A Robust Chinese Remainder Theorem With Its Applications in Frequency Estimation From Undersampled Waveforms

Xiaowei Li, Hong Liang, and Xiang-Gen Xia, *Fellow, IEEE*

***Abstract*—The Chinese remainder theorem (CRT) allows to reconstruct a large integer from its remainders modulo several moduli. In this paper, we propose a robust reconstruction algorithm called robust CRT when the remainders have errors. We show that, using the proposed robust CRT, the reconstruction error is upper bounded by the maximal remainder error range named remainder error bound, if the remainder error bound is less than one quarter of the greatest common divisor (gcd) of all the moduli. We then apply the robust CRT to estimate frequencies when the signal waveforms are undersampled multiple times. It shows that with the robust CRT, the sampling frequencies can be significantly reduced.**

***Index Terms*—Chinese remainder theorem (CRT), frequency estimation, robust CRT, sensor networks, undersampling.**

I. Introduction

THE Chinese remainder theorem (CRT) allows to reconstruct a large integer from its remainders modulo a set of moduli. When all the moduli are co-prime, CRT has a simple single formula, which is well-known not robust, i.e., small errors from any remainders may cause a large reconstruction error. This is perhaps why CRT has applications in cryptography but not desired in some other applications, such as frequency estimation from undersampled waveforms with its applications, for example, phase unwrapping in radar signal processing [1], [6]–[10] and sensor networks [5]. In terms of reconstruction of large integers from remainders, it is not restricted to co-prime moduli. The unique reconstruction is possible if and only if the large integers are less than the least common multiple (lcm) of all the moduli. A type of robust CRT has been recently proposed in [2] when the large integers to determine are of some special forms, which was motivated from a robust phase unwrapping algorithm also proposed in [2] with applications in radar imaging of moving targets [1], [6], [7]. Their fast implementations are recently reported in [3] and [4].

Motivated from the robust phase unwrapping algorithm and the special form of the robust CRT obtained in [2], we propose a general robust CRT, i.e., robust reconstruction of general large integers from their remainders with errors, which often occurs in practical applications. Note that this general robust CRT is different from the preliminary one in [2] that is only limited to special integers N with the form of $N = n_0 \prod_{i=1}^{i=L} \Gamma_i$ for some integer n_0 while Γ_i are fixed integers as indicated in Section III in [2].

In this paper, we show that, using the newly proposed robust CRT, the reconstruction error is upper bounded by the maximal remainder error range τ named remainder error bound, if the remainder error bound τ is less than one quarter of the greatest common divisor (gcd) of all the moduli M_i, i.e., $\tau < \gcd(M_1, M_2, \cdots, M_L)/4$, where L is the number of moduli used. Note that this robust CRT is different from the existing CRT with errors in for example [5], [13] where sufficiently many moduli are used so that only a few of the remainders have errors does not affect the unique reconstruction, i.e., if there are only a few remainder errors, then they can be corrected and the reconstruction is accurate. This robust CRT is also different from the one in [14], whose correctness is probabilistic over a sufficiently large number of prime moduli, where all remainders contaminated by a small additive noise bounded in the Lee norm (even with wraparound errors) may be corrected [14]. In contrast, in our proposed robust CRT, the reconstruction may not be accurate but with an error deterministically in the same range of the remainder errors and every remainder may be erroneous, where all remainders are assumed non-negative. After saying so, although its correctness is probabilistic, the algorithm in [14] may tolerate much larger errors in the remainders than our proposed algorithm does when the gcd of the moduli M_i is small. (The algorithm in [14] can tolerate errors with magnitudes approaching $\min_i M_i$ probabilistically whereas the proposed algorithm in this paper tolerates errors with non-negative amplitudes approaching $\gcd(M_1, M_2, \cdots, M_L)/4$ deterministically.)

We then apply the robust CRT to estimate frequencies when the signal waveforms are undersampled multiple times. It shows that with the robust CRT, the sampling frequencies can be significantly reduced, and/or the number of samples can be significantly reduced.

The remaining of this paper is organized as follows. In Section II, we first briefly describe the problem and then present the robust CRT. In Section III, we present fast imple-

Manuscript received October 28, 2008; revised May 12, 2009. First published June 10, 2009; current version published October 14, 2009. This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-08-1-0219 and a DEPSCoR Grant W911NF-07-1-0422 through ARO.

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

H. Liang is with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA. She is also with the College of Marine, Northwestern Polytechnical University, Xi'an, 710072, China (e-mail: liang@ee.udel.edu).

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/TSP.2009.2025079

mentation and efficient algorithms. In Section IV, we present an application of the robust CRT in frequency estimation from multiple undersampled waveforms. We also present some simulation results.

II. Robust Chinese Remainder Theorem

Let us first see the problem. Let N be a positive integer, $0 < M_1 < M_2 < \cdots < M_L$ be the L moduli, and $r_1, r_2, \cdots, r_L$ be the L remainders of N, i.e.,

$$N \equiv r_i \bmod M_i \text{ or } N = n_i M_i + r_i, \tag{1}$$

where $0 \leq r_i < M_i$ and n_i is an unknown integer, for $1 \leq i \leq L$. It is not hard to see that N can be uniquely reconstructed from its L remainders r_i if and only if $0 \leq N < \operatorname{lcm}(M_1, M_2, \cdots, M_L)$. If all the moduli M_i are co-prime, then CRT has a simple formula [11], [12].

The problem we are interested in this paper is how to robustly reconstruct N when the remainders r_i have errors:

$$0 \leq \tilde{r}_i \leq M_i - 1 \quad \text{and} \quad |\tilde{r}_i - r_i| \leq \tau \tag{2}$$

where $\tau < \min_{1 \leq i \leq L} M_i$ is the maximal error level, called remainder error bound. We now want to reconstruct N from these erroneous remainders $\tilde{r}_i$ and the known moduli M_i. With these erroneous remainders, (1) becomes

$$N = n_i M_i + \tilde{r}_i + \triangle r_i, \quad 1 \leq i \leq L \tag{3}$$

where n_i are unknown and $\triangle r_i = r_i - \tilde{r}_i$ denote the errors of the remainders. From (2), $|\triangle r_i| \leq \tau$. The basic idea for our robust CRT is to accurately determine the unknown integers n_i in (3) which are the folding integers that may cause large errors in the reconstructions if they are erroneous. Motivated from the robust phase unwrapping algorithm in [2], we propose the following robust CRT.

Let M denote the gcd of all the moduli M_i. Then

$$M_i = M\Gamma_i, \quad 1 \leq i \leq L \tag{4}$$

and all Γ_i, $1 \leq i \leq L$, are co-prime, i.e., the gcd of any pair Γ_i and Γ_j for $i \neq j$ is 1.

For $1 \leq i \leq L$, let

$$\gamma_i \triangleq \Gamma_1 \cdots \Gamma_{i-1}\Gamma_{i+1} \cdots \Gamma_L \tag{5}$$

where $\gamma_1 \triangleq \Gamma_2 \cdots \Gamma_L$ and $\gamma_L \triangleq \Gamma_1 \cdots \Gamma_{L-1}$. Since $M_1 < M_2 < \cdots < M_L$, we have $\Gamma_1 < \Gamma_2 < \cdots < \Gamma_L$. For each i with $2 \leq i \leq L$, define

$$S_i \triangleq \left\{ (\bar{n}_1, \bar{n}_i) = \arg\min_{\substack{\hat{n}_1 = 0,1,\cdots,\gamma_1 - 1 \\ \hat{n}_i = 0,1,\cdots,\gamma_i - 1}} |\hat{n}_i M_i + \tilde{r}_i - \hat{n}_1 M_1 - \tilde{r}_1| \right\} \tag{6}$$

and let $S_{i,1}$ denote the set of all the first components $\bar{n}_1$ of the pairs $(\bar{n}_1, \bar{n}_i)$ in set S_i, i.e.,

$$S_{i,1} \triangleq \{\bar{n}_1 | (\bar{n}_1, \bar{n}_i) \in S_i \text{ for some } \bar{n}_i\} \tag{7}$$

and define

$$S \triangleq \bigcap_{i=2}^{L} S_{i,1}. \tag{8}$$

Then, we have the following result.

Theorem 1: If all Γ_i, $1 \leq i \leq L$, are pair-wisely co-prime

$$0 \leq N < \operatorname{lcm}(M_1, M_2, \cdots, M_L) = \frac{1}{M^{L-1}} M_1 M_2 \cdots M_L \tag{9}$$

and

$$M > 4\tau \tag{10}$$

then, set S defined above contains only element n_1, i.e., $S = \{n_1\}$, and furthermore if $(n_1, \bar{n}_i) \in S_i$, then $\bar{n}_i = n_i$ for $2 \leq i \leq L$, where n_i, $1 \leq i \leq L$, are the true solutions in (3).

Its proof is similar to the proof of Theorem 1 in [2], which, for the completeness, can be found in Appendix I. Note that Although the proof is similar to the one in [2], the result in the above Theorem 1 is much more general than the one in [2] as explained in Introduction. In [2], N has to be a special form of multiples of the product $\prod_{i=1}^{L} \Gamma_i$ while N in Theorem 1 is arbitrary.

When the folding integers n_i in (3) are accurately solved, the unknown parameter N can be estimated as

$$\hat{N} = \left[\frac{1}{L} \sum_{i=1}^{L} (n_i M_i + \tilde{r}_i) \right] \tag{11}$$

where $[\cdot]$ stands for the rounding integer (rounding to the closest integer) and the estimate error is thus upper bounded by

$$|N - \hat{N}| \leq \tau \tag{12}$$

when the condition (10) holds. The above estimate error of N is due to the remainder errors $r_i - \tilde{r}_i$ that has the maximal level τ. One can clearly see that this reconstruction is robust and thus called robust CRT. Note that, in the above robust CRT, the integer N is arbitrary as long as it falls in the range $0 \leq N < \operatorname{lcm}(M_1, M_2, \cdots, M_L)$, while the robust CRT obtained in [2] requires that N has to have the form of $N = n_0 \Gamma_1 \Gamma_2 \cdots \Gamma_L$ for some integer n_0 in the range $0 \leq n_0 < M$.

From Theorem 1, one can see that when all moduli are co-prime, i.e., $M = 1$, the remainder error bound τ is forced to be 0 in (10). This means that the above reconstruction may not guarantee a robust solution that is not conflict with the well-known knowledge that the traditional CRT is not robust.

One can also see that the above robust CRT is based on the sets defined in (6) that need $L - 1$ many 2 dimensional (2-D) searches of $\hat{n}_1$ and $\hat{n}_i$ in the 2-D range $[0, \gamma_1 - 1] \times [0, \gamma_i - 1]$ for $2 \leq i \leq L$. When Γ_i are large, γ_i become large and therefore the 2-D searches may have a high computational complexity. In next section, we simplify the searching and also propose a 1-D searching algorithm.

Another remark is that from (12), one can clearly see that when the remainders are error-free, i.e., $\tau = 0$, the reconstruction is then accurate, i.e., $\hat{N} = N$. In this case, different from the methods in [11], [12], the above result provides an alternative way to determine integer N from its remainders and moduli that are not co-prime. Furthermore, the fast algorithms presented in next section still applies in this error-free case, and thus provide fast algorithms for the reconstruction from error-free remainders and non-co-prime moduli.

III. Fast Algorithms

The order of the $L-1$ many 2-D searches of $\hat{n}_1$ and $\hat{n}_i$ in the 2-D range $[0,\gamma_1-1]\times[0,\gamma_i-1]$ for S_i in (6) is about $(\Gamma_2\Gamma_3\cdots\Gamma_L)^2$. This order was reduced significantly in [3] where the following result was obtained.

Theorem 2: [3] Let

$$\begin{aligned}\Omega_i' \overset{\Delta}{=} &\{(\hat{n}_1,\hat{n}_i)|0\le\hat{n}_1\le\Gamma_i-1, 0\le\hat{n}_i\le\Gamma_1-1\}\\ &\bigcup\{(\hat{n}_1,\hat{n}_i)|\Gamma_i\le\hat{n}_1\le2\Gamma_i-1, 0\le\hat{n}_i\le\Gamma_1-1\}\\ &\bigcup\{(\hat{n}_1,\hat{n}_i)|0\le\hat{n}_1\le\Gamma_i-1, \Gamma_1\le\hat{n}_i\le2\Gamma_1-1\} \quad (13)\end{aligned}$$

and S_i' be defined in (14) at the bottom of the page. Then, we have $S_i'=S_i$ for $2\le i\le L$.

Clearly, Theorem 2 applies to the problem in Section II. From Theorem 2, one can see that the number of searches to obtain S_i' is only in the order of $\Gamma_1\Gamma_i$, i.e., the size of set Ω_i'.

Next, we propose a different fast algorithm to find the folding integers n_i similar to [4]. Instead of finding the whole set S_i, we find only one element in S_i for each i with $2\le i\le L$ and then use some properties to determine n_i. We show that one only needs the order of $\Gamma_1+\Gamma_i$ number of searches for the new algorithm. To do so, we first present some properties listed in the following lemmas, whose proofs are similar to those in [4].

Lemma 1: Assume that all the conditions in Theorem 1 hold, i.e., (9) and (10) hold. Let n_i, $1\le i\le L$, be the true solutions in (3). Then, $(\bar{n}_1,\bar{n}_i)\in S_i$ if and only if $\bar{n}_1=n_1+m_i\Gamma_i$ and $\bar{n}_i=n_i+m_i\Gamma_1$ for some integer m_i and $0\le\bar{n}_i\le\gamma_i-1$ for $2\le i\le L$.

Its proof is the same as the proof of Lemma 1 in [4].

Lemma 2: Under the conditions in Theorem 1, let

$$\begin{aligned}\Omega_i = &\{(\hat{n}_1,\hat{n}_i)|0\le\hat{n}_1\le\Gamma_i-1, 0\le\hat{n}_i\le\gamma_i-1\}\\ &\bigcup\{(\hat{n}_1,\hat{n}_i)|0\le\hat{n}_i\le\Gamma_1-1, 0\le\hat{n}_1\le\gamma_1-1\}. \quad (15)\end{aligned}$$

Then, for any element $(\bar{n}_1,\bar{n}_i)\in S_i$, there exists an integer m_i such that

$$(\bar{n}_1+m_i\Gamma_i, \bar{n}_i+m_i\Gamma_1)\in\Omega_i\cap S_i.$$

Its proof is the same as the proof of Lemma 2 in [4].

Lemma 3: Let $(\bar{n}_1,\bar{n}_i)\in S_i$. If one component of $(\bar{n}_1,\bar{n}_i)$, $\bar{n}_1$ or $\bar{n}_i$, is fixed, then, the other one, $\bar{n}_i$ or $\bar{n}_1$ is uniquely determined.

The following proof is an improvement of the proof of Lemma 3 in [4].

Proof: For $(\bar{n}_1,\bar{n}_i)\in S_i$ with $2\le i\le L$, we claim

$$L(\bar{n}_1,\bar{n}_i)\overset{\Delta}{=}|\bar{n}_1M_1+\tilde{r}_1-\bar{n}_iM_i-\tilde{r}_i|<\frac{M_1}{2}. \quad (16)$$

This claim (16) is proved in Appendix II.

We first consider the case when $\hat{n}_1$ is fixed. In this case, from (16) its corresponding $\hat{n}_i$ in S_i must satisfy

$$\begin{aligned}\hat{n}_i\in\Bigg(&\frac{\Gamma_1}{\Gamma_i}\hat{n}_1+\frac{\tilde{r}_1}{M\Gamma_i}-\frac{\tilde{r}_i}{M\Gamma_i}-\frac{\Gamma_1}{2\Gamma_i},\\ &\frac{\Gamma_1}{\Gamma_i}\hat{n}_1+\frac{\tilde{r}_1}{M\Gamma_i}-\frac{\tilde{r}_i}{M\Gamma_i}+\frac{\Gamma_1}{2\Gamma_i}\Bigg) \quad (17)\end{aligned}$$

where the right-hand side interval length is $(\Gamma_1/\Gamma_i)<1$ for $2\le i\le L$ and therefore this interval contains only one integer, i.e., $\hat{n}_i$ is unique and determined by (17).

We next consider the case when $\hat{n}_i$ is fixed. In this case, from (16) its corresponding $\hat{n}_1$ in S_i satisfies

$$\begin{aligned}\hat{n}_1\in\Bigg(&\frac{\Gamma_i}{\Gamma_1}\hat{n}_i+\frac{\tilde{r}_i}{M\Gamma_1}-\frac{\tilde{r}_1}{M\Gamma_1}-\frac{1}{2},\\ &\frac{\Gamma_i}{\Gamma_1}\hat{n}_i+\frac{\tilde{r}_i}{M\Gamma_1}-\frac{\tilde{r}_1}{M\Gamma_1}+\frac{1}{2}\Bigg) \quad (18)\end{aligned}$$

where the right-hand side interval length is 1, and thus this open interval contains only one integer as well, i.e., $\hat{n}_1$ is unique and determined by (18). ■

From the above proof of Lemma 3, one can see that the lower bound (16) plays the key role for the determination. In fact, it can be further improved as follows.

For $2\le i\le L$, let $\Gamma_i=\eta_i\Gamma_1+\delta_i$ with $0\le\delta_i\le\Gamma_1-1$, i.e., δ_i is the remainder of Γ_i modulo Γ_1. Since Γ_i and Γ_1 are co-prime, we have

$$1\le\delta_i\le\Gamma_1-1. \quad (19)$$

Corollary 1: For $(\bar{n}_1,\bar{n}_i)\in S_i$ with $2\le i\le L$, if $L\ge3$, then

$$L(\bar{n}_1,\bar{n}_i)\le\frac{M\delta_i}{2}<\frac{M_1}{2}. \quad (20)$$

This corollary, i.e., inequality (20), is proved in Appendix III.

Lemmas 1-3 tell us that the two dimensional searching for $(\bar{n}_1,\bar{n}_i)$ is not necessary and instead we only need to search one of possible $\bar{n}_1$ and $\bar{n}_i$ and the other then uniquely follows, i.e., we only need to do one dimensional searching. With the above three lemmas, a fast algorithm to determine the folding integers n_i can be described by the following steps.

$$S_i'=\left\{(\bar{n}_1'+h_i\Gamma_i, \bar{n}_i'+h_i\Gamma_1)\;\middle|\;\begin{array}{c}(\bar{n}_1',\bar{n}_i')=\arg\min_{(\hat{n}_1,\hat{n}_i)\in\Omega_i'}|\hat{n}_iM_i+\tilde{r}_i-\hat{n}_1M_1-\tilde{r}_1|\\ h_i=\begin{cases}0,1,\cdots,\prod_{j=2,j\neq i}^{L}\Gamma_j-1, & \text{if}\begin{cases}0\le\bar{n}_1'\le\Gamma_i-1\\0\le\bar{n}_i'\le\Gamma_1-1\end{cases},\\ 0,1,\cdots,\prod_{j=2,j\neq i}^{L}\Gamma_j-2, & \text{otherwise}\end{cases}\end{array}\right\} \quad (14)$$

We first want to find one element $(\bar{n}_{1,i}, \bar{n}_i) \in S_i$ for each i with $2 \le i \le L$. Based on Lemma 2, we can find an element in Ω_i that belongs to S_i and therefore, we only need to search over set Ω_i. We first search all integers $\hat{n}_1$ from 0 to $\Gamma_i - 1$. From the proof of Lemma 3, when $\hat{n}_1$ is fixed, its corresponding $\hat{n}_i$ in S_i is determined by (17) and denoted by $\hat{n}_i = \hat{n}_i(\hat{n}_1)$. Then, this pair $(\hat{n}_1, \hat{n}_i(\hat{n}_1))$ is evaluated by the criterion in (6), and its minimum is searched among all $\hat{n}_1$ from 0 to $\Gamma_i - 1$. We next search all integers $\hat{n}_i$ from 0 to $\Gamma_1 - 1$. Also from the above proof of Lemma 3, we know that when $\hat{n}_i$ is fixed, its corresponding $\hat{n}_1$ in S_i is determined by (18) and denoted as $\hat{n}_1(\hat{n}_i)$. Then, similarly the pair $(\hat{n}_1(\hat{n}_i), \hat{n}_i)$ is evaluated under (6), and its minimum is searched among all $\hat{n}_i$ from 0 to $\Gamma_1 - 1$. We then find the minimum of these two minimums and let $(\bar{n}_{1,i}, \bar{n}_i)$ denote the element that minimizes the function in (6) over Ω_i. From Lemma 2, $(\bar{n}_{1,i}, \bar{n}_i) \in S_i$. Note that the total number of the searches in this case is $\Gamma_1 + \Gamma_i$.

After we have found an element $(\bar{n}_{1,i}, \bar{n}_i) \in S_i$ for each i with $2 \le i \le L$, we next show how to determine the folding integers n_i for $1 \le i \le L$. By Lemma 1, we know that $\bar{n}_{1,i}$ and n_1 have the same remainder, say $\xi_{1,i}$, for $2 \le i \le L$, i.e.,

$$\bar{n}_{1,i} = \xi_{1,i} \bmod \Gamma_i, \quad \text{and} \quad n_1 = \xi_{1,i} \bmod \Gamma_i. \tag{21}$$

Thus, from $\bar{n}_{1,i}$ we obtain the remainder $\xi_{1,i}$ of n_1 modulo Γ_i for each i with $2 \le i \le L$. This gives $L-1$ remainders of n_1 modulo Γ_i for $2 \le i \le L$. Therefore, n_1 can be determined by these remainders by using the conventional CRT [11], [12] if $n_1 < \Gamma_2 \cdots \Gamma_L = \gamma_1$ that is ensured by Theorem 1. Thus, we have

$$n_1 = \sum_{i=2}^{L} \xi_{1,i} b_i \frac{\gamma_1}{\Gamma_i} \tag{22}$$

where b_i is determined from

$$b_i \frac{\gamma_1}{\Gamma_i} = 1 \bmod \Gamma_i, \quad \text{for } 2 \le i \le L. \tag{23}$$

When folding integer n_1 is determined as above, we can obtain other folding integers n_i for $2 \le i \le L$ as follows. For each i with $2 \le i \le L$, from Lemma 1, we have

$$\frac{n_i - \bar{n}_i}{\Gamma_1} = \frac{n_1 - \bar{n}_{1,i}}{\Gamma_i}. \tag{24}$$

Thus, we have

$$n_i = \bar{n}_i + \frac{\Gamma_i}{\Gamma_1}(n_1 - \bar{n}_{1,i}). \tag{25}$$

When all the folding integers n_i for $1 \le i \le L$ are determined, the unknown integer N can be estimated as before in (11) with an estimate error upper bound (12).

We now compare the total numbers of searches needed for solving for n_i with $1 \le i \le L$ for the above three different methods. The total number of searches for region $[0, \gamma_1 - 1] \times [0, \gamma_i - 1]$ for S_i in (6) is

$$\gamma_1 \sum_{i=2}^{L} \gamma_i = \Gamma_2 \cdots \Gamma_L (\Gamma_1 \Gamma_3 \cdots \Gamma_L + \Gamma_1 \Gamma_2 \Gamma_4 \cdots \Gamma_L + \cdots + \Gamma_1 \Gamma_2 \cdots \Gamma_{L-1}) \tag{26}$$

which is in the order of $(L-1)\Gamma_i^{2(L-1)}$. The total number of searches for the region Ω_i' for $S_i' = S_i$ in (13) and (14) is

$$3\Gamma_1(\Gamma_2 + \Gamma_3 + \cdots + \Gamma_L) \tag{27}$$

which is in the order of $3(L-1)\Gamma_i^2$. The total number of searches for the above 1-D searching algorithm is

$$(L-1)\Gamma_1 + \Gamma_2 + \Gamma_3 + \cdots + \Gamma_L \tag{28}$$

which is in the order of $2(L-1)\Gamma_i$.

As an example, let us consider the case when $L = 3$ and three moduli are $M_1 = 27$, $M_2 = 36$, $M_3 = 45$, and $M = \gcd\{M_1, M_2, M_3\} = 9$. Thus, in this case, we have $\Gamma_1 = 3$, $\Gamma_2 = 4$, and $\Gamma_3 = 5$. The total number of searches in (26) is $\Gamma_1 \Gamma_2 \Gamma_3^2 + \Gamma_1 \Gamma_2^2 \Gamma_3 = 540$; the total number of searches in (27) is $3\Gamma_1(\Gamma_2 + \Gamma_3) = 81$; and the total number of searches in (28) is only $2\Gamma_1 + \Gamma_2 + \Gamma_3 = 15$ that is far less than the other two 2-D searching algorithms. This complexity reduction becomes even more significant when the parameters get larger.

IV. Application in Frequency Estimation From Undersampled Waveforms

CRT can be naturally applied to frequency estimation when a signal waveform is undersampled multiple times as discussed in [5], such as in sensor network applications. Let $f_0 = N$ Hz be an unknown frequency we are interested in a signal and it may be high. An analog signal is

$$y(t) = a \exp(j2\pi f_0 t) + w(t) \tag{29}$$

where a is a non-zero constant and $w(t)$ is an additive noise, and $y(t)$ is a received signal. For $i = 1, 2, \cdots, L$, let M_i Hz be the sampling frequencies and sampled signals are

$$y_i(n/M_i) = a \exp(j2\pi N n/M_i) + w(n/M_i) \tag{30}$$

and thus, the samples in T seconds, an observation time duration, are

$$y_i(n/M_i) = a \exp(j2\pi N n/M_i) + w(n/M_i), \quad 0 \le n < TM_i. \tag{31}$$

For the above single frequency signal, the M_i-point DFT of each of the above sampled signals may provide an estimation of the frequency $f_0 = N$ Hz. However, if the sampling frequency is smaller than the unknown frequency f_0, $M_i < N$, i.e., undersampling, then the M_i-point DFT only provides a folded frequency or remainder r_i of N mod M_i: $r_i = N \bmod M_i$, and this remainder r_i may be erroneous when the additive noise $w(n/M_i)$ is significant and/or the observation time duration T is short. Now the question is how to estimate the true frequency f_0 from these erroneous remainders, which is precisely the robust CRT problem discussed in this paper and our proposed robust CRT may provide a robust solution for this problem.

Note that in practice, there might be wraparound effects for the residues (that has been considered by some other methods as in [14]), leading to the fact that the condition in (10) does not always hold. Under this circumstance, the upper bound of the frequency estimation result in (12) cannot always be guaranteed. However, although our error estimate result may not hold occasionally when the residue errors do not satisfy the proposed

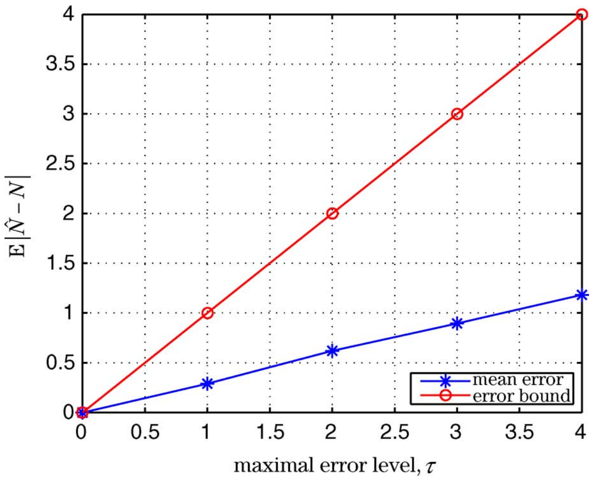


Fig. 1. Estimation errors and bound using the robust CRT for integers.

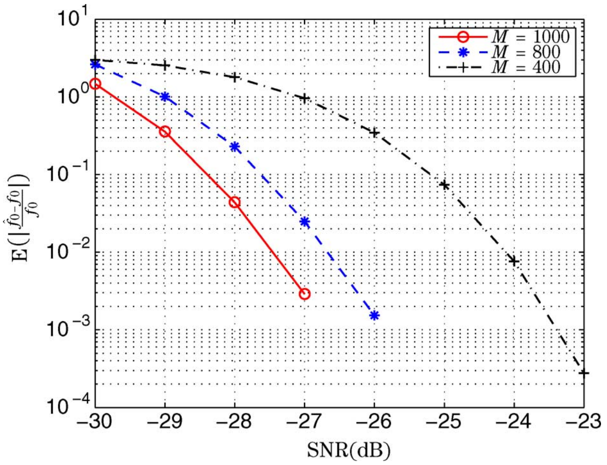


Fig. 2. Estimation error comparison in terms of different M, signal duration is 1 s.

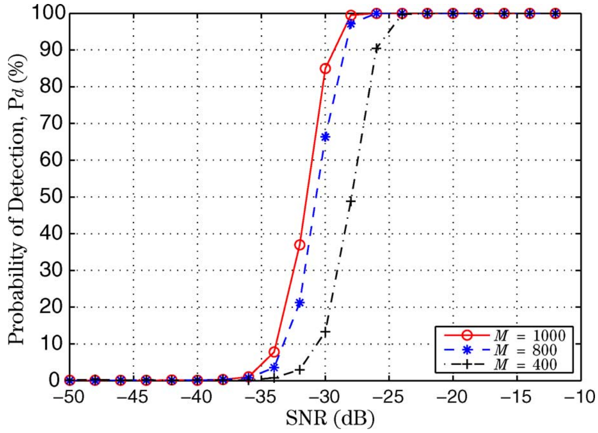


Fig. 3. Comparison of the probability of detection in terms of different M, signal duration is 1 s.

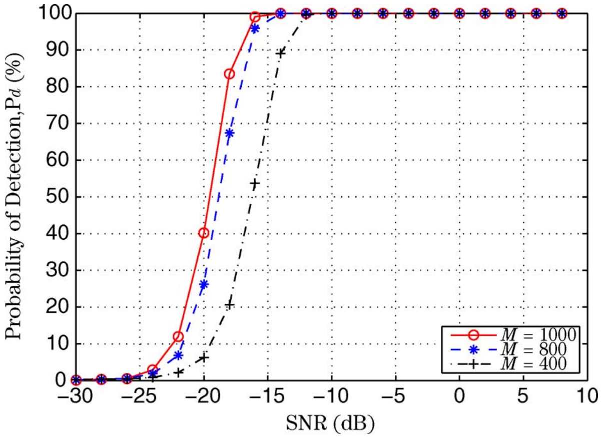


Fig. 4. Comparison of the probability of detection in terms of different M, signal duration is 0.05 s.

conditions, the estimation algorithm still applies as shown later in our simulations where more practical additive noises (rather than direct remainder errors) are considered.

We next show some simulation results to illustrate the robust CRT performance. We first evaluate the proposed robust CRT algorithm for integers.

Let us first consider the case when $M = 17, \Gamma_1 = 9, \Gamma_2 = 10, \Gamma_3 = 11$. In this case, according to Theorem 1, the maximal range of determinable N is 16 830 from (9) and the maximal error level τ is upper bounded by $\tau \leq 4$ from (10). In this simulation, the unknown integer N is chosen uniformly at random from the interval [0, 16 830). We consider the maximal remainder error levels $\tau = 0, 1, 2, 3, 4$, and 16 000 trials for each of them. The mean error $E(|N - \hat{N}|)$ between the estimated $\hat{N}$ and the true N is plotted by the solid line marked with $*$, and the estimation error upper bound (12) is plotted by the solid line marked with $\circ$ in Fig. 1. Clearly, one can see that the reconstruction errors of N from the erroneous remainders are small compared to the range of N.

For the application in frequency estimation, we set two sampling frequencies $M_1 = 17M$ Hz and $M_2 = 18M$ Hz, where three possibilities of M are considered: $M = 400, 800, 1000$. According to Theorem 1, these three different M give three different remainder error bounds $\tau = 100, 200, 250$, respectively, with that our robust CRT applies. Fig. 2 shows the mean relative error $E(|f_0 - \hat{f}_0|/|f_0|)$ between the true f_0 and its reconstruction $\hat{f}_0$ using the robust CRT for three $M = 400, 800, 1000$, respectively, where the x axis is the signal-to-noise ratio (SNR) in (29) and the observation time duration T is 1 s, and 120 000 trials for each SNR are implemented. In this figure, $f_0 = N$ is taken integers randomly and uniformly distributed in the range $[0, \mathrm{lcm}(M_1, M_2))$ for each M. The additive noise in this simulation is AWGN. The sampling rates are about 15 times less than the signal frequency.

In addition, we simulate the probability of detection, P_d, to illustrate the estimation accuracy, where we say that the frequency is correctly detected if the estimated frequency $\hat{f}_0$ is within 0.1% range, i.e., $|\hat{f}_0 - f_0| < f_0/1000 = 120\,\mathrm{Hz}$. In this simulation, we set $f_0 = N = 120\,\mathrm{kHz}$ and clearly this frequency falls in the range (9) where the smallest of the three in terms of M is $400 \times 17 \times 18 = 122\,400\,\mathrm{Hz}$, in Theorem 1. Fig. 3 shows the three P_d versus SNR curves for $M = 400, 800, 1000$, respectively, where the observation time T is 1 second. Fig. 4 shows the three P_d versus SNR curves for $M = 400, 800, 1000$, respectively, where the observation time T is 0.05 s, and in this case, if the number of samples is less than the DFT size, i.e., M_i, then zeros are padded to the end of the samples. In these two figures, 10 000 trials are implemented. One can see that the difference between Fig. 3 and Fig. 4 is basically an SNR shift due to the zero paddings.

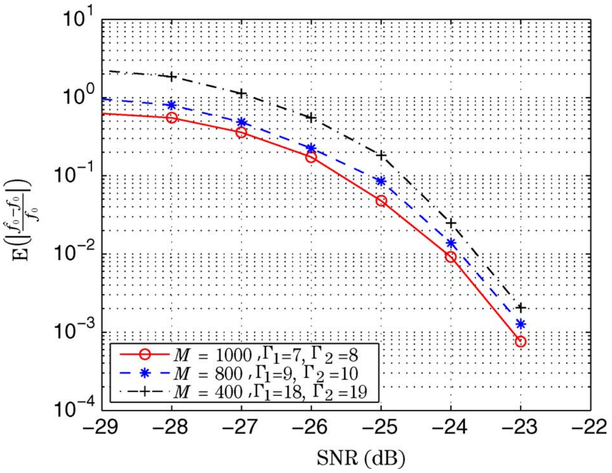


Fig. 5. Estimation error comparison in terms of different M, but similar sampling rates and the same number, 6000, of samples.

In the last simulation, we simulate the mean error curves similar to the ones in Fig. 2 but for the three curves, the sampling rates are similar and the numbers of the sampling points used are the same and all are 6000 samples. The DFT sizes are $M_i = M\Gamma_i$ and if they are larger than 6000, zeros are padded at the ends as before. The two sampling rates for the cases when $M = 400$, $M = 800$, and $M = 1000$ are $M_1 = 400 \times 18 = 7200$ Hz and $M_2 = 400 \times 19 = 7600$ Hz, $M_1 = 800 \times 9 = 7200$ Hz and $M_2 = 800 \times 10 = 8000$ Hz, and $M_1 = 1000 \times 7 = 7000$ Hz and $M_2 = 1000 \times 8 = 8000$ Hz, respectively. The mean error curves are shown in Fig. 5. From this figure, one can see that while other parameters are similar, the larger M is, the better the estimation error is, i.e., the better the performance is, which confirms our theory.

V. Conclusion

In this paper, we proposed a robust Chinese remainder theorem (robust CRT) that can robustly reconstruct a large integer from its smaller erroneous remainders modulo several moduli. Our robust CRT says that the reconstructed integer is within an error range that is the same as the error range of the remainder errors as long as the remainder error range is less than one quarter of the greatest common divisor (gcd) of all the moduli and the true integer to determine is less than the least common multiple (lcm) of all the moduli. We also proposed one fast 2-D implementation and another different fast 1-D search algorithm. We then applied the robust CRT to frequency estimation in multiple undersampled waveforms. We finally presented some simple simulations to illustrate the theory. We believe that the robust CRT proposed in this paper will have applications far beyond the frequency estimation from undersampled waveforms.

As a remark, this paper only considers single integer and single frequency determination. Multiple integers and multiple frequencies robust determination would be certainly interesting as a future research problem, where, for example, iterative estimations might be applicable. Note that multiple integers and multiple frequencies determination has been studied in [5] where only a few remainders/sets have errors and the reconstruction is accurate. Another interesting future research problem is how to deal with the wraparound effects as mentioned earlier in this paper.

Appendix I
Proof of Theorem 1

Proof: If the conditions in Theorem 1 are satisfied, it is not hard to see that the true solution n_i in (3) falls in the range $0 \le n_i < \gamma_i$ for $1 \le i \le L$. Thus, for any pair $(\bar{n}_1, \bar{n}_i) \in S_i$ for $2 \le i \le L$, we have

$$|\bar{n}_i M_i + \tilde{r}_i - \bar{n}_1 M_1 - \tilde{r}_1| \le |n_i M_i + \tilde{r}_i - n_1 M_1 - \tilde{r}_1|. \quad (32)$$

Let $\mu_i = \bar{n}_i - n_i$ for $1 \le i \le L$, and replace $\tilde{r}_i$ by $N - n_i M_i - \Delta r_i$ in both sides of (32) and we then have

$$|\mu_i M_i - \mu_1 M_1 - (\Delta r_i - \Delta r_1)| \le |\Delta r_i - \Delta r_1|. \quad (33)$$

Therefore, according to (2) and (10), we have

$$\begin{aligned} |\mu_i M_i - \mu_1 M_1| &\le 2|\Delta r_i - \Delta r_1| \\ &\le 2\left(|\Delta r_i| + |\Delta r_1|\right) \\ &\le 4\tau < M. \end{aligned} \quad (34)$$

Dividing M in both sides of (34), we have

$$|\mu_i \Gamma_i - \mu_1 \Gamma_1| < 1. \quad (35)$$

Since μ_i, Γ_i, μ_1, and Γ_1 are all integers, (35) implies

$$\mu_i \Gamma_i = \mu_1 \Gamma_1, \text{ for } i = 2, 3, \dots, L. \quad (36)$$

Since Γ_i and Γ_1 are co-prime for $2 \le i \le L$, we have

$$\mu_1 = h\Gamma_i \text{ and } \mu_i = h\Gamma_1, \text{ i.e., } \bar{n}_1 = n_1 + h\Gamma_i \text{ and } \bar{n}_i = n_i + h\Gamma_1 \quad (37)$$

for integer h with $|h| < \min(\gamma_i, \gamma_1)$. Replacing (37) into (32), we obtain

$$|\bar{n}_i M_i + \tilde{r}_i - \bar{n}_1 M_1 - \tilde{r}_1| = |n_i M_i + \tilde{r}_i - n_1 M_1 - \tilde{r}_1| \quad (38)$$

which implies $(n_1, n_i) \in S_i$ for $i = 2, 3, \dots, L$. This proves $n_1 \in S$. We next show $S = \{n_1\}$. Property (37) also implies

$$\begin{aligned} S_i = \{&(n_1 + h\Gamma_i, n_i + h\Gamma_1) : \\ &\text{for integers } h \text{ with } |h| < \min(\gamma_i, \gamma_1)\}. \end{aligned} \quad (39)$$

If $\bar{n}_1 \in S$, then $\bar{n}_1 \in S_{i,1}$ for $i = 2, 3, \dots, L$, and therefore, according to the definition of $S_{i,1}$ in (6) and (39), we have $\bar{n}_1 - n_1 = h\Gamma_i$ for some integer h with $|h| < \min(\gamma_i, \gamma_1)$ for $i = 2, 3, \dots L$. This implies that $\bar{n}_1 - n_1$ is divisible by all Γ_i for $i = 2, 3, \dots, L$, and thus is a multiple of the product of Γ_i, $i = 2, 3, \dots, L$, i.e., a multiple of γ_1. Since $0 \le \bar{n}_1, n_1 \le \gamma_1 - 1$, we can conclude $\bar{n}_1 - n_1 = 0$. This proves that $S = \{n_1\}$. In the meantime, $\bar{n}_1 = n_1$ implies $h = 0$ in (39), i.e., $\bar{n}_i = n_i$ for $i = 2, 3, \dots, L$. Hence, Theorem 1 is proved. ■

Appendix II
Proof of (16)

Proof: If $L(\bar{n}_1, \bar{n}_i) \ge M_1/2$, we then have the following four cases.

Case A. If $\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i > M_1/2$, then we have the following two subcases.

Subcase i. If $\bar{n}_1 = 0$, from the assumption

$$\tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i > M_1/2$$

we have

$$\begin{aligned}0 \le \bar{n}_i &< \frac{(\tilde{r}_1-\tilde{r}_i)-M_1/2}{M_i}\\ &< \frac{M_1-M_1/2}{M_i} = \Gamma_1/2\Gamma_i < 1/2\end{aligned} \tag{40}$$

which leads to $\bar{n}_i = 0$. Thus, from $1 \le \delta_i < \Gamma_1$ in (19), i.e., $M \le M\delta_i < M_1$, we have

$$\begin{aligned}&L(\bar{n}_1+\eta_i, \bar{n}_i+1)\\ &\quad = L(\eta_i, 1)\\ &\quad = |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i - M\delta_i|\\ &\quad < |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i|\\ &\quad = L(\bar{n}_1, \bar{n}_i).\end{aligned} \tag{41}$$

Also, $0 \le \bar{n}_1 + \eta_i = \eta_i < \Gamma_i \le \gamma_1$. Therefore, (41) contradicts with the definition of $(\bar{n}_1, \bar{n}_i) \in S_i$.

Subcase ii. If $\bar{n}_1 \ne 0$, we have

$$\begin{aligned}L(\bar{n}_1-1, \bar{n}_i) &= |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i - M_1|\\ &< |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i|\\ &= L(\bar{n}_1, \bar{n}_i),\end{aligned} \tag{42}$$

and $0 \le \bar{n}_1 - 1 \le \gamma_1 - 1$. This contradicts with the definition of $(\bar{n}_1, \bar{n}_i) \in S_i$.

Case B. If $\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i = M_1/2$, we have the following two subcases.

Subcase i. If $\bar{n}_1 = 0$, from the assumption

$$\tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i = M_1/2,$$

we have

$$\begin{aligned}0 \le \bar{n}_i &= \frac{(\tilde{r}_1-\tilde{r}_i)-M_1/2}{M_i}\\ &< \frac{M_1-M_1/2}{M_i} = \Gamma_1/2\Gamma_i < 1/2\end{aligned} \tag{43}$$

which leads to $\bar{n}_i = 0$. Then, similar to Subcase i in the previous Case A, we have

$$\begin{aligned}&L(\bar{n}_1+\eta_i, \bar{n}_i+1)\\ &\quad = L(\eta_i, 1)\\ &\quad = |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i - M\delta_i| < M_1/2\\ &\quad = |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i|\\ &\quad = L(\bar{n}_1, \bar{n}_i),\end{aligned} \tag{44}$$

and $0 \le \bar{n}_1 + \eta_i = \eta_i < \Gamma_i \le \gamma_1$. Therefore, (44) contradicts with the definition of $(\bar{n}_1, \bar{n}_i) \in S_i$.

Subcase ii. If $\bar{n}_1 \ne 0$, we have

$$\begin{aligned}L(\bar{n}_1-1, \bar{n}_i) &= |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i - M_1|\\ &= M_1/2\\ &= |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i|\\ &= L(\bar{n}_1, \bar{n}_i),\end{aligned} \tag{45}$$

and $0 \le \bar{n}_1 - 1 \le \gamma_1 - 1$. This means that $(\bar{n}_1 - 1, \bar{n}_i) \in S_i$. From Lemma 1, $\bar{n}_1 - (\bar{n}_1 - 1) = m_i\Gamma_i$ for some integer m_i, i.e., $1 = m_i\Gamma_i$ for some integer m_i, which is impossible.

Case C. If $\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i < -M_1/2$, we then have the following two subcases.

Subcase i. If $\bar{n}_1 = \gamma_1 - 1$, from the assumption

$$(\gamma_1 - 1)M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i < -M_1/2,$$

we have

$$\begin{aligned}\bar{n}_i &> \frac{(\gamma_1-1)M_1 + (\tilde{r}_1-\tilde{r}_i)+M_1/2}{M_i}\\ &> \frac{\gamma_1 M_1 - M_i - M_1/2}{M_i}\\ &= \gamma_i - 1 - \Gamma_1/2\Gamma_i > \gamma_i - 3/2.\end{aligned}$$

Since $\bar{n}_i$ is an integer, we thus have $\bar{n}_i \ge \gamma_i - 1 \ge 1$. Similar to Subcase i in Case A,

$$\begin{aligned}&L(\bar{n}_1-\eta_i, \bar{n}_i-1)\\ &\quad = |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i + M\delta_i|\\ &\quad < |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i|\\ &\quad = L(\bar{n}_1, \bar{n}_i).\end{aligned} \tag{46}$$

Also, $\bar{n}_1 - \eta_i = \gamma_1 - 1 - \eta_i \ge 0$. Thus, $0 \le \bar{n}_1 - \eta_i \le \gamma_1 - 1$ and $0 \le \bar{n}_i - 1 \le \gamma_i - 1$. This contradicts with the definition of $(\bar{n}_1, \bar{n}_i) \in S_i$.

Subcase ii. If $\bar{n}_1 \ne \gamma_1 - 1$, we have

$$\begin{aligned}L(\bar{n}_1+1, \bar{n}_i) &= |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i + M_1|\\ &< |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i| = L(\bar{n}_1, \bar{n}_i),\end{aligned} \tag{47}$$

and $0 \le \bar{n}_1 + 1 \le \gamma_1 - 1$. This contradicts with the definition of $(\bar{n}_1, \bar{n}_i) \in S_i$.

Case D. If $\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i = -M_1/2$, we have the following two subcases.

Subcase i. If $\bar{n}_1 = \gamma_1 - 1$, from the assumption

$$(\gamma_1 - 1)M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i = -M_1/2,$$

we have

$$\begin{aligned}\bar{n}_i &= \frac{(\gamma_1-1)M_1 + (\tilde{r}_1-\tilde{r}_i)+M_1/2}{M_i}\\ &> \frac{\gamma_1 M_1 - M_i - M_1/2}{M_i}\\ &= \gamma_i - 1 - \Gamma_1/2\Gamma_i > \gamma_i - 3/2.\end{aligned}$$

Since $\bar{n}_i$ is an integer, we thus have $\bar{n}_i \ge \gamma_i - 1 \ge 1$. Similar to Subcase i in Case C,

$$\begin{aligned}&L(\bar{n}_1-\eta_i, \bar{n}_i-1)\\ &\quad = |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i + M\delta_i|\\ &\quad < |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i|\\ &\quad = L(\bar{n}_1, \bar{n}_i),\end{aligned} \tag{48}$$

and it contradicts with the definition of $(\bar{n}_1, \bar{n}_i) \in S_i$.

Subcase ii. If $\bar{n}_1 \neq \gamma_1 - 1$, we have

$$\begin{aligned} &L(\bar{n}_1+1,\bar{n}_i) \\ &\quad= |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i + M_1| \\ &\quad= M_1/2 = |\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i| \\ &\quad= L(\bar{n}_1,\bar{n}_i), \end{aligned} \tag{49}$$

and $0 \le \bar{n}_1 + 1 \le \gamma_1 - 1$. This implies $(\bar{n}_1+1,\bar{n}_i) \in S_i$. From Lemma 1, $\bar{n}_1 + 1 - \bar{n}_1 = m_i\Gamma_i$ for some integer m_i, i.e., $1 = m_i\Gamma_i$ for some integer m_i, which is impossible.

By summarizing the above four cases, (16) is proved. ■

Appendix III
Proof of (20)

Proof: If $L(\bar{n}_1,\bar{n}_i) > (M\delta_i/2)$, then we have the following two cases.

Case A. If $\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i > (M\delta_i/2)$, we then have the following two subcases.

Subcase i. If $\bar{n}_1 + \eta_i \le \gamma_1 - 2$, i.e., $\bar{n}_1 \le \gamma_1 - \eta_i - 2$, then, from $\Gamma_i = \eta_i\Gamma_1 + \delta_i$, we have

$$\begin{aligned} &L(\bar{n}_1+\eta_i,\bar{n}_i+1) \\ &\quad= |(\bar{n}_1+\eta_i)M_1 + \tilde{r}_1 - (\bar{n}_i+1)M_i - \tilde{r}_i| \\ &\quad= |(\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i) - M\delta_i| \\ &\quad< |(\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i)| \\ &\quad= L(\bar{n}_1,\bar{n}_i), \end{aligned} \tag{50}$$

and $0 \le \bar{n}_1 + \eta_i \le \gamma_1 - 1$. We next show $\bar{n}_i + 1 \le \gamma_i - 1$, i.e., $\bar{n}_i \neq \gamma_i - 1$. This is true, since otherwise

$$\begin{aligned} &(\bar{n}_1 M_1 + \tilde{r}_1) - (\bar{n}_i M_i + \tilde{r}_i) \\ &\quad< (\gamma_1 - \eta_i - 2)M_1 + M_1 - (\gamma_i - 1)M_i \\ &\quad= M_i - M_1\eta_i - M_1 = M\delta_i - M_1 < M\delta_i/2, \end{aligned}$$

which contradicts with the assumption of the above Case A. Thus, (50) contradicts with the definition of $(\bar{n}_1,\bar{n}_i) \in S_i$.

Subcase ii. If $\bar{n}_1 + \eta_i \ge \gamma_1 - 1$, i.e., $\bar{n}_1 \ge \gamma_1 - \eta_i - 1$, we have

$$\begin{aligned} &L(\bar{n}_1+\eta_i-\Gamma_i,\bar{n}_i+1-\Gamma_1) \\ &\qquad= L(\bar{n}_1+\eta_i,\bar{n}_i+1) < L(\bar{n}_1,\bar{n}_i). \end{aligned} \tag{51}$$

Also, $\bar{n}_1 + \eta_i - \Gamma_i < \bar{n}_1 + \Gamma_i/\Gamma_1 - \Gamma_i < \bar{n}_1 \le \gamma_1 - 1$ and $\bar{n}_1 + \eta_i - \Gamma_i \ge \gamma_1 - 1 - \Gamma_i \ge 0$, where $\gamma_1 - 1 - \Gamma_i \ge 0$ is because $L \ge 3$. This proves $0 \le \bar{n}_1 + \eta_i - \Gamma_i \le \gamma_1 - 1$. In the meantime, $\bar{n}_i + 1 - \Gamma_1 < \bar{n}_i \le \gamma_i - 1$. We next show $\bar{n}_i + 1 - \Gamma_1 \ge 0$, i.e., $\bar{n}_i \ge \Gamma_1 - 1$. From (16), we have $\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i < M_1/2$. Thus,

$$\begin{aligned} \bar{n}_i &> \frac{\bar{n}_1 M_1 + \tilde{r}_1 - \tilde{r}_i - M_1/2}{M_i} \\ &> \frac{(\gamma_1 - \eta_i - 1)M_1 - M_i - M_1/2}{M_i} \\ &= \gamma_i - \frac{(M_i - M\delta_i) + M_i + 3M_1/2}{M_i} \\ &= \gamma_i - 2 + \delta_i/\Gamma_i - 3\Gamma_1/2\Gamma_i \\ &> \gamma_i - 2 - 3/2 = \gamma_i - 7/2, \end{aligned}$$

which implies $\bar{n}_i \ge \gamma_i - 3 \ge \Gamma_1 - 1$, where $\gamma_i - 3 \ge \Gamma_1 - 1$ is because $L \ge 3$. Thus, $0 \le \bar{n}_i + 1 - \Gamma_1 \le \gamma_i - 1$ and (51) contradicts with the definition of $(\bar{n}_1,\bar{n}_i) \in S_i$.

Case B. If $\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i < -(M\delta_i/2)$, we then have the following two subcases.

Subcase i. If $\bar{n}_1 - \eta_i \le 0$, i.e., $\bar{n}_1 \le \eta_i$, we have

$$\begin{aligned} &L(\bar{n}_1-\eta_i+\Gamma_i,\bar{n}_i-1+\Gamma_1) \\ &\quad= L(\bar{n}_1-\eta_i,\bar{n}_i-1) \\ &\quad= |(\bar{n}_1-\eta_i)M_1 + \tilde{r}_1 - (\bar{n}_i-1)M_i - \tilde{r}_i| \\ &\quad= |(\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i) + M\delta_i| \\ &\quad< |(\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i)| = L(\bar{n}_1,\bar{n}_i), \end{aligned} \tag{52}$$

and $0 \le \bar{n}_1 - \eta_i + \Gamma_i \le \gamma_1 - 1$. We now show

$$\bar{n}_i - 1 + \Gamma_1 \le \gamma_i - 1,$$

i.e., $\bar{n}_i \le \gamma_i - \Gamma_1$. This is true, since from (16), $\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i > -M_1/2$, and thus we have

$$\begin{aligned} \bar{n}_i &< \frac{\bar{n}_1 M_1 + \tilde{r}_1 - \tilde{r}_i + M_1/2}{M_i} < \frac{\eta_i M_1 + M_1 + M_1/2}{M_i} \\ &= \frac{(M_i - M\delta_i) + 3M_1/2}{M_i} = 1 + \frac{3\Gamma_1 - 2\delta_i}{2\Gamma_i} \\ &< 1 + 3/2 = 5/2, \end{aligned}$$

which means $\bar{n}_i \le 2 \le \gamma_i - \Gamma_1$, where $2 \le \gamma_i - \Gamma_1$ is because $L \ge 3$. Also, it is clear that $\bar{n}_i - 1 + \Gamma_1 \ge 0$. Therefore, (52) contradicts with the definition of $(\bar{n}_1,\bar{n}_i) \in S_i$.

Subcase ii. If $\bar{n}_1 - \eta_i \ge 1$, i.e., $\bar{n}_1 \ge \eta_i + 1$, we have

$$\begin{aligned} L(\bar{n}_1-\eta_i,\bar{n}_i-1) = {} & |(\bar{n}_1-\eta_i)M_1 \\ & < +\tilde{r}_1 - (\bar{n}_i-1)M_i - \tilde{r}_i|\ L(\bar{n}_1,\bar{n}_i), \end{aligned} \tag{53}$$

where the reason why the last inequality holds is the same as that in (52). We also have $0 \le \bar{n}_1 - \eta_i \le \gamma_1 - 1$. We next show $0 \le \bar{n}_i - 1$, i.e., $\bar{n}_i \ge 1$. If $\bar{n}_i = 0$, we then have

$$\begin{aligned} &\bar{n}_1 M_1 + \tilde{r}_1 - \bar{n}_i M_i - \tilde{r}_i \\ &\quad\ge (\eta_i + 1)M_1 + 0 - 0 - (M_i - 1) \\ &\quad= \eta_i M_1 - M_i + M_1 + 1 \\ &\quad= M_1 - M\delta_i + 1 = M(\Gamma_1 - \delta_i) + 1 \\ &\quad\ge M + 1 > -M\delta_i/2, \end{aligned}$$

which contradicts with the assumption of Case B. Thus, $0 \le \bar{n}_i - 1 \le \gamma_i - 1$. Therefore, (53) contradicts with the definition of $(\bar{n}_1,\bar{n}_i) \in S_i$.

By summarizing all the above cases, (20) is proved.

References

[1] G. Wang, X.-G. Xia, V. C. Chen, and R. L. Fiedler, "Detection, location, and imaging of fast moving targets using multifrequency antenna array SAR," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 40, no. 1, pp. 345–355, Jan. 2004.

[2] 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.

[3] G. Li, J. Xu, Y.-N. Peng, and X.-G. Xia, "An efficient implementation of robust phase-unwrapping algorithm," *IEEE Signal Process. Lett.*, vol. 14, pp. 393–396, Jun. 2007.

[4] X. Li and X.-G. Xia, "A fast robust Chinese remainder theorem based phase unwrapping algorithm," *IEEE Signal Process. Lett.*, vol. 15, pp. 665–668, Oct. 2008.

[5] 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, pp. 768–771, Nov. 2005.

[6] G. Li, J. Xu, Y.-N. Peng, and X.-G. Xia, "Moving target location and imaging using dual-speed velocity SAR," *IET Radar Sonar Navig.*, vol. 1, no. 2, pp. 158–163, 2007.

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

[8] W. Xu, E. C. Chang, L. K. Kwoh, H. Lim, and W. C. A. Heng, "Phase unwrapping of SAR interferogram with multi-frequency or multi-baseline," in *Proc. IGARSS*, 1994, pp. 730–732.

[9] D. P. Jorgensen, T. R. Shepherd, and A. S. Goldstein, "A dual-pulse repetition frequency scheme for mitigating velocity ambiguities of the NOAA P-3 airborne Doppler radar," *J. Atmos. Ocean. Technol.*, vol. 17, no. 5, pp. 585–594, May 2000.

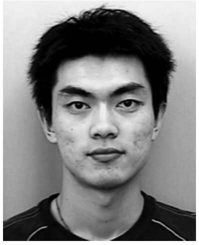
[10] M. Ruegg, E. Meier, and D Nuesch, "Capabilities of dual-frequency millimeter wave SAR with monopulse processing for ground moving target indication," *IEEE Trans. Geosci. Remote Sens.*, vol. 45, no. 3, pp. 539–553, Mar. 2007.

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

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

[13] O. Goldreich, D. Ron, and M. Sudan, "Chinese remaindering with errors," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 1330–1338, Jul. 2000.

[14] I. E. Shparlinski and R. Steinfeld, "Noisy Chinese remaindering in the Lee norm," *J. Complex.*, vol. 20, pp. 423–437, 2004.



Xiaowei Li was born in Hubei, China. He received the B.S. degree from Wuhan University, Wuhan, China, in 2004, and the M.S. degree in electrical engineering from Institute of Electronics, Chinese Academy of Sciences, Beijing, China, in 2007. He is currently working towards the Ph.D. degree in electrical engineering at the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE.

His current research interests lie in the area of signal and image processing, including target detection, sensor array signal processing in radar system, and SAR imaging of maneuvering targets.

Hong Liang received the M.S. degree and the Ph.D. degree in signal and information processing from Northwestern Polytechnical University (NPU), Xi'an, China, in 1995 and 2004, respectively.

Currently, she is an Associate Professor at NPU. In 2008, she was with the Department of Electrical and Computer Engineering, University of Delaware, Newark, as a Visiting Professor. Her main research interests include signal detection, parameter estimation, and adaptive signal processing.

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

He was a Senior/Research Staff Member 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. He was a Visiting Professor at the Chinese University of Hong Kong during 2002–2003, where he is an Adjunct Professor. Before 1995, he held visiting positions in a few institutions. His current research interests include space-time coding, MIMO and OFDM systems, digital signal processing, and SAR and ISAR imaging. He has over 185 refereed journal articles published and accepted and seven U.S. patents awarded and 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 an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON SIGNAL PROCESSING, the *Signal Processing (EURASIP)*, and the *Journal of Communications and Networks* (JCN). He was a Guest Editor of Space-Time Coding and Its Applications in the *EURASIP Journal of Applied Signal Processing* in 2002. He served as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING during 1996 to 2003, the IEEE TRANSACTIONS ON MOBILE COMPUTING during 2001 to 2004, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY during 2005 to 2008, the IEEE SIGNAL PROCESSING LETTERS during 2003 to 2007, and the *EURASIP Journal of Applied Signal Processing* during 2001 to 2004. He served as a Member of the Signal Processing for Communications Committee from 2000 to 2005 and is currently a Member of the Sensor Array and Multichannel (SAM) Technical Committee (from 2004) in the IEEE Signal Processing Society. He has served as IEEE Sensors Council Representative of IEEE Signal Processing Society since 2002 and served as the Representative of IEEE Signal Processing Society to the Steering Committee for IEEE TRANSACTIONS ON MOBILE COMPUTING during 2005 to 2006. He is Technical Program Chair of the Signal Processing Symposium, the IEEE GLOBECOM 2007 in Washington DC, and the General Co-Chair of the International Conference of Acoustics, Speech and Signal Processing (ICASSP) 2005 in Philadelphia, PA.