A Closed-Form Robust Chinese Remainder Theorem and Its Performance Analysis

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

***Abstract*—Chinese remainder theorem (CRT) reconstructs an integer from its multiple remainders that is well-known not robust in the sense that a small error in a remainder may cause a large error in the reconstruction. A robust CRT has been recently proposed when all the moduli have a common factor and the robust CRT is a searching based algorithm and no closed-from is given. In this paper, a closed-form robust CRT is proposed and a necessary and sufficient condition on the remainder errors for the closed-form robust CRT to hold is obtained. Furthermore, its performance analysis is given. It is shown that the reason for the robustness is from the remainder differential process in both searching based and our proposed closed-form robust CRT algorithms, which does no exist in the traditional CRT. We also propose an improved version of the closed-form robust CRT. Finally, we compare the performances of the traditional CRT, the searching based robust CRT and our proposed closed-form robust CRT (and its improved version) algorithms in terms of both theoretical analysis and numerical simulations. The results demonstrate that the proposed closed-form robust CRT (its improved version has the best performance) has the same performance but much simpler form than the searching based robust CRT.**

***Index Terms*—Chinese remainder theorem (CRT), phase unwrapping, radar signal processing, robustness.**

I. Introduction

CHINESE remainder theorem (CRT) [1], [2] tells that a positive integer N can be uniquely reconstructed from its remainders modulo L positive integers, $M_1, M_2, \ldots, M_L$, if $N < \text{lcm}\{M_1, M_2, \ldots, M_L\}$ where lcm stands for the least common multiple, and furthermore it provides a simple reconstruction formula if all moduli M_i are co-prime. CRT has numerous applications in, such as, cryptography [2], channel coding [4], [5], signal processing [1], [6], [8], [21], and radar systems [9]–[20]. CRT is, however, well known not robust, i.e., a small error from any remainder may cause a large reconstruction error. In order to resist remainder errors, two kinds of methods are proposed in the literature, i.e., remainder number redundancy methods [4]–[6] and remainder redundancy methods [8]–[10], [18], [20]. The first kind of methods are based on the fact that if we pick $K > L$ co-prime integers $M_1 < M_2 < \cdots < M_K$ and $N < M_1 M_2 \cdots M_L$, then N can be uniquely recovered by any L of the K remainders and errors in the remaining $K - L$ remainders may be corrected. The K remainders form a redundant representation of N. Note that the solution of N from this kind of methods is accurate but only a few of the remainders are allowed to have errors and most of the remainders have to be error-free. In the classical CRT, the greatest common divisor (gcd) of any pair M_i and M_j for $i \neq j$ is 1. In the second kind of methods, the gcd is assumed to be M. This kind of methods are that if all the moduli M_i have a common gcd $M > 1$, then the solution of N is robust to the remainder errors, if $N < \text{lcm}\{M_1, M_2, \ldots, M_L\} = M_1 M_2 \cdots M_L / M^{L-1}$ and the remainder error level is less than $M/4$. In these methods, the redundancy exists in each remainder value, $r_i = N \bmod M_i$, which will be seen clearly later. Note that the solution from this kind of methods may not be accurate but robust to the remainder errors and all the remainders are allowed to have errors that may not be too large. In terms of channel coding applications, the first kind methods fit well, while in terms of signal processing applications including radar signal processing, the second kind methods may suit better since all remainders may have small errors in the applications. A different probabilistic approach to deal with noises in CRT is proposed in [7] where all the moduli are required to be primes.

In this paper, we are interested in the second kind error resistance of remainders in CRT, i.e., remainder redundancy method. As a remainder redundancy method, a searching based robust CRT has been recently proposed in [8], [9], where instead of the remainders r_i, their differentials $r_i - r_1$, $2 \leq i \leq L$, are used to determine integer N. This searching based robust CRT has been applied in robust phase unwrapping in radar systems in, for example, [15]–[20]. Although the original 2-D searching used in [9] is reduced to a 1-D searching in [8] and [10], they are still searching based and no closed-form solution is provided. In this paper, motivated from [9], [8], [10], we first propose a closed-form robust CRT where no searching is needed by also using the remainder differential process. We present a necessary and sufficient condition on the remainder errors for the closed-form robust CRT to hold. In fact, the robustness in

Manuscript received May 14, 2010; accepted August 05, 2010. Date of publication August 16, 2010; date of current version October 13, 2010. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Xiqi Gao. This work was done while W. Wang was visiting the Department of Electrical and Computer Engineering, University of Delaware, Newark. The work of W. Wang was supported in part by the NSFC (Grants 60772095 and 60971113) and the Foundation for Innovative Research Groups of the NSFC (Grant 60921003). The work of X.-G. Xia was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-08-1-0219 and the World Class University (WCU) Program 2008-000-20014-0, National Research Foundation, Korea.

W. Wang is with the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, Shaanxi, China (e-mail: wjwang@xjtu.edu.cn).

X.-G. Xia is with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA, and also with the Institute of Information and Communication, Chonbuk National University, Jeonju 561-756, Korea (e-mail: xxia@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.2010.2066974

[9], [8], [10] and this paper is due to the differential process that is not involved in the traditional CRT. However, it is known that the differential process, $r_i - r_1$, increases the noise variances for all i. Considering that the above reference remainder r_1 is arbitrarily selected, we can reduce the noise variance by properly/optimally selecting the reference remainder. Based on this idea, we then propose an improved robust CRT. We also obtain the theoretical performance analysis for both closed-form robust CRT and its improved version. Finally, we compare the performances of the traditional CRT, the searching based robust CRT and our proposed closed-form robust CRT (and its improved version) algorithms in terms of both theoretical analysis and numerical simulations. The results show that the proposed closed-form robust CRT (its improved version has the best performance) has the same performance but much simpler form than the searching based robust CRT.

The remaining of this paper is organized as follows. In Section II, we first briefly introduce the traditional CRT and analyze the reason why they are not robust. We also briefly describe the searching based robust CRT obtained in [8]. In Section III, we present a closed-form robust CRT and derive a necessary and sufficient condition for the closed-form robust CRT to hold. In Section IV, we present an improved robust CRT and generalize it from integers to reals. In Section V, we present the performance analysis for our proposed algorithms. Lastly, in Section VI, we present some simulation results to compare the performances of the CRT, the searching based robust and the closed-form robust CRT (and its improved version) algorithms.

II. CRT and Searching Based Robust CRT

In this section, we first briefly describe the traditional CRT in the cases when all the moduli are co-prime and when all the moduli have a common factor. We then briefly describe the searching based robust CRT in [8] and [9].

A. The Conventional CRT and Its Noise Sensitivity

Let N be a positive integer, $0 < M_1 < M_2 < \cdots < M_L$ be L moduli, and $r_1, r_2, \ldots, r_L$ 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 $0 \le r_i < M_i$ and n_i is an unknown integer (called folding integer), for $1 \le i \le L$. It is not hard to see that N can be uniquely reconstructed from its L remainders if and only if $0 \le N < \text{lcm}\{M_1, M_2, \ldots, M_L\}$. If all the moduli M_i are co-prime, then CRT has a simple formula (we call it the classical CRT) [1], [2]. If any pair moduli M_i have gcd M (in this case, all the moduli have gcd M), then the CRT has the following general form (we call it the traditional CRT or simply CRT for convenience) [3].

Let

$$\Gamma_i = M_i/M, \ \ 1 \le i \le L. \tag{2}$$

Then, all $\Gamma_i, 1 \le i \le L$, are co-prime, i.e., the gcd of any pair Γ_i and Γ_j for $i \ne j$ is 1. Define $\Gamma \triangleq \Gamma_1 \Gamma_2 \cdots \Gamma_L$. For $1 \le i \le L$, let

$$\gamma_i \triangleq \Gamma_1 \cdots \Gamma_{i-1} \Gamma_{i+1} \cdots \Gamma_L = \Gamma/\Gamma_i. \tag{3}$$

Clearly, Γ_i and γ_i are co-prime, so the modular multiplicative inverse of γ_i modulo Γ_i exists, which is denoted by $\bar{\gamma}_i$, i.e.,

$$\bar{\gamma}_i \gamma_i \equiv 1 \bmod \Gamma_i \ \text{ or } \ \bar{\gamma}_i \gamma_i + k\Gamma_i = 1, \text{for some } k \in \mathbb{Z} \tag{4}$$

where $\mathbb{Z}$ denotes the set of integers. Define

$$q_i \triangleq \lfloor r_i/M \rfloor \tag{5}$$

where $\lfloor \cdot \rfloor$ denotes the flooring operation, and then

$$r_i = q_i M + r^c \tag{6}$$

where $r^c = N \bmod M$ is the common remainder of r_i modulo M for $1 \le i \le L$. Define

$$N_0 \triangleq \lfloor N/M \rfloor. \tag{7}$$

Then, according to the classical CRT formula, we have the following conclusion. If and only if $0 \le N_0 < \Gamma$, N_0 can be uniquely reconstructed as

$$N_0 = \sum_{i=1}^{L} \bar{\gamma}_i \gamma_i q_i \bmod \Gamma. \tag{8}$$

Therefore, N can be uniquely reconstructed by

$$N = M N_0 + r^c. \tag{9}$$

Now a natural question is what will happen to the above CRT when the remainders have errors. We next consider this problem. Let the ith erroneous remainder be

$$\hat{r}_i \triangleq r_i + \Delta r_i \tag{10}$$

where Δr_i denotes the error or noise and we assume $|\Delta r_i| \le \tau$, where τ is the maximal error level, called remainder error bound. In order to reconstruct N, from (8) and (9), we first need to determine q_i from the erroneous remainders $\hat{r}_i$ for $1 \le i \le L$. With these erroneous remainders, (5) becomes

$$\hat{q}_i = \lfloor \hat{r}_i/M \rfloor = \left\lfloor \frac{q_i M + r^c + \Delta r_i}{M} \right\rfloor = q_i + \left\lfloor \frac{r^c + \Delta r_i}{M} \right\rfloor. \tag{11}$$

If the remainder errors are constrained as

$$-r^c \le \Delta r_i < M - r^c, 1 \le i \le L \tag{12}$$

then $\hat{q}_i = q_i$ and N_0 can be accurately reconstructed by (8). Therefore, the unknown N can be estimated as

$$\begin{aligned}\hat{N} &= MN_0 + \left[\frac{1}{L}\sum_{i=1}^{L}\hat{r}_i - M\hat{q}_i\right] \\ &= MN_0 + r^c + \left[\frac{1}{L}\sum_{i=1}^{L}\Delta r_i\right] \\ &= N + \Delta\bar{r} \end{aligned} \tag{13}$$

where $\Delta\bar{r}$ is the average of the remainders errors, and $[\cdot]$ stands for the rounding integer, i.e., for any $x \in \mathbb{R}$, $[x]$ is an integer and subject to

$$-\frac{1}{2} \le x - [x] < \frac{1}{2}. \tag{14}$$

In fact, $[x] = \lfloor x + 0.5 \rfloor$. Clearly we have $|\hat{N} - N| \le \tau$. In this case, N_0 can be accurately reconstructed and we have a robust estimation of N. Now let us consider the condition (12) for the accurate determination of q_i. From this condition, we know that the probability to accurately determine q_i and therefore accurately determine N_0 is determined by r^c. Different r^c result in different remainder error resistance performances. For example, if $r^c = M - 1$, Δr_i needs to satisfy $-M + 1 \le \Delta r_i < 1$ to guarantee the accuracy of q_i. It is easy to see that if the distribution of $\Delta r_i, 1 \le i \le L$, is symmetrical with respect to 0, the correct probability of determining q_i is less than $1/2$ no matter how low the variance of Δr_i is. In other words, even though r_i has the minimal error level, i.e., $\Delta r_i = 1$, q_i can not be accurately determined in the case of $r^c = M - 1$. From (8), we know, as $\bar{\gamma}_i\gamma_i$ is usually a large integer, a small error in any q_i for $1 \le i \le L$ may cause a larger error in N_0 and then a large error in N. Hence, the above CRT is noise/error sensitive, i.e., not robust, which will be seen from our numerical results later.

B. Searching Based Robust CRT

To provide a robust solution for the above problem, a searching based robust algorithm (we call it searching based robust CRT) has been proposed in [8] and [9] that provides another way to reconstruct N from erroneous remainders, where the folding integers n_i, instead of q_i, are first determined. It is briefly described as follows.

With the erroneous remainders in (10), (1) becomes

$$\hat{N}(i) = n_i M_i + r_i + \Delta r_i, 1 \le i \le L. \tag{15}$$

When the folding integers n_i in (15) are accurately solved, the unknown parameter N can be estimated as

$$\hat{N} = \left[\frac{1}{L}\sum_{i=1}^{L}\hat{N}(i)\right] = N + \Delta\bar{r} \tag{16}$$

and thus $|\hat{N} - N| \le \tau$, i.e., $\hat{N}$ is a robust estimate of N. We now show how to accurately determine the folding integers n_i as in [8]. For each i with $2 \le i \le L$, define

$$S_i \triangleq \left\{(\bar{n}_1, \bar{n}_i) = \underset{\substack{0\le\hat{n}_1\le\gamma_1-1\\ 0\le\hat{n}_i\le\gamma_i-1}}{\arg\min} |\hat{n}_i M_i + \hat{r}_i - \hat{n}_1 M_1 - \hat{r}_1|\right\}. \tag{17}$$

Let $S_{i,1}$ denote the set of all the first components $\bar{n}_1$ of the pairs in set S_i, i.e.,

$$S_{i,1} \triangleq \{\bar{n}_1 | (\bar{n}_1, \bar{n}_i) \in S_i \text{ for some } \bar{n}_i\} \tag{18}$$

and define

$$S \triangleq \cap_{i=2}^{L} S_{i,1}. \tag{19}$$

It is proved in [8] that if the remainder error bound τ is less than a quarter of M, i.e., $\tau < M/4$, the folding integers $n_i, 1 \le i \le L$, can be accurately determined from S and S_i: Set S has one and only one element n_1 and if $(n_1, k) \in S_i$ then $n_i = k$. Recall that the remainder error bound $\tau = \max_{1\le i\le L}|\Delta r_i|$. Then, the estimate error of N is thus upper bounded by $|N - \hat{N}| \le \tau$. The above estimate error of N is due to the remainder errors Δr_i that has the maximal level τ, in other words, the reconstruction is robust.

According to (17), a 2-D searching process is needed to solve for n_i. In order to reduce the computational complexity, [8] has reduced the above 2-D to 1-D searching where the total number of searches is in the order of $2(L-1)\Gamma_i$. When L or Γ_i gets large, the computational complexity is still high.

III. A Closed-Form Robust CRT

Motivated from [9] and [8], we next present a closed-form algorithm to solve for n_i and thus robustly reconstruct N.

From the definition of N_0 in (7), we have $N_0 = n_i\Gamma_i + q_i$ for $1 \le i \le L$, which is the solution of the following system of simultaneous congruences:

$$\begin{cases} N_0 = n_1\Gamma_1 + q_1 \\ N_0 = n_2\Gamma_2 + q_2 \\ \quad\vdots \\ N_0 = n_L\Gamma_L + q_L. \end{cases} \tag{20}$$

Unlike the traditional CRT, which directly reconstructs N_0 by solving the above system of simultaneous congruences, we first determine n_i for $1 \le i \le L$. To do so, we let the last $L - 1$ equations in (20) subtract the first one and we then have

$$\begin{cases} n_1\Gamma_1 - n_2\Gamma_2 = q_{2,1} \\ n_1\Gamma_1 - n_3\Gamma_3 = q_{3,1} \\ \quad\vdots \\ n_1\Gamma_1 - n_L\Gamma_L = q_{L,1} \end{cases} \tag{21}$$

where $q_{i,1} \triangleq q_i - q_1$ for $2 \le i \le L$. Note that in the above differences (or differentials) we arbitrarily select the first equation (or remainder) to be a reference to subtract. In next section, we

will show how to improve the performance by selecting a proper reference equation (or remainder) to differentiate.

As N_0 and n_i for $1 \le i \le L$ are a solution of (20), obviously, n_i for $1 \le i \le L$ are also a solution of (21). Assume $(\tilde{n}_1, \tilde{n}_i)$ is a solution pair of the $(i-1)$th equation in (21) for $2 \le i \le L$, we have the following lemma.

Lemma 1: Consider Equation $i-1$ in (21), $2 \le i \le L$. If Γ_i and Γ_1 are co-prime, then $(\tilde{n}_1, \tilde{n}_i)$ has the following form:

$$\begin{cases} \tilde{n}_1 = q_{i,1}\bar{\Gamma}_{i,1} + kq_{i,1}\Gamma_i \\ \tilde{n}_i = \frac{q_{i,1}\bar{\Gamma}_{i,1}\Gamma_1 - q_{i,1}}{\Gamma_i} + kq_{i,1}\Gamma_1 \end{cases} \tag{22}$$

where $k \in \mathbb{Z}$ and $\bar{\Gamma}_{i,1}$ is the modular multiplicative inverse of Γ_1 modulo Γ_i.

Proof: Considering the following Bézout's identity:

$$x\Gamma_1 + y\Gamma_i = 1 \tag{23}$$

since Γ_i and Γ_1 are co-prime, by Bézout's lemma we know that (23) has integer solutions and the modular multiplicative inverse of Γ_1 modulo Γ_i, i.e., $\bar{\Gamma}_{i,1}$, is a solution of x. However, the solution of x is not unique and the other solutions of x are given by $\bar{\Gamma}_{i,1} + k\Gamma_i$ for $k \in \mathbb{Z}$. Therefore, the solutions of y are given by $(1 - \bar{\Gamma}_{i,1}\Gamma_1)/(\Gamma_i) - k\Gamma_1$ for $k \in \mathbb{Z}$.

Now, we consider the $(i-1)$th equation in (21), $2 \le i \le L$. Multiplying both sides of (23) by $q_{i,1}$ and substituting $q_{i,1}x$ and $q_{i,1}y$ by $\tilde{n}_1$ and $-\tilde{n}_i$, respectively, (23) then becomes the $(i-1)$th equation in (21). Therefore, $\tilde{n}_1 = q_{i,1}x$ and $\tilde{n}_i = -q_{i,1}y$, i.e., (22) are the pairs of solutions of Equation $i-1$ in (21). ■

From Lemma 1 we know the $(i-1)$th equation in (21) has multiple solutions. As (21) has fewer equations than unknown variables, it seems to have multiple solutions too. We next show as n_i for $1 \le i \le L$ are all constrained to be integers, they can be uniquely solved by the following algorithm.

Clearly, we can use $[(\hat{r}_i - \hat{r}_1)/M]$ as an estimate of $q_{i,1}$, i.e.,

$$\hat{q}_{i,1} = \left[\frac{\hat{r}_i - \hat{r}_1}{M}\right], 2 \le i \le L. \tag{24}$$

Recall that $[\cdot]$ stands for the rounding integer which is defined in (14). Let $\hat{n}_i$ for $1 \le i \le L$ denote a set of solution of (21) when $q_{i,1}$ is replaced by $\hat{q}_{i,1}$ for $2 \le i \le L$. We have the following algorithm.

Closed-Form Robust Chinese Remainder Theorem Algorithm:

- **Step 1**: Calculate $\hat{q}_{i,1}$ for $2 \le i \le L$ in (24) from given erroneous remainders $\hat{r}_i$ for $1 \le i \le L$.
- **Step 2**: Calculate the remainder of $\hat{q}_{i,1}\bar{\Gamma}_{i,1}$ modulo Γ_i:

$$\hat{\xi}_{i,1} = \hat{q}_{i,1}\bar{\Gamma}_{i,1} \bmod \Gamma_i$$

  for $2 \le i \le L$, where $\bar{\Gamma}_{i,1}$ is the modular multiplicative inverse of Γ_1 modulo Γ_i and can be calculated in advance.
- **Step 3**: Calculate $\hat{n}_1$:

$$\hat{n}_1 = \sum_{i=2}^{L} \hat{\xi}_{i,1} b_{i,1} \frac{\gamma_1}{\Gamma_i} \bmod \gamma_1 \tag{25}$$

  where $b_{i,1}$ is the modular multiplicative inverse of γ_1/Γ_i modulo Γ_i, which can be calculated in advance, and γ_1 is defined in (3).
- **Step 4**: Calculate $\hat{n}_i$ for $2 \le i \le L$:

$$\hat{n}_i = \frac{\hat{n}_1\Gamma_1 - \hat{q}_{i,1}}{\Gamma_i}. \tag{26}$$

Then, we have the following result.

Theorem 1: Assume that all Γ_i, for $1 \le i \le L$, are pairwisely co-prime and

$$0 \le N < \text{lcm}\,(M_1, M_2, \ldots, M_L) = M\Gamma_1\Gamma_2\cdots\Gamma_L = M\Gamma. \tag{27}$$

Then, $\hat{n}_i = n_i$ for all $1 \le i \le L$ if and only if

$$-M/2 \le \Delta r_i - \Delta r_1 < M/2, \text{ for all } 2 \le i \le L. \tag{28}$$

Proof: From (6), (10), and (24) we have

$$\hat{q}_{i,1} = q_{i,1} + \left[\frac{\Delta r_i - \Delta r_1}{M}\right], 2 \le i \le L. \tag{29}$$

We first prove the sufficiency. Considering the condition in (28) and the definition in (14), we have $[(\Delta r_i - \Delta r_1)/M] = 0$ and therefore $\hat{q}_{i,1} = q_{i,1}$. Then, from Lemma 1, n_1 and $\hat{q}_{i,1}\bar{\Gamma}_{i,1}$ have the same remainder modulo Γ_i. Since $\hat{q}_{i,1}\bar{\Gamma}_{i,1} \equiv \hat{\xi}_{i,1} \bmod \Gamma_i$, we have $n_1 \equiv \hat{\xi}_{i,1} \bmod \Gamma_i$ for $2 \le i \le L$, which forms another system of simultaneous congruences.

Considering $N < M\Gamma$ and $N = n_1M_1 + r_1$, we have $n_1 < \gamma_1$. Thus, according to the classical CRT, n_1 can be uniquely reconstructed by solving the above system of simultaneous congruences as (25). Hence, we have $\hat{n}_1 = n_1$.

After n_1 is determined, we can obtain other integers n_i for $2 \le i \le L$ by substituting n_1 back into (21) as (26). Therefore, $\hat{n}_i = n_i$, for $2 \le i \le L$. Hence, the sufficiency is proved.

We next prove the necessity. Assume there exists at least one remainder that does not satisfy (28), say, for example, the jth remainder, $2 \le j \le L$. Then, $[(\Delta r_j - \Delta r_1)/M] \ne 0$ and therefore $\hat{q}_{j,1} \ne q_{j,1}$. We then have the following two cases.

Case A: There exists one j with $2 \le j \le L$ such that $[(\Delta r_j - \Delta r_1)/M] \ne k\Gamma_j$ for any $k \in \mathbb{Z}$. We want to prove that the remainders of $\hat{q}_{j,1}\bar{\Gamma}_{j,1}$ and $q_{j,1}\bar{\Gamma}_{j,1}$ modulo Γ_j are different. Assume $\hat{q}_{j,1}\bar{\Gamma}_{j,1}$ and $q_{j,1}\bar{\Gamma}_{j,1}$ have the same remainder modulo Γ_j, i.e.,

$$\hat{q}_{j,1}\bar{\Gamma}_{j,1} - q_{j,1}\bar{\Gamma}_{j,1} = k\Gamma_j, \text{ for some } k \in \mathbb{Z}. \tag{30}$$

Multiplying both sides of (30) by Γ_1 and considering $\Gamma_1\bar{\Gamma}_{j,1} = 1 + k\Gamma_j$ for some $k \in \mathbb{Z}$, we have

$$\hat{q}_{j,1} - q_{j,1} = k\Gamma_j, \text{ for some } k \in \mathbb{Z}. \tag{31}$$

According to (29) we have

$$\left[\frac{\Delta r_j - \Delta r_1}{M}\right] = k\Gamma_j, \text{ for some } k \in \mathbb{Z}. \tag{32}$$

This contradicts with the assumption that $[(\Delta r_j - \Delta r_1)/M] \ne k\Gamma_j$ for any $k \in \mathbb{Z}$. Hence, the remainders of $\hat{q}_{j,1}\bar{\Gamma}_{j,1}$ and $q_{j,1}\bar{\Gamma}_{j,1}$ modulo Γ_j are different.

On the other hand, from Lemma 1, we have $n_1 \equiv q_{j,1}\bar{\Gamma}_{j,1} \bmod \Gamma_j$. From Step 2 and Step 3 in the algorithm, we know $\hat{n}_1 \equiv \hat{q}_{j,1}\bar{\Gamma}_{j,1} \bmod \Gamma_j$. Since we have just proved that the remainders of $\hat{q}_{j,1}\bar{\Gamma}_{j,1}$ and $q_{j,1}\bar{\Gamma}_{j,1}$ modulo Γ_j are different, hence, $\hat{n}_1 \neq n_1$.

Case B: For every i, $2 \leq i \leq L$, $[(\Delta r_i - \Delta r_1)/M] = k\Gamma_i$ for some $k \in \mathbb{Z}$ but there exists at least one j with $2 \leq j \leq L$ such that $[(\Delta r_j - \Delta r_1)/M] \neq 0$, i.e., $\hat{q}_{j,1} \neq q_{j,1}$.

From (29), we have $\hat{q}_{i,1}\bar{\Gamma}_{i,1} \equiv q_{i,1}\bar{\Gamma}_{i,1} \bmod \Gamma_i$ for $2 \leq i \leq L$. Then, from Lemma 1, n_1 and $\hat{q}_{i,1}\bar{\Gamma}_{i,1}$ have the same remainder modulo Γ_i. Since $\hat{q}_{i,1}\bar{\Gamma}_{i,1} \equiv \hat{\xi}_{i,1} \bmod \Gamma_i$, we have $n_1 \equiv \hat{\xi}_{i,1} \bmod \Gamma_i$ for $2 \leq i \leq L$, which forms another system of simultaneous congruences.

Since $N < M\Gamma$ and $N = n_1 M_1 + r_1$, we have $n_1 < \gamma_1$. Thus, according to the classical CRT, n_1 can be uniquely reconstructed by solving the above system of simultaneous congruences as (25). Hence, we have $\hat{n}_1 = n_1$.

Since $\hat{q}_{j,1} \neq q_{j,1}$, from (26) we have $\hat{n}_j \neq n_j$. This proves the necessity. ∎

Although the condition (28) in Theorem 1 is necessary and sufficient (under the assumption of (27)) for the uniqueness of the solution of the folding integers n_i from our proposed closed-form robust CRT, it involves with two remainder errors and hard to check in practice. We next present a simpler sufficient condition.

Corollary 1: Assume that all Γ_i, for $1 \leq i \leq L$, are pairwisely co-prime and

$$0 \leq N < \text{lcm}\,(M_1, M_2, \ldots, M_L) = M\Gamma_1\Gamma_2\cdots\Gamma_L = M\Gamma. \tag{33}$$

If

$$\tau < \frac{M}{4} \tag{34}$$

then, we have $\hat{n}_i = n_i$ for $1 \leq i \leq L$.

Proof: Recall that τ is the maximal remainder error level, i.e., $|\Delta r_i| \leq \tau$, for $1 \leq i \leq L$. If $\tau < M/4$, we have

$$|\Delta r_i - \Delta r_1| < M/2, \text{ for } 2 \leq i \leq L. \tag{35}$$

Clearly, (35) implies the sufficient condition (28) in Theorem 1. Thus, Corollary is proved. ∎

The above sufficient condition is the same as that in [8] for the searching based robust CRT as we described in Section II. Similar to the searching based robust CRT, after every n_i for $1 \leq i \leq L$ is uniquely determined, the unknown parameter N can be estimated as (16) and the estimate error of N is thus upper bounder by $|N - \hat{N}| \leq \tau$. Therefore, the above reconstruction algorithm is robust similar to the searching based robust CRT obtained in [8].

Comparison With the Traditional CRT: From Section II, for the traditional CRT, we know that the reason why the traditional CRT is not robust is because N_0 can not be accurately reconstructed even when the remainder errors are small for some r^c. In other words, the remainder error resistance performance is different for different r^c. One might ask why this problem does not occur in our proposed robust CRT. The main difference between the traditional CRT and our proposed robust CRT is that, in our proposed robust CRT, we do not determine these q_i in (5)–(6) directly as what is done in the traditional CRT, but we determine their differentials. Since the common remainder r^c of $r_i \bmod M$ is canceled in the differentials of q_i and q_1, i.e., $q_{i,1}$, the condition of accurately determining $q_{i,1}$ is independent to r^c. Therefore, the above problem is avoided in our proposed robust CRT in this paper.

Comparison With the Searching Based CRT: The searching based CRT in [8] also involves with the differentials of q_i and q_1 to determine n_i and n_1 by performing searching. So, it is also robust as shown in [8]. The main difference with our proposed robust CRT in this paper is that the searching based one is to solve for n_1 by searching via (17) and does not have a closed-form, while the one in this paper is to determine n_i via (21) with a closed-form solution as shown in the above algorithm from Step 1 to Step 4 and no searching is needed.

In both searching based and closed-form robust CRTs, $|\Delta r_i| < M/4$ for every $1 \leq i \leq L$ is a sufficient condition to guarantee accurately determining the folding integers n_i. The larger M, i.e., the larger of the gcd of all the moduli M_i, is, the more possible values for each remainder exist to accurately determine n_i. This is what we called remainder redundancy in Introduction. One can see that when all moduli are co-prime, i.e., $M = 1$, the remainder error bound τ is forced to be zero. This means that only the true remainders can guarantee the accurate reconstruction, where there is no redundancy in remainders.

IV. An Improvement and Generalization

In this section, we first present an improved algorithm by selecting a proper/optimal reference remainder before performing the above closed-form robust CRT. We then generalize the proposed closed-form robust CRT (and the improved version) from integers to reals.

A. Performance Improvement by Reference Remainder Selection

As we explained in the previous section, the major difference between our proposed robust CRT and the traditional CRT described in Section II is that in our proposed CRT, the differences of two remainders are used, while in the traditional CRT, the remainders are directly used. Due to the existence of the gcd between all the moduli M_i, the use of remainder differences provides the robustness of the reconstruction. However, the noise variances of the differences of two remainders are larger than those of the remainders themselves. The idea to improve our proposed closed-form robust CRT below is to reduce the noise variances of the remainder differences. Notice that the remainder differences used in (24) in our proposed algorithm are taken with respect to the first remainder $\hat{r}_1$, i.e., the first remainder is used as the reference, which is clearly not necessary. In fact, any remainder can be used as the reference. Therefore, if we can choose the one with the smallest noise variance as the reference, all the noise variances of the remainder differences will be the smallest too. We next show how we choose the smallest noise variance remainder.

From (6) we know, all remainders r_i have the common remainder r^c modulo M in the error-free case. But, for noisy remainders $\hat{r}_i$, their remainders modulo M, i.e.,

$$\hat{r}_i^c = \hat{r}_i \bmod M,$$

may be different from each other due to the errors. We first need to estimate the common remainder r^c from $\hat{r}_i^c$. Since $\hat{r}_i^c$ for $1 \leq i \leq L$ are folded integers, we can not estimate r^c by simply averaging them. Instead, we define a special averaging operation of $\hat{r}_i^c$ as

$$\hat{r}^c \triangleq \arg \min_{0 \leq m \leq M-1} \sum_{i=1}^{L} d^2\left(\hat{r}_i^c, m\right) \tag{36}$$

where $d(\cdot,\cdot)$ is a kind of distance function that is defined as follows. For integers m and n with $0 \leq m \leq M-1$ and $0 \leq n \leq M-1$, the distance of m to n is defined as

$$d(m,n) \triangleq m - n - k_0 M, \tag{37}$$

where

$$k_0 = \arg \min_{k \in \{-1,0,1\}} |m - n - kM|. \tag{38}$$

In fact, it is not hard to see that

$$k_0 = \left\lceil \frac{m-n}{M} \right\rceil \tag{39}$$

is always a solution of (38) and is always used in what follows.

Note that in the above, the non-absolute-valued $d(\cdot,\cdot)$ is used for convenience later but $|d(\cdot,\cdot)|$ is in fact the distance effectively involved in the above and the following optimizations. Then, the optimal remainder is the one whose remainder modulo M is closest to $\hat{r}^c$, i.e.,

$$j_0 = \arg \min_{1 \leq j \leq L} d^2\left(\hat{r}_j^c, \hat{r}^c\right) \tag{40}$$

is the index of the optimal remainder (with the smallest noise variance) among the erroneous remainders $\hat{r}_i$ for $1 \leq i \leq L$. Then, we select $\hat{r}_{j_0}$ as the reference remainder. If $j_0 \neq 1$, we exchange the indexes of j_0 and 1 for Γ_1, Γ_{j_0} and $\hat{r}_1, \hat{r}_{j_0}$, and then perform the closed-form robust CRT. We call this method as an improved version of the closed-form robust CRT. Since with this improved version, all the noise variances of the remainder differences are smaller than those in the closed-form robust CRT, it has a better performance as we will see from our theoretical and simulation results later. Note that if we apply the above remainder selection scheme to the searching based robust CRT, its performance will be improved as well.

B. Generalization to Reals

The above studies are all for integers. In some applications, an unknown, such as the phase in phase unwrapping in radar systems [9], [13], is real valued in general. We next generalize the above closed-form robust CRT to general real numbers, which is also helpful for the performance analysis for the closed-form robust CRT in the next section. To distinguish from integers in the previous sections, in what follows we use boldface symbols to denote the corresponding real variables of non-boldface integer variables.

Let $\boldsymbol{N}$ be a positive real number, which can be expressed as

$$\boldsymbol{N} = n_i \boldsymbol{M} \Gamma_i + \boldsymbol{r}_i, \ 1 \leq i \leq L \tag{41}$$

where n_i is an unknown integer (or folding integer) for $1 \leq i \leq L$ and all Γ_i, $1 \leq i \leq L$, are known positive integers and co-prime, $\boldsymbol{M}$ is a known real-valued normalization factor decided by the system design and $\boldsymbol{r}_i$ denotes the real-valued remainder with $0 \leq \boldsymbol{r}_i < \boldsymbol{M}\Gamma_i$, which is a real-valued version of the previously appeared integer remainder r_i, for $1 \leq i \leq L$.

Define

$$q_i \triangleq \lfloor \boldsymbol{r}_i / \boldsymbol{M} \rfloor \tag{42}$$

and then

$$\boldsymbol{r}_i = q_i \boldsymbol{M} + \boldsymbol{r}^c \tag{43}$$

where $\boldsymbol{r}^c \triangleq \boldsymbol{N} - \boldsymbol{M}\lfloor \boldsymbol{N}/\boldsymbol{M} \rfloor$ is the common remainder of $\boldsymbol{r}_i$ modulo $\boldsymbol{M}$ and is corresponding to the common remainder of r_i modulo M for $1 \leq i \leq L$ in integers version. The goal here is to robustly determine $\boldsymbol{N}$ from given noisy real-valued remainders $\hat{\boldsymbol{r}}_i$ that are the noised versions of $\boldsymbol{r}_i$.

Since (24) is just a quantization process, it applies to real values too. So, we can directly obtain integer $\hat{q}_{i,1}$:

$$\hat{q}_{i,1} = \left\lceil \frac{\hat{\boldsymbol{r}}_i - \hat{\boldsymbol{r}}_1}{\boldsymbol{M}} \right\rfloor, \ 2 \leq i \leq L \tag{44}$$

where $\hat{q}_{i,1} = \hat{q}_i - \hat{q}_1$, and $\hat{q}_i \triangleq \lfloor \hat{\boldsymbol{r}}_i / \boldsymbol{M} \rfloor$ for $1 \leq i \leq L$. Note that q_i, $\hat{q}_i$, and $\hat{q}_{i,1}$ are not boldfaces since they are all integers. The proposed closed-form robust CRT can directly apply to these integers. Therefore, we use Steps 2–4 of the proposed closed-form robust CRT in Section III to determine n_i for $1 \leq i \leq L$. For the uniqueness, we have the following result.

Corollary 2: Assume that all Γ_i, for $1 \leq i \leq L$, are pairwisely co-prime and

$$0 \leq \lfloor \boldsymbol{N}/\boldsymbol{M} \rfloor < \Gamma_1 \Gamma_2 \cdots \Gamma_L. \tag{45}$$

Then, $\hat{n}_i = n_i$ for all $1 \leq i \leq L$ if and only if

$$-\boldsymbol{M}/2 \leq \Delta \boldsymbol{r}_i - \Delta \boldsymbol{r}_1 < \boldsymbol{M}/2, \text{ for all } 2 \leq i \leq L \tag{46}$$

where $\Delta \boldsymbol{r}_i = \hat{\boldsymbol{r}}_i - \boldsymbol{r}_i$ for $1 \leq i \leq L$. In particular, if

$$|\Delta \boldsymbol{r}_i| < \frac{\boldsymbol{M}}{4}, \text{ for all } 1 \leq i \leq L, \tag{47}$$

then $\hat{n}_i = n_i$ for all $1 \leq i \leq L$.

Proof: We first derive an equivalent problem in integers. Define $N_0 \triangleq \lfloor \boldsymbol{N}/\boldsymbol{M} \rfloor$. Then, from (41) we have

$$N_0 = n_i \Gamma_i + q_i, 1 \leq i \leq L. \tag{48}$$

If we use $[(\boldsymbol{r}_i - \boldsymbol{r}_1)/\boldsymbol{M}]$ as an estimate of $q_{i,1} = q_i - q_1$, we have

$$\hat{q}_{i,1} = q_{i,1} + \left[\frac{\Delta \boldsymbol{r}_i - \Delta \boldsymbol{r}_1}{\boldsymbol{M}}\right], \ 2 \le i \le L. \tag{49}$$

From (45), we know

$$0 \le N_0 < \Gamma_1 \Gamma_2 \cdots \Gamma_L. \tag{50}$$

From (46) and (49), we have

$$-1/2 \le \hat{q}_{i,1} - q_{i,1} < 1/2, \text{ for all } 2 \le i \le L. \tag{51}$$

If we use these $\hat{q}_{i,1}$ to determine n_i for $1 \le i \le L$ by Step 2 to Step 4 of the proposed closed-form robust CRT in Section III, we then can apply the result and the Proof of Theorem 1. Since all Γ_i, for $1 \le i \le L$, are assumed pair-wisely co-prime and (50) holds, then, $\hat{n}_i = n_i$ for all $1 \le i \le L$ if and only if (51) holds.

Similar to Corollary 1, when (47) holds, we have $\hat{n}_i = n_i$ for all $1 \le i \le L$. ∎

After every n_i for $1 \le i \le L$ is uniquely determined, the unknown real number $\boldsymbol{N}$ can be estimated as

$$\hat{\boldsymbol{N}} = \boldsymbol{N} + \frac{1}{L}\sum_{i=1}^{L} \Delta \boldsymbol{r}_i. \tag{52}$$

When $|\Delta \boldsymbol{r}_i| \le \tau < \boldsymbol{M}/4$, the estimate error of $\boldsymbol{N}$ is thus upper bounded by $|\boldsymbol{N} - \hat{\boldsymbol{N}}| \le \tau$. This means that the above reconstruction is also robust.

Discussion of the Normalization Factor $\boldsymbol{M}$: The real-valued normalization factor $\boldsymbol{M}$ is the most important system parameter which decides the reconstruction performance. First, it is a parameter for the redundancy level as the gcd M in the closed-form robust CRT for integers in Section III. According to the condition in (46), we know the larger $\boldsymbol{M}$ is, the more possible values for each remainder exist to accurately determine n_i and therefore the more robust the reconstruction algorithm is. Second, $\boldsymbol{M}$ is used to define signal-to-noise ratio (SNR). As the remainders are all folded numbers, we can not directly use the remainders to measure the signal power. However, as the signals are all normalized by $\boldsymbol{M}$, the noises should also be normalized by $\boldsymbol{M}$. Hence, the SNR is defined as

$$\mathrm{SNR} = 20 \log \frac{\boldsymbol{M}}{\sigma} \tag{53}$$

where σ^2 is the variance of noise.

At the end of this section, we show that the improved closed-form robust CRT can also be generalized to reals by the following algorithm.

Improved Closed-Form Robust Chinese Remainder Theorem Algorithm for Reals:

- **Step 1**: From given noisy remainders $\hat{\boldsymbol{r}}_i$, calculate their remainders modulo $\boldsymbol{M}$ by

$$\hat{\boldsymbol{r}}_i^c = \hat{\boldsymbol{r}}_i - \boldsymbol{M}\left\lfloor \frac{\hat{\boldsymbol{r}}_i}{\boldsymbol{M}} \right\rfloor. \tag{54}$$

- **Step 2**: Calculate the average of $\hat{\boldsymbol{r}}_i^c$ as

$$\hat{\boldsymbol{r}}^c = \arg \min_{\boldsymbol{m} \in \mathbb{R}, 0 \le \boldsymbol{m} < \boldsymbol{M}} \sum_{i=1}^{L} d^2\left(\hat{\boldsymbol{r}}_i^c, \boldsymbol{m}\right) \tag{55}$$

where the distance function $d(\cdot,\cdot)$ for reals is correspondingly defined as follows. For real numbers $\boldsymbol{m}$ and $\boldsymbol{n}$ with $0 \le \boldsymbol{m} < \boldsymbol{M}$ and $0 \le \boldsymbol{n} < \boldsymbol{M}$, the distance of $\boldsymbol{m}$ to $\boldsymbol{n}$ is defined as

$$d(\boldsymbol{m}, \boldsymbol{n}) \triangleq \boldsymbol{m} - \boldsymbol{n} - k_0 \boldsymbol{M} \tag{56}$$

where

$$k_0 = \arg \min_{k \in \{-1,0,1\}} |\boldsymbol{m} - \boldsymbol{n} - k\boldsymbol{M}|. \tag{57}$$

- **Step 3**: Select the reference remainder index by

$$j_0 = \arg \min_{1 \le j \le L} d^2\left(\hat{\boldsymbol{r}}_j^c, \hat{\boldsymbol{r}}^c\right). \tag{58}$$

- **Step 4**: If $j_0 \ne 1$, exchange the indexes of j_0 and 1 for Γ_1, Γ_{j_0} and $\hat{\boldsymbol{r}}_1, \hat{\boldsymbol{r}}_{j_0}$, and calculate $\hat{q}_{i,1}$ by (44). Then, use Step 2 to Step 4 of the proposed closed-form robust CRT in Section III to determine n_i for $1 \le i \le L$.
- **Step 5**: Estimate $\boldsymbol{N}$ by (52).

Similar to (38) and (39), it is not hard to see that

$$k_0 = \left[\frac{\boldsymbol{m} - \boldsymbol{n}}{\boldsymbol{M}}\right] \tag{59}$$

is always a solution of (57) and is always used in what follows.

V. Performance Analysis

Since the above robust CRT algorithms are similar for both integers and reals and the uniqueness of the folding integer determination is the same, for convenience we only study the performance analysis for real values.

The robust CRT is to robustly reconstruct $\boldsymbol{N}$ from its multiple noisy remainders. Here we assume that the noises for different remainders are independently and identically distributed (i.i.d.) random variables, whose expectation, variance and probability density function (pdf) are zero, σ^2 and $f(x)$, respectively. We first consider the root mean-square error (RMSE) of $\boldsymbol{N}$, which is defined as

$$\boldsymbol{N}_{\mathrm{RMSE}} = \sqrt{\mathrm{E}\{|\hat{\boldsymbol{N}} - \boldsymbol{N}|^2\}} \tag{60}$$

where $\mathrm{E}\{\cdot\}$ denotes the expectation.

From (52) we know that if every n_i for $1 \le i \le L$ is accurately determined, the RMSE for closed-form robust CRT is given by

$$\boldsymbol{N}_{\mathrm{RMSE}} = \sqrt{\mathrm{E}\left\{\left|\frac{1}{L}\sum_{i=1}^{L} \Delta \boldsymbol{r}_i\right|^2\right\}} = \frac{\sigma}{\sqrt{L}}. \tag{61}$$

By generalizing (13) to reals, we have that if N_0 is accurately determined, the RMSE for the traditional CRT is also given by (61).

From (61), it looks like that both traditional CRT and our proposed robust CRT were robust because their RMSE are proportional to σ. This is in fact not true because obtaining (61) is conditioned on the fact that N_0 or n_i for $1 \le i \le L$ are accurately determined. Therefore, the probability to accurately determine N_0 or n_i for $1 \le i \le L$ is the key performance for both methods. Hence, we define the process of determining N_0 or n_i for $1 \le i \le L$ as a trial. In each trial, if N_0 or n_i for $1 \le i \le L$ are all accurately determined, the trial is passed, otherwise, the trial is failed. We take the trial fail rate (TFR) as the performance measure.

A. Traditional CRT TFR Performance

By generalizing (12) to reals, we have the probability to accurately determine q_i for $1 \le i \le L$:

$$p_i^T = P\left\{-\boldsymbol{r}^c \le \Delta \boldsymbol{r}_i \le \boldsymbol{M} - \boldsymbol{r}^c\right\} = \int_{-\boldsymbol{r}^c}^{\boldsymbol{M}-\boldsymbol{r}^c} f(x)dx. \quad (62)$$

Considering q_i for every $1 \le i \le L$ must be accurately determined to uniquely reconstruct N_0, we have the probability to accurately reconstruct N_0:

$$\begin{aligned} p_s^T &= P\{-\boldsymbol{r}^c \le \Delta \boldsymbol{r}_i \le \boldsymbol{M} - \boldsymbol{r}^c \text{ for every } 1 \le i \le L\} \\ &= \left\{\int_{-\boldsymbol{r}^c}^{\boldsymbol{M}-\boldsymbol{r}^c} f(x)dx\right\}^L \end{aligned} \quad (63)$$

where we use the independence for all noises $\Delta \boldsymbol{r}_i$. Clearly, p_s^T depends on $\boldsymbol{r}^c$. Assume that $\boldsymbol{r}^c$ is the uniform distribution in the range of $[0, \boldsymbol{M})$. Then, the average TFR is

$$p_{\mathrm{TFR}}^T = 1 - \frac{1}{\boldsymbol{M}} \int_0^{\boldsymbol{M}} \left\{\int_{-u}^{M-u} f(x)dx\right\}^L du. \quad (64)$$

If noise $\Delta \boldsymbol{r}_i$ is a normal distribution, then p_{TFR}^T can be simplified as

$$p_{\mathrm{TFR}}^T = 1 - \frac{1}{\boldsymbol{M}} \int_0^{\boldsymbol{M}} \left\{Q\left(-\frac{u}{\sigma}\right) - Q\left(\frac{\boldsymbol{M}-u}{\sigma}\right)\right\}^L du \quad (65)$$

where $Q(u)$ is Q-function defined by

$$Q(u) = \frac{1}{\sqrt{2\pi}} \int_u^{+\infty} \exp\left(-\frac{x^2}{2}\right) dx. \quad (66)$$

B. Closed-Form Robust CRT TFR Performance

According to (46) in Corollary 2, the probability to accurately determine $q_i - q_1$ for $2 \le i \le L$ is

$$p_i^C = P\{-\boldsymbol{M}/2 \le \Delta \boldsymbol{r}_i - \Delta \boldsymbol{r}_1 < \boldsymbol{M}/2\}. \quad (67)$$

Note that in the above probability, two random variables, i.e., $\Delta \boldsymbol{r}_i$ and $\Delta \boldsymbol{r}_1$ are involved. Their difference $Z_i = \Delta \boldsymbol{r}_i - \Delta \boldsymbol{r}_1$ is also a random variable. Considering $q_i - q_1$ for every $2 \le i \le L$ must be accurately determined to uniquely reconstruct n_i, the probability to accurately reconstruct n_i can be written as

$$p_s^C = P\{-\boldsymbol{M}/2 \le Z_i < \boldsymbol{M}/2 \text{ for every } 2 \le i \le L\}. \quad (68)$$

For a given $\Delta \boldsymbol{r}_1 = u$, random variables $Z_i = \Delta \boldsymbol{r}_i - u$ for $2 \le i \le L$ have the same distribution and are independent with each other. Thus, p_s^C has the following form:

$$p_s^C(u) = \left\{\int_{-\boldsymbol{M}/2+u}^{\boldsymbol{M}/2+u} f(x)dx\right\}^{L-1}. \quad (69)$$

Then, p_s^C is the expectation of $p_s^C(\Delta \boldsymbol{r}_1)$ and the TFR for closed-form robust CRT can be written as

$$\begin{aligned} p_{\mathrm{TFR}}^C &= 1 - p_s^C \\ &= 1 - \int_{-\infty}^{+\infty} f(u) \left\{\int_{-\boldsymbol{M}/2+u}^{\boldsymbol{M}/2+u} f(x)dx\right\}^{L-1} du. \end{aligned} \quad (70)$$

If noise $\Delta \boldsymbol{r}_i$ is a uniform distribution with the following pdf:

$$f(x) = \begin{cases} \frac{1}{2B}, & \text{if } |x| \le B \\ 0, & \text{otherwise} \end{cases} \quad (71)$$

then, p_{TFR}^C has the following simple form:

$$p_{\mathrm{TFR}}^C = \begin{cases} 0, & \text{if } B < \boldsymbol{M}/4 \\ \frac{\boldsymbol{M}}{B}\left(\frac{1}{2} - \frac{1}{L} + \frac{1}{2^L L}\right), & \text{if } B \ge \boldsymbol{M}/2 \\ 2 - \frac{2}{L} - \frac{\boldsymbol{M}}{2B} + \frac{2\boldsymbol{M}^L}{4^L L B^L}, & \text{otherwise.} \end{cases} \quad (72)$$

In the above uniform distribution case, B is just the maximal error level, i.e., $\tau = B$. And the result in (72) when $B < \boldsymbol{M}/4$ coincides with the results in Corollaries 1 and 2.

If noise $\Delta \boldsymbol{r}_i$ is a normal distribution, then p_{TFR}^C has the following simple form:

$$\begin{aligned} p_{\mathrm{TFR}}^C = 1 &- \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} \exp\left(-\frac{u^2}{2}\right) \\ &\times \left\{Q\left(-\frac{\boldsymbol{M}}{2\sigma} + u\right) - Q\left(\frac{\boldsymbol{M}}{2\sigma} + u\right)\right\}^{L-1} du. \end{aligned} \quad (73)$$

As a remark, for the searching based robust CRT, the above theoretical performance applies similarly but with a little more tedious analysis that is omitted here, which will be verified from our numerical simulations later.

C. Improved Closed-Form Robust CRT TFR Performance

In the improved closed-form robust CRT, a reference remainder is first selected and its noise variance is smaller than others due to the selection process. We now show how to get its distribution and corresponding TFR performance.

From the distance function definition in (56) and (59), it is not hard to see

$$d\left(\hat{\boldsymbol{r}}_i^c, \hat{\boldsymbol{r}}^c\right) = d\left(d\left(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c\right), d\left(\hat{\boldsymbol{r}}^c, \boldsymbol{r}^c\right)\right). \quad (74)$$

Define $\Delta \boldsymbol{r}_i \triangleq \hat{\boldsymbol{r}}_i - \boldsymbol{r}_i$. From (43) and (54), we have

$$\Delta \boldsymbol{r}_i = \hat{\boldsymbol{r}}_i^c - \boldsymbol{r}^c + k_i \boldsymbol{M}, \text{ for some } k_i \in \mathbb{Z}. \quad (75)$$

Since $\hat{\boldsymbol{r}}_i^c$ and $\hat{\boldsymbol{r}}^c$ are both folded, they are all constrained in the range $[0, \boldsymbol{M})$. From the distance function definition in (56), it is easy to see $|d(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c)| \leq \boldsymbol{M}/2$. From the right-hand side of (75), we have that, if $|\hat{\boldsymbol{r}}_i^c - \boldsymbol{r}^c| \neq \boldsymbol{M}/2$, there exists one and only one integer k_i' such that $|\hat{\boldsymbol{r}}_i^c - \boldsymbol{r}^c + k_i'\boldsymbol{M}| < \boldsymbol{M}/2$, and in this case, from (56) and (59) we then have $d(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c) = \hat{\boldsymbol{r}}_i^c - \boldsymbol{r}^c + k_i'\boldsymbol{M}$. Hence, if $|\Delta \boldsymbol{r}_i| < \boldsymbol{M}/2$, it can be uniquely expressed by $d(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c)$, i.e.,

$$\Delta \boldsymbol{r}_i = d\left(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c\right) = \hat{\boldsymbol{r}}_i^c - \boldsymbol{r}^c. \tag{76}$$

Similarly, we can prove that if $|d(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c) - d(\hat{\boldsymbol{r}}^c, \boldsymbol{r}^c)| < \boldsymbol{M}/2$, we have

$$d\left(d\left(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c\right), d\left(\hat{\boldsymbol{r}}^c, \boldsymbol{r}^c\right)\right) = d\left(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c\right) - d\left(\hat{\boldsymbol{r}}^c, \boldsymbol{r}^c\right), \tag{77}$$

and if $|\Delta \boldsymbol{r}^c| < \boldsymbol{M}/2$, we have

$$\Delta \boldsymbol{r}^c = d\left(\hat{\boldsymbol{r}}^c, \boldsymbol{r}^c\right) \tag{78}$$

where $\Delta \boldsymbol{r}^c$ denotes the error of the common remainder, i.e., $\Delta \boldsymbol{r}^c \triangleq \hat{\boldsymbol{r}}^c - \boldsymbol{r}^c$.

Although $|\Delta \boldsymbol{r}_i|$, $|d(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c) - d(\hat{\boldsymbol{r}}^c, \boldsymbol{r}^c)|$ and $|\Delta \boldsymbol{r}^c|$ may be greater than or equal to $\boldsymbol{M}/2$, the probability is small especially for the case of the high signal to noise ratio (SNR) and we ignore this case. Therefore, from (74)–(78) we have

$$d\left(\hat{\boldsymbol{r}}_i^c, \hat{\boldsymbol{r}}^c\right) = \Delta \boldsymbol{r}_i - \Delta \boldsymbol{r}^c \text{ for } 1 \leq i \leq L. \tag{79}$$

Assume that $\boldsymbol{m}$ is in a neighborhood of $\hat{\boldsymbol{r}}^c$, i.e., $\boldsymbol{m} \in (\hat{\boldsymbol{r}}^c - \epsilon, \hat{\boldsymbol{r}}^c + \epsilon)$, where ϵ is an arbitrarily small positive number, if $\hat{\boldsymbol{r}}^c \neq 0$. If $\hat{\boldsymbol{r}}^c = 0$, $\boldsymbol{m} \in (0, \hat{\boldsymbol{r}}^c + \epsilon)$. It is clear that if $|\Delta \boldsymbol{r}^c| < \boldsymbol{M}/2 - \epsilon$ and $|d(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c) - d(\hat{\boldsymbol{r}}^c, \boldsymbol{r}^c)| < \boldsymbol{M}/2 - \epsilon$, then $|\boldsymbol{m} - \boldsymbol{r}^c| < \boldsymbol{M}/2$ and $|d(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c) - d(\boldsymbol{m}, \boldsymbol{r}^c)| < \boldsymbol{M}/2$. Similar to (77) and (78), we have

$$\begin{aligned} d\left(\hat{\boldsymbol{r}}_i^c, \boldsymbol{m}\right) &= d\left(d\left(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c\right), d\left(\boldsymbol{m}, \boldsymbol{r}^c\right)\right) \\ &= d\left(\hat{\boldsymbol{r}}_i^c, \boldsymbol{r}^c\right) - d\left(\boldsymbol{m}, \boldsymbol{r}^c\right) \\ &= \Delta \boldsymbol{r}_i - m + \boldsymbol{r}^c. \end{aligned} \tag{80}$$

Hence, if $\boldsymbol{m}$ is in a neighborhood of $\hat{\boldsymbol{r}}^c$, the derivative of $\sum_{i=1}^{L} d^2(\hat{\boldsymbol{r}}_i^c, \boldsymbol{m})$ exists. Note that if $\hat{\boldsymbol{r}}^c = 0$, the right derivative exists. From (55), we have that if $\sum_{i=1}^{L} d^2(\hat{\boldsymbol{r}}_i^c, \boldsymbol{m})$ reaches the minimum when $\boldsymbol{m} = \hat{\boldsymbol{r}}^c$, then

$$\left.\frac{\partial \sum_{i=1}^{L} d^2\left(\hat{\boldsymbol{r}}_i^c, \boldsymbol{m}\right)}{\partial \boldsymbol{m}}\right|_{\boldsymbol{m}=\hat{\boldsymbol{r}}^c} = 0. \tag{81}$$

From (80), we have

$$\sum_{i=1}^{L} d\left(\hat{\boldsymbol{r}}_i^c, \hat{\boldsymbol{r}}^c\right) = 0. \tag{82}$$

Therefore, from (79) we have

$$\Delta \boldsymbol{r}^c = \frac{1}{L} \sum_{i=1}^{L} \Delta \boldsymbol{r}_i. \tag{83}$$

Since $\Delta \boldsymbol{r}_i$ for $1 \leq i \leq L$ are independent with each other and have the same pdf $f(x)$, the pdf of $\Delta \boldsymbol{r}^c$ is $g(x) = \underbrace{f(x) * f(x) * \cdots * f(x)}_{L}$, where $*$ denotes the convolution operation. If $\Delta \boldsymbol{r}_i$ is normal distributed, then $\Delta \boldsymbol{r}^c$ is also normal distributed with variance of σ^2/L.

From (79), the reference remainder error has the following form:

$$\Delta \boldsymbol{r}_{j_0} = d\left(\hat{\boldsymbol{r}}_{j_0}^c, \hat{\boldsymbol{r}}^c\right) + \Delta \boldsymbol{r}^c. \tag{84}$$

This means that the error of the reference remainder is the sum of two random variables. To simplify the notation, let $Z = \Delta \boldsymbol{r}_{j_0}$, $X = d(\hat{\boldsymbol{r}}_{j_0}^c, \hat{\boldsymbol{r}}^c)$ and $Y = \Delta \boldsymbol{r}^c$. We know that the pdf of Y is $g(y)$ as we explained before. We next consider X.

From (79), we reformulate (58) as

$$j_0 = \arg \min_{1 \leq j \leq L} \left(\Delta \boldsymbol{r}_j - \Delta \boldsymbol{r}^c\right)^2. \tag{85}$$

From (83), the correlation coefficient of $\Delta \boldsymbol{r}^c$ with any $\Delta \boldsymbol{r}_i$ for $1 \leq i \leq L$ is $1/\sqrt{L}$, which is small especially for a larger L. To simplify the derivations, we assume that $\Delta \boldsymbol{r}^c$ and any $\Delta \boldsymbol{r}_i$ for $1 \leq i \leq L$ are uncorrelated.

Consider any remainder error $\Delta \boldsymbol{r}_j$ with $1 \leq j \leq L$. For a given $Y = \Delta \boldsymbol{r}^c = y$ and $\Delta \boldsymbol{r}_j = u$, then $j_0 = j$ if and only if the other $L-1$ remainders errors satisfy $|\Delta \boldsymbol{r}_i - y| \geq |u - y|$ for $1 \leq i \leq L$ and $i \neq j$. As the remainders errors are i.i.d. random variables with pdf $f(x)$, the conditional probability of $j_0 = j$ is

$$P(j_0 = j | Y = y, \Delta \boldsymbol{r}_j = u) \left\{1 - \left| \int_{-u+y}^{u-y} f(v+y) dv \right|\right\}^{L-1}. \tag{86}$$

Since any remainder $\boldsymbol{r}_j$ for $1 \leq j \leq L$ has the same probability to be a reference remainder, the conditional distribution function of X is

$$\begin{aligned} F_X(x|Y=y) &= P(X < x | Y = y) \\ &= \sum_{j=1}^{L} P(j_0 = j, \Delta \boldsymbol{r}_j - Y < x | Y = y). \end{aligned} \tag{87}$$

Therefore, the conditional pdf of X is

$$\begin{aligned} &f_X(x|Y=y) \\ &= \lim_{\Delta x \to 0} \frac{F_X(x + \Delta x | Y = y) - F_X(x | Y = y)}{\Delta x} \\ &= \sum_{j=1}^{L} \lim_{\Delta x \to 0} \frac{P(j_0 = j, x \leq \boldsymbol{r}_j - Y < x + \Delta x | Y = y)}{\Delta x} \\ &= \sum_{j=1}^{L} \lim_{\Delta x \to 0} \frac{P(x \leq \Delta \boldsymbol{r}_j - y < x + \Delta x)}{\Delta x} \\ &\quad \times P(j_0 = j | Y = y, x \leq \Delta \boldsymbol{r}_j - y < x + \Delta x) \\ &= L f(x+y) \left\{1 - \left| \int_{-x}^{x} f(v+y) dv \right|\right\}^{L-1}. \end{aligned} \tag{88}$$

Then, the joint pdf of (X, Y) can be expressed as

$$f_{XY}(x, y) = L f(x+y) \left\{1 - \left| \int_{y-x}^{y+x} f(v) dv \right|\right\}^{L-1} g(y). \tag{89}$$

Therefore, the pdf of the reference remainder error is

$$f_Z(z) = \int_{-\infty}^{+\infty} f_{XY}(z-y, z)dy = Lf(z)\int_{-\infty}^{+\infty}\left\{1-\left|\int_{2y-z}^{z} f(v)dv\right|\right\}^{L-1} g(y)dy. \quad (90)$$

Thus, similar to the closed-form robust CRT, the TFR for the improved closed-form robust CRT can be written as

$$p_{\mathrm{TFR}}^{I} = 1 - \int_{-\infty}^{+\infty} f_Z(u)\left\{\int_{-\boldsymbol{M}/2+u}^{\boldsymbol{M}/2+u} f(x)dx\right\}^{L-1} du. \quad (91)$$

If noise $\Delta \boldsymbol{r}_i$ is a normal distribution, then p_{TFR}^{I} and $f_Z(z)$ have the following simple forms:

$$p_{\mathrm{TFR}}^{I} = 1 - \int_{-\infty}^{+\infty} f_Z(u) \times \left\{Q\left(-\frac{\boldsymbol{M}}{2\sigma}+u\right) - Q\left(\frac{\boldsymbol{M}}{2\sigma}+u\right)\right\}^{L-1} du \quad (92)$$

$$f_Z(z) = \frac{L\sqrt{L}}{2\pi}\exp\left(-\frac{z^2}{2}\right)\int_{-\infty}^{+\infty}\exp\left(-\frac{Ly^2}{2}\right) \times \{1-|Q(2y-z)-Q(z)|\}^{L-1} dy. \quad (93)$$

VI. Simulation Results

The configuration in simulations is $3 \le L \le 12$, $\boldsymbol{M} = 100$, and Γ_1 to Γ_{12} are $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}$. $\boldsymbol{N}$ is a real number and is uniformly distributed between 0 to $\boldsymbol{M}\Gamma$. We implement 10 000 trials for different methods.

We first consider the TFR performances of the traditional CRT, the searching based robust CRT, the closed-form robust CRT and the improved closed-form CRT. Fig. 1 shows TFR versus SNR for different methods, where $L = 8$, the remainder noise is a normal distribution and SNR is defined as in (53). The theory curves are based on (65), (73), and (92), where numerical integrations are used. Fig. 1 shows that for the TFR performances and one can see that the simulation results match well with the theoretical performance analyses in Section V. The TFR of the searching based CRT is close to that of the proposed closed-form CRT. However, after performing the remainder selection, the performance of the closed-form CRT is remarkably improved.

In Fig. 2, we show the TFR performance versus the number of remainders, i.e., L. The remainder noise is also a normal distribution and the SNR for this example is 18 dB. The results demonstrate that the improvement due to the reference remainder selection is more notable as L increases. Fig. 2 also shows that the closed-form robust CRT TFR increases monotonically as predicted by the theory of Section V. The improved closed-form robust CRT TFR simulation is close to the theory prediction as L increases, which is due to the assumption of large L in the derivations of the theoretical performance analysis in Section V-C.

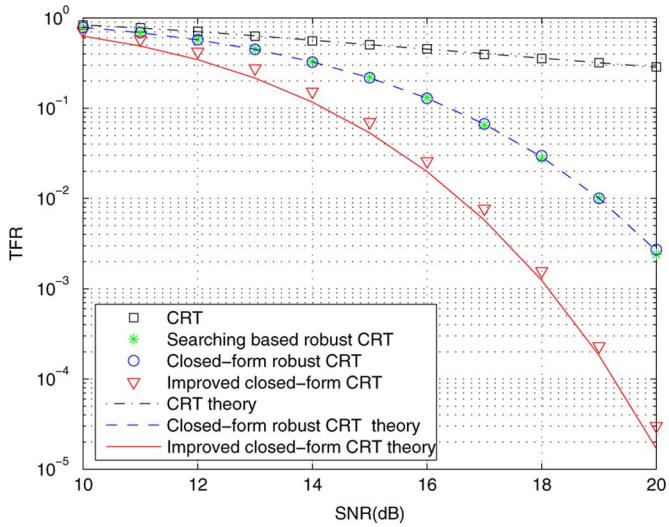

Fig. 1. TFR versus SNR for different methods and remainder noises are Gaussian.

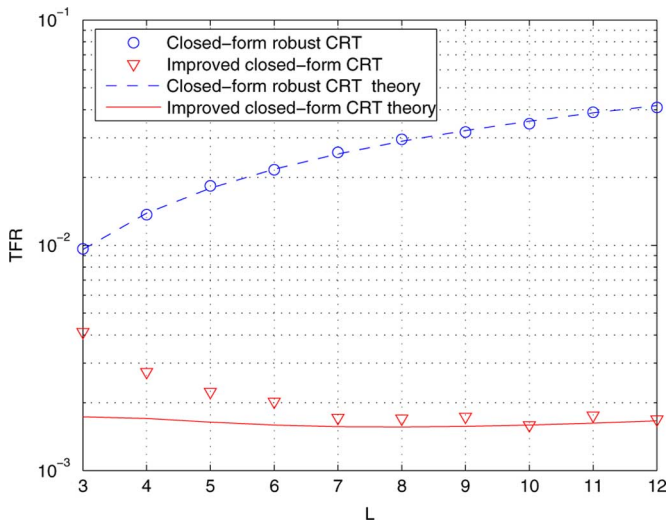

Fig. 2. TFR versus number of remainders, L, and SNR is 18 dB with Gaussian noise.

In Fig. 3, we compare the robustness of the traditional CRT and the proposed closed-form robust CRT by investigating their RMSE and TFR performances, where $L = 3$. The theory curves for RMSE and TFR are based on (61) and (72) respectively. Fig. 3 shows RMSE and TFR versus SNR for the CRT and the proposed robust CRT. In this simulation, we assume that the remainder noise is uniformly distributed between $[-\tau, \tau]$. According to Corollaries 1 and 2, we know that the remainder error bound is $\boldsymbol{M}/4$ to guarantee accurately recovering n_i for $1 \le i \le L$. When $\tau = \boldsymbol{M}/4$, SNR bound in this example is 16.8 dB as illustrated in the figure. Fig. 3 shows that if the SNR is larger than the bound, the TFR of the proposed robust CRT is equal to zero and the corresponding RMSE decreases linearly with σ just as predicted by (61). So, the proposed robust CRT is robust. For the CRT, it has the same form of $\boldsymbol{N}_{\mathrm{RMSE}}$ as the proposed robust CRT, but it is not robust due to the reason that the TFR is never 0 no matter how high the SNR is.

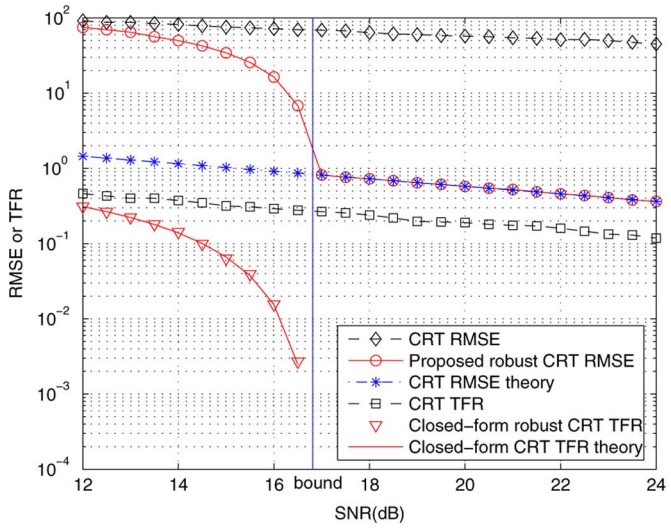

Fig. 3. RMSE and TFR versus SNR and remainder noises have uniform distribution.

VII. Conclusion

In this paper, we have proposed a closed-form robust CRT that can robustly reconstruct an integer from its smaller erroneous remainders modulo several moduli. The robustness is built upon the assumption of the existence of the gcd between all the moduli. Compared with the traditional CRT, it solves the noise sensitivity problem. Compared with the searching based robust CRT, it has a closed-from and much less computational complexity. The complexity reduction becomes even more significant when the parameters get larger. We have presented the theoretical performance analysis. The theoretical analysis and numerical simulations demonstrate that the remainder noise/error resistance performance can be significantly improved by performing the reference remainder selection. We have also generalized the proposed robust CRT from integers to reals.

As a final remark, in [22], Huang and Wan obtained a different robust CRT where the integer N is robustly solved but not the folding integers n_i are uniquely solved, while in this paper the folding integers n_i are uniquely solved.

Acknowledgment

The authors would like to thank the anonymous reviewers for their detailed comments that have helped the presentation of this paper.

References

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

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

[3] O. Ore, "The general Chinese remainder theorem," *Amer. Math. Monthly*, vol. 59, no. 6, pp. 365–370, Jun.–Jul. 1952.

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

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

[6] 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.

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

[8] X. W. Li, H. Liang, and X.-G. Xia, "A robust Chinese remainder theorem with its applications in frequency estimation from undersampled waveforms," *IEEE Trans. Signal Process.*, vol. 57, no. 11, pp. 4314–4322, Nov. 2009.

[9] 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.

[10] X. W. 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] Y. M. Zhang and M. Amin, "MIMO radar exploiting narrowband frequency-hopping waveforms," presented at the 16th Eur. Signal Processing Conf. (EUSIPCO), Lausanne, Switzerland, Aug. 25–29, 2008.

[16] J. Bioucas-Dias, V. Katkovnik, J. Astola, and K. Egiazarian, "Multifrequency phase unwrapping from noisy data: Adaptive local maximum likelihood approach," in *Image Analysis, Lecture Notes in Computer Science*. New York: Springer, Jul. 2009, vol. 5575/2009, pp. 310–320.

[17] 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. Tech.*, vol. 31, no. 10, pp. 2493–2496, Oct. 2009.

[18] G. Li, H. Meng, X.-G. Xia, and Y.-N. Peng, "Range and velocity estimation of moving targets using multiple stepped-frequency pulse trains," *Sensors*, vol. 8, pp. 1343–1350, 2008.

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

[20] X. W. Li and X.-G. Xia, "Multiple-frequency interferomentric velocity SAR location and imaging of elevated moving target," in *Proc. Int. Conf. Acoustics, Speech, Signal Processing (IEEE ICASSP)*, Dallas, TX, Mar. 2010, pp. 2810–2813.

[21] C. Wang, Q. Y. Yin, and W. J. Wang, "An efficient ranging mehtod for wireless sensor networks," in *Proc. Int. Conf. Acoustics, Speech, Signal Processing (IEEE ICASSP)*, Dallas, TX, Mar. 2010, pp. 2846–2849.

[22] Z. Huang and Z. Wan, "Range ambiguity resolution in multiple PRF pulse Doppler radars," in *Proc. Int. Conf. Acoustics, Speech, Signal Processing (IEEE ICASSP)*, Dallas, TX, Apr. 1987, pp. 1786–1789.

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.

Currently, he is an Associate Professor at Xi'an Jiaotong University and a Visiting Professor of the Department of Electrical and Computer Engineering, University of Delaware, Newark. His main research interests include MIMO and OFDM systems, digital signal processing, and wireless sensor networks.

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

He was a Senior/Research Staff Member at Hughes Research Laboratories, Malibu, CA, during academic year 1995–1996. In September 1996, he joined the Department of Electrical and Computer Engineering, University of Delaware, Newark, where he is the Charles Black Evans Professor. During academic year 2002–2003, he was a Visiting Professor at the Chinese University of Hong Kong , 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 200 refereed journal articles published and accepted, and seven U.S. patents awarded. He is the author of the book *Modulated Coding for Intersymbol Interference Channels* (New York: Marcel Dekker, 2000).

Dr. Xia received the National Science Foundation (NSF) Faculty Early Career Development (CAREER) Program Award in 1997, the Office of Naval Research (ONR) Young Investigator Award in 1998, and the Outstanding Overseas Young Investigator Award from the National Nature Science Foundation of China in 2001. He 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, 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 from 1996 to 2003, the IEEE TRANSACTIONS ON MOBILE COMPUTING from 2001 to 2004, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2005 to 2008, the IEEE SIGNAL PROCESSING LETTERS from 2003 to 2007, and the *EURASIP Journal of Applied Signal Processing* from 2001 to 2004. He served as a Member of the Signal Processing for Communications Committee from 2000 to 2005 and a Member of the Sensor Array and Multichannel (SAM) Technical Committee from 2004 to 2009 in the IEEE Signal Processing Society. Since 2002, he has served as the IEEE Sensors Council Representative of the IEEE Signal Processing Society and as the Representative of the IEEE Signal Processing Society to the Steering Committee for the IEEE TRANSACTIONS ON MOBILE COMPUTING from 2005 to 2006. He is Technical Program Chair of the Signal Processing Symposium, IEEE GLOBECOM 2007 in Washington DC, and the General Co-Chair of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2005 in Philadelphia, PA.