Signal Processing 117 (2015) 242–246

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Fast communication

A new robust Chinese remainder theorem with improved performance in frequency estimation from undersampled waveforms ☆

Li Xiao *, Xiang-Gen Xia

Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716, USA

ARTICLE INFO

Article history:
Received 11 December 2014
Received in revised form
17 March 2015
Accepted 27 May 2015
Available online 9 June 2015

Keywords:
Chinese remainder theorem (CRT)
Frequency estimation from undersampled waveforms
Remainder errors
Robust CRT

ABSTRACT

A robust Chinese remainder theorem (CRT) has been recently proposed, that is, a large integer less than the least common multiple (lcm) of all the moduli can be robustly reconstructed from its erroneous remainders when all remainder errors are assumed small. In this paper, we propose a new robust CRT when a combined occurrence of multiple unrestricted errors and an arbitrary number of small errors is in the remainders, where a determinable integer is required to be less than the lcm of a subset of the moduli. A reconstruction algorithm is also proposed. We then apply the reconstruction algorithm to frequency estimation from undersampled waveforms. It shows that the newly proposed algorithm leads to a better performance than the previous existing robust CRT algorithm.

1. Introduction

It is well known that the conventional Chinese remainder theorem (CRT) with pairwise coprime moduli is not robust, i.e., a small error in a remainder may cause a large reconstruction error [1,2]. In order to resist remainder errors, redundancy has to be added in moduli. Two different methods of adding redundancy are usually adopted in the literature, namely, error-correcting codes (residue codes) [3–7] and robust CRT [8–11]. Residue codes are based on a Redundant Residue Number System (RRNS), i.e., given L pairwise coprime moduli $M_1 < \cdots < M_K < \cdots < M_L$, an integer N with $0 \le N < \prod_{i=1}^{K} M_i$ can be *accurately* reconstructed if there are $\lfloor (L-K)/2 \rfloor$ or fewer arbitrary errors (called unrestricted errors in this paper) in the remainders of N modulo M_i for $1 \le i \le L$, where $\lfloor \star \rfloor$ is the floor function. Robust CRT was recently developed based on the assumption that all the moduli have a common factor $M > 1$, i.e., $M_i = M\Gamma_i$ for $1 \le i \le L$ and $\Gamma_1 < \cdots < \Gamma_L$ are pairwise coprime. In this case, an integer N with $0 \le N < \mathrm{lcm}(M_1, \ldots, M_L) = M\Gamma_1 \cdots \Gamma_L$ can be *robustly* reconstructed if all remainder errors are small, i.e., the reconstruction error is upper bounded by the remainder error level τ if τ is smaller than $M/4$. Note that in residue codes the reconstruction of N is accurate but only a few of the remainders are allowed to have errors and most of the remainders have to be error-free, while in the robust CRT the reconstruction of N may not be accurate but robust and all the remainders are allowed to have small errors. The robust CRT has applications in frequency estimation from undersampled waveforms, for example, phase unwrapping in radar signal processing [12–15], multiwavelength optical interferometry [16], and sensor networks using multiple sensors [17,18].

In this paper, we propose a new robust CRT under the same assumption that moduli $M_i = M\Gamma_i$ for $1 \le i \le L$, $M > 1$, and $\Gamma_1 < \cdots < \Gamma_L$ are pairwise coprime. Different

☆ This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-12-1-0055.

* Corresponding author.
E-mail addresses: lixiao@ee.udel.edu (L. Xiao), xxia@ee.udel.edu (X.-G. Xia).

http://dx.doi.org/10.1016/j.sigpro.2015.05.017
0165-1684/

from the previous robust CRT in [8–11], it relaxes the constraint that all remainder errors have to be small, but sacrifices the dynamic range of a determinable large integer. It basically says that an integer N with $0 \le N < M\Gamma_1 \cdots \Gamma_K$, $K < L$, can be robustly reconstructed from its erroneous remainders when a combined occurrence of $\lfloor (L-K)/2 \rfloor$ or fewer unrestricted errors and an arbitrary number of small errors is in the remainders. The main idea in this new robust CRT is to incorporate the error correction algorithm for residue codes to determine the folding numbers (quotients) of N divided by M_i, while the folding numbers are directly determined via the conventional CRT in the previous robust CRT in [11]. Accordingly, a robust reconstruction algorithm is also proposed in this paper. With this newly proposed algorithm, an improvement in the performance of frequency estimation from undersampled waveforms is illustrated. Throughout the paper, $[\star]$ is defined as the rounding function, i.e., $[\star] = \lfloor \star + 1/2 \rfloor$.

The rest of the paper is organized as follows. In Section 2, we review the CRT and the error correction algorithm for residue codes, respectively. In Section 3, we propose our new robust CRT. A corresponding reconstruction algorithm is also proposed. In Section 4, with the proposed algorithm, we present some simulation results on frequency estimation from undersampled waveforms. In Section 5, we conclude this paper.

2. Preliminaries

Consider the following system of congruences in an unknown positive integer X:

$$x_i \equiv X \mod m_i, \quad 1 \le i \le L, \tag{1}$$

where remainders x_i with $0 \le x_i < m_i$ are known and moduli m_i are pairwise coprime positive integers, for $1 \le i \le L$. Then, if and only if $0 \le X < m = \prod_{i=1}^{L} m_i$, X can be uniquely reconstructed via the conventional CRT [1] as

$$X \equiv \sum_{j=1}^{L} x_j T_j \frac{m}{m_j} \bmod m, \tag{2}$$

where T_j is the modular multiplicative inverse of m/m_j modulo m_j, i.e., $1 \equiv T_j \frac{m}{m_j} \bmod m_j$.

Without loss of generality, assume that $m_1 < \cdots < m_K < \cdots < m_L$ with $K < L$ and X is selected from the subrange $[0, \prod_{i=1}^{K} m_i)$. Let $\tilde{x}_i$ for $1 \le i \le L$ denote the received remainders after passing through a noisy system. For the residue code based on the RRNS with moduli $m_1, \ldots, m_L$, it can correct up to $\lfloor (L-K)/2 \rfloor$ errors in the remainders [3,4], i.e., if there are $t \le \lfloor (L-K)/2 \rfloor$ received remainders $\tilde{x}_{i_v}$ for $1 \le v \le t$ such that $\tilde{x}_{i_v} \ne x_{i_v}$, where $\{i_1, \ldots, i_t\}$ is a subset of $\{1, \ldots, L\}$, then an integer X with $0 \le X < \prod_{i=1}^{K} m_i$ can be accurately reconstructed from $\tilde{x}_i$ for $1 \le i \le L$, with the following error correction algorithm as stated in [5].

1) Compute $\tilde{X}$ from the received remainder vector $(\tilde{x}_1, \ldots, \tilde{x}_L)$ using a formula based on (2):

$$\tilde{X} \equiv \sum_{j=1}^{L} \tilde{x}_j T_j \frac{m}{m_j} \bmod m. \tag{3}$$

2) If $0 \le \tilde{X} < \prod_{i=1}^{K} m_i$, stop and output $\tilde{X}$. Otherwise, go to Step 3).

3) Let $\mathbf{Z} = \left\{ \prod_{\beta=1}^{L-\lfloor (L-K)/2 \rfloor} m_{l_\beta} : \text{where } \{l_1, \ldots, l_{L-\lfloor (L-K)/2 \rfloor}\} \text{ is enumerated in all } \binom{L}{\lfloor (L-K)/2 \rfloor} \text{ possible different choices of } L - \lfloor (L-K)/2 \rfloor \text{ distinct elements in } \{1, \ldots, L\} \right\}$. For every element z in $\mathbf{Z}$, calculate

$$\hat{X}(z) \equiv \tilde{X} \bmod z. \tag{4}$$

If there is only one z_0 in $\mathbf{Z}$ such that $0 \le \hat{X}(z_0) < \prod_{i=1}^{K} m_i$, stop and output $\hat{X}(z_0)$.

(4) Otherwise, indicate that there are more than $\lfloor (L-K)/2 \rfloor$ errors in the remainders and end the algorithm without an output.

Remark 1 (*Goh and Siddiqi [5]*). In the above algorithm, if there are no errors in the remainders, i.e., $\tilde{x}_i = x_i$ for all $1 \le i \le L$, X can be accurately determined in Step 2), i.e., $\tilde{X} = X$; if there are $1 \le t \le \lfloor (L-K)/2 \rfloor$ errors in the remainders, X can be accurately determined in Step 3), i.e., $\hat{X}(z_0) = X$. However, if there are more than $\lfloor (L-K)/2 \rfloor$ errors in the remainders, the output in Step 2) or 3) may be not equal to X, or even the algorithm ends without an output.

3. A new robust CRT

Based on the above error correction algorithm for residue codes in [5] and robust CRT in [11], a new robust CRT is presented and the corresponding robust reconstruction algorithm is also proposed in this section.

Of particular interest in this paper is to study robust reconstruction from erroneous remainders when the greatest common divisor (gcd) of all the moduli is more than 1 and the remaining integers factorized by the gcd of all the moduli are pairwise coprime, i.e., moduli $M_i = M\Gamma_i$ for $1 \le i \le L$, $M > 1$, and $\Gamma_1 < \cdots < \Gamma_L$ are pairwise coprime positive integers. To begin with, let us review the result of the previous robust CRT in [8–11].

Let N be a positive integer and $r_1, \ldots, r_L$ be the L remainders of N, i.e.,

$$r_i \equiv N \bmod M_i \quad \text{or} \quad N = n_i M_i + r_i, \tag{5}$$

where $0 \le r_i < M_i$ and n_i is called a folding integer. The robust CRT problem is how to robustly reconstruct N with $0 \le N < \mathrm{lcm}(M_1, \ldots, M_L) = M\Gamma_1 \cdots \Gamma_L$ from the erroneous remainders $\tilde{r}_i$, i.e., for $1 \le i \le L$,

$$0 \le \tilde{r}_i < M_i \quad \text{and} \quad |\tilde{r}_i - r_i| \le \tau, \tag{6}$$

where $\Delta r_i = \tilde{r}_i - r_i$ denote the remainder errors and τ is called the remainder error level that may be determined by, for example, the signal-to-noise ratio (SNR). The basic idea is to accurately determine the folding integers n_i as in (5), and then an estimate of N is the average of $\hat{N}(i)$ as