A Generalized Chinese Remainder Theorem for Residue Sets With Errors and Its Application in Frequency Determination From Multiple Sensors With Low Sampling Rates

Xiang-Gen Xia and Kejing Liu

***Abstract*—The Chinese remainder theorem (CRT) has been recently generalized from determining a single integer from its remainders to determining multiple integers from their sets (residue sets) of remainders. In this letter, we consider the generalized CRT when the residue sets have errors. We first obtain a sufficient condition on the number of erroneous residue sets so that multiple integers still can be uniquely determined from their residue sets. We then propose a determination algorithm of multiple integers from their residue sets with errors. Finally, we apply the newly proposed algorithm to multiple frequency determination from multiple sensors with low sampling rates and show the effectiveness of the proposed algorithm with considering residue set errors over the one without considering residue set errors.**

***Index Terms*—Chinese remainder theorem (CRT), multiple frequency determination, remainder errors, sensor networks, undersampling.**

I. Introduction

THE conventional Chinese remainder theorem (CRT) is to determine a single integer from its remainders from a set of modulos. It has tremendous applications in various areas, such as cryptography [11] and digital signal processing [10]. CRT has various generalizations [11]. A different generalization of CRT has been recently proposed in [1]–[3], where (instead of a single integer in CRT) multiple integers need to be determined from (not a sequence of remainders but) a sequence of sets, residue sets, of remainders. A residue set consists of the remainders of multiple integers modulo a modulus integer, and the residue set is not ordered, i.e., the correspondence between the elements in the residue set and the multiple integers is not specified. The generalized CRT studied in [1] was motivated from the determination of multiple frequencies in a superpositioned signal of multiple sinusoids from its multiple undersampled waveforms. This has applications in a sensor network, where multiple sensors have low power and low transmission rates, and their sampling rates may be low and much lower than the Nyquist rate of a signal of interest in the field. The generalized CRT has been used in synthetic aperture radar (SAR) imaging of moving targets [4] and polynomial phase signal detection [5].

In the study of the generalized CRT in [1]–[3] and [6], it is assumed that the residue sets do not have errors, i.e., all remainders are assumed error free. In some applications, such as the multiple frequency determination studied in [1], errors may occur in the remainders. The main goal of this letter is to consider the generalized CRT when some of the remainders in residue sets have errors. We first present a sufficient condition on the number of residue sets with errors so that the multiple integers still can be uniquely determined from the residue sets with errors and the corresponding modulos. We then present a determination algorithm. Finally, we apply the proposed algorithm for the generalized CRT with residue set errors to the multiple frequency determination in a superpositioned signal contaminated by additive noise from its undersampled signals at multiple sensors. Our simulation results show that the error rates of multiple frequencies can be significantly reduced with the proposed algorithm considering residue errors compared to the one in [3] without considering residue set errors. Note that the conventional CRT with remainder errors has been nicely studied in [7]–[9].

This letter is organized as follows. In Section II, we describe the problem. In Section III, we first present a sufficient condition on the number of residue sets of errors for the unique determination and then present an algorithm for the unique determination. In Section IV, we apply the proposed algorithm in a sensor network with low sampling rates.

II. Problem Formulation

Let $S = \{N_1, N_2, \ldots, N_\rho\}$ be a set of distinct positive integers and $P = \{p_1, p_2, \ldots, p_\gamma\}$ be a set of positive integers that, without loss of generality, is assumed relatively coprime, i.e., any two of $p_r, 1 \le r \le \gamma$ are coprime, and $p_1 < p_2 < \cdots < p_\gamma$. The remainder (or residue) of N_l modulo p_r is

$$k_{l,r} \equiv N_l \bmod p_r \quad \text{for } 1 \le l \le \rho, \quad 1 \le r \le \gamma. \tag{1}$$

For $1 \le r \le \gamma$, define the residue set of S modulo p_r

$$S_r(N_1, N_2, \ldots, N_\rho) \triangleq \{k_{l,r} : l = 1, 2, \ldots, \rho\}. \tag{2}$$

Thus, there are γ residue sets $S_r(N_1, N_2, \ldots, N_\rho), 1 \le r \le \gamma$. Furthermore, some of these residue sets may have errors.

Manuscript received June 13, 2005; revised July 14, 2005. This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant F49620-02-1-0157 and Grant FA9550-05-1-0161 and in part by the National Science Foundation under Grant CCR-0097240 and Grant CCR-0325180. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Hakan Johansson.

The authors are with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: xxia@ee.udel.edu; liu@ee.udel.edu).

Digital Object Identifier 10.1109/LSP.2005.856877

What we know is $\tilde{S}_r(N_1, N_2, \ldots, N_\rho), 1 \le r \le \gamma$, that are $S_r(N_1, N_2, \ldots, N_\rho), 1 \le r \le \gamma$, contaminated with errors. Suppose the correspondence between error contaminated residue set $\tilde{S}_r(N_1, N_2, \ldots, N_\rho)$ and $p_r \in P$ for $1 \le r \le \gamma$ is specified, but the correspondence between N_l and its remainder $k_{l,r}$ is not known.

The *problem* is to determine set S of multiple integers $N_1, N_2, \ldots, N_\rho$ from the γ error contaminated residue sets $\tilde{S}_r(N_1, N_2, \ldots, N_\rho)$ and their corresponding modulos $p_r, 1 \le r \le \gamma$.

There are three questions associated with the above problem. 1) What is the dynamic range of these multiple integers N_l so that they can be uniquely determined? 2) How many errors of the residue sets can be corrected? 3) How can these multiple integers be determined? When $\rho = 1$ and there are no errors in remainders, CRT provides a complete solution for the above problem. When $\rho = 1$ but there are errors in remainders, it is the CRT with errors [7]. When $\rho > 1$ and there are no errors in remainders, it is the generalized CRT studied in [1]–[3] and [6]. In [1], a dynamic range for the uniqueness of the determination of the multiple integers when the residue sets do not have any errors is given: If

$$\max\{N_1, N_2, \ldots, N_\rho\} < \max\{p, p_\gamma\} \tag{3}$$

where

$$p = \min_{1 \le r_1 < r_2 < \cdots < r_\eta \le \gamma} \operatorname{lcm}\{p_{r_1}, p_{r_2}, \ldots, p_{r_\eta}\} = p_1 p_2 \ldots p_\eta \tag{4}$$

where

$$\gamma = \eta\rho + \theta \tag{5}$$

for some $0 \le \theta < \rho$. In [3], based on the above dynamic range, an efficient determination algorithm is proposed. In the following, the results obtained in [1] and [3] are generalized to the case when residue sets have errors.

III. Uniqueness and a Determination Algorithm

We first have a uniqueness result on the determination of $N_l, 1 \le l \le \rho$, from their erroneous residue sets $\tilde{S}_r(N_1, \ldots, N_\rho)$ and $p_r, 1 \le r \le \gamma$.

For $0 < \xi < \eta$ with η defined in (5), let

$$p(\xi) \triangleq p_1 p_2 \ldots p_\xi \tag{6}$$

and let e denote the size of the following set (i.e., the number of residue sets with errors):

$$\{r : \tilde{S}_r(N_1, \ldots, N_\rho) \ne S_r(N_1, \ldots, N_\rho), 1 \le r \le \gamma\}. \tag{7}$$

Then, we have the following result.

Theorem 1: If integers $\{N_l\}$ and the number e of residue sets with errors satisfy, respectively

$$\max\{N_1, \ldots, N_\rho\} < \max\{p(\xi), p_\gamma\} \tag{8}$$

$$e \le \frac{(\eta - \xi)\rho + \theta}{2} \tag{9}$$

where θ and η are defined in (5), then integers $N_l, 1 \le l \le \rho$, can be uniquely determined from $\tilde{S}_r(N_1, \ldots, N_\rho)$ and $p_r, 1 \le r \le \gamma$.

Proof: Assume there are two sets of integers $\{N_1, \ldots, N_\rho\}$ and $\{M_1, \ldots, M_\rho\}$ satisfying the above conditions with the same residue sets $\tilde{S}_r(N_1, \ldots, N_\rho)$ and modulos $p_r, 1 \le r \le \gamma$. From condition (9), we have $\gamma - 2e \ge \xi\rho$, and thus, these two sets of integers share at least $\xi\rho$ common residue sets without errors. By noticing the dynamic range (8), one may replace η in the proof in [1] with ξ and the rest of the proof to show $\{N_1, \ldots, N_\rho\} = \{M_1, \ldots, M_\rho\}$ is the same as the one in [1]. ∎

We next generalize the algorithm proposed in [3] to residue sets with errors, which will also confirm the result in Theorem 1. Based on the known γ error contaminated residue sets $\tilde{S}_r(N_1, \ldots, N_\rho)$, we define their product set

$$\tilde{S}(N_1, \ldots, N_\rho) = \tilde{S}_1(N_1, \ldots, N_\rho) \times \cdots \times \tilde{S}_\gamma(N_1, \ldots, N_\rho). \tag{10}$$

A. Determination Algorithm

Step 1: Arbitrarily take a vector $(k_1, \ldots, k_\gamma) \in \tilde{S}(N_1, \ldots, N_\rho)$ in (10). We know that there are at most e remainders in the residue vector $(k_1, \ldots, k_\gamma)$ wrong, i.e., there are at least $\gamma - e$ correct remainders in this residue vector.

Step 2: For each $r, 1 \le r \le \gamma$, define the coset of k_r

$$\mathcal{N}_r = \{k_r + np_r : k_r \le k_r + np_r < p(\xi), \text{and integers } n\} \tag{11}$$

where $p(\xi)$ is defined in (6). Note that all the numbers in set $\mathcal{N}_r$ have the same remainder k_r modulo p_r.

Step 3: From (9), it is easy to check that $\gamma - e \ge \xi\rho$, i.e., there are at least $\xi\rho$ error-free residue sets, but there are only ρ different integers $N_l \in S$. Thus, there are at least ξ correct remainders sharing a common integer in S, i.e., there exist integers $r_1, \ldots, r_\xi$ with $1 \le r_1 < \cdots < r_\xi \le \gamma$ such that the remainders $k_{r_1}, \ldots, k_{r_\xi}$ are error free and from a common integer, which means that

$$\mathcal{U} \triangleq \mathcal{N}_{r_1} \cap \mathcal{N}_{r_2} \cap \cdots \cap \mathcal{N}_{r_\xi} \ne \emptyset.$$

Based on this observation, Step 3 is to look for indices $1 \le r_1 < \cdots < r_\xi \le \gamma$ such that $\mathcal{U} \ne \emptyset$. Due to the dynamic range condition (8) and (11), by the conventional CRT, set $\mathcal{U} \ne \emptyset$ has only one element, i.e., $\mathcal{U} = \{\bar{N}\}$. Note that, for indices $1 \le r_1 < \cdots < r_\xi \le \gamma$ such that $\mathcal{U} = \{\bar{N}\}$, its remainders $k_{r_1}, \ldots, k_{r_\xi}$ may not be necessarily remainders of a single integer in S. If they were remainders of a single integer in S, we would have $\bar{N} \in S$. The next step is to check when $\bar{N} \in S$.

Step 4: Check whether $\bar{N}$ is a valid integer; check how many remainders $\bar{k}_r = \bar{N} \bmod p_r$ belong to $\tilde{S}_r(N_1, \ldots, N_\rho)$ for $1 \le r \le \gamma$. Let $\bar{\gamma}$ be the cardinality of the set $R \triangleq \{\bar{k}_r \in \tilde{S}_r(N_1, \ldots, N_\rho) : 1 \le r \le \gamma\}$. If

$$\bar{\gamma} \ge \gamma - \frac{(\eta - \xi)\rho + \theta}{2} = \frac{\gamma}{2} + \frac{\xi\rho}{2} \tag{12}$$

then $\bar{N}$ is a valid integer, i.e., $\bar{N} \in S$.

In fact, when (12) holds, due to (9), the remainder set R has at least

$$\bar{\gamma} - \frac{(\eta-\xi)\rho+\theta}{2} \geq \gamma - ((\eta-\xi)\rho+\theta) = \xi\rho$$

correct remainders. Since there are only ρ integers in S, there exist at least ξ remainders in R sharing a common integer N_l in S. With the same argument as in Step 3, we conclude that $\bar{N} = N_l \in S$.

If $\bar{N}$ is not a valid integer, take another index set $\{r_1, r_2, \ldots, r_\xi\}$ such that

$$\mathcal{N}_{r_1} \cap \mathcal{N}_{r_2} \cap \cdots \cap \mathcal{N}_{r_\xi} \neq \emptyset = \{\bar{N}\}$$

until $\bar{N}$ is a valid integer. Denote the valid integer as N_ρ. Note that the existence of such a valid $\bar{N}$ is ensured by the analysis in Step 3.

Step 5: For $r = 1, 2, \ldots, \gamma$, remove $k_{\rho,r} = N_\rho \bmod p_r$ from the residue set $\tilde{S}_r(N_1, \ldots, N_\rho)$ to form a new residue set $\tilde{S}_r(N_1, \ldots, N_{\rho-1})$ given in (13), shown at the bottom of the page, for $1 \leq r \leq \gamma$, where $|\cdot|$ denotes the cardinality of a set. If $k_{\rho,r} \notin \tilde{S}_r(N_1, \ldots, N_\rho)$, an erroneous residue set is detected, and it is removed from the residue sets for any further consideration. We replace γ by $\gamma - 1$ and e by $e-1$, or it is kept unchanged for the next iteration because some of its elements may be correct remainders. We also remove N_ρ from S and set $S = S - \{N_\rho\}$.

Step 6: Go to Step 1 by replacing ρ with $\rho - 1$ and changing the residue product set $\tilde{S}(N_1, \ldots, N_\rho)$ into $\tilde{S}(N_1, \ldots, N_{\rho-1})$. Repeat this process until N_1 is determined.

End of the algorithm.

Note that the above validation of the algorithm also confirms that when the dynamic range (8) holds and the number of erroneous residue sets satisfies (9), multiple integers can be uniquely determined from their residue sets with errors. Comparing with the generalized CRT without residue set errors obtained in [1] and [3], the robustness to the residue set errors studied in this letter comes from the sacrifice of the dynamic range of ρ uniquely determinable integers $N_l \in S$, which is reduced from $p_1 \ldots p_\eta$ to $p_1 \ldots p_\xi$ with $\xi < \eta$. As a remark, the above algorithm may have high complexity when the parameters are large. Any faster algorithm would be interesting.

As an example, consider two integers, i.e., $\rho = 2$ and $\gamma = 15$ relatively coprime integers: 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, or 67. Choose $\xi = 4$. In this case, $\eta = 7$. Then, according to the above results, if two positive integers $N_1, N_2 < 11 \times 13 \times 17 \times 19 = 46\,189$; then, these two integers can be uniquely determined from their 15 residue sets, even when three of these 15 residue sets are erroneous. Corresponding to the multiple frequency determination application studied in [1], two frequencies as high as 46 188 Hz in a superpositioned signal can be uniquely determined from 15 undersampled waveforms with the highest sampling rate 67 Hz, where any three of the undersampled waveforms may be completely damaged. Note that if there are no errors in residue sets, from the results obtained in [1] and [2], two uniquely determinable frequencies can go as high as $11 \times 13 \times 17 \times 19 \times 23 \times 29 \times 31 - 1 = 955\,049\,952$ Hz with the same sampling rates as above.

IV. Frequency Determination From Multiple Sensors With Low Sampling Rates

In this section, we apply the proposed algorithm in Section III to determine multiple frequencies from multiple sensors with undersampling rates. Consider γ sensors with sampling rates p_r Hz and p_r to satisfy the assumptions made in the beginning of Section II, $1 \leq r \leq \gamma$. Consider ρ multiple frequencies $f_1 = N_1$ Hz, $\ldots$, $f_\rho = N_\rho$ Hz in a superpositioned waveform. At the rth sensor, the received analog signal is of the following form:

$$x_r(t) = \sum_{l=1}^{\rho} A_{l,r} e^{2\pi j f_l t} + w_r(t) \tag{14}$$

where $A_{l,r}, 1 \leq l \leq \rho$ are nonzero complex coefficients, and $w_r(t)$ is the additive white noise. The sampled signal at the rth sensor with sampling rate p_r Hz is

$$x_r[n] = x_r\left(\frac{n}{p_r}\right) = \sum_{l=1}^{\rho} A_{l,r} e^{2\pi j f_l n/p_r} + w_r\left(\frac{n}{p_r}\right) \tag{15}$$

which also can be thought of as a received signal at a base station from the rth sensor. The problem is to determine the multiple frequencies $f_l = N_l, 1 \leq l \leq \rho$, from the above sampled data $x_r[n], 1 \leq r \leq \gamma$, where the sampling rates p_r may be much lower than the signal frequencies N_l. Note that the above undersampling may be necessary when the transmission rates of multiple sensors are low.

Based on the sampled data $x_r[n]$ at the rth sensor, we take p_r-point discrete Fourier transform (DFT) and obtain

$$X_r[k] = \mathrm{DFT}_{p_r}(x_r[n]) = \sum_{l=1}^{\rho} \sqrt{p_r} A_{l,r} \delta(k - k_{l,r}) + W_r[k] \tag{16}$$

for $0 \leq k \leq p_r - 1$, where $k_{l,r}$ is the remainder of N_l modulo p_r. which is the same as in Section II. Clearly, if the noise power of $W_r[k]$ is not too high, i.e., the signal-to-noise ratio (SNR) is not too low, the remainder $k_{l,r}$ can be correctly detected from the DFT coefficients $X_r[k]$ through (16). Otherwise, the remainder $k_{l,r}$ may have an error, which precisely corresponds to the problem studied in Sections II and III. Thus, we may apply the algorithm developed in Section III to the above multiple frequency determination problem.

$$\tilde{S}_r(N_1, \ldots, N_{\rho-1}) \triangleq \begin{cases} \tilde{S}_r(N_1, \ldots, N_\rho) - \{k_{\rho,r}\}, & \text{if } k_{\rho,r} \in \tilde{S}_r(N_1, \ldots, N_\rho) \text{ and } |\tilde{S}_r(N_1, \ldots, N_\rho)| = \rho \\ \tilde{S}_r(N_1, \ldots, N_\rho), & \text{if } k_{\rho,r} \in \tilde{S}_r(N_1, \ldots, N_\rho) \text{ and } |\tilde{S}_r(N_1, \ldots, N_\rho)| < \rho \end{cases} \tag{13}$$

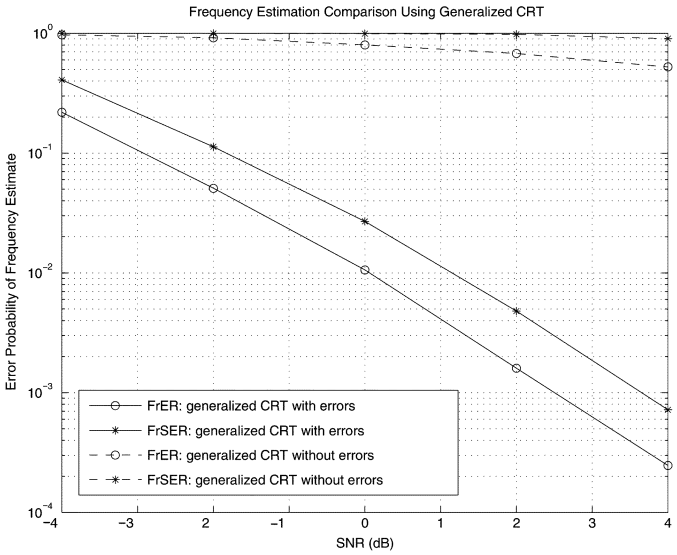

Fig. 1. Multiple frequency estimation comparison between generalized CRT with errors proposed in this letter and without errors proposed in [3].

We next see a simulation. In the simulation, consider three frequencies, i.e., $\rho = 3$, and 15 sensors with the sampling rates of primes from 11 to 67 (the same as the previous example) and choose $\xi = 3$. Thus, the dynamic range in (8) is $p(\xi) = p(3) = 11 \times 13 \times 17 = 2431$. The SNR is defined as the ratio of the variance of $A_{l,r}$ over the variance of the additive white Gaussian noise $w_r(n/p_r)$. In the simulation, three distinct frequencies N_1, N_2, N_3 are randomly chosen in the range between 2000 and 2431. The coefficients $A_{l,r}$ are randomly chosen from zero-mean complex Gaussian distributions, independently and identically in terms of l and r. From the theory we developed in Section III, three frequencies can be determined when any three signal waveforms from sensors are damaged or any three residue sets have errors. Two kinds of frequency detection error rates are calculated. One is the error rate of individual frequencies (FrER), and the other is the error rate of a frequency set (FrSER), i.e., when any of the three frequencies in the set is wrong, the set is counted wrong. In the simulation, for convenience, three remainders in $\tilde{S}_r(N_1, N_2, N_3)$ are selected after the p_r-point DFT from the three largest absolute values of the DFT coefficients for $1 \le r \le 15$. Also, when no valid integer $\bar{N}$ can be found in Step 4, a frequency set error and three frequency errors are counted, respectively. It is similarly done for the algorithm in [3]. The proposed algorithm (solid lines in Fig. 1) in Section III is compared with the algorithm (dashed lines in Fig. 1) in [3], where residue errors are not considered. From Fig. 1, one can see that the newly proposed algorithm significantly outperforms the one in [3] with a comparable complexity.

V. Conclusion

In this letter, we considered the generalized CRT with erroneous residue sets, i.e., the determination of multiple integers from a set of modulos and the corresponding residue sets with errors. We obtained a sufficient condition on the number of erroneous residue sets when a dynamic range of multiple integers is given, so that the multiple integers can be uniquely determined. We then presented an algorithm for the determination. The results in this letter are generalizations of the ones in [1] and [3] from error-free residue sets to erroneous residue sets, and the robustness to the errors in residue sets comes from the sacrifice of the dynamic range of multiple uniquely determinable integers. We finally applied the proposed algorithm to determine multiple frequencies from multiple sensors with much lower sampling rates than the Nyquist rate of a signal. Our simulation result shows that the error rates of the detected frequencies can be significantly reduced by using the algorithm proposed in this letter with considering residue errors from the ones using the algorithm proposed in [3] without considering residue errors.

References

[1] 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.

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

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

[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, "Dynamic range of the detectable parameters for polynomial phase signals using multiple-lag diversities in high-order ambiguity functions," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 1378–1384, May 2001.

[6] H. Liao and X.-G. Xia, "A sharpened dynamic range of a generalized Chinese remainder theorem for multiple integers," *Preprint*.

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

[8] 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.

[9] I. E. Shparlinski and R. Steinfeld, "Noisy Chinese remaindering in the Lee norm," *Preprint*.

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

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