Phase Unwrapping and A Robust Chinese Remainder Theorem

Xiang-Gen Xia and Genyuan Wang

Abstract—**In the conventional Chinese remainder theorem (CRT), a small error in a remainder may cause a large error in the solution of an integer, i.e., CRT is not robust. In this letter, we first propose a robust phase unwrapping algorithm with applications in radar signal processing. Motivated from the phase unwrapping algorithm, we then derive a type of robust CRT.**

Index Terms—**Chinese remainder theorem, phase unwrapping, radar signal processing, remainder errors, synthetic aperture radar (SAR).**

I. Introduction

The CHINESE remainder theorem (CRT) has tremendous applications in many fields [9], [10], including phase unwrapping [8] in radar signal processing. It is to determine an integer (usually larger) from its remainders (usually smaller) modulo several moduli. The CRT is not robust in the sense that a small error in its remainders may cause a large error in the determined integer by the CRT. CRT with remainder errors has been studied in the literature, see, for example, [1]–[3] and [7] for a generalized CRT, where the remainder errors are corrected by using sufficiently enough remainders/moduli. What is interested in this letter, however, is not necessarily to correct the remainder errors but to reduce the CRT reconstruction errors due to the remainder errors, and there is no requirement on the number of remainders or moduli. To do so, we first propose a robust phase unwrapping algorithm. The problem is described as follows.

Consider a multifrequency antenna array synthetic aperture radar (SAR) [4]. The SAR value at the mth antenna from the ith frequency of a moving target is approximately: for $m = 1, 2, \ldots, M$, $i = 1, 2, \ldots, L$

$$s_i(m) = c_i \exp\left(j2\pi \frac{\sigma x}{\lambda_i}(m-1)\right) \tag{1}$$

where $c_i \neq 0$ is independent of m, M is the total number of antennas, L is the total number of frequencies, λ_i is the wavelength of the transmitted signal with the ith frequency, σ is a known parameter that is related to the range R_0 of the radar to the moving target and the distance d between adjacent antennas, x is an unknown parameter (Doppler shift) to be determined, and x is related to the speed and location of the moving target. Due to the motion of the target, its Doppler shift x may cause the target shifted in the SAR image domain. Since x is unknown, the shift amount is unknown, and therefore, a moving target is usually mislocated in a conventional SAR image. However, when $M > 1$ and $L > 1$, a reasonable size x can be solved, and therefore, a moving target can be correctly relocated in the SAR image [4].

From (1), for each i, $1 \leq i \leq L$, by taking the M-point discrete Fourier transform (DFT) of $s_i(m)$, $1 \leq m \leq M$, we obtain (only) integer remainders k_i with $0 \leq k_i \leq M-1$ as follows:

$$f_i \triangleq \frac{\sigma x}{\lambda_i} = n_i + \frac{k_i}{M} + \epsilon_i \tag{2}$$

where n_i is a nonnegative unknown integer, and ϵ_i is an unknown real number with

$$|\epsilon_i| \leq \frac{1}{2M}. \tag{3}$$

Clearly, to determine the unknown parameter x, it is sufficient to determine f_i. Thus, the problem is to determine f_i from the integer remainders k_i. From (2), one can see that ϵ_i is the precision error, and n_i is the folding error. While the precision error ϵ_i causes a small error on f_i, the folding error n_i may cause a large error on f_i. Thus, in order to robustly determine f_i, it is necessary to correctly determine n_i. *The problem of interest* in this letter is how to uniquely determine n_i, $1 \leq i \leq L$, in (2) from k_i, λ_i, $1 \leq i \leq L$, and σ and M, where the remainders k_i, $1 \leq i \leq L$ may have errors that may occur when there is an additive noise in signal $s_i(m)$ in (1). In Section II, we shall propose a solution for this problem under some minor conditions on the wavelengths λ_i.

The above problem is related to the CRT as follows. Let Γ be a positive number such that $\Gamma_i = \Gamma\lambda_i$, $1 \leq i \leq L$, are all positive integers. If the precision error $\epsilon_i = 0$ in (2), then

$$M\Gamma\sigma x = n_i\Gamma_i M + k_i\Gamma_i, \quad 1 \leq i \leq L. \tag{4}$$

Let

$$M_i \triangleq \Gamma_i M, \quad n \triangleq M\Gamma\sigma x, \text{ and } r_i \triangleq k_i\Gamma_i, \ 1 \leq i \leq L \tag{5}$$

then

$$n = n_i M_i + r_i, \quad 0 \leq r_i \leq M_i - 1, \ 1 \leq i \leq L \tag{6}$$

which is analogous to the CRT problem of determining n from its remainders r_i and moduli M_i, $1 \leq i \leq L$.

II. Robust Solution

When the remainders k_i in (2) have errors that are possible from the M-point DFT detection of the signal $s_i(m)$, what we have is $\tilde{k}_i$

$$0 \leq \tilde{k}_i \leq M-1 \text{ and } |\tilde{k}_i - k_i| \leq \tau \tag{7}$$

Manuscript received July 21, 2006; revised August 30, 2006. This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant No. FA9550-05-1-0161 and in part by the National Science Foundation under Grants CCR-0097240 and CCR-0325180. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Yimin Zhang.

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

G. Wang is with Navini Networks, Richardson, TX 75082 USA (e-mail: genyuanwangzz@yahoo.com).

Digital Object Identifier 10.1109/LSP.2006.884898

where $\tau < M$ is the maximal error level in the remainders k_i. In this case, (2) becomes

$$f_i = \frac{\sigma x}{\lambda_i} = n_i + \frac{\tilde{k}_i}{M} + \tilde{\epsilon}_i, \quad 1 \le i \le L \tag{8}$$

where

$$|\tilde{\epsilon}_i| \le \frac{1+2\tau}{2M}. \tag{9}$$

We want to uniquely determine n_i in (8) from $\tilde{k}_i$, λ_i, and M, $1 \le i \le L$. To do so, let Γ be the smallest positive number such that

$$\Gamma_i = \Gamma\lambda_i \quad 1 \le i \le L \tag{10}$$

are all integers, and Γ_i and Γ_j are co-prime for $1 \le i \neq j \le L$. Note that this condition may not hold for all possible positive real numbers λ_i, $1 \le i \le L$, but there are enough such λ_i in any range. Thus, in what follows, we always assume that the above condition is satisfied. In fact, in SAR applications, λ_i are the wavelengths that we can design by ourselves and therefore flexible to choose.

Without loss of generality, we assume

$$\Gamma_1 < \Gamma_2 < \cdots < \Gamma_L \text{ or equivalently } \lambda_1 < \lambda_2 < \cdots < \lambda_L. \tag{11}$$

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

$$\gamma_i \triangleq \Gamma_1 \ldots \Gamma_{i-1}\Gamma_{i+1} \ldots \Gamma_L \tag{12}$$

where $\gamma_1 \triangleq \Gamma_2 \ldots \Gamma_L$ and $\gamma_L \triangleq \Gamma_1 \ldots \Gamma_{L-1}$. For each i with $2 \le i \le L$, define

$$S_i \triangleq \left\{ (\bar{n}_1, \bar{n}_i) = \underset{\substack{\hat{n}_1 = 0,1,\ldots,\gamma_1 - 1 \\ \hat{n}_i = 0,1,\ldots,\gamma_i - 1}}{\operatorname{argmin}} \left| \hat{n}_i\Gamma_i + \frac{\tilde{k}_i\Gamma_i}{M} - \hat{n}_1\Gamma_1 - \frac{\tilde{k}_1\Gamma_1}{M} \right| \right\} \tag{13}$$

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.,

$$S_{i,1} \triangleq \{\bar{n}_1 : (\bar{n}_1, \bar{n}_i) \in S_i \text{ for some } \bar{n}_i\} \tag{14}$$

and define

$$S \triangleq \bigcap_{i=2}^{L} S_{i,1}. \tag{15}$$

We then have the following result.

Theorem 1: Assume Γ_i and Γ_j defined in (10) are co-prime for $1 \le i \neq j \le L$. If

$$x < \frac{1}{\sigma\Gamma}\Gamma_1\Gamma_2 \ldots \Gamma_L \tag{16}$$

and

$$M > (1+2\tau)(\Gamma_1 + \Gamma_L) \tag{17}$$

then set S defined above contains only element n_1, i.e., $S = \{n_1\}$, and $(n_1, \bar{n}_i) \in S_i$ implies $\bar{n}_i = n_i$ for $1 \le i \le L$, where n_i, $1 \le i \le L$ are the true solution in (8). □

Its proof is in the Appendix. Note that the case when $\tau = 0$ has been considered in [4], but there is an error in the result [4, Theorem 1] obtained in [4] where the set S_i may not necessarily contain only one pair (n_1, n_i), and also, the proof in [4] has errors. From the above result, we can see that, when conditions (16) and (17) hold, the folding integers n_i in (8) can be uniquely solved, and the above results in fact provide an algorithm for the solution of n_i from the erroneous remainders $\tilde{k}_i$. When n_i in (8) are correctly solved, the unknown parameter x can be estimated as

$$\hat{x} = \frac{1}{\sigma L}\sum_{i=1}^{L}\left(n_i + \frac{\tilde{k}_i}{M}\right)\lambda_i \tag{18}$$

and the estimate error can be upper bounded by

$$|x - \hat{x}| \le \frac{1+2\tau}{2M\sigma}\frac{1}{L}\sum_{i=1}^{L}\lambda_i. \tag{19}$$

The above estimate error of x is due to the precision errors ϵ_i and the remainder errors $k_i - \tilde{k}_i$.

III. Robust Chinese Remainder Theorem

We now go back to the CRT problem (4)–(6) where the precision errors $\epsilon_i = 0$ are because the CRT concerns only integers and there are no fractional errors. From (4) and (5), we can see that, for each i with $1 \le i \le L$, modulo $M_i = M\Gamma_i$ and remainder r_i have a common factor Γ_i, and thus, integer n also has factor Γ_i. Since a remainder is known *a priori* to have a factor Γ_i, its erroneous version $\tilde{r}_i$ has a factor Γ_i, too, i.e., $\tilde{r}_i = \tilde{k}_i\Gamma_i$. Thus,

$$\tilde{r}_i - r_i = \epsilon_i\Gamma_i. \tag{20}$$

Assume

$$|\epsilon_i| \le \tau, \text{ i.e., } |\tilde{k}_i - k_i| \le \tau. \tag{21}$$

Then, for $1 \le i \le L$

$$n = n_iM_i + \tilde{k}_i\Gamma_i + \epsilon_i\Gamma_i. \tag{22}$$

Since n has factors Γ_i for $1 \le i \le L$, integer n has to have the form $n = n_0\Gamma_1\Gamma_2 \ldots \Gamma_L$ for some integer n_0. Using Theorem 1, we immediately have the following corollary.

Corollary 1: Let $n = n_0\Gamma_1\Gamma_2 \ldots \Gamma_L$ for some nonnegative integer n_0. If $n_0 < M$ and $M > 2\tau(\Gamma_1 + \Gamma_L)$, then n_i, $1 \le i \le L$, in (22) can be uniquely determined from $\tilde{k}_i$, Γ_i, and M, $1 \le i \le L$, via (12)–(15). An estimate of n is

$$\hat{n} = \frac{1}{L}\sum_{i=1}^{L}(n_iM_i + \tilde{k}_i\Gamma_i) \tag{23}$$

and its error is upper bounded by

$$|\hat{n} - n| = \frac{1}{L}\left|\sum_{i=1}^{L}\epsilon_i\Gamma_i\right| \le \frac{\tau}{L}\sum_{i=1}^{L}\Gamma_i. \tag{24}$$

□

In the conventional CRT, the moduli have to be pair-wisely co-prime, such as Γ_i. In this case, the reconstruction of n would be expressed as

$$\hat{n} = \sum_{i=1}^{L} \tilde{r}_i \gamma_i N_i \tag{25}$$

where N_i is a positive integer such that $N_i\gamma_i = 1 \bmod \Gamma_i$, and $\tilde{r}_i$ is an erroneous remainder of n modulo Γ_i with error $|\epsilon_i| = |r_i - \tilde{r}_i| \le \tau$, $1 \le i \le L$. Clearly, the above estimate error due to the erroneous remainders is at least

$$\epsilon_i \Gamma_1 \Gamma_2 \dots \Gamma_{L-1}$$

which is at least in the order of

$$\tau \Gamma_1 \Gamma_2 \dots \Gamma_{L-1}. \tag{26}$$

Comparing (26) with the error estimate (24) in Corollary 1, our proposed robust CRT has much less error than the conventional CRT does. Furthermore, in our case here, the moduli $M_i = M\Gamma_i$, $1 \le i \le L$ and have a common divisor M, and therefore, the conventional CRT reconstruction formula (25) does not apply. Our study above also provides a reconstruction algorithm of an integer n from its erroneous remainders when moduli are not pair-wisely co-prime.

IV. Simulations

We now see some simple simulations. We first consider our proposed robust phase unwrapping algorithm in Section II. Consider the case when $L = 3$, $\lambda_1 = 0.4$, $\lambda_2 = 0.5$, $\lambda_3 = 0.7$, and $\sigma = 1$. We take $\Gamma = 10$. Thus, $\Gamma_1 = 4$, $\Gamma_2 = 5$, and $\Gamma_3 = 7$. In this case, the maximal range of determinable x in (16) is 14. In our simulations, the unknown parameter x is uniformly distributed of any real value in the interval $[0, 14)$. We take $M = (1+2\tau)(\Gamma_1 + \Gamma_L) + 1$ in (17) and consider the maximal remainder error levels $\tau = 0,1,2,3,4,5$. The error between the estimate $\hat{x}$ in (18) and the true value x is plotted by the solid line marked with $\times$, and the error upper bound in (19) is plotted by the solid line marked with $*$ in Fig. 1. Noticing that the mean value of x is 7, one can see that the reconstruction errors of x from the erroneous remainders $\tilde{k}_i$ in (8) are small. Since the parameter x is a general real number, there is a precision error ϵ_i in (2) that is reflected from error curves shown in Fig. 1 when there is no remainder errors, i.e., when $\tau = 0$. The results shown in Fig. 1 are obtained from 200 trials.

For the robust CRT proposed in Section III, we use the same parameters as in Fig. 1, namely, $L = 3$, $\Gamma_1 = 4$, $\Gamma_2 = 5$, $\Gamma_3 = 7$, and the maximal remainder error levels $\tau = 0,1,2,3,4,5$. We also take $M = (1 + 2\tau)(\Gamma_1 + \Gamma_L) + 1$. Note that $M = 2\tau(\Gamma_1 + \Gamma_L) + 1$ is sufficient as stated in Corollary 1 but is not taken to avoid $M = 1$ when $\tau = 0$, which can be, however, easily verified similarly. For an integer $n = n_0\Gamma_1\Gamma_2 \dots \Gamma_L$, integer n_0 is uniformly taken in the interval $[0, M-1]$, including 0 and $M - 1$. The estimate error of $\hat{n}$ in (23) from the true n is plotted by the solid line marked with $\times$ in Fig. 2. The estimate error upper bound in (24) is plotted by the solid line marked with $*$ in Fig. 2. The errors shown in Fig. 2 can be thought of as absolute errors. The relative errors are shown in Fig. 3, and the curves in Fig. 3 are the error curves shown in Fig. 2 divided by the mean values of n, respectively. The results shown in Figs. 2 and 3 are obtained from 500 trials. One can see that our robust CRT provides small relative estimate errors when the remainders are erroneous, which the conventional CRT cannot provide. Compared to the robust phase unwrapping algorithm dealing with real numbers x in Fig. 1, we are dealing with integers n here, and thus, there are no precision errors, i.e., $\epsilon_i = 0$, in (2). The reconstruction (23) is accurate when there is no remainder errors, i.e., $\tau = 0$, which can be verified from Figs. 2 and 3, where the errors are all zero when $\tau = 0$.

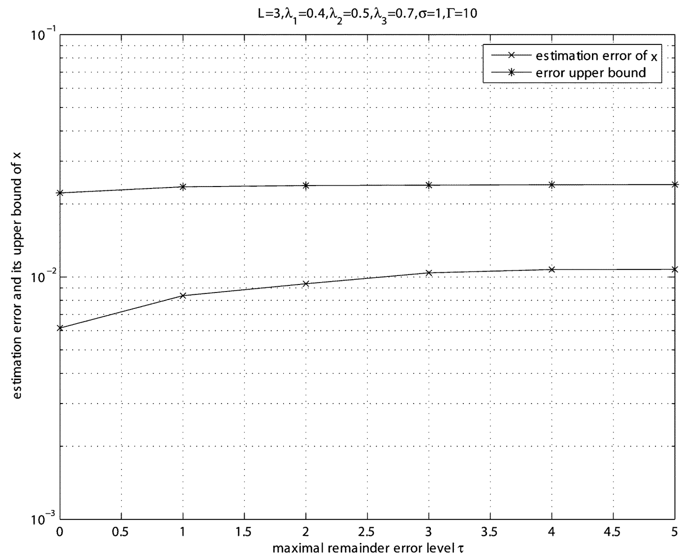

Fig. 1. Estimate error of $\hat{x}$ in (18) and its upper bound in (19) using proposed robust phase unwrapping algorithm. x is a uniformly distributed real number in $[0, 14)$.

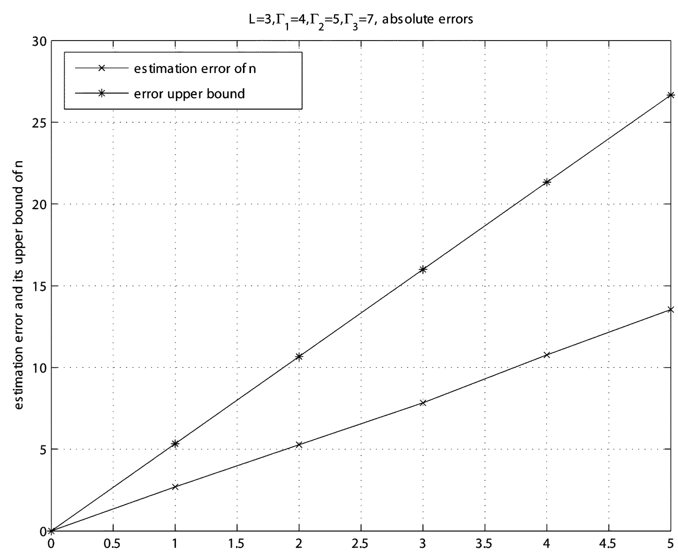

Fig. 2. Absolute estimate error of $\hat{n}$ in (23) and its upper bound in (24) using proposed robust CRT.

V. Conclusion

In this letter, we proposed a robust phase unwrapping algorithm when the remainders have errors. Motivated from the robust phase unwrapping algorithm, we proposed a type of robust CRT for erroneous remainders. As we have mentioned before, what we want to emphasize here is that our proposed robust CRT is not trying to correct remainder errors nor precisely reconstruct an integer as in [1]–[3] but to reduce the reconstruction error

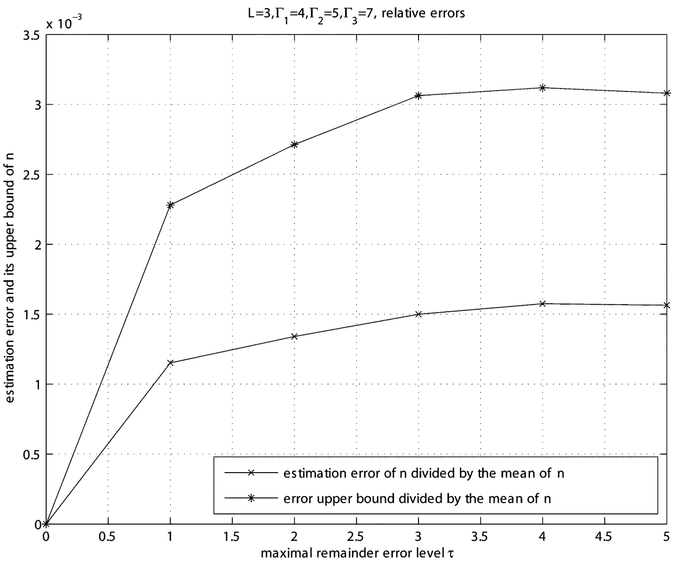

Fig. 3. Relative estimate error of $\hat{n}$ in (23) and its upper bound in (24) using proposed robust CRT.

from the conventional (non-robust) CRT. Also, what we studied in this letter is only for one integer (one x or one target) and different from the generalized CRT recently studied in [5]–[7], where multiple integers (multiple x or multiple targets) and sufficiently many moduli (remainder sets) are involved. Simulation results were provided to verify the theory. As a remark, this letter not only corrected an error on a result obtained in [4] but also considered a more general case for erroneous remainders than in [4].

APPENDIX
PROOF OF THEOREM 1

From Condition (16) on x, it is not hard to see that the true solution n_i in (8) falls in the range $0 \le n_i < \gamma_i$ for $1 \le i \le L$. Thus, for $2 \le i \le L$ and any $(\bar{n}_1, \bar{n}_i) \in S_i$, we have

$$\left|\bar{n}_i\Gamma_i + \frac{\tilde{k}_i\Gamma_i}{M} - \bar{n}_1\Gamma_1 - \frac{\tilde{k}_1\Gamma_1}{M}\right| \le \left|n_i\Gamma_i + \frac{\tilde{k}_i\Gamma_i}{M} - n_1\Gamma_1 - \frac{\tilde{k}_1\Gamma_1}{M}\right|. \quad (27)$$

From (8)

$$\Gamma\sigma x = n_i\Gamma_i + \frac{\tilde{k}_i}{M}\Gamma_i + \epsilon_i\Gamma_i, \quad 1 \le i \le L. \quad (28)$$

Let $\mu_i \triangleq \bar{n}_i - n_i$ for $1 \le i \le L$. From (28), we replace $(\tilde{k}_i/M)\Gamma_i$ by $\Gamma\sigma x - n_i\Gamma_i - \epsilon_i\Gamma_i$ in both sides of (27) and have

$$|\mu_i\Gamma_i - \mu_1\Gamma_1 - (\epsilon_i\Gamma_i - \epsilon_1\Gamma_1)| \le |\epsilon_i\Gamma_i - \epsilon_1\Gamma_1|.$$

Thus, using (9) and (17), we have

$$|\mu_i\Gamma_i - \mu_1\Gamma_1| \le 2|\epsilon_i\Gamma_i - \epsilon_1\Gamma_1| \le \frac{1+2\tau}{M}(\Gamma_1 + \Gamma_i) < 1. \quad (29)$$

Since μ_i, Γ_i, μ_1, and Γ_1 are all integers, (29) implies

$$\mu_i\Gamma_i = \mu_1\Gamma_1, \quad i = 2, 3, \ldots, L. \quad (30)$$

Since Γ_i and Γ_1 are co-prime, (30) implies

$$\mu_1 = m_i\Gamma_i \text{ and } \mu_i = m_i\Gamma_1$$
$$\text{i.e., } \bar{n}_1 = n_1 + m_i\Gamma_i \text{ and } \bar{n}_i = n_i + m_i\Gamma_1 \quad (31)$$

for some integers m_i with $|m_i| < \min(\gamma_i, \gamma_1)$. Replacing (31) into (27), we find that

$$\left|n_i\Gamma_i + \frac{\tilde{k}_i\Gamma_i}{M} - n_1\Gamma_1 - \frac{\tilde{k}_1\Gamma_1}{M}\right| = \left|\bar{n}_i\Gamma_i + \frac{\tilde{k}_i\Gamma_i}{M} - \bar{n}_1\Gamma_1 - \frac{\tilde{k}_1\Gamma_1}{M}\right| \quad (32)$$

which means $(n_1, n_i) \in S_i$ for $i = 2, 3, \ldots, L$. This proves $n_1 \in S$. We next show $S = \{n_1\}$. Property (31) also implies

$$S_i = \{(n_1 + m_i\Gamma_i, \quad n_i + m_i\Gamma_1) : \text{ for some integers } m_i \text{ with } |m_i| < \min(\gamma_i, \gamma_1)\}. \quad (33)$$

If $\bar{n}_1 \in S$, then $\bar{n}_1 \in S_{i,1}$ for $i = 2, 3, \ldots, L$, and therefore, from the definition of $S_{i,1}$ in (14) and (33), we have $\bar{n}_1 - n_1 = m_i\Gamma_i$ for some integer m_i with $|m_i| < \min(\gamma_i, \gamma_1)$ for $i = 2, 3, \ldots, L$. This implies that $\bar{n}_1 - n_1$ divides all Γ_i for $i = 2, 3, \ldots, L$, and therefore, from (12), $\bar{n}_1 - n_1$ is a multiple of γ_1. Since $0 \le \bar{n}_1, n_1 \le \gamma_1 - 1$, we conclude $\bar{n}_1 - n_1 = 0$. This proves that $S = \{n_1\}$. In the meantime, $\bar{n}_1 = n_1$ implies $m_i = 0$ in (33), i.e., $\bar{n}_i = n_i$ for $i = 2, 3, \ldots, L$. Hence, Theorem 1 is proved. As a remark, despite the fact that [4] only considers the case when $\tau = 0$, the proof in [4] has errors.

REFERENCES

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

[2] 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.

[3] I. E. Shparlinski and R. Steinfeld, *Noisy Chinese Remaindering in the Lee Norm*, to be published.

[4] 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.

[5] X.-G. Xia, "Estimation of multiple frequencies in undersampled complex valued waveforms," *IEEE Trans. Signal Process.*, vol. 47, no. 12, pp. 3417–3419, Dec. 1999.

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

[7] X.-G. Xia and K. Liu, "A generalized Chinese remainder theorem for residue sets with errors and its application in frequency determination from multiple sensors with low sampling rates," *IEEE Signal Process. Lett.*, vol. 12, no. 11, pp. 768–771, Nov. 2005.

[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. IGASS*, 1994, pp. 730–732.

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

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