{2,K}\}$. Hence, for all $l=1,2$; $k=1,\ldots,K$, either $\tilde{r}^c_{l,k}$ or $\tilde{r}^c_{l,k}-M$ is included in Ω', and in the meanwhile, Ω' only consists of these $2K$ elements. In the following, for convenience, we call both $\tilde{r}^c_{l,k}$ and $\tilde{r}^c_{l,k}-M$ as the common remainders of $\tilde{r}_{l,k}$.

When $\hat{Q}_1\neq\hat{Q}_2$, we know from the traditional CRT that there exists at least a subscript $k\in\{1,\ldots,K\}$ such that

$$\hat{q}_{1,k}\neq\hat{q}_{2,k}. \tag{34}$$

Let

$$\mathcal{K}\triangleq\{k_1,\ldots,k_\ell\},\ 1\le k_i\le K$$

be all the distinct subscripts of $\hat{q}_{1,k_i}$ (or $\hat{q}_{2,k_i}$) satisfying (34), i.e., $\hat{q}_{1,k_i}\neq\hat{q}_{2,k_i}$, and thus from (34), we have $\ell\ge 1$. When $\hat{q}_{1,k_i}\neq\hat{q}_{2,k_i}$, the correspondence between $\{\hat{q}_{1,k_i},\hat{q}_{2,k_i}\}$ and $\{\hat{Q}_1,\hat{Q}_2\}$ is known because we can determine $\hat{q}_{l,k_i}$ by the obtained integers $\hat{Q}_l$ modulo m_{k_i}, i.e.,

$$\hat{q}_{l,k_i}=\left\langle\hat{Q}_l\right\rangle_{m_{k_i}},\quad l=1,2 \tag{35}$$

for every i, $1\le i\le\ell$. Note that the obtained values $\hat{q}_{1,k_i}$ and $\hat{q}_{2,k_i}$ above are the same the values as determined by (29) from the residue set $\{\tilde{r}_{1,k_i},\tilde{r}_{2,k_i}\}$. Since $\hat{q}_{1,k_i}\neq\hat{q}_{2,k_i}$, we have $\tilde{r}_{1,k_i}\neq\tilde{r}_{2,k_i}$. Thus, the correspondence between $\{\hat{q}_{1,k_i},\hat{q}_{2,k_i}\}$ and $\{\tilde{r}_{1,k_i},\tilde{r}_{2,k_i}\}$ (or $\{\hat{Q}_1,\hat{Q}_2\}$) is known as well, which can be uniquely determined by (29). Assume that the common remainders of $\tilde{r}_{1,k_i}$ and $\tilde{r}_{2,k_i}$ in Ω' are $\hat{r}^c_{1,k_i}$ and $\hat{r}^c_{2,k_i}$, respectively. As discussed above, $\hat{r}^c_{1,k_i}$ are either $\tilde{r}^c_{1,k_i}$ or $\tilde{r}^c_{1,k_i}-M$, and $\hat{r}^c_{2,k_i}$ are either $\tilde{r}^c_{2,k_i}$ or $\tilde{r}^c_{2,k_i}-M$. Thus, $\hat{r}^c_{1,k_i},\hat{r}^c_{2,k_i}\in\Omega'$ can be determined by

$$d_M(\tilde{r}^c_{1,k_i},\hat{r}^c_{1,k_i})=0, d_M(\tilde{r}^c_{2,k_i},\hat{r}^c_{2,k_i})=0 \tag{36}$$

where $k_i\in\mathcal{K}$. By (15), we know that $\hat{r}^c_{1,k_i}$ and $\hat{r}^c_{2,k_i}$ can also be determined by

$$d_M(\tilde{r}_{1,k_i},\hat{r}^c_{1,k_i})=0, d_M(\tilde{r}_{2,k_i},\hat{r}^c_{2,k_i})=0. \tag{37}$$

Clearly, $\hat{r}^c_{1,k_i}$ and $\hat{r}^c_{2,k_i}$ correspond to the remainders $\tilde{r}_{1,k_i}$ and $\tilde{r}_{2,k_i}$, respectively. Hence, $\hat{r}^c_{1,k_i}$ corresponds to $\hat{Q}_1$, while $\hat{r}^c_{2,k_i}$ corresponds to $\hat{Q}_2$. In other words, $\{\hat{r}^c_{1,k_1},\ldots,\hat{r}^c_{1,k_\ell}\}$ and $\{\hat{r}^c_{2,k_1},\ldots,\hat{r}^c_{2,k_\ell}\}$ correspond to the common remainders r^c_1 and r^c_2, respectively. Under the least square estimate criterion, the two common remainders can be modified as

$$\begin{aligned}\hat{r}^c_1&\triangleq\arg\min_{x\in[c_1,c_2]}\sum_{i=1}^{\ell}\|x-\hat{r}^c_{1,k_i}\|^2,\\ \hat{r}^c_2&\triangleq\arg\min_{x\in[c_3,c_4]}\sum_{i=1}^{\ell}\|x-\hat{r}^c_{2,k_i}\|^2\end{aligned} \tag{38}$$

where the variable x takes integer values, and

$$\begin{aligned}c_1=\min\{\hat{r}^c_{1,k_1},\ldots,\hat{r}^c_{1,k_\ell}\}, c_2=\max\{\hat{r}^c_{1,k_1},\ldots,\hat{r}^c_{1,k_\ell}\},\\ c_3=\min\{\hat{r}^c_{2,k_1},\ldots,\hat{r}^c_{2,k_\ell}\}, c_4=\max\{\hat{r}^c_{2,k_1},\ldots,\hat{r}^c_{2,k_\ell}\}.\end{aligned}$$

Therefore, the estimates $\{\hat{N}_1,\hat{N}_2\}$ can be reconstructed as

$$\left\{\hat{N}_1,\hat{N}_2\right\}=\left\{M\hat{Q}_1+\hat{r}^c_1,M\hat{Q}_2+\hat{r}^c_2\right\}. \tag{39}$$

Noting that the estimates $\{\hat{N}_1,\hat{N}_2\}$ obtained by (32) or (39) may be non-integers. For this case, we use $\left\{[\hat{N}_1],[\hat{N}_2]\right\}$ as the estimates of the integers $\{N_1,N_2\}$, where $[\cdot]$ denotes the rounding operation defined in (26).

Example 5: Let us consider Example 4. Note that $\{\hat{Q}_1,\hat{Q}_2\}=\{11,19\}$ calculated before. Then the remainders of $\hat{Q}_1=11$ and $\hat{Q}_2=19$ modulo $\mathcal{M}'$ are $\{\hat{q}_{1,1},\hat{q}_{1,2},\hat{q}_{1,3}\}=\{2,1,4\}$ and $\{\hat{q}_{2,1},\hat{q}_{2,2},\hat{q}_{2,3}\}=\{1,4,5\}$, respectively. Clearly, $\hat{q}_{1,k}\neq\hat{q}_{2,k}$, for $k=1,2,3$. According to (29), we deduce that

$$\begin{aligned}\{\tilde{r}_{1,1},\tilde{r}_{1,2},\tilde{r}_{1,3}\}=\{209,92,397\},\\ \{\tilde{r}_{2,1},\tilde{r}_{2,2},\tilde{r}_{2,3}\}=\{108,399,507\}.\end{aligned}$$

By (33), we have

$$\Omega'=\{\omega'_1,\omega'_2,\omega'_3,v_1,v_2,v_3\}=\{-8,-3,-1,7,8,9\}.$$

Since $d_M(\tilde{r}_{1,1},9)=0$, $d_M(\tilde{r}_{1,2},-8)=0$, $d_M(\tilde{r}_{1,3},-3)=0$, we obtain from (37) that

$$\hat{r}^c_{1,1}=9,\ \hat{r}^c_{1,2}=-8,\ \hat{r}^c_{1,3}=-3.$$

By (38), we can obtain the estimate

$$\hat{r}^c_1=-1.$$

Similarly, we have

$$d_M(\tilde{r}_{2,1},8)=0,\ d_M(\tilde{r}_{2,2},-1)=0,\ d_M(\tilde{r}_{2,3},7)=0.$$

Hence,

$$\hat{r}^c_{2,1}=8,\ \hat{r}^c_{2,2}=-1,\ \hat{r}^c_{2,3}=7$$

and then we obtain $\hat{r}^c_2=5$. By (39), we have

$$\left\{\hat{N}_1,\hat{N}_2\right\}=\{1099,1905\}.$$

Next theorem shows that the above estimates $\left\{\hat{N}_1,\hat{N}_2\right\}$ of the two integers $\{N_1,N_2\}$ are robust when the remainder error bound is less than $M/8$.

Theorem 2: Let $\tau=\max\{|\Delta r_{l,k}|,l=1,2;k=1,\ldots,K\}$, where $\Delta r_{l,k}$ are the remainder errors as defined in (5). If $\tau<M/8$, then

$$\left|\hat{N}_l-N_l\right|\le\tau,\ l=1,2 \tag{40}$$

where $\left\{\hat{N}_1,\hat{N}_2\right\}$ are defined in (32) or (39).

The proof of this theorem can be divided into three steps. First, obtain the two estimates $\overline{\omega}_1$ and $\overline{\omega}_2$ from the given residue sets $\{\tilde{r}_{1,1},\tilde{r}_{2,1}\},\ldots,\{\tilde{r}_{1,K},\tilde{r}_{2,K}\}$. Then check the two integers $\{\hat{Q}_1,\hat{Q}_2\}$, where the two integers are determined by solving the quadratic equation that is obtained by the residue sets $\{\hat{q}_{1,1},\hat{q}_{2,1}\},\ldots,\{\hat{q}_{1,K},\hat{q}_{2,K}\}$. Finally, check the reconstructions $\{\hat{N}_1,\hat{N}_2\}$ after the estimates $\{\hat{r}^c_1,\hat{r}^c_2\}$ and $\{\hat{Q}_1,\hat{Q}_2\}$ are properly corresponded. More details can be seen Appendix B.

Let us recall the example presented at the beginning of this section. Note that the remainder error bound $\tau=11$, which is less than the robustness error upper bound $M/8=12.5$. By Theorem 2, we know that the estimates are robust. In fact, the true values of the two integers are $\{1098,1898\}$ and the estimates are $\{1099,1905\}$. Hence, the maximal estimation error of the two integers is 7, which is small than the remainder error bound τ and conforms the result obtained in Theorem 2.

Algorithm 1 Robust Generalized CRT for Two Integers

Step 1 Calculate $\tilde{r}_{l,k}^{c}$ in (15) and sort them in the increasing order as (16).

Step 2 Compute k_0 as

$$k_0 = \arg \max_{k\in\{1,\ldots,K\}} \left\{D_k + D_{k+K}\right\} \tag{41}$$

where D_k is defined in (17).

Step 3 Obtain the two clusters Ω_1 and Ω_2 by (20).

Step 4 Calculate $\overline{\omega}_1$ and $\overline{\omega}_2$ by (28).

Step 5 Determine residue sets $R_k(\hat{Q}_1, \hat{Q}_2)$ as

$$R_k\left(\hat{Q}_1, \hat{Q}_2\right) = \left\{\hat{q}_{1,k}, \hat{q}_{2,k}\right\} \tag{42}$$

where $\hat{q}_{l,k}$ are defined in (29).

Step 6 Reconstruct $\{\hat{Q}_1, \hat{Q}_2\}$ by using the generalized CRT for two integers obtained in [13].

Step 7 Reconstruct $\left\{\hat{N}_1, \hat{N}_2\right\}$ by (32) or (39).

B. Robust Generalized CRT Algorithm for Two Integers

To summarize what we have studied before, we obtain Algorithm 1.

Although the above robust generalized CRT is for two integers, it is straightforward to be generalized to two reals as the case of one integer in our previous work [36], [37].

V. Simulation Results

In this section, we show some simulations to illustrate the performance of the proposed robust generalized CRT for two integers and its application in two frequency determination from multiple undersampled waveforms.

A. Simulation of the Robust Generalized CRT

Let us first consider the estimation error versus the error upper bound for the proposed robust generalized CRT for two integers. By Theorem 2, we know that the maximal error level τ needs to be upper bounded by $\tau < M/8$ for the robustness. In the simulation, parameter $M = 100$, and the co-prime integers from m_1 to m_3 are 3, 5, and 7, respectively. Two unknown integers $\{N_1, N_2\}$ are chosen uniformly at random from the interval $(0, 2000)$ and the maximal error levels are set as $0, 1, \ldots, 15$. For these maximal error levels, the last three parameters, 13, 14, and 15, do not satisfy the robustness upper bound $\tau < M/8 = 12.5$. We call the process of determining $\{N_1, N_2\}$ as a trial, and 10000 trials for each of the maximal error level are simulated. In Fig. 3, we present the curve of the mean error E_N versus the maximal error level. The mean error is defined as

$$E_N = E_{trials}\left\{\frac{1}{2}\sum_{l=1}^{2}|\hat{N}_l - N_l|\right\} \tag{43}$$

where E_{trials} stands for the mean over all the trials, N_l and $\hat{N}_l$ are the true integers and the estimates in one trial, respectively. Fig. 3 shows that the two integers can be robustly reconstructed from their erroneous residue sets by using the proposed robust generalized CRT method,

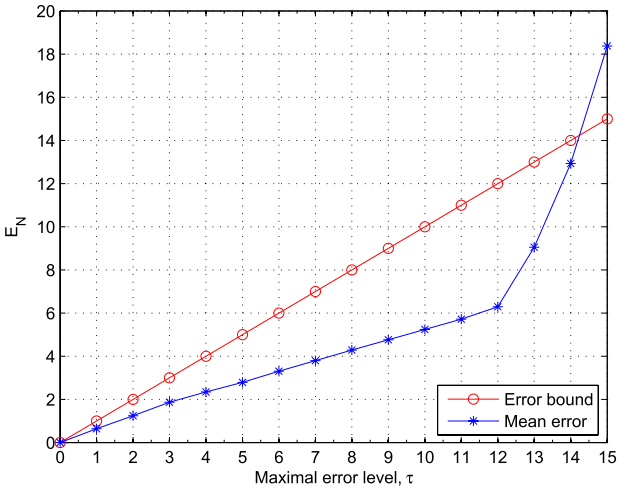

Fig. 3. Estimation errors versus the maximal error level.

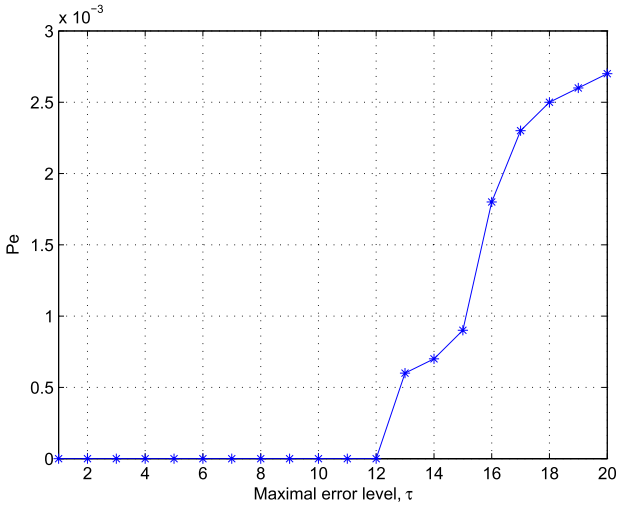

Fig. 4. Probability P_e versus the maximal error level.

i.e., when all the errors of the remainders are less than the error upper bound, the reconstruction errors of $\{N_1, N_2\}$ are also less than this bound. It also shows that the reconstruction errors of the two integers are small compared to their dynamic range. When the remainder errors are larger than the upper bound, the reconstruction errors increase rapidly.

In Fig. 4, we give the curve of the probability P_e versus the remainder error bound τ, where

$$P_e = P\left(\max\{\Delta N_l\} > \max\{\Delta r_{l,k}\} \middle| |\Delta r_{l,k}| \le \tau\right). \tag{44}$$

It shows that the probability is zero when the error bound $\tau < 13$ is satisfied and non-zero when $\tau \ge 13$, i.e., the error bound is not satisfied. In other words, the reconstruction is not robust when the remainder errors are larger than the error upper bound $M/8$, which agrees with Theorem 2. It also shows that the probability increases with the increase of τ, i.e., the larger remainder errors, the higher probability P_e or the worse estimation performance.

B. Two-Frequency Determination From Multiple Undersampled Waveforms

In the simulations, two frequencies $\{f_1, f_2\}$ are taken randomly and uniformly distributed in the range $(0, 2000)$, and three sampling frequencies are set to be 300, 500, and 700. The noise $w(t)$ in (1) is additive white Gaussian noise with mean zero and variance $10^{-SNR/10}$, and the observation of the time duration is 10s. For each signal-to-noise ratio (SNR), the number of trials is 10000. Beyond the proposed robust generalized CRT, three other methods are considered: the generalized CRT proposed in Section III, the robust CRT based method, and the (optimal) searching based method.

For the generalized CRT, we choose the average of the common remainders by using an arbitrary grouping. After cancelling the common remainders from the erroneous remainders, the two integers are reconstructed by using the generalized CRT for two integers proposed in [13].

For the robust CRT based method, we consider all possible remainder combinations of $\{f_1, f_2\}$ from their residue sets. Note that the remainders in each residue set are unordered, we have four cases, i.e.,

$$\begin{aligned}
&\left\{\{\tilde{r}_{1,1}, \tilde{r}_{1,2}, \tilde{r}_{1,3}\}, \{\tilde{r}_{2,1}, \tilde{r}_{2,2}, \tilde{r}_{2,3}\}\right\};\\
&\left\{\{\tilde{r}_{1,1}, \tilde{r}_{2,2}, \tilde{r}_{1,3}\}, \{\tilde{r}_{1,1}, \tilde{r}_{1,2}, \tilde{r}_{2,3}\}\right\};\\
&\left\{\{\tilde{r}_{1,1}, \tilde{r}_{1,2}, \tilde{r}_{2,3}\}, \{\tilde{r}_{2,1}, \tilde{r}_{2,2}, \tilde{r}_{1,3}\}\right\};\\
&\left\{\{\tilde{r}_{1,1}, \tilde{r}_{2,2}, \tilde{r}_{2,3}\}, \{\tilde{r}_{2,1}, \tilde{r}_{1,2}, \tilde{r}_{1,3}\}\right\}. \qquad (45)
\end{aligned}$$

For each case, we estimate f_1 and f_2 by using the fast MLE algorithm proposed in [37]. Take the first case as an example, f_1 and f_2 can be determined by $\{\tilde{r}_{1,1}, \tilde{r}_{1,2}, \tilde{r}_{1,3}\}$ and $\{\tilde{r}_{2,1}, \tilde{r}_{2,2}, \tilde{r}_{2,3}\}$ modulo M_1, M_2, M_3, respectively. If both of the two estimates $\{\hat{f}_1, \hat{f}_2\}$ are within the dynamic range, then they can be viewed as the estimates of $\{f_1, f_2\}$.

For the searching based method, the two frequencies $\{f_1, f_2\}$ are determined by solving the four minimization problems, which correspond to the four cases in (45). Take the first case as an example, $\{f_1, f_2\}$ can be determined by solving the following minimization problem:

$$\begin{aligned}
\min_{f_1, f_2} \Big\{ & d^2_{M_1}(f_1, \tilde{r}_{1,1}) + d^2_{M_2}(f_1, \tilde{r}_{1,2}) + d^2_{M_3}(f_1, \tilde{r}_{1,3})\\
& + d^2_{M_1}(f_2, \tilde{r}_{2,1}) + d^2_{M_2}(f_2, \tilde{r}_{2,2}) + d^2_{M_3}(f_2, \tilde{r}_{2,3}) \Big\} \qquad (46)
\end{aligned}$$

where f_1 and f_2 take integer values. The minimum value of (46) is denoted as S_1. Similarly, for the other three cases in (45), we can obtain the minimum values S_2, S_3, S_4, respectively. Hence, the optimal estimates of $\{f_1, f_2\}$ are the frequencies that correspond to the minimum of $\{S_1, \ldots, S_4\}$.

Now, we compare the different methods by investigating the root mean square error (RMSE) and the test fail rate (TFR). The RMSE is defined as

$$f_{RMSE} = \sqrt{E\left\{\frac{1}{2}\sum_{l=1}^{2}(\hat{f}_l - f_l)^2\right\}} \qquad (47)$$

where f_l and $\hat{f}_l$ are the true frequencies and the estimates in one trial, respectively. In each trail, if the estimation errors of the two frequencies are no larger than the given positive number τ, i.e.,

$$|\hat{f}_l - f_l| \le \tau, \ l = 1, 2$$

we say that the test is successful, otherwise, the test is failed. In the simulations, we set $\tau = 12.5$.

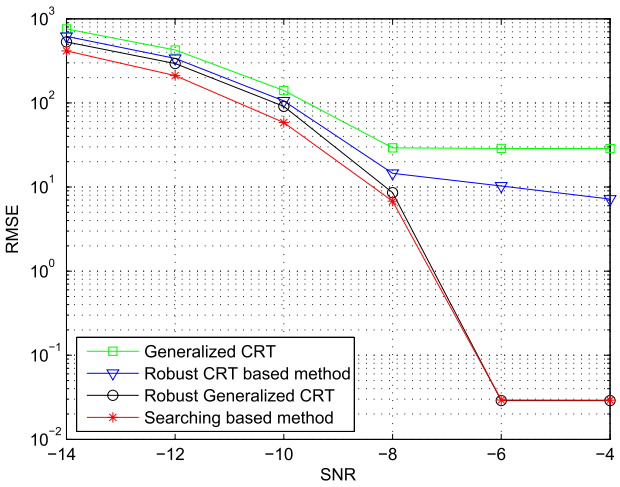

Fig. 5. RMSE versus SNR.

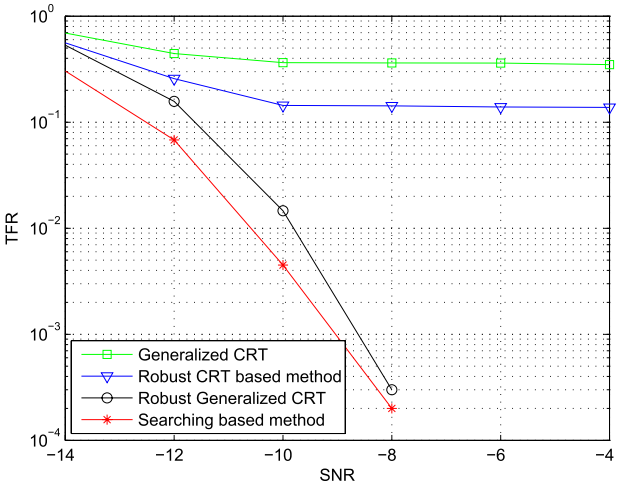

Fig. 6. TFR versus SNR.

From Figs. 5 and 6, one can see that the error floors of the generalized CRT and the robust CRT based method are high, i.e., the RMSE or the TFR will not decrease or decrease very slowly at high SNR. On the contrary, the RMSE or the TFR of the robust generalized CRT and the searching based method decreases sharply as SNR, while there are also error floors at high SNR. The reason for the error floors at high SNR for the robust generalized CRT and the searching based method is because a finite size FFT has a limited resolution in frequency domain and it causes remainder errors and results in error floors at high SNR. Compared with the generalized CRT method, the robust generalized CRT has a much better performance, which is because the two common remainders are optimally estimated. For the robust CRT based method, the two estimates may not be optimal when the correspondence

between the two frequencies and the remainders are not proper. It is clear that the searching based method has the best performance. For our proposed robust generalized CRT, it performs slightly worse than the searching based method, but has a much less computation. In fact, the computational complexity of the searching based method and our proposed method are in the order of $(6M\Gamma)^2$ and $6K^2$, respectively.

VI. Conclusion

In this paper, we studied a robust generalized CRT for determining two integers from their residue sets and moduli, where the remainders of the two integers in each residue set are not ordered and may have errors. We first obtained the largest dynamic range of two integers from their error free residue sets of a given modulus set, where all the moduli have a gcd M larger than 1 and the remaining integers factorized by the gcd, M, of all the moduli are pairwisely co-prime. We also presented an efficient reconstruction algorithm of two integers from their error free residue sets, when the two integers are within the largest dynamic range. We then proved that the two integers can be robustly reconstructed if their remainder errors are less than the eighth of the gcd of all the moduli. Finally, we applied the proposed robust generalized CRT for two integers to the determination of two frequencies from multiple undersampled waveforms. Our numerical results showed that the frequency determination performance using our newly proposed robust generalized CRT is better than that using the generalized CRT and the robust CRT based method. Compared with the optimal searching based method, it has a slightly worse performance but much less computation.

Appendix

A. Proof of Lemma 2

Proof: Without loss of generality, we suppose $r_1^c \le r_2^c$. Our proof consists of two steps: firstly, we prove that there exists a subscript $k_0 \in \{1,\dots,K\}$ satisfying (19). Furthermore, we obtain two clusters, Ω_1 and Ω_2, and prove that they satisfy (21). Then we prove the uniqueness of such k_0. By the definition of circular distance in (25), we obtain

$$0 \le \left|d_M(r_1^c, r_2^c)\right| \le M/2. \tag{48}$$

Then we have two cases below.

Case 1: $0 \le \left|d_M(r_1^c, r_2^c)\right| < M/4$.

In this case, we have $0 \le r_2^c - r_1^c < M/4$ or $3M/4 < r_2^c - r_1^c < M$. Let ρ and π be two permutations of the set $\{1,\dots,K\}$ satisfy

$$\Delta r_{\rho(1)} \le \cdots \le \Delta r_{\rho(K)} \text{ and } \Delta r_{\pi(1)} \le \cdots \le \Delta r_{\pi(K)} \tag{49}$$

respectively, where $\Delta r_{\rho(k)} \in \{\Delta r_{1,1},\dots,\Delta r_{1,K}\}$, $\Delta r_{\pi(k)} \in \{\Delta r_{2,1},\dots,\Delta r_{2,K}\}$ for $k = 1,\dots,K$. Define $\{c_1,\dots,c_{2K}\}$ as in (50), as shown at the bottom of this page, where c_i are sorted in the increasing order as

$$c_1 \le \cdots \le c_{2K}. \tag{51}$$

Note that $\left|\Delta_{l,k}\right| < M/8$ for $l = 1,2; k = 1,\dots,K$. If $0 \le r_2^c - r_1^c < M/4$, then we have

$$-M/4 < r_2^c + \Delta r_{\pi(K)} - r_1^c - \Delta r_{\rho(1)} < M/2. \tag{52}$$

If $3M/4 < r_2^c - r_1^c < M$, then we have

$$-M/4 < r_1^c + \Delta r_{\rho(K)} - (r_2^c + \Delta r_{\pi(1)} - M) < M/2. \tag{53}$$

Therefore,

$$0 \le c_{2K} - c_1 < M/2. \tag{54}$$

Let

$$c_i = \alpha_i + \ell_i M,\ i = 1,\dots,2K \tag{55}$$

where $0 \le \alpha_i < M$ and $\ell_i \in \mathbb{Z}$. Then, we obtain from (51) that

$$\ell_1 \le \cdots \le \ell_{2K}. \tag{56}$$

By (54) and (55), we have

$$0 \le \alpha_{2K} - \alpha_1 + (\ell_{2K} - \ell_1)M < M/2. \tag{57}$$

Since $0 \le \alpha_i < M$, we have $-M < \alpha_{2K} - \alpha_1 < M$. It follows from (56) and (57) that

$$\ell_{2K} - \ell_1 = 0 \text{ or } 1.$$

Subcase 1: $\ell_{2K} - \ell_1 = 0$.

In this case, $\ell_1 = \cdots = \ell_{2K}$. From (57), we have

$$0 \le \alpha_{2K} - \alpha_1 < M/2 \tag{58}$$

and from (51) and (55) we have

$$0 \le \alpha_1 \le \cdots \le \alpha_{2K} < M. \tag{59}$$

From (5) and (11), we have

$$\tilde{r}_{l,k} = Mq_{l,k} + r_l^c + \Delta r_{l,k},\ l = 1,2;\ k = 1,\dots,K. \tag{60}$$

Hence,

$$\langle \tilde{r}_{l,k} \rangle_M = \langle r_l^c + \Delta r_{l,k} \rangle_M,\ l = 1,2;\ k = 1,\dots,K. \tag{61}$$

On the other hand, we obtain from (55) that

$$\langle c_i \rangle_M = \alpha_i,\ i = 1,\dots,2K. \tag{62}$$

Combining (50), (61), and (62), we have that $\{\alpha_1,\dots,\alpha_{2K}\}$ are the $2K$ remainders $\{\tilde{r}_1^c,\dots,\tilde{r}_{2K}^c\}$. Hence, (16) is equivalent to (59). If we let $k_0 = K$, then we obtain from (58) that

$$\begin{aligned} D_{k_0} + D_{k_0+K} &= D_{k_0} + \tilde{r}_{\varsigma(1)}^c - \tilde{r}_{\varsigma(2K)}^c + M \\ &= D_{k_0} + \alpha_1 - \alpha_{2K} + M \\ &> M/2. \end{aligned}$$

$$\{c_1,\dots,c_{2K}\} \triangleq \begin{cases} \{r_1^c + \Delta r_{\rho(1)},\dots,r_1^c + \Delta r_{\rho(K)}, r_2^c + \Delta r_{\pi(1)},\dots,r_2^c + \Delta r_{\pi(K)}\}, & \text{if } 0 \le r_2^c - r_1^c < M/4 \\ \{r_1^c + \Delta r_{\rho(1)},\dots,r_1^c + \Delta r_{\rho(K)}, r_2^c + \Delta r_{\pi(1)} - M,\dots,r_2^c + \Delta r_{\pi(K)} - M\}, & \text{if } 3M/4 < r_2^c - r_1^c < M. \end{cases} \tag{50}$$

By the definitions of Ω_1 and Ω_2, we obtain from (59) that

$$\begin{aligned}\Omega_1 &= \{\alpha_{K+1},\ldots,\alpha_{2K}\}\\ &= \{c_{K+1}-\ell_{K+1}M,\ldots,c_{2K}-\ell_{2K}M\}\\ \Omega_2 &= \{\alpha_1,\ldots,\alpha_K\} = \{c_1-\ell_1 M,\ldots,c_K-\ell_K M\}\end{aligned} \tag{63}$$

Recall that $c_1,\ldots,c_{2K}$ are sorted in the increasing order from erroneous remainders $r_1^c+\Delta r_{\rho(1)},\ldots,r_1^c+\Delta r_{\rho(K)}, r_2^c+\Delta r_{\pi_{(1)}},\ldots,r_2^c+\Delta r_{\pi_{(K)}}$. Since $\left|\Delta r_{l,k}\right| \le \tau$ for $l=1,2$; $k=1,\ldots,K$, we have

$$c_K - c_1 \le 2\tau,\ c_{2K}-c_{K+1}\le 2\tau. \tag{64}$$

Thus,

$$\begin{aligned}\omega_K-\omega_1 &= \alpha_{2K}-\alpha_{K+1} = c_{2K}-c_{K+1}\le 2\tau,\\ v_K - v_1 &= \alpha_K-\alpha_1 = c_K-c_1\le 2\tau.\end{aligned}$$

Subcase 2: $\ell_{2K}-\ell_1=1$.

In this case, there exist some $j\in\{1,\ldots,2K\}$ satisfying $\ell_{j+1}-\ell_j=1$. Due to (56), such subscript j is the only one. Moreover, we have $\ell_1=\cdots=\ell_j$ and $\ell_{j+1}=\cdots=\ell_{2K}$. From (51), (54), and (55), we have

$$\alpha_1\le\cdots\le\alpha_j,\ \alpha_{j+1}\le\cdots\le\alpha_{2K}$$

and

$$\alpha_j-\alpha_1<M/2,\ \alpha_{2K}-\alpha_{j+1}<M/2.$$

Since $0\le c_{2K}-c_1<M/2$ and $\ell_{2K}-\ell_1=1$, we obtain from (55) that $\alpha_{2K}-\alpha_1<-M/2$, i.e.,

$$\alpha_1-\alpha_{2K}>M/2. \tag{65}$$

Thus,

$$0\le\alpha_{j+1}\le\cdots\le\alpha_{2K}<\alpha_1\le\cdots\le\alpha_j<M. \tag{66}$$

Note that $\{\alpha_1,\ldots,\alpha_{2K}\}$ are the $2K$ remainders $\{\tilde r_1^c,\ldots,\tilde r_{2K}^c\}$. Hence, (16) is equivalent to (66). 1) If $j<K$ and let $k_0=K-j$, then we obtain from (65) that

$$\begin{aligned}D_{k_0}+D_{k_0+K} &= D_{k_0}+\tilde r^c_{\varsigma(2K-j+1)}-\tilde r^c_{\varsigma(2K-j)}\\ &= D_{k_0}+\alpha_1-\alpha_{2K}\\ &> M/2.\end{aligned}$$

By the definitions of Ω_1 and Ω_2, we obtain from (66) that

$$\begin{aligned}\Omega_1 &= \{\alpha_{K+1},\ldots,\alpha_{2K}\}\\ &= \{c_{K+1}-\ell_{K+1}M,\ldots,c_{2K}-\ell_{2K}M\}\\ \Omega_2 &= \{\alpha_1-M,\ldots,\alpha_j-M,\alpha_{j+1},\ldots,\alpha_K\}\\ &= \{c_1-M-\ell_1M,\ldots,c_j-M-\ell_jM,c_{j+1}-\ell_{j+1}M,\\ &\qquad \ldots,c_K-\ell_KM\}.\end{aligned} \tag{67}$$

Hence, similar to (64), we have

$$\omega_K-\omega_1=c_{2K}-c_{K+1}\le 2\tau,\ v_K-v_1=c_K-c_1\le 2\tau.$$

2) If $j\ge K$ and let $k_0=2K-j$, then we obtain from (65) that

$$\begin{aligned}D_{k_0}+D_{k_0+K} &= \tilde r^c_{\varsigma(2K-j+1)}-\tilde r^c_{\varsigma(2K-j)}+D_{k_0+K}\\ &= \alpha_1-\alpha_{2K}+D_{k_0+K}\\ &> M/2.\end{aligned}$$

By the definitions of Ω_1 and Ω_2, we obtain from (66) that

$$\begin{aligned}\Omega_1 &= \{\alpha_1,\ldots,\alpha_K\} = \{c_1-\ell_1M,\ldots,c_K-\ell_KM\}\\ \Omega_2 &= \{\alpha_{K+1}-M,\ldots,\alpha_j-M,\alpha_{j+1},\ldots,\alpha_{2K}\}\\ &= \{c_{K+1}-M-\ell_{K+1}M,\ldots,c_j-M-\ell_jM,\\ &\qquad c_{j+1}-\ell_{j+1}M,\ldots,c_{2K}-\ell_{2K}M\}\end{aligned} \tag{68}$$

Hence,

$$\begin{aligned}\omega_K-\omega_1 &= \alpha_K-\alpha_1 = c_K-c_1\le 2\tau,\\ v_K-v_1 &= \alpha_{2K}-\alpha_{K+1}+M = c_{2K}-c_{K+1}\le 2\tau.\end{aligned}$$

Case 2: $M/4\le\left|d_M(r_1^c,r_2^c)\right|\le M/2$.

In this case, we have $M/4\le r_2^c-r_1^c\le M/2$ or $M/2<r_2^c-r_1^c\le 3M/4$. Hence, $M/4\le r_2^c-r_1^c\le 3M/4$. Since $|\Delta r_{l,k}|<M/8$ for $l=1,2$; $k=1,\ldots,K$, we have

$$0<r_2^c+\Delta r_{\pi_{(k_2)}}-r_1^c-\Delta r_{\rho_{(k_1)}}<M \tag{69}$$

for any $k_1,k_2\in\{1,\ldots,K\}$. Hence, we obtain

$$r_2^c+\Delta r_{\pi_{(1)}}>r_1^c+\Delta r_{\rho(K)} \tag{70}$$

and

$$r_2^c+\Delta r_{\pi_{(K)}}<r_1^c+\Delta r_{\rho_{(1)}}+M. \tag{71}$$

Since $0\le r_1^c,r_2^c<M$, $r_2^c-r_1^c\ge M/4$ and $|\Delta r_{l,k}|<M/8$, we have

$$-M/8<r_1^c+\Delta r_{\rho(k_1)}\le r_2^c-M/4+\Delta r_{\rho(k_2)}<M \tag{72}$$

and

$$0<r_1^c+M/4+\Delta r_{\pi(k_1)}\le r_2^c+\Delta r_{\pi(k_2)}<9M/8 \tag{73}$$

for any $k_1,k_2\in\{1,\ldots,K\}$. By (69) and (72), we obtain that if there exist some $k\in\{1,\ldots,K\}$ satisfying $r_1^c+\Delta r_{\rho(k)}<0$, then we have $r_2^c+\Delta r_{\pi(k_2)}<M$ for any $k_2\in\{1,\ldots,K\}$. By (69) and (73), we obtain that if there exist some $k\in\{1,\ldots,K\}$ satisfying $r_2^c+\Delta r_{\pi(k)}>M$, then we have $r_1^c+\Delta r_{\rho(k_1)}>0$ for any $k_1\in\{1,\ldots,K\}$. Hence, we have three cases below.

Subcase 1: $r_1^c+\Delta r_{\rho(k)}<0$ for some $k\in\{1,\ldots,K\}$.

Define $k'\in\{1,\ldots,K\}$ as

$$k' \triangleq \begin{cases}K, & \text{if } r_1^c+\Delta r_{\rho(K)}<0\\ \max\left\{k: r_1^c+\Delta r_{\rho(k)}\right.\\ \qquad \left.<0, r_1^c+\Delta r_{\rho(k+1)}\ge 0\right\}, & \text{otherwise.}\end{cases}$$

1) $k'=K$.

Combining (70) and (71), we have

$$\begin{aligned}0<r_2^c+\Delta r_{\pi(1)}&\le\cdots\le r_2^c+\Delta r_{\pi(K)}<r_1^c+\Delta r_{\rho(1)}+M\\ &\le\cdots\le r_1^c+\Delta r_{\rho(K)}+M<M.\end{aligned} \tag{74}$$

From (61) and (74), we obtain that $\{r_1^c+\Delta r_{\rho(1)}+M,\ldots,r_1^c+\Delta r_{\rho(K)}+M, r_2^c+\Delta r_{\pi(1)},\ldots,r_2^c+\Delta r_{\pi(K)}\}$ are the $2K$ remainders $\left\{\tilde r_1^c,\ldots,\tilde r_{2K}^c\right\}$. Hence, (16) is equivalent to (74). If we let $k_0=K$, then we have

$$\begin{aligned}&D_{k_0}+D_{k_0+K}\\ &= \tilde r^c_{\varsigma(K+1)}-\tilde r^c_{\varsigma(K)}+\tilde r^c_{\varsigma(1)}-\tilde r^c_{\varsigma(2K)}+M\\ &= r_1^c+\Delta r_{\rho(1)}+M-r_2^c-\Delta r_{\pi(K)}+r_2^c+\Delta r_{\pi(1)}-r_1^c-\Delta r_{\rho(K)}\\ &= \Delta r_{\rho(1)}+M-\Delta r_{\pi(K)}+\Delta r_{\pi(1)}-\Delta r_{\rho(K)}.\end{aligned}$$

Since $\left|\Delta r_{l,k}\right| < M/8$ for $l = 1, 2$; $k = 1, \ldots, K$, we have

$$D_{k_0} + D_{k_0+K} > M/2.$$

By the definitions of Ω_1 and Ω_2, we obtain from (74) that

$$\begin{aligned}\Omega_1 &= \{r_1^c + \Delta r_{\rho(1)} + M, \ldots, r_1^c + \Delta r_{\rho(K)} + M\}\\ \Omega_2 &= \{r_2^c + \Delta r_{\pi_{(1)}}, \ldots, r_2^c + \Delta r_{\pi_{(K)}}\}\end{aligned} \tag{75}$$

Thus,

$$\omega_K - \omega_1 \le 2\tau,\ \ v_K - v_1 \le 2\tau.$$

2) $k' \in \{1, \ldots, K-1\}$.

Combining (70) and (71), we have

$$\begin{aligned}0 &\le r_1^c + \Delta r_{\rho(k'+1)} \le \cdots \le r_1^c + \Delta r_{\rho(K)} < r_2^c + \Delta r_{\pi_{(1)}}\\ &\le \cdots \le r_2^c + \Delta r_{\pi_{(K)}} < r_1^c + \Delta r_{\rho(1)} + M \le \cdots\\ &\le r_1^c + \Delta r_{\rho_{(k')}} + M < M.\end{aligned} \tag{76}$$

From (61) and (76), we obtain that $\{r_1^c + \Delta r_{\rho_{(1)}} + M, \ldots, r_1^c + \Delta r_{\rho_{(k')}} + M, r_1^c + \Delta r_{\rho_{(k'+1)}}, \ldots, r_1^c + \Delta r_{\rho_{(K)}}, r_2^c + \Delta r_{\pi_{(1)}}, \ldots, r_2^c + \Delta r_{\pi_{(K)}}\}$ are the $2K$ remainders $\{\tilde{r}_1^c, \ldots, \tilde{r}_{2K}^c\}$. Hence, (16) is equivalent to (76). If we let $k_0 = K - k'$, then we have

$$\begin{aligned}&D_{k_0} + D_{k_0+K}\\ &= \tilde{r}^c_{\varsigma(K-k'+1)} - \tilde{r}^c_{\varsigma(K-k')} + \tilde{r}^c_{\varsigma(2K-k'+1)} - \tilde{r}^c_{\varsigma(2K-k')}\\ &= r_2^c + \Delta r_{\pi_{(1)}} - r_1^c - \Delta r_{\rho(K)} + r_1^c + \Delta r_{\rho(1)} + M - r_2^c - \Delta r_{\pi(K)}\\ &= \Delta r_{\pi_{(1)}} - \Delta r_{\rho(K)} + \Delta r_{\rho(1)} - \Delta r_{\pi(K)} + M\\ &> M/2.\end{aligned}$$

By the definitions of Ω_1 and Ω_2, we obtain from (76) that

$$\begin{aligned}\Omega_1 &= \{r_2^c + \Delta r_{\pi_{(1)}}, \ldots, r_2^c + \Delta r_{\pi_{(K)}}\}\\ \Omega_2 &= \{r_1^c + \Delta r_{\rho_{(1)}}, \ldots, r_1^c + \Delta r_{\rho(K)}\}\end{aligned} \tag{77}$$

Thus,

$$\omega_K - \omega_1 \le 2\tau,\ \ v_K - v_1 \le 2\tau.$$

Subcase 2: $r_1^c + \Delta r_{\rho(k)} \ge 0$ and $r_2^c + \Delta r_{\pi_{(k)}} < M$ for all k.

According to (70), we have

$$\begin{aligned}0 &\le r_1^c + \Delta r_{\rho(1)} \le \cdots \le r_1^c + \Delta r_{\rho(K)} < r_2^c + \Delta r_{\pi_{(1)}}\\ &\le \cdots \le r_2^c + \Delta r_{\pi_{(K)}} < M.\end{aligned} \tag{78}$$

From (61) and (78), we obtain that

$$\left\{r_1^c + \Delta r_{\rho(1)}, \ldots, r_1^c + \Delta r_{\rho(K)}, r_2^c + \Delta r_{\pi_{(1)}}, \ldots, r_2^c + \Delta r_{\pi_{(K)}}\right\}$$

are the $2K$ remainders $\left\{\tilde{r}_1^c, \ldots, \tilde{r}_{2K}^c\right\}$. Hence, (16) is equivalent to (78). If we let $k_0 = K$, then we have

$$\begin{aligned}&D_{k_0} + D_{k_0+K}\\ &= \tilde{r}^c_{\varsigma(K+1)} - \tilde{r}^c_{\varsigma(K)} + \tilde{r}^c_{\varsigma(1)} - \tilde{r}^c_{\varsigma(2K)} + M\\ &= r_2^c + \Delta r_{\pi_{(1)}} - r_1^c - \Delta r_{\rho(K)} + r_1^c + \Delta r_{\rho(1)} - r_2^c - \Delta r_{\pi(K)} + M\\ &= \Delta r_{\pi_{(1)}} - \Delta r_{\rho(K)} + \Delta r_{\rho(1)} - \Delta r_{\pi(K)} + M\\ &> M/2.\end{aligned}$$

By the definitions of Ω_1 and Ω_2, we obtain from (78) that

$$\begin{aligned}\Omega_1 &= \{r_2^c + \Delta r_{\pi_{(1)}}, \ldots, r_2^c + \Delta r_{\pi_{(K)}}\}\\ \Omega_2 &= \{r_1^c + \Delta r_{\rho_{(1)}}, \ldots, r_1^c + \Delta r_{\rho(K)}\}\end{aligned} \tag{79}$$

Thus,

$$\omega_K - \omega_1 \le 2\tau,\ \ v_K - v_1 \le 2\tau.$$

Subcase 3: $r_2^c + \Delta r_{\pi_{(k)}} \ge M$ for some $k \in \{1, \ldots, K\}$.

Define $k'' \in \{1, \ldots, K\}$ as

$$k'' \triangleq \begin{cases}1, & \text{if } r_2^c + \Delta r_{\pi_{(1)}} \ge M\\ \min\left\{k : r_2^c + \Delta r_{\pi_{(k-1)}} < M, r_2^c + \Delta r_{\pi_{(k)}} \ge M\right\}, & \text{otherwise.}\end{cases}$$

1) $k'' = 1$.

Combining (70) and (71), we have

$$\begin{aligned}0 &\le r_2^c + \Delta r_{\pi_{(1)}} - M \le \cdots \le r_2^c + \Delta r_{\pi_{(K)}} - M\\ &< r_1^c + \Delta r_{\rho_{(1)}} \le \cdots \le r_1^c + \Delta r_{\rho_{(K)}} < M.\end{aligned} \tag{80}$$

From (61) and (80), we obtain that $\{r_1^c + \Delta r_{\rho_{(1)}}, \ldots, r_1^c + \Delta r_{\rho_{(K)}}, r_2^c + \Delta r_{\pi_{(1)}} - M, \ldots, r_2^c + \Delta r_{\pi_{(K)}} - M\}$ are the $2K$ remainders $\left\{\tilde{r}_1^c, \ldots, \tilde{r}_{2K}^c\right\}$. Hence, (16) is equivalent to (80). If we let $k_0 = K$, then we have

$$\begin{aligned}&D_{k_0} + D_{k_0+K}\\ &= \tilde{r}^c_{\varsigma(K+1)} - \tilde{r}^c_{\varsigma(K)} + \tilde{r}^c_{\varsigma(1)} - \tilde{r}^c_{\varsigma(2K)} + M\\ &= r_1^c + \Delta r_{\rho_{(1)}} - r_2^c - \Delta r_{\pi_{(K)}} + M + r_2^c + \Delta r_{\pi_{(1)}} - M - r_1^c\\ &\quad - \Delta r_{\rho(K)} + M\\ &= \Delta r_{\rho_{(1)}} - \Delta r_{\pi_{(K)}} + \Delta r_{\pi_{(1)}} - \Delta r_{\rho(K)} + M\\ &> M/2.\end{aligned}$$

By the definitions of Ω_1 and Ω_2, we obtain from (80) that

$$\begin{aligned}\Omega_1 &= \{r_1^c + \Delta r_{\rho_{(1)}}, \ldots, r_1^c + \Delta r_{\rho(K)}\}\\ \Omega_2 &= \{r_2^c + \Delta r_{\pi_{(1)}} - M, \ldots, r_2^c + \Delta r_{\pi_{(K)}} - M\}\end{aligned} \tag{81}$$

Thus,

$$\omega_K - \omega_1 \le 2\tau,\ \ v_K - v_1 \le 2\tau.$$

2) $k'' \in \{2, \ldots, K\}$.

Combining (70) and (71), we have

$$\begin{aligned}0 &\le r_2^c + \Delta r_{\pi_{(k'')}} - M \le \cdots \le r_2^c + \Delta r_{\pi_{(K)}} - M\\ &< r_1^c + \Delta r_{\rho_{(1)}} \le \cdots \le r_1^c + \Delta r_{\rho(K)} < r_2^c + \Delta r_{\pi_{(1)}}\\ &\le \cdots \le r_2^c + \Delta r_{\pi_{(k''-1)}} < M.\end{aligned} \tag{82}$$

From (61) and (82), we obtain that $\{r_1^c + \Delta r_{\rho_{(1)}}, \ldots, r_1^c + \Delta r_{\rho(K)}, r_2^c + \Delta r_{\pi_{(1)}}, \ldots, r_2^c + \Delta r_{\pi_{(k''-1)}}, r_2^c + \Delta r_{\pi_{(k'')}} - M, \ldots, r_2^c + \Delta r_{\pi_{(K)}} - M\}$ are the $2K$ remainders $\left\{\tilde{r}_1^c, \ldots, \tilde{r}_{2K}^c\right\}$. Hence, (16) is equivalent to (82). If we let $k_0 = K - k'' + 1$, then we have

$$\begin{aligned}&D_{k_0} + D_{k_0+K}\\ &= \tilde{r}^c_{\varsigma(K-k''+2)} - \tilde{r}^c_{\varsigma(K-k''+1)} + \tilde{r}^c_{\varsigma(2K-k''+2)} - \tilde{r}^c_{\varsigma(2K-k''+1)}\\ &= r_1^c + \Delta r_{\rho_{(1)}} - r_2^c - \Delta r_{\pi_{(K)}} + M + r_2^c + \Delta r_{\pi_{(1)}} - r_1^c - \Delta r_{\rho(K)}\\ &= \Delta r_{\rho_{(1)}} - \Delta r_{\pi_{(K)}} + \Delta r_{\pi_{(1)}} - \Delta r_{\rho(K)} + M\\ &> M/2.\end{aligned}$$

By the definitions of Ω_1 and Ω_2, we obtain from (82) that

$$\begin{aligned}\Omega_1 &= \{r_1^c + \Delta r_{\rho_{(1)}}, \ldots, r_1^c + \Delta r_{\rho(K)}\}\\ \Omega_2 &= \{r_2^c + \Delta r_{\pi_{(1)}} - M, \ldots, r_2^c + \Delta r_{\pi_{(K)}} - M\}\end{aligned} \tag{83}$$

Thus,

$$\omega_K - \omega_1 \le 2\tau,\ \ \upsilon_K - \upsilon_1 \le 2\tau.$$

Next, we prove that k_0 is the only subscript satisfying (19). In fact, for any $k^* \in \{1, \ldots, K\} \setminus \{k_0\}$, we obtain from (18) that

$$\begin{aligned} D_{k^*} + D_{k^*+K} &\le \sum_{k \ne k_0} (D_k + D_{k+K}) \\ &= M - (D_{k_0} + D_{k_0+K}) \\ &< M/2. \end{aligned}$$

This completes the proof. ∎

B. Proof of Theorem 2

Proof: From (29) and (60), we obtain

$$\begin{aligned} \hat{q}_{l,k} &= \left\lceil \frac{M q_{l,k} + r_l^c + \Delta r_{l,k} - \overline{\omega}_t}{M} \right\rceil \\ &= q_{l,k} + \left\lceil \frac{r_l^c + \Delta r_{l,k} - \overline{\omega}_t}{M} \right\rceil \end{aligned} \tag{84}$$

where $l = 1, 2; k = 1, \ldots, K$, and t is defined in (30). For convenience, we denote

$$\overline{\Delta r_l} \triangleq \frac{1}{K} \sum_{k=1}^{K} \Delta r_{l,k},\ \ l = 1, 2.$$

Clearly, $|\overline{\Delta r_l}| \le \tau$.

Case 1: $0 \le \left| d_M(r_1^c, r_2^c) \right| < M/4$.

Since the proof of the two cases $0 \le r_2^c - r_1^c < M/4$ and $3M/4 < r_2^c - r_1^c < M$ are similar, we only consider the case $3M/4 < r_2^c - r_1^c < M$. Note that two sets Ω_1 and Ω_2 are described in Fig. 2(a). As previously shown in (54) that $c_{2K} - c_1 < M/2$, which means $\omega_K - \upsilon_1 < M/2$. According to (27), we have

$$\omega_k' = \omega_k,\ \ k = 1, \ldots, K. \tag{85}$$

By the definitions of $\overline{\omega}_t$ in (28), we know that either

$$\begin{aligned} &\overline{\omega}_1 = r_1^c + \epsilon_1,\ \overline{\omega}_2 = r_2^c - M + \epsilon_2 \text{ or} \\ &\overline{\omega}_1 = r_2^c - M + \epsilon_2,\ \overline{\omega}_2 = r_1^c + \epsilon_1 \end{aligned} \tag{86}$$

hold for some $|\epsilon_t| \le \tau$, $t = 1, 2$. Now, we check $\{\hat{q}_{1,k}, \hat{q}_{2,k}\}$ for $k = 1, \ldots, K$.

According to (29), either $\overline{\omega}_1$ or $\overline{\omega}_2$ is subtracted from $\tilde{r}_{l,k}$. Hence, we obtain from (84) that $\hat{q}_{l,k}$ is either

$$\begin{aligned} \hat{q}_{l,k} &= q_{l,k} + \left\lceil \frac{r_l^c + \Delta r_{l,k} - \overline{\omega}_1}{M} \right\rceil \text{ or} \\ \hat{q}_{l,k} &= q_{l,k} + \left\lceil \frac{r_l^c + \Delta r_{l,k} - \overline{\omega}_2}{M} \right\rceil. \end{aligned} \tag{87}$$

When $l = 1$, $\overline{\omega}_1 = r_1^c + \epsilon_1$, and $\overline{\omega}_2 = r_2^c - M + \epsilon_2$, we have

$$\begin{aligned} r_1^c + \Delta r_{1,k} - \overline{\omega}_1 &= \Delta r_{1,k} - \epsilon_1, \\ r_1^c + \Delta r_{1,k} - \overline{\omega}_2 &= r_1^c + \Delta r_{1,k} - r_2^c + M - \epsilon_2. \end{aligned}$$

Since $3M/4 < r_2^c - r_1^c < M$, $\left|\Delta r_{1,k}\right| \le \tau$, and $\tau < M/8$, we obtain

$$\begin{aligned} &-M/4 < \Delta r_{1,k} - \epsilon_1 < M/4, \\ &-M/4 < r_1^c + \Delta r_{1,k} - r_2^c + M - \epsilon_2 < M/2. \end{aligned}$$

Hence,

$$\left\lceil \frac{r_1^c + \Delta r_{1,k} - \overline{\omega}_1}{M} \right\rceil = 0, \quad \left\lceil \frac{r_1^c + \Delta r_{1,k} - \overline{\omega}_2}{M} \right\rceil = 0.$$

It follows from (87) that

$$\hat{q}_{1,k} = q_{1,k},\ \ k = 1, \ldots, K. \tag{88}$$

Similarly, when $l = 1$, $\overline{\omega}_1 = r_2^c - M + \epsilon_2$, and $\overline{\omega}_2 = r_1^c + \epsilon_1$, we also have (88).

When $l = 2$, $\overline{\omega}_1 = r_1^c + \epsilon_1$, and $\overline{\omega}_2 = r_2^c - M + \epsilon_2$, we have

$$\begin{aligned} r_2^c + \Delta r_{2,k} - \overline{\omega}_1 &= r_2^c + \Delta r_{2,k} - r_1^c - \epsilon_1, \\ r_2^c + \Delta r_{2,k} - \overline{\omega}_2 &= \Delta r_{2,k} + M - \epsilon_2. \end{aligned}$$

Note that $M/2 < r_2^c + \Delta r_{2,k} - r_1^c - \epsilon_1 < 5M/4$ and $3M/4 < \Delta r_{2,k} + M - \epsilon_2 < 5M/4$. Then we have

$$\left\lceil \frac{r_2^c + \Delta r_{2,k} - \overline{\omega}_1}{M} \right\rceil = 1, \quad \left\lceil \frac{r_2^c + \Delta r_{2,k} - \overline{\omega}_2}{M} \right\rceil = 1.$$

By (87), we have

$$\hat{q}_{2,k} = q_{2,k} + 1,\ \ k = 1, \ldots, K. \tag{89}$$

Similarly, when $l = 2$, $\overline{\omega}_1 = r_2^c - M + \epsilon_2$, and $\overline{\omega}_2 = r_1^c + \epsilon_1$, we also have (89). Therefore,

$$\{\hat{q}_{1,k}, \hat{q}_{2,k}\} = \{q_{1,k}, q_{2,k} + 1\},\ \ k = 1, \ldots, K.$$

By the generalized CRT for two integers obtained in [13], we have

$$\{\hat{Q}_1, \hat{Q}_2\} = \{Q_1, Q_2 + 1\}.$$

Next, we check $\{\hat{N}_1, \hat{N}_2\}$ for the cases $\hat{Q}_1 = \hat{Q}_2$ and $\hat{Q}_1 \ne \hat{Q}_2$.

1) $\hat{Q}_1 = \hat{Q}_2 = Q_1 = Q_2 + 1$.

In this case, we obtain from (32) and (86) that

$$\{\hat{N}_1, \hat{N}_2\} = \{N_1 + \epsilon_1, N_2 + \epsilon_2\}.$$

Thus, (40) holds.

2) $\hat{Q}_1 \ne \hat{Q}_2$.

For simplicity, we suppose that $\hat{q}_{1,k} \ne \hat{q}_{2,k}$ for all $k = 1, \ldots, K$. By (33) and (85), we obtain

$$\begin{aligned} \Omega' &= \{\omega_1, \ldots, \omega_K, \upsilon_1, \ldots, \upsilon_K\} \\ &= \{r_1^c + \Delta r_{1,1}, \ldots, r_1^c + \Delta r_{1,K}, r_2^c + \Delta r_{2,1} - M, \ldots, \\ &\qquad r_2^c + \Delta r_{2,K} - M\}. \end{aligned}$$

According to (60), we have

$$d_M(\tilde{r}_{1,k}, r_1^c + \Delta r_{1,k}) = 0,\ \ d_M(\tilde{r}_{2,k}, r_2^c + \Delta r_{2,k} - M) = 0.$$

It follows from (37) that

$$\hat{r}_{1,k}^c = r_1^c + \Delta r_{1,k},\ \ \hat{r}_{2,k}^c = r_2^c + \Delta r_{2,k} - M.$$

From (38), we obtain the estimates

$$\hat{r}_1^c = r_1^c + \epsilon_3,\ \ \hat{r}_2^c = r_2^c - M + \epsilon_4$$

where ϵ_3 and ϵ_4 are some integers satisfying $|\epsilon_t| \le \tau, t = 3, 4$. By (39), we have

$$\{\hat{N}_1, \hat{N}_2\} = \{N_1 + \epsilon_3, N_2 + \epsilon_4\}.$$

Thus, (40) holds.

Case 2: $M/4 \le \left|d_M(r_1^c, r_2^c)\right| \le M/2$.

In this case, all the possible cases of the two clusters, Ω_1 and Ω_2, are described in Fig. 2(b) and given by (75), (77), (79), (81), and (83) in details. Since the proofs of these cases are similar, we only consider the case of (75), i.e.,

$$\begin{aligned}\Omega_1 &= \{\omega_1, \ldots, \omega_K\} \\ &= \left\{r_1^c + M + \Delta r_{\rho(1)}, \ldots, r_1^c + M + \Delta r_{\rho(K)}\right\}, \\ \Omega_2 &= \{\upsilon_1, \ldots, \upsilon_K\} = \left\{r_2^c + \Delta r_{\pi(1)}, \ldots, r_2^c + \Delta r_{\pi(K)}\right\}.\end{aligned}$$

Without loss of generality, we suppose that $0 < \omega_K - \upsilon_1 \le M/2$. By the definitions of ω_k' in (27), we have

$$\omega_k' = \omega_k, \ k = 1, \ldots, K. \tag{90}$$

According to the definitions of $\overline{\omega}_t$ in (28), we obtain

$$\overline{\omega}_1 = r_1^c + M + \overline{\Delta r}_1, \ \overline{\omega}_2 = r_2^c + \overline{\Delta r}_2. \tag{91}$$

Now, we check $\{\hat{q}_{1,k}, \hat{q}_{2,k}\}$ for $k = 1, \ldots, K$.

According to (29) and (84), we have

$$\begin{aligned}\hat{q}_{1,k} &= \left[\frac{\tilde{r}_{1,k} - \overline{\omega}_1}{M}\right] = q_{1,k} - 1, \\ \hat{q}_{2,k} &= \left[\frac{\tilde{r}_{2,k} - \overline{\omega}_2}{M}\right] = q_{2,k}.\end{aligned}$$

Therefore,

$$\{\hat{q}_{1,k}, \hat{q}_{2,k}\} = \{q_{1,k} - 1, q_{2,k}\}, \ k = 1, \ldots, K.$$

By the generalized CRT for two integers obtained in [13], we have

$$\{\hat{Q}_1, \hat{Q}_2\} = \{Q_1 - 1, Q_2\}.$$

Next, we check $\{\hat{N}_1, \hat{N}_2\}$ for the cases $\hat{Q}_1 = \hat{Q}_2$ and $\hat{Q}_1 \ne \hat{Q}_2$.

1) $\hat{Q}_1 = \hat{Q}_2$.

By (32) and (91), we have

$$\{\hat{N}_1, \hat{N}_2\} = \{N_1 + \overline{\Delta r}_1, N_2 + \overline{\Delta r}_2\}.$$

Thus, (40) holds.

2) $\hat{Q}_1 \ne \hat{Q}_2$.

For simplicity, we suppose that $\hat{q}_{1,k} \ne \hat{q}_{2,k}$ for all $k = 1, \ldots, K$. By (33) and (90), we obtain

$$\begin{aligned}\Omega' &= \{\omega_1', \ldots, \omega_K', \upsilon_1, \ldots, \upsilon_K\} \\ &= \{r_1^c + M + \Delta r_{1,1}, \ldots, r_1^c + M + \Delta r_{1,K}, r_2^c + \Delta r_{2,1}, \ldots, \\ &\qquad r_2^c + \Delta r_{2,K}\}.\end{aligned}$$

According to (60), we have

$$\begin{aligned}d_M(\tilde{r}_{1,k}, r_1^c + \Delta r_{1,k}) = 0, \\ d_M(\tilde{r}_{2,k}, r_2^c + \Delta r_{2,k}) = 0.\end{aligned}$$

It follows from (37) that

$$\hat{r}_{1,k}^c = r_1^c + M + \Delta r_{1,k}, \ \hat{r}_{2,k}^c = r_2^c + \Delta r_{2,k}.$$

From (38), we obtain the estimates

$$\hat{r}_1^c = r_1^c + M + \epsilon_5, \ \hat{r}_2^c = r_2^c + \epsilon_6$$

where ϵ_5 and ϵ_6 are some integers satisfying $|\epsilon_t| \le \tau, t = 5, 6$. By (39), we have

$$\{\hat{N}_1, \hat{N}_2\} = \{N_1 + \epsilon_5, N_2 + \epsilon_6\}.$$

Thus, (40) holds. This completes the proof of the theorem. ■

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their useful comments that have helped to improve the presentation of this paper. This work was done when Xiaoping Li was visiting the University of Delaware.

REFERENCES

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

[2] N. Koblitz, *A Course in Number Theory and Cryptography*. New York, NY, USA: Springer-Verlag, 1994.

[3] K. H. Rosen, *Elementary Number Theory and Its Applications*, 6th ed. Reading, MA, USA: Addison-Wesley, 2010.

[4] C. Li, Y. Liu, L. Y. Zhang, and K.-W. Wong, "Cryptanalyzing a class of image encryption schemes based on Chinese remainder theorem," *Signal Process., Image Commun.*, vol. 29, pp. 914–920, Sep. 2014.

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

[6] B. Arazi, "A generalization of the Chinese remainder theorem," *Pacific J. Math.*, vol. 70, pp. 289–296, Jun. 1977.

[7] G. Zhou and X.-G. Xia, "Multiple frequency detection in undersampled complex-valued waveforms with close multiple frequencies," *Electron. Lett.*, vol. 33, pp. 1294–1295, Jul. 1997.

[8] 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.

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

[10] L. Xiao and X.-G. Xia, "A generalized Chinese remainder theorem for two integers," *IEEE Signal Process. Lett.*, vol. 21, no. 1, pp. 55–59, Jan. 2014.

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

[12] X.-G. Xia and 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.*, vol. 12, no. 11, pp. 768–771, Nov. 2005.

[13] W. Wang, X. Li, X.-G. Xia, and W. Wang, "The largest dynamic range of a generalized Chinese remainder theorem for two integers," *IEEE Signal Process. Lett.*, vol. 22, no. 2, pp. 254–258, Feb. 2015.

[14] X.-G. Xia, "Dynamic range of the detectable parameters for polynomial phase signals using multiple-lag diversities in high-order ambiguity functions," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1378–1384, May 2001.

[15] Y. Cheng, X. Wang, T. Caelli, and B. Moran, "Tracking and localizing moving targets in the presence of phase measurement ambiguities," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3514–3525, Aug. 2011.

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

[17] R. G. McKilliam, B. G. Quinn, I. V. L. Clarkson, B. Moran, and B. N. Vellambi, "Polynomial phase estimation by least squares phase unwrapping," *IEEE Trans. Signal Process.*, vol. 62, no. 8, pp. 1962–1975, Apr. 2014.

[18] Y. Zhang, W. Qi, G. Li, and S. Zhang, "Performance of ML range estimator in radio interferometric positioning systems," *IEEE Signal Process. Lett.*, vol. 22, no. 2, pp. 162–166, Feb. 2015.

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

[20] A. Akhlaq, R. G. McKilliam, and R. Subramanian, "Basis construction for range estimation by phase unwrapping," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 2152–2156, Nov. 2015.
[21] K. Falaggis, D. P. Towers, and C. E. Towers, "Method of excess fractions with application to absolute distance metrology: Analytical solution," *Appl. Opt.*, vol. 52, no. 23, pp. 5758–5765, Aug. 2013.
[22] K. Falaggis, D. P. Towers, and C. E. Towers, "Algebraic solution for phase unwrapping problems in multiwavelength interferometry," *Appl. Opt.*, vol. 53, no. 17, pp. 3737–3747, Jun. 2014.
[23] G. Wang, X.-G. Xia, V. C. Chen, and R. L. Fielder, "Detection, location, and imaging of fast moving targets using multifrequency antenna array SAR," *IEEE Trans. Arrosep. Electron Syst.*, vol. 40, no. 1, pp. 345–355, Jan. 2004.
[24] M. Rüegg, E. Meier, and D. Nüesch, "Capabilities of dual-frequency millimeter wave SAR with monopulse processing for ground moving target indication," *IEEE Trans. Geosci. Remote Sens.*, vol. 45, no. 3, pp. 539–553, Mar. 2007.
[25] G. Li, J. Xu, Y.-N. Peng, and X.-G. Xia, "Location and imaging of moving targets using nonuniform linear antenna array SAR," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 43, no. 3, pp. 1214–1220, Jul. 2007.
[26] Y. Zhang and M. Amin, "MIMO radar exploiting narrowband frequency-hopping waveforms," in *Proc. 16th Eur. Signal Process. Conf. (EUSIPCO)*, Lausanne, Switzerland, Aug. 2008, pp. 25–29.
[27] W.-K. Qi, Y.-W. Dang, and W.-D. Yu, "Deblurring velocity ambiguity of distributed space-borne SAR based on Chinese remainder theorem," *J. Electron. Inf. Technol.*, vol. 31, no. 10, pp. 2493–2497, Oct. 2009.
[28] P. Beauseroy and R. Lengellé, "Nonintrusive turbomachine blade vibration measurement system," *Mech. Syst. Signal Process.*, vol. 21, pp. 1717–1738, May 2007.
[29] 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.
[30] W. Li, X. Wang, X. Wang, and B. Moran, "Distance estimation using wrapped phase measurements in noise," *IEEE Trans. Signal Process.*, vol. 61, no. 7, pp. 1676–1688, Apr. 2013.
[31] Z. Huang and Z. Wan, "Range ambiguity resolution in multiple PRF pulse Doppler radars," in *Proc. ICASSP*, Dallas, TX, USA, Apr. 1987, pp. 1786–1789.
[32] 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.
[33] G. Li, J. Xu, Y.-N. Peng, and X.-G. Xia, "An efficient implementation of a robust phase-unwrapping algorithm," *IEEE Signal Process. Lett.*, vol. 14, no. 6, pp. 393–396, Jun. 2007.
[34] X. Li and X.-G. Xia, "A fast robust Chinese remainder theorem based phase unwrapping algorithm," *IEEE Signal Process. Lett.*, vol. 15, no. 10, pp. 665-668, Oct. 2008.
[35] 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.
[36] 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.
[37] W. Wang, X. Li, W. Wang, and X.-G. Xia, "Maximum likelihood estimation based robust Chinese remainder theorem for real numbers and its fast algorithm," *IEEE Trans. Signal Process.*, vol. 63, no. 13, pp. 3317–3331, Jul. 2015.
[38] B. Yang, W. Wang, Q. Yin, and X.-G. Xia, "Phase detection based range estimation with a dual-band robust Chinese remainder theorem," *Sci. China Inf. Sci.*, vol. 57, no. 2, pp. 1–9, Feb. 2014.
[39] 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.
[40] O. Ore, "The general Chinese remainder theorem," *Amer. Math. Monthly*, vol. 59, no. 6, pp. 365–370, Jun./Jul. 1952.

Xiaoping Li received his B.S. degree in mathematics from Sichuan Normal University, Chengdu, China, and his Ph.D. degree in information and communication engineering from Xi'an Jiaotong University, Xi'an, China, in 2006 and 2016, respectively. From 2006-2010, he was an assistant professor in the College of Information Engineering, Tarim University, Alar, China. From December 2013 to January 2015, he was a visiting scholar at the Department of Electrical and Computer Engineering, University of Delaware, Newark, Delaware.

Currently, he is a lecturer at the School of Mathematical Science, University of Electronic Science and Technology of China, Chengdu, China. His main research interests include signal processing with applications in communication systems and coding theory.

Xiang-Gen Xia (M'97–S'00–F'09) received his B.S. degree in mathematics from Nanjing Normal University, Nanjing, China, and his M.S. degree in mathematics from Nankai University, Tianjin, China, and his Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1983, 1986, and 1992, respectively.

He was a Senior/Research Staff Member at Hughes Research Laboratories, Malibu, California, during 1995-1996. In September 1996, he joined the Department of Electrical and Computer Engineering, University of Delaware, Newark, Delaware, where he is the Charles Black Evans Professor. His current research interests include spacetime coding, MIMO and OFDM systems, digital signal processing, and SAR and ISAR imaging. Dr. Xia is the author of the book Modulated Coding for Intersymbol Interference Channels (New York, Marcel Dekker, 2000).

Dr. Xia received the National Science Foundation (NSF) Faculty Early Career Development (CAREER) Program Award in 1997, the Office of Naval Research (ONR) Young Investigator Award in 1998, and the Outstanding Overseas Young Investigator Award from the National Nature Science Foundation of China in 2001. He also received the Outstanding Junior Faculty Award of the Engineering School of the University of Delaware in 2001. He is currently serving and has served as an Associate Editor for numerous international journals including IEEE Wireless Communications Letters, IEEE TRANSACTIONS ON SIGNAL PROCESSING, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON MOBILE COMPUTING, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. Dr. Xia is Technical Program Chair of the Signal Processing Symp., Globecom 2007 in Washington D.C. and the General Co-Chair of ICASSP 2005 in Philadelphia.

Wenjie Wang (M'10) received the B.S., M.S., and Ph.D. degrees in information and communication engineering from Xi'an Jiaotong University, Xi'an, China, in 1993, 1998, and 2001, respectively. From 2009 to 2010, he was a visiting scholar at the Department of Electrical and Computer Engineering, University of Delaware, Newark, Delaware. Currently, he is a Professor at Xi'an Jiaotong University.

His main research interests include information theory, broadband wireless communications, signal processing with applications in communication systems, array signal processing and cooperative communications in distributed networks.

Wei Wang received the B.S. and M.S. degrees from Central South University, Changsha, China, in 2004 and 2006, respectively, both in mathematics. Currently, he is an Associate Professor in the College of Information Engineering, Tarim University, Alar, China. He is also a Ph.D. candidate in mathematics at Xiamen University, Xiamen, China.

His research interests are graph theory and combinatorics. He has been a reviewer for Mathematical Reviews since 2013.