sensors

MDPI

Article

An Efficient CRT Based Algorithm for Frequency Determination from Undersampled Real Waveform

Yao-Wen Zhang, Xian-Feng Han and Guo-Qiang Xiao *

College of Computer and Information Science, Southwest University, Chongqing 400715, China
* Correspondence: gqxiao@swu.edu.cn

Abstract: The Chinese Remainder Theorem (CRT) based frequency estimation has been widely studied during the past two decades. It enables one to estimate frequencies by sub-Nyquist sampling rates, which reduces the cost of hardware in a sensor network. Several studies have been done on the complex waveform; however, few works studied its applications in the real waveform case. Different from the complex waveform, existing CRT methods cannot be straightforwardly applied to handle a real waveform's spectrum due to the spurious peaks. To tackle the ambiguity problem, in this paper, we propose the first polynomial-time closed-form Robust CRT (RCRT) for the single-tone real waveform, which can be considered as a special case of RCRT for arbitrary two numbers. The time complexity of the proposed algorithm is $O(L)$, where L is the number of samplers. Furthermore, our algorithm also matches the optimal error-tolerance bound.

Keywords: robust Chinese Remainder Theorem; frequency estimation; undersampling; error bound; sensor network

Citation: Zhang, Y.-W.; Han, X.-F.; Xiao, G.-Q. An Efficient CRT Based Algorithm for Frequency Determination from Undersampled Real Waveform. *Sensors* **2023**, *23*, 452. https://doi.org/10.3390/s23010452

Academic Editors: Giacomo Capizzi, Grazia Lo Sciuto and Luca Di Nunzio

Received: 14 November 2022
Revised: 20 December 2022
Accepted: 27 December 2022
Published: 1 January 2023

1. Introduction

Chinese Remainder Theorem (CRT) is a fundamental number theory result, which shows the reconstruction of a single integer X from its residues modulo multiple co-prime moduli. It has been extensively used in various applications, such as wireless sensor networks [1,2], coding theory [3–7], phase unwrapping [8,9], and frequency estimation from undersampled waveforms [10–17]. In particular, the CRT-based method enables one to estimate frequencies with exponentially smaller sub-Nyquist rates in a distributed setup. This could significantly reduce hardware cost [18,19]. In practice, errors may occur in the spectrum measurement, while CRT is known highly sensitive to residue perturbation [20]. Moreover, in some applications of multiple parameter estimation, we may need to recover multiple real numbers simultaneously. To this end, many works have been proposed during the last two decades to solve the two issues, which can be summarized as follows.

(i) Robustness: On the one hand, to make CRT robust against small errors in residues, Wang et al. introduced a common factor Γ as redundancy to the co-prime moduli $\{M_1, M_2, \ldots, M_L\}$ in a form $\{m_l = M_l\Gamma | l = 1, 2, \ldots, L\}$. This forms the foundation of the first closed-form Robust CRT (RCRT) for a single real number [20]. RCRT can recover the folding number $\lfloor X/\Gamma \rfloor$ once the error in each residue is upper bounded by $\Gamma/4$. Hence, one can ensure the reconstruction error is upper bounded by $\Gamma/4$. The $\Gamma/4$ error tolerance bound is also proved to be tight in the follow-up works [21].

(ii) Residue Ambiguity: On the other hand, since the observed residues are unordered, there is no clear correspondence between N numbers $\{X_i | i = 1, 2, \ldots N\}$ and residues in each residue set $R_l = \{r_{i,l} | i = 1, 2, \ldots, N\}$, $l = 1, 2, \ldots, L$. Here, $r_{i,l}$ denotes the residue of X_i modulo m_l. Thus, the residue ambiguity makes reconstruction much more complicated for multiple numbers. When $N = 2$, Xiao et al. proposed a robust generalized CRT, addressing the residue ambiguity by carefully-designed quadratic symmetric polynomials [22]. It is shown that the correspondence between these two

numbers and residues can be uniquely determined while the error bound is sacrificed to $\Gamma/8$ [23]. As shown in recent works [24,25]; theoretically, one can approach the optimal error bound $\Gamma/4$ independent of N when the least common multiple of moduli is sufficiently large. However, to the best of our knowledge, no existing polynomial-time algorithm matches the optimal bound.

In this paper, we focus on CRT based algorithm for frequency determination from the undersampled real waveform. The proposed method can be applied in a sensor network with low power and low transmission rates sensors [26,27] or Synthetic Aperture Radar (SAR) imaging of moving targets [28]. However, in the real waveform scenario, the CRT-based method encounters both the above-mentioned challenges, robustness, and residue ambiguity, simultaneously.

Notably, the real waveform sampling needs less hardware, i.e., only one Analog-to-Digital Converter (ADC) per sampling frequency is required in real waveform sampling rather than two ADCs in complex waveform [29]. However, existing CRT methods for the complex waveform cannot be applied to the real waveform directly due to the existence of the spurious peak [24]. In this paper, we set out to solve these mentioned issues. Our main contributions can be concluded as follows.

- We present the first polynomial-time closed-form RCRT for frequency determination from undersampled single-tone real waveform, which provides a feasible and efficient solution. Moreover, the proposed method fixes the gap in the CRT-based method for frequency determination for the real waveform case.
- By fully utilizing the prior knowledge of the real waveform, we reach the optimal error tolerance bound, i.e., $\Gamma/4$, which is twice better than the best-known robust generalized CRT proposed in [23].

The remaining content is organized as follows. In Section 2, we give an overview of the problem formulation. Section 3 details our closed-form reconstruction for the real waveform. In Section 4, we present some simulation results to support the theory. In Section 5, we discuss and interpret the simulation results. The conclusion is drawn in Section 6.

2. Problem Formulation

We first describe the frequency estimation model from the undersampled real waveforms.

2.1. Signal Model and Sampling

A sinusoidal waveform is defined as

$$x(t) = A\cos(2\pi Xt) = \frac{1}{2}(Ae^{(2\pi jXt)} + Ae^{(-2\pi jXt)}), \tag{1}$$

where A denotes the amplitude, X represents the frequency. Sampling $x(t)$ with L ADCs at frequency rates of $\{m_l | l = 1, 2, \ldots, L\}$ [24,30], where $\max_l m_l < 2X$, i.e., the sampling rates are below the Nyquist rate, we have

$$x_{m_l}[u] = \frac{1}{2}(Ae^{\frac{2\pi jXu}{m_l}} + Ae^{\frac{-2\pi jXu}{m_l}}), \quad u \in \mathbb{Z}. \tag{2}$$

Applying the m_l-point Discrete Fourier Transform (DFT) to $x_{m_l}[u]$ [31,32], we obtain

$$DFT_{x_{m_l}[u]}[k] = \frac{A}{2}\delta(k - \langle X\rangle_{m_l}) + \frac{A}{2}\delta(k - \langle -X\rangle_{m_l}). \tag{3}$$

Here, $\delta(*)$ is the the Kronecker delta function, i.e., $\delta(k - \langle X\rangle_{m_l})$ equals 1 when $k = \langle X\rangle_{m_l}$ or 0 otherwise, where k represents a frequency bin and $\langle X\rangle_{m_l}$ denote the residue of X modulo m_l. Clearly, the locations of the spectrum peaks correspond to the residues $\langle X\rangle_{m_l}$ and $\langle -X\rangle_{m_l}$, which leads to two symmetric peaks over the frequency spectrum domain in the noiseless case. Thus, one can recover the frequency X with sampling rates (moduli) m_l and the locations of the spectrum peaks (residues) $\langle X\rangle_{m_l}$ via CRT.

2.2. Noise Model and RCRT Procedure

In the following, we further consider the noisy case and review RCRT. Still, let $X_i \in \{X_1, X_2\}$ represent the real number to be recovered, where $X_1 > 0$ and $X_2 = -X_1$. The moduli are in a form $\{m_l = M_l\Gamma | l = 1, 2, \dots L\}$, where $\{M_l\}$ are pairwise co-prime. $\tilde{r}_{i,l} = \langle X_i + \Delta_{i,l} \rangle_{m_l}$ denotes the erroneous residue of X_i modulo m_l, where $\Delta_{i,l}$ represents the underlying error such that $|\Delta_{i,l}| < \Gamma/4$. Moreover, $r_i^c = \langle X_i \rangle_\Gamma$ denotes the common residue of X_i. $\tilde{r}_{i,l}^c = \langle X_i + \Delta_{i,l} \rangle_\Gamma = \langle r_i^c + \Delta_{i,l} \rangle_\Gamma$ denotes the erroneous common residue. In practical cases, $\tilde{r}_{i,l}^c$ is calculated from $\tilde{r}_{i,l}$ based on the number theory, i.e., $\tilde{r}_{i,l}^c = \langle X_i + \Delta_{i,l} \rangle_\Gamma = \langle \langle X_i + \Delta_{i,l} \rangle_{M_l\Gamma} \rangle_\Gamma = \langle \tilde{r}_{i,l} \rangle_\Gamma$, which ensures that $\tilde{r}_{i,l}^c$ and $\tilde{r}_{i,l}$ share the same $\Delta_{i,l}$. For clarity, all the notations are listed in Table 1. In the following, we aim to estimate the real number X_1 with known erroneous residues $\tilde{r}_{i,l}$ and moduli m_l.

Table 1. List of Notations.

Notations	Explanation
M_l	Co-prime moduli
m_l	Moduli selected
X_i	Number to be recovered
$\hat{X}_i$	Estimation of X_i
$\lfloor X_i/\Gamma \rfloor$	The folding number of X_i
q_i	Estimation of $\lfloor X_i/\Gamma \rfloor$
$\tilde{r}_{i,l} = \langle X_i + \Delta_{i,l} \rangle_{m_l}$	Erroneous residue of X_i modulo m_l
$r_i^c = \langle X_i \rangle_\Gamma$	Common residue of X_i
$\tilde{r}_{i,l}^c = \langle r_i^c + \Delta_{i,l} \rangle_\Gamma$	Erroneous common residue of X_i
$\hat{r}_{i,l}^c$	Shifted common residue of X_i
$d(\tilde{r}_{i,l_1}^c, \tilde{r}_{i,l_2}^c)$	Minimum circular distance between $\tilde{r}_{i,l_1}^c$ and $\tilde{r}_{i,l_2}^c$ on the circle of length Γ
$I(\tilde{r}_{i,l_1}^c, \tilde{r}_{i,l_2}^c)$	Interval between $\tilde{r}_{i,l_1}^c$ and $\tilde{r}_{i,l_2}^c$

Since $X_i = \lfloor X_i/\Gamma \rfloor \Gamma + r_i^c$, we recover X_i by estimating the folding number $\lfloor X_i/\Gamma \rfloor$ and common residue r_i^c successively. We adopt the reconstruction framework proposed in [24], which consists of three steps:

(i) Estimate the folding number: Based on the fact that $X_i = k_i m_l + r_{i,l} = k_i M_l \Gamma + r_{i,l}$, where $k_i \in \mathbb{Z}$, we have $\lfloor X_i/\Gamma \rfloor = k_i M_l + \lfloor r_{i,l}/\Gamma \rfloor = k_i M_l + (r_{i,l} - \langle r_{i,l} \rangle_\Gamma)/\Gamma$. Clearly, $\langle r_{i,l} \rangle_\Gamma = \langle \langle X_i \rangle_{M_l\Gamma} \rangle_\Gamma = \langle X_i \rangle_\Gamma = r_i^c$. Thus, we have $\lfloor X_i/\Gamma \rfloor = k_i M_l + (r_{i,l} - r_i^c)/\Gamma$. By taking the modulo arithmetic, one can obtain

$$\lfloor \frac{X_i}{\Gamma} \rfloor \equiv \frac{r_{i,l} - r_i^c}{\Gamma} \mod M_l, \tag{4}$$

From (4), the folding number $\lfloor X_i/\Gamma \rfloor$ is estimated by the equation below via CRT [24],

$$q_i \equiv \frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma} \mod M_l, \tag{5}$$

where q_i denotes the estimation of $\lfloor X_i/\Gamma \rfloor$.

(ii) Estimate the common residues: Calculate $\sum_{l=1}^{L} \tilde{r}_{i,l}^c / L$ as the estimation of the common residue r_i^c.

(iii) Estimate the number: Based on $X_i = \lfloor X_i/\Gamma \rfloor \Gamma + r_i^c$, X_i is reconstructed by

$$\hat{X}_i = q_i \Gamma + \frac{\sum_{l=1}^{L} \tilde{r}_{i,l}^c}{L}, \tag{6}$$

where $\hat{X}_i$ represents the estimation of X_i.

2.3. Key Issues in Real Waveform

(i) Robustness: Trivially estimating the folding number by (5) may lead to large errors due to the ambiguity of $(\tilde{r}_{i,l} - \tilde{r}^c_{i,l})/\Gamma$. In other words, since $r^c_i \in [0, \Gamma)$ and $|\Delta_{i,l}| < \Gamma/4$, $(\tilde{r}_{i,l} - \tilde{r}^c_{i,l})/\Gamma$ must satisfy one of the three subcases below based on (4) [33],

$$\frac{\tilde{r}_{i,l} - \tilde{r}^c_{i,l}}{\Gamma} \equiv \begin{cases} \lfloor X_i/\Gamma \rfloor \mod M_l, & \text{if } r^c_i + \Delta_{i,l} \in [0, \Gamma) \\ \lfloor X_i/\Gamma \rfloor - 1 \mod M_l, & \text{if } r^c_i + \Delta_{i,l} \in (-\Gamma/4, 0) \\ \lfloor X_i/\Gamma \rfloor + 1 \mod M_l, & \text{if } r^c_i + \Delta_{i,l} \in [\Gamma, 5\Gamma/4) \end{cases} \tag{7}$$

If $r^c_i + \Delta_{i,l_1}$ and $r^c_i + \Delta_{i,l_2}$ fall into different subcases in (7), where $l_1, l_2 \in \{1, 2, \ldots, L\}$, simply aggregating them via CRT will bring unpredictable reconstruction errors. Thus, we need to unify $(\tilde{r}_{i,l} - \tilde{r}^c_{i,l})/\Gamma$ such that all of them fall into one subcase in (7) to ensure robustness. This can be achieved by sorting $\tilde{r}^c_{i,l}$, where $\tilde{r}^c_{i,l} = \langle r^c_i + \Delta_{i,l} \rangle_\Gamma$, in the order such that the corresponding $\Delta_{i,l}$ are in an ascending order for each i. However, the above operation is only implementable when $|\Delta_{i,l}| < \Gamma/8$ [34], while it still remains open in the generic setup $|\Delta_{i,l}| < \Gamma/4$.

(ii) Residue Ambiguity: Due to the loss of the correspondence between X_i and $\tilde{r}_{i,l}$, we cannot cluster $\tilde{r}_{i,l}$ corresponding to X_i to calculate q_i from (5) for each i.

3. Robust Reconstruction for Frequency Estimation of Single-Tone Real Waveform

This section presents the polynomial-time RCRT-based frequency estimation for a noisy single-tone real waveform. Before proceeding, the following notations are introduced.

We first define a metric to represent the minimum circular distance between $\tilde{r}^c_{i,l_1}$ and $\tilde{r}^c_{i,l_2}$ on the circle of length Γ, i.e.,

$$d(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2}) = \min_z |\tilde{r}^c_{i,l_1} - \tilde{r}^c_{i,l_2} + z\Gamma|, \; z \in \{-1, 0, 1\}. \tag{8}$$

For example, if $\Gamma = 12$, $d(1, 11) = 2$. Let $I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$ denote the interval between $\tilde{r}^c_{i,l_1}$ and $\tilde{r}^c_{i,l_2}$ on the circle (such as $I(\tilde{r}^c_{1,1}, \tilde{r}^c_{1,3})$ shown in Figure 1), whose length is $d(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$. $\max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$ represents the interval whose length is maximal. As shown in Figure 1, when $i = 1$, the maximum interval is $I(\tilde{r}^c_{1,1}, \tilde{r}^c_{1,3})$; when $i = 2$, $I(\tilde{r}^c_{2,1}, \tilde{r}^c_{2,3})$ is the maximum one.

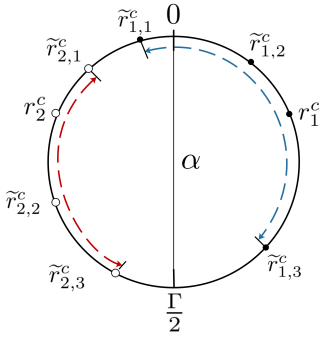


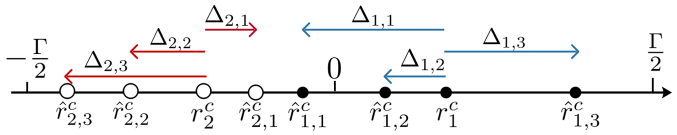
Figure 1. Illustration of the intervals.

3.1. The Order of Residues

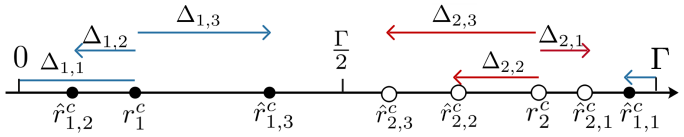
Now, we consider the first key issue stated in Section 2.3, i.e., sorting $\tilde{r}^c_{i,l}$ in the order such that the corresponding errors $\Delta_{i,l}$ are in ascending order for each i, where $\tilde{r}^c_{i,l} = \langle r^c_i + \Delta_{i,l} \rangle_\Gamma$. According to [21], sorting is equivalent to finding a cutting point ξ on the circle of length Γ and stretching it to a real axis. If $\xi \notin \max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$ for each i, the shifted common residues $\hat{r}^c_{i,l}$ on the real axis are sorted in ascending order of $\Delta_{i,l}$.

For example, in Figure 1, $\Gamma/2$ is not in the maximum intervals, i.e., $I(\tilde{r}^c_{1,1}, \tilde{r}^c_{1,3})$ and $I(\tilde{r}^c_{2,1}, \tilde{r}^c_{2,3})$. Then, cutting the circle at $\Gamma/2$ leads to $\hat{r}^c_{2,3} < \hat{r}^c_{2,2} < \hat{r}^c_{2,1}$ and $\hat{r}^c_{1,1} < \hat{r}^c_{1,2} < \hat{r}^c_{1,3}$ sorted in ascending order of $\Delta_{i,l}$, i.e., $\Delta_{2,3} < \Delta_{2,2} < 0 < \Delta_{2,1}$ and $\Delta_{1,1} < \Delta_{1,2} < 0 < \Delta_{1,3}$

shown in Figure 2a. On the contrary, if we cut the circle at 0, where $0 \in I(\tilde{r}^c_{1,1}, \tilde{r}^c_{1,3})$, $\Delta_{1,1}$ breaks the ascending order, as shown in Figure 2b. Here, $\hat{r}^c_{1,2} < \hat{r}^c_{1,3} < \hat{r}^c_{1,1}$, but $\Delta_{1,2}, \Delta_{1,3}, \Delta_{1,1}$ are in non-ascending order.



(a) $\xi = \Gamma/2$



(b) $\xi = 0$

Figure 2. Sketch of the Definition of $\hat{r}^c_{i,l}$.

However, the key remaining problem is how to find the proper cutting point without the correspondence between $\tilde{r}^c_{i,l}$ and X_i, i.e., $\max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$ is unknown. To this end, ref. [21] sacrifices the error bound to $\Gamma/8$. Nonetheless, we reach the error bound $\Gamma/4$ by using the symmetry of residues, i.e.,

$$r^c_2 = \langle X_2 \rangle_\Gamma = \langle -X_1 \rangle_\Gamma = \Gamma - r^c_1.$$

That is to say, r^c_1 and r^c_2 are axially symmetric about line α shown in Figure 1. Since $|\Delta_{i,l}| < \Gamma/4$, $d(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2}) < d(r^c_i - \Gamma/4, r^c_i + \Gamma/4) = \Gamma/2$, i.e., $\max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$ cannot contain 0 and $\Gamma/2$ simultaneously. Based on the symmetry, $\max_l I(\tilde{r}^c_{1,l_1}, \tilde{r}^c_{1,l_2}) \cup \max_l I(\tilde{r}^c_{2,l_1}, \tilde{r}^c_{2,l_2})$ cannot contain both 0 and $\Gamma/2$. Thus, either 0 or $\Gamma/2$ is the cutting point. To figure out the cutting point, we state Lemma 1, which is proved in Appendix A, that once $0 \in \max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$, $\min_{il} d(0, \tilde{r}^c_{i,l}) < \min_{il} d(\Gamma/2, \tilde{r}^c_{i,l})$ holds. Similarly, $\min_{il} d(0, \tilde{r}^c_{i,l}) > \min_{il} d(\Gamma/2, \tilde{r}^c_{i,l})$ is true when $\max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$ contains $\Gamma/2$. Thus, the unknown $\max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$ problem is converted to distance comparison, i.e., $\min_{il} d(0, \tilde{r}^c_{i,l})$ and $\min_{il} d(\Gamma/2, \tilde{r}^c_{i,l})$.

Before giving Lemma 1, we define Operation 1 and 2 corresponding to the cutting point is 0 and $\Gamma/2$, respectively.

- Operations 1:

$$\hat{r}^c_{i,l} = \tilde{r}^c_{i,l} \tag{9}$$

- Operation 2:

$$\hat{r}^c_{i,l} = \tilde{r}^c_{i,l} \text{ if } \tilde{r}^c_{i,l} \in [0, \frac{\Gamma}{2}), \text{ otherwise } \hat{r}^c_{i,l} = \tilde{r}^c_{i,l} - \Gamma \tag{10}$$

Lemma 1. *If* $\min_{il} d(0, \tilde{r}^c_{i,l}) < \min_{il} d(\Gamma/2, \tilde{r}^c_{i,l})$*, where* $1 \le i \le 2$ *and* $1 \le l \le L$*, apply Operation 2 on* $\tilde{r}^c_{i,l}$*; otherwise, Operation 1. The resultant* $\hat{r}^c_{i,l}$ *are sorted in ascending order of* $\Delta_{i,l}$ *for each i.*

For example, as shown in Figure 1, $\min_{il} d(0, \tilde{r}^c_{i,l}) = d(0, \tilde{r}^c_{1,1}) < \min_{il} d(\Gamma/2, \tilde{r}^c_{i,l}) = d(\Gamma/2, \tilde{r}^c_{2,3})$. Thus, Operation 2 is applied. The resultant $\hat{r}^c_{i,l}$ are sorted in the order that the corresponding $\Delta_{i,l}$ are in ascending order for each i, shown in Figure 2a.

3.2. Residue Ambiguity

With $\hat{r}^c_{i,l}$ sorted in ascending order of $\Delta_{i,l}$, $(\tilde{r}_{i,l} - \hat{r}^c_{i,l})/\Gamma$ fall into one subcase in (7) [24]. Now, we discuss the second key issue, i.e., residue ambiguity. If we can divide $\tilde{r}_{i,l}$ into two

sets corresponding to X_1 and X_2, respectively, the folding number $\lfloor X_i/\Gamma \rfloor$ can be estimated based on (5) [34]:

$$q_i \equiv \frac{\tilde{r}_{i,l} - \hat{r}^c_{i,l}}{\Gamma} \mod M_l. \tag{11}$$

However, the correspondence between $\tilde{r}_{i,l}$ and X_i is unknown. To determine the correspondence, Li et al. proposed a scheme for positive numbers, which cannot be directly applied to the real waveform since $X_2 < 0$ [23]. To solve this issue, we form a quadratic equation by the prior condition $X_2 = -X_1$. First, we consider the two residues $\{(\tilde{r}_{1,l} - \hat{r}^c_{1,l})/\Gamma, (\tilde{r}_{2,l} - \hat{r}^c_{2,l})/\Gamma\}$ as a pair for each l. By multiplying each pair, we can reconstruct $q_1 q_2$ via CRT based on (11) [22], i.e.,

$$q_1 q_2 \equiv \frac{\tilde{r}_{1,l} - \hat{r}^c_{1,l}}{\Gamma} \times \frac{\tilde{r}_{2,l} - \hat{r}^c_{2,l}}{\Gamma} \mod M_l. \tag{12}$$

Then, with $X_2 = -X_1$, it can be proved that either $q_2 = -q_1$ or $q_2 = -q_1 - 1$ holds, which is stated in Lemma 2 and proved in Appendix B. Hence, we can form a quadratic equation in one unknown by replacing q_2 with $-q_1$ or $-q_1 - 1$ in (12) based on Lemma 2. In a nutshell, the residue ambiguity is addressed by solving one of the two quadratic equations below via CRT, corresponding to $q_2 = -q_1$ and $q_2 = -q_1 - 1$, respectively.

$$q_1^2 \equiv M_l - \frac{\tilde{r}_{1,l} - \hat{r}^c_{1,l}}{\Gamma} \times \frac{\tilde{r}_{2,l} - \hat{r}^c_{2,l}}{\Gamma} \mod M_l \tag{13}$$

$$q_1^2 + q_1 \equiv M_l - \frac{\tilde{r}_{1,l} - \hat{r}^c_{1,l}}{\Gamma} \times \frac{\tilde{r}_{2,l} - \hat{r}^c_{2,l}}{\Gamma} \mod M_l \tag{14}$$

Lemma 2. *If* $|\Delta_{i,l}| < \Gamma/4$, $\{q_1, q_2\}$ *must fall into one of the following two cases:*

- $q_2 = -q_1 - 1$, *when Operation 1 is the appropriate operation and performed on* $\tilde{r}^c_{i,l}$, *where* $q_1 = \lfloor X_1/\Gamma \rfloor$.
- $q_2 = -q_1$, *when Operation 2 is the appropriate operation and performed on* $\tilde{r}^c_{i,l}$. *If* $r^c_1 \in [0, \Gamma/2)$, $q_1 = \lfloor X_1/\Gamma \rfloor$. *Otherwise,* $q_1 = \lfloor X_1/\Gamma \rfloor + 1$.

3.3. Reconstruction Scheme

With identified q_1, we consider the last two steps mentioned in Section 2.2. Clearly, $\hat{r}^c_{1,l}$ can be distinguished from (11) since q_1 is determined. Thus, X_1 is estimated based on Section 2.2:

$$\hat{X}_1 = q_1\Gamma + \frac{\sum_{l=1}^{L} \hat{r}^c_{1,l}}{L}. \tag{15}$$

With the above understanding, we state the final conclusion, i.e., Theorem 1, that reconstruction error is bounded by $\Gamma/4$, where the proof is in Appendix C.

Theorem 1. *If* $X_1 \in [0, \lfloor\sqrt{M}\rfloor\Gamma - \Gamma/2)$ *and* $|\Delta_{i,l}| < \Gamma/4$, $|\hat{X}_1 - X_1| < \Gamma/4$ *holds, where* $M = \prod_{l=1}^{L} M_l$.

For step 4 of Algorithm 1, the time complexity of solving the Equation (13) or (14) via CRT is $O(1)$. Since we need to process at most $2L$ $\tilde{r}^c_{i,l}$ or $\hat{r}^c_{i,l}$ in each step, the time complexity of Algorithm 1 is $O(L)$.

Algorithm 1 Robust frequency estimation for the single-tone real waveform.

Input: Moduli: $\{m_l | m_l = M_l\Gamma, l = 1, 2, \ldots, L\}$.
Erroneous residue sets: $S_l = \{\tilde{r}_{1,l}, \tilde{r}_{2,l}\}, l = 1, 2, \ldots, L$.

1: Calculate the erroneous common residues $\tilde{r}^c_{i,l} = \langle \tilde{r}_{i,l} \rangle_\Gamma$.
2: Calculate $\min_{il} d(0, \tilde{r}^c_{i,l})$ and $\min_{il} d(\Gamma/2, \tilde{r}^c_{i,l})$ from (8).
3: If $\min_{il} d(0, \tilde{r}^c_{i,l}) < \min_{il} d(\Gamma/2, \tilde{r}^c_{i,l})$, perform (10) on $\tilde{r}^c_{i,l}$ to obtain $\hat{r}^c_{i,l}$. Otherwise, perform (9).
4: If (9) is applied, solve the Equation (14) via CRT to obtain q_1. Otherwise, solve the Equation (13).
5: Cluster the shifted common residues $\hat{r}^c_{i,l}$ satisfying (11).
6: Calculate $\hat{X}_1$ according to (15).

Output: $\hat{X}_1$

Example 1. *Operation 1 is applied. The moduli are* $m_l = M_l\Gamma \in \{3 \times 10, 5 \times 10, 7 \times 10\}$, *where the greatest common divisor* $\Gamma = 10$ *and* $|\Delta_{i,l}| < \Gamma/4$. *If* $X_1 = 94$ *and* $X_2 = -94$, *we assume the erroneous residue sets are* $S_1 = \{2, 25\}$, $S_2 = \{44, 7\}$, *and* $S_3 = \{23, 48\}$. *Thus, the erroneous common residues are* $\{\tilde{r}^c_{1,1}, \tilde{r}^c_{2,1}\} = \{2, 5\}$, $\{\tilde{r}^c_{1,2}, \tilde{r}^c_{2,2}\} = \{4, 7\}$, *and* $\{\tilde{r}^c_{1,3}, \tilde{r}^c_{2,3}\} = \{3, 8\}$. *Clearly,* $\min_{il} d(0, \tilde{r}^c_{i,l}) = 2 > \min_{il} d(5, \tilde{r}^c_{i,l}) = 0$, *so Operation 1 is performed, i.e.,* $\hat{r}^c_{i,l} = \tilde{r}^c_{i,l}$. *According to (14), we obtain: (1).* $q_1^2 + q_1 \equiv 0 \mod 3$; *(2).* $q_1^2 + q_1 \equiv 0 \mod 5$; *(3).* $q_1^2 + q_1 \equiv 6 \mod 7$. *One can obtain* $q_1^2 + q_1 = 90$ *via CRT, which leads to* $q_1 = 9$. *From (11), the shifted common residues* $\hat{r}^c_{i,l}$ *of* q_1 *are* $\{2, 4, 3\}$. *So* $\hat{X}_1 = 9 \times 10 + (2 + 4 + 3)/3 = 93$.

Example 2. *Operation 2 is applied. Likewise, the moduli are* $m_l = M_l\Gamma \in \{3 \times 10, 5 \times 10, 7 \times 10\}$. *If* $X_1 = 81$ *and* $X_2 = -81$, *the erroneous residue sets are assumed as* $S_1 = \{20, 11\}$, $S_2 = \{29, 18\}$, *and* $S_3 = \{12, 57\}$. *Correspondingly, the erroneous common residues are* $\{\tilde{r}^c_{1,1}, \tilde{r}^c_{2,1}\} = \{0, 1\}$, $\{\tilde{r}^c_{1,2}, \tilde{r}^c_{2,2}\} = \{9, 8\}$, *and* $\{\tilde{r}^c_{1,3}, \tilde{r}^c_{2,3}\} = \{2, 7\}$. *Clearly,* $\min_{il} d(0, \tilde{r}^c_{i,l}) = 0 < \min_{il} d(5, \tilde{r}^c_{i,l}) = 2$, *so Operation 2 is applied on* $\tilde{r}^c_{i,l}$. *Thus, we obtain the shifted residues based on (10):* $\{\hat{r}^c_{1,1}, \hat{r}^c_{2,1}\} = \{0, 1\}$, $\{\hat{r}^c_{1,2}, \hat{r}^c_{2,2}\} = \{-1, -2\}$, *and* $\{\hat{r}^c_{1,3}, \hat{r}^c_{2,3}\} = \{2, -3\}$. *According to (13), one can derive that: (1).* $q_1^2 \equiv 1 \mod 3$; *(2).* $q_1^2 \equiv 4 \mod 5$; *(3).* $q_1^2 \equiv 1 \mod 7$. *Based on CRT, we have* $q_1^2 = 64$, *resulting in* $q_1 = 8$. *With determined* q_1, *we continue to figure out the corresponding shifted common residues based on (11), i.e.,* $\{0, -1, 2\}$. *As a result,* $\hat{X}_1 = 8 \times 10 + (0 - 1 + 2)/3 = 80.33$.

4. Simulation Results

In this section, we first present some simulations to verify our proposed theory. Then the simulation results are shown to demonstrate the performance of the proposed method compared with that of the robust generalized CRT [23] and searching−based algorithm [29].

In the following, we first consider the estimation error versus the error upper bound for our proposed theory, i.e., Theorem 1. To begin with, the simulation setup is given as follows. The moduli are $m_l = \{11 \times 80, 13 \times 80, 17 \times 80\}$, where the greatest common factor $\Gamma = 80$ and the maximal error level $\tau \in \{1, 2, \ldots, 25\}$. Based on Theorem 1, τ needs to be bounded by $\Gamma/4 = 20$ to ensure robustness.

For a trial, one unknown real number X is chosen randomly, which belongs to the dynamic range $[0, 3880)$, where the negative duplicate is $-X$. Moreover, 10,000 trials are implemented for each τ.

Figure 3 shows the mean absolute error E_τ between the estimate $\hat{X}$ and the true number X for each error bound. The mean absolute error E_τ is defined as below,

$$E_\tau = E_{trials}(|\hat{X} - X|), \tag{16}$$

where E_{trials} denotes the mean of all the trials, $\hat{X}$ and X are the estimate and true number in a trial, respectively. Clearly, E_τ is less than τ when $\tau \leq \Gamma/4 = 20$, which matches well with our conclusion. Once τ exceeds the error bound, the reconstruction error increases rapidly.

In Figure 4, we present the curve of the probability of failure P_e versus the error bound τ, where

$$P_e = P(|\hat{X} - X| > \tau). \tag{17}$$

One can see that when $\tau \leq \Gamma/4$, the probability of failure is zero while non$-$zero when τ exceeds the bound. In a word, if $\tau < \frac{\Gamma}{4}$, the reconstruction error is linearly bounded by τ, the probability of which is 1.

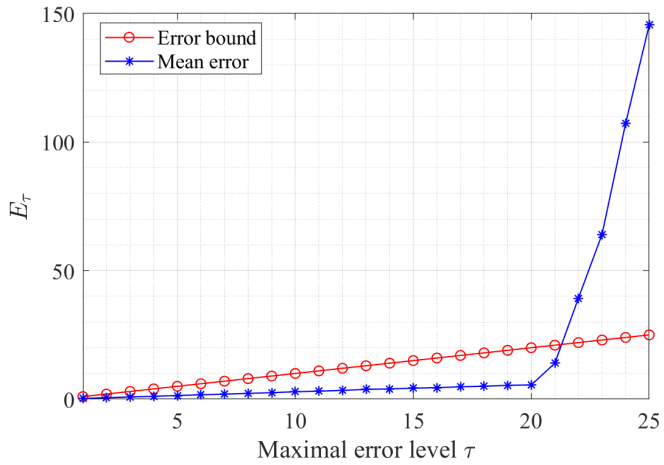


Figure 3. Estimation errors versus the maximal error level.

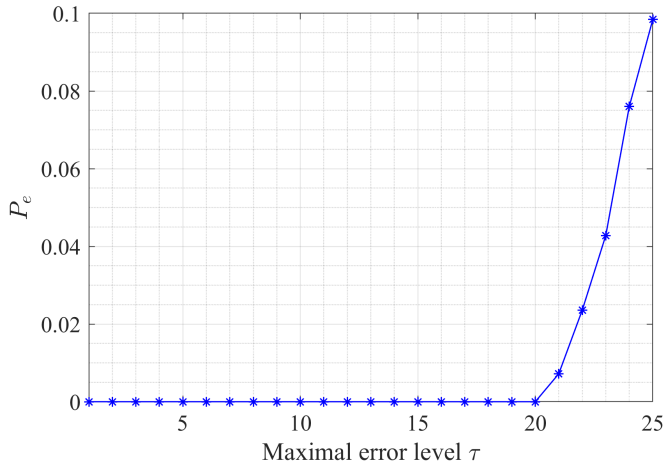


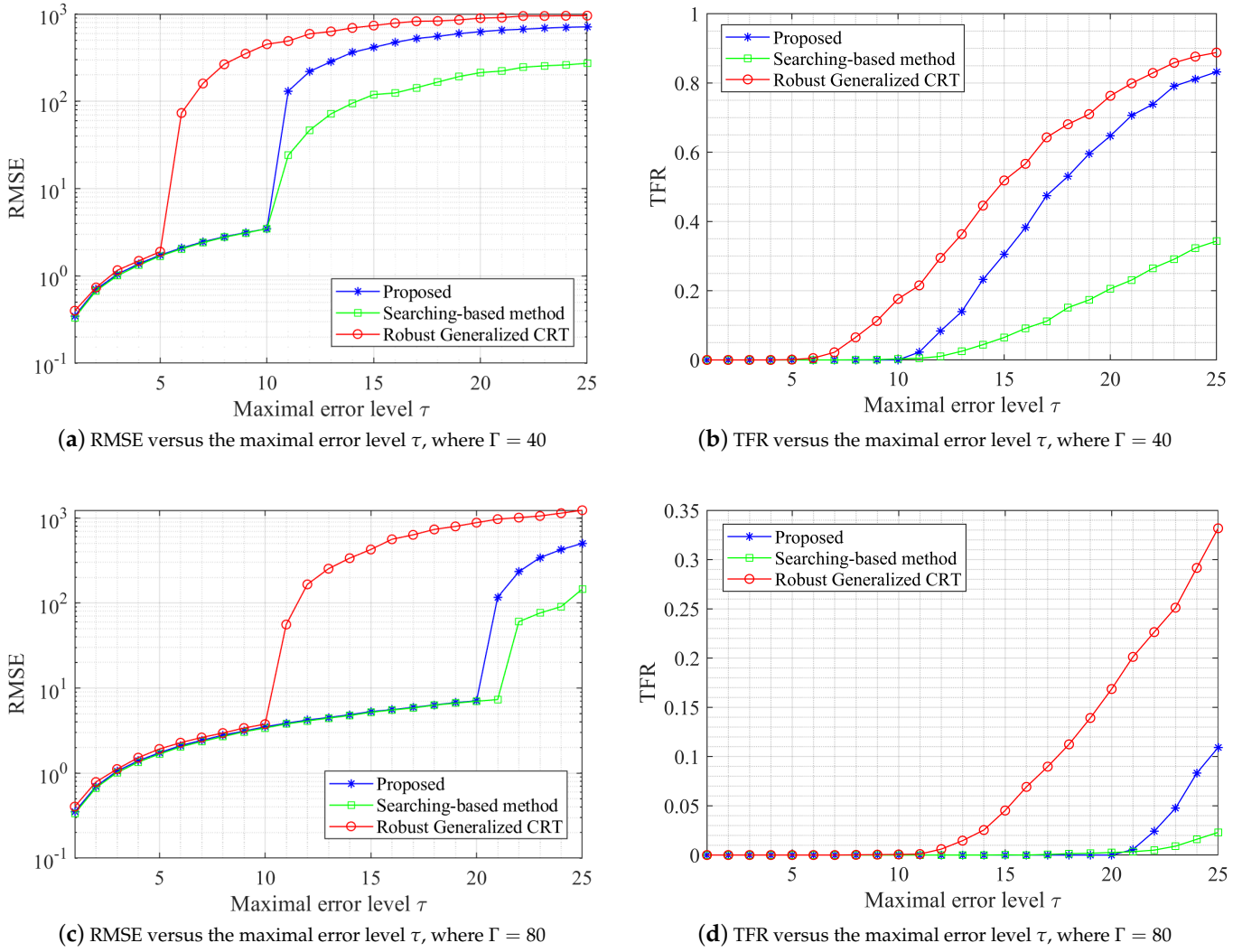
Figure 4. Probability P_e versus the maximal error level.

Next, we compare the performance of the proposed algorithm with that of the robust generalized CRT for two numbers in [23] and the searching$-$based algorithm in [29]. We consider the real sinusoidal waveform case and select $L = 3$ sampling rates (moduli) in a form $m[1:L] = \Gamma \times \{11, 13, 17\}$, which share a greatest common factor Γ. We test different sampling rates where $\Gamma = \{40, 80\}$. The unknown frequency X is randomly selected from the range $[0, 48.5 \times \Gamma)$. Each noise $\Delta_{i,l}$ is assumed to be some independent uniform noise within $(-\tau, \tau)$, where τ varies from 1 to 25.

We repeat 5000 trials for each selection of Γ and τ. On the on hand, the root mean square error (RMSE) is investigated, where

$$\text{RMSE} = \{E(\hat{X} - X)^2\}^{1/2}. \tag{18}$$

Figure 5a,c show that our method outperforms the best known robust generalized CRT, where the maximal error tolerance is improved from $\Gamma/8$ to $\Gamma/4$. Morever, our method performs as well as the best searching$-$based method when the maximal error level is less than $\Gamma/4$.



(a) RMSE versus the maximal error level τ, where $\Gamma = 40$

(b) TFR versus the maximal error level τ, where $\Gamma = 40$

(c) RMSE versus the maximal error level τ, where $\Gamma = 80$

(d) TFR versus the maximal error level τ, where $\Gamma = 80$

Figure 5. Performance simulation comparison among searching-based method [29], robust generalized CRT [23] and proposed RCRT.

On the other hand, we compare the test fail rate (TFR). We say that the test fails when

$$\text{TFR} = P(|\hat{X} - X| > \Gamma/4). \tag{19}$$

As shown in Figure 5b,d, if $\tau \leq \Gamma/4$, the estimation error is bounded by $\Gamma/4$, the probability of which is one. Once the maximal error level exceeds $\Gamma/4$, the reconstruction error is almost unpredictable. In a word, our method outperforms the robust generalized CRT while slightly worse than the searching−based algorithm when $\tau > \Gamma/4$. However, it's worth pointing out that our method provides a closed−form solution that cannot be realized by the searching−based method. Then, we consider the real running time consumption, where the computing equipment is Lenovo xiaoxin Pro 13. The real running time of our method that runs for 125,000 times is about 7.96 s, while the robust generalized CRT proposed in [23] requires about 86.05 s since the algorithm involves a lot of loops. The searching-based method proposed in [29] sightly outperforms our method, which only needs about 5.75 s.

5. Discussion

The experiment results in Figure 5 suggest a clear improvement in the error bound from $\Gamma/8$ to $\Gamma/4$ compared with the method proposed in [23]. The reason why we can

improve the error bound is that we fully utilized the prior knowledge of the real waveform, i.e., symmetry. For the real waveform, the real peak and the corresponding spurious peak are symmetric at about 0 points in the spectrum. Thus, the frequency determination from undersampled single-tone real waveform can be formulated as RCRT for two numbers $\{X_1, X_2\}$, where these two numbers are in a form $X_1 = -X_2$. Based on this symmetry, the corresponding error-free common residues $\{r_1^c, r_2^c\}$ are symmetric on the circle of length Γ. The geometric property of symmetry ensures that even if the error bound is improved to $\Gamma/4$, we can still shift the erroneous common residues correctly to obtain a robust reconstruction. In addition, our algorithm is also highly efficient according to the real running time and the theoretical analysis. We use the prior condition of the real waveform to form a quadratic equation in one unknown to determine the folding numbers, which realizes the high efficiency of the algorithm.

In summary, our proposed method provides a feasible solution for the frequency determination from the undersampled single-tone real waveform. In addition, we complete the study of CRT-based frequency determination from undersampled waveform, which shows that the optimal error tolerance bound can be achieved in the real waveform case. The limitation of our proposed method is that since it is based on the prior knowledge of the real waveform and the prior condition is invalid; it cannot handle the complex waveform. In addition, this algorithm cannot deal with the case of multiple frequency estimation from undersampled real waveforms. We will investigate these problems in our future studies.

6. Conclusions

We proposed the first polynomial-time RCRT-based frequency estimation for a noisy single-tone real waveform, which matches the optimal error bound. The proposed method can be applied in SAR imaging of moving targets or sensor networks where the sampling rate may be lower than the Nyquist rate of the input signal. The time complexity of the proposed method is linear to the number of samplers. Moreover, the proposed method can estimate the frequency from the real waveform by sub-Nyquist rates, which reduces the cost and system size, especially in sensor networks that require noticeable sensors. We believe the method can be further extended to the multiple frequencies case.

Author Contributions: The contribution of the authors for this publication article are as follows: Y.-W.Z.: methodology, software, conceptualization, writing—original draft, writing—review and editing. X.-F.H.: writing—review and editing. G.-Q.X.: conceptualization, supervision, writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Proof of Lemma 1

Proof. For brevity, we only consider the case when $r_1^c \leq r_2^c$, i.e., r_1^c is on the right half of the circle Γ. For the case $r_1^c \geq r_2^c$, which is obviously symmetric with $r_1^c \leq r_2^c$, one can obtain the same conclusion based on the following idea.

Since $\max_l I(\tilde{r}_{1,l_1}^c, \tilde{r}_{1,l_2}^c) \cup \max_l I(\tilde{r}_{2,l_1}^c, \tilde{r}_{2,l_2}^c)$ can not contain 0 and $\Gamma/2$ simultaneously, the intervals must satisfy one of the three cases:

(1) $0 \in \max_l I(\tilde{r}_{i,l_1}^c, \tilde{r}_{i,l_2}^c)$
(2) $\Gamma/2 \in \max_l I(\tilde{r}_{i,l_1}^c, \tilde{r}_{i,l_2}^c)$
(3) $\max_l I(\tilde{r}_{i,l_1}^c, \tilde{r}_{i,l_2}^c)$ contains neither 0 nor $\Gamma/2$

Case (1): $0 \in \max_l I(\tilde{r}_{1,l_1}^c, \tilde{r}_{1,l_2}^c)$ or $\max_l I(\tilde{r}_{2,l_1}^c, \tilde{r}_{2,l_2}^c)$.

If $0 \in \max_l I(\tilde{r}^c_{1,l_1}, \tilde{r}^c_{1,l_2})$, there must exist at least one $\tilde{r}^c_{1,k}$ to the left of the point 0, and another $\tilde{r}^c_{1,l}$ to the right of the point 0, where $k, l \in \{1, 2, \ldots, L\}$. Since r^c_1 is on the right half of the circle Γ while $\tilde{r}^c_{1,k} = \langle r^c_1 + \Delta_{1,k} \rangle_\Gamma$ is to the left of the point 0 and $|\Delta_{1,k}| < \Gamma/4$, we have $r^c_1 \in [0, \Gamma/4)$. Based on the fact that $r^c_2 = \Gamma - r^c_1$, $r^c_2 \in (3\Gamma/4, \Gamma]$. The same conclusion can be derived if $0 \in \max_l I(\tilde{r}^c_{2,l_1}, \tilde{r}^c_{2,l_2})$. Since $r^c_1 \in [0, \Gamma/4)$ and $\tilde{r}^c_{1,k}$ is to the left of the point 0, we obtain

$$\min_{il} d(0, \tilde{r}^c_{i,l}) \leq d(0, \tilde{r}^c_{1,k}) < d(0, r^c_1 - \frac{\Gamma}{4}) = \frac{\Gamma}{4} - r^c_1. \tag{A1}$$

Now, we calculate $\min_{il} d(\frac{\Gamma}{2}, \tilde{r}^c_{i,l})$. When $i = 1$, since $r^c_1 \in [0, \Gamma/4)$ and $|\Delta_{i,l}| < \Gamma/4$, it's clear that $\min_l d(\frac{\Gamma}{2}, \tilde{r}^c_{1,l}) > d(\frac{\Gamma}{2}, r^c_1 + \frac{\Gamma}{4}) = \frac{\Gamma}{4} - r^c_1$. When $i = 2$, replacing r^c_2 with $\Gamma - r^c_1$, we have $\min_l d(\frac{\Gamma}{2}, \tilde{r}^c_{2,l}) > d(\frac{\Gamma}{2}, r^c_2 - \frac{\Gamma}{4}) = \frac{\Gamma}{4} - r^c_1$. In conclusion, when $0 \in \max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$, we have

$$\min_{il} d(0, \tilde{r}^c_{i,l}) < \frac{\Gamma}{4} - r^c_1 < \min_{il} d(\frac{\Gamma}{2}, \tilde{r}^c_{i,l}). \tag{A2}$$

Since Cases (1) and (2) cannot hold simultaneously, we have $\frac{\Gamma}{2} \notin \max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$ for each i. Thus, cutting the circle at $\Gamma/2$, i.e., applying Operation 2 on $\tilde{r}^c_{i,l}$ leads to $\hat{r}^c_{i,l}$ sorted in ascending order of $\Delta_{i,l}$.

Case (2): $\Gamma/2 \in \max_l I(\tilde{r}^c_{1,l_1}, \tilde{r}^c_{1,l_2})$ or $\max_l I(\tilde{r}^c_{2,l_1}, \tilde{r}^c_{2,l_2})$. Case (2) is obviously symmetric with case (1) on the circle of length Γ. The conclusion can be derived based on the same idea. If $\Gamma/2 \in \max_l I(\tilde{r}^c_{1,l_1}, \tilde{r}^c_{1,l_2})$, there must exist at least one $\tilde{r}^c_{1,k}$ to the left of the point $\Gamma/2$, and another $\tilde{r}^c_{1,l}$ to the right of the point $\Gamma/2$. Likewise, since $\tilde{r}^c_{1,k} = \langle r^c_1 + \Delta_{1,k} \rangle_\Gamma$ is to the left of the point $\Gamma/2$ while r^c_1 is on the right half and $|\Delta_{1,k}| < \Gamma/4$, we have $r^c_1 \in (\Gamma/4, \Gamma/2]$ and $r^c_2 \in [\Gamma/2, 3\Gamma/4)$. The same conclusion can be derived if $\Gamma/2 \in \max_l I(\tilde{r}^c_{2,l_1}, \tilde{r}^c_{2,l_2})$. Since $r^c_1 \in (\Gamma/4, \Gamma/2]$ and $\tilde{r}^c_{1,k}$ is to the left of the point $\Gamma/2$, we obtain

$$\min_{il} d(\frac{\Gamma}{2}, \tilde{r}^c_{i,l}) \leq d(\frac{\Gamma}{2}, \tilde{r}^c_{1,k}) < d(\frac{\Gamma}{2}, r^c_1 + \frac{\Gamma}{4}) = r^c_1 - \frac{\Gamma}{4}. \tag{A3}$$

Then, we discuss $\min_{il} d(0, \tilde{r}^c_{i,l})$. When $i = 1$, since $r^c_1 \in (\Gamma/4, \Gamma/2]$ and $|\Delta_{i,l}| < \Gamma/4$, one can obtain $\min_l d(0, \tilde{r}^c_{1,l}) > d(0, r^c_1 - \frac{\Gamma}{4}) = r^c_1 - \frac{\Gamma}{4}$. When $i = 2$, replacing r^c_2 with $\Gamma - r^c_1$, we have $\min_l d(0, \tilde{r}^c_{2,l}) > d(0, r^c_2 + \frac{\Gamma}{4}) = r^c_1 - \frac{\Gamma}{4}$. Based on the discussion above, when $\Gamma/2 \in \max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$, we have

$$\min_{il} d(\frac{\Gamma}{2}, \tilde{r}^c_{i,l}) < r^c_1 - \frac{\Gamma}{4} < \min_{il} d(0, \tilde{r}^c_{i,l}). \tag{A4}$$

Since Cases (1) and (2) cannot hold simultaneously, we have $0 \notin \max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$ for each i. Thus, cutting the circle at 0, i.e., applying Operation 1 on $\tilde{r}^c_{i,l}$ leads to $\hat{r}^c_{i,l}$ sorted in ascending order of $\Delta_{i,l}$. Case (3): Since neither 0 nor $\frac{\Gamma}{2}$ is covered by $\max_l I(\tilde{r}^c_{i,l_1}, \tilde{r}^c_{i,l_2})$ for each i, we can implement either of the two operations on $\tilde{r}^c_{i,l}$. Q.E.D. □

Appendix B. Proof of Lemma 2

Proof. The proof has two parts to handle the following two cases, respectively.

(1) $\min d(0, \tilde{r}^c_{i,l}) \geq \min d(\frac{\Gamma}{2}, \tilde{r}^c_{i,l})$

(2) $\min d(0, \tilde{r}^c_{i,l}) < \min d(\frac{\Gamma}{2}, \tilde{r}^c_{i,l})$

Case (1): Since Operation 1 is the appropriate operation based on Lemma 1, we have $\hat{r}^c_{i,l} = \tilde{r}^c_{i,l}$ based on (9). Therefore, replacing $\hat{r}^c_{i,l}$ with $\tilde{r}^c_{i,l}$, (11) is equal to

$$q_i \equiv \frac{\tilde{r}_{i,l} - \tilde{r}^c_{i,l}}{\Gamma} \mod M_l. \tag{A5}$$

Then, we discuss $r^c_i + \Delta_{i,l}$, which determines q_i in (A5). With $r^c_i \in [0, \Gamma)$ and $|\Delta_{i,l}| < \frac{\Gamma}{4}$, $r^c_i + \Delta_{i,l}$ must fall into one of the three subcases:

(a) $r_i^c + \Delta_{i,l} \in (0, \Gamma)$
(b) $r_i^c + \Delta_{i,l} \in (-\frac{\Gamma}{4}, 0)$
(c) $r_i^c + \Delta_{i,l} \in (\Gamma, \frac{5\Gamma}{4})$

If $r_i^c + \Delta_{i,l}$ satisfy subcase (b), it leads to $\min_{il} d(0, \tilde{r}_{i,l}^c) < \frac{\Gamma}{4} < \min_{il} d(\frac{\Gamma}{2}, \tilde{r}_{i,l}^c)$, a contradiction to $\min_{il} d(0, \tilde{r}_{i,l}^c) \geq \min_{il} d(\frac{\Gamma}{2}, \tilde{r}_{i,l}^c)$. Similarly, if $r_i^c + \Delta_{i,l}$ satisfy subcase (c), we have $\min_{il} d(0, \tilde{r}_{i,l}^c) < \frac{\Gamma}{4} < \min_{il} d(\frac{\Gamma}{2}, \tilde{r}_{i,l}^c)$, a contradiction to $\min_{il} d(0, \tilde{r}_{i,l}^c) \geq \min_{il} d(\frac{\Gamma}{2}, \tilde{r}_{i,l}^c)$. Consequently, only subcase (a), i.e., $r_i^c + \Delta_{i,l} \in (0, \Gamma)$ holds, leading to $\frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma}$ satisfying subcase (1) in (7). Thus, $(\frac{\tilde{r}_{1,l} - \tilde{r}_{1,l}^c}{\Gamma}, \frac{\tilde{r}_{2,l} - \tilde{r}_{2,l}^c}{\Gamma})$ are residues of $(\lfloor \frac{X_1}{\Gamma} \rfloor, \lfloor \frac{X_2}{\Gamma} \rfloor)$ modulo M_l, where $\lfloor \frac{X_2}{\Gamma} \rfloor = \lfloor \frac{-X_1}{\Gamma} \rfloor = -\lfloor \frac{X_1}{\Gamma} \rfloor - 1$. Therefore, when Operation 1 is the appropriate operation, $q_2 = -q_1 - 1$ and $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$.

Case (2): In this case, Operation 2 is the appropriate operation based on Lemma 1. Then, based on (10), $\hat{r}_{i,l}^c = \tilde{r}_{i,l}^c$ when $\tilde{r}_{i,l}^c \in [0, \Gamma/2)$; otherwise, $\hat{r}_{i,l}^c = \tilde{r}_{i,l}^c - \Gamma$. Thus, replacing $\hat{r}_{i,l}^c$ with $\tilde{r}_{i,l}^c$, (11) is equal to

$$q_i \equiv \begin{cases} \frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma} \mod M_l, \text{ if } \tilde{r}_i^c \in [0, \Gamma/2) \\ \frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma} + 1 \mod M_l, \text{ otherwise} \end{cases} \tag{A6}$$

Likewise, we discuss $r_i^c + \Delta_{i,l}$ in the following to figure out q_i, where $r_i^c + \Delta_{i,l}$ must fall into one of the five subcases:

(a) $r_i^c + \Delta_{i,l} \in (\frac{\Gamma}{4}, \frac{3\Gamma}{4})$
(b) $r_i^c + \Delta_{i,l} \in [0, \frac{\Gamma}{4}]$
(c) $r_i^c + \Delta_{i,l} \in [\frac{3\Gamma}{4}, \Gamma)$
(d) $r_i^c + \Delta_{i,l} \in (-\frac{\Gamma}{4}, 0)$
(e) $r_i^c + \Delta_{i,l} \in (\Gamma, \frac{5\Gamma}{4})$

If $r_i^c + \Delta_{i,l}$ satisfies subcase a), we have $\min_{il} d(0, \tilde{r}_{i,l}^c) > \frac{\Gamma}{4} > \min_{il} d(\frac{\Gamma}{2}, \tilde{r}_{i,l}^c)$, a contradiction to $\min_{il} d(0, \tilde{r}_{i,l}^c) \leq \min_{il} d(\frac{\Gamma}{2}, \tilde{r}_{i,l}^c)$. Consequently, subcase (a) cannot happen. Next, we set out to figure out q_i corresponding to subcases (b), (c), (d), and (e).

Subcase (b): Since $r_i^c + \Delta_{i,l} \in [0, \frac{\Gamma}{4}]$, we have $\tilde{r}_{i,l}^c = \langle r_i^c + \Delta_{i,l} \rangle_\Gamma \in [0, \frac{\Gamma}{4}]$. Thus, based on (A6), we have $q_i \equiv \frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma}$. Moreover, it is clear that $\frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma}$ are residues of $\lfloor \frac{X_i}{\Gamma} \rfloor$ modulo M_l based on (7). So $q_i = \lfloor \frac{X_i}{\Gamma} \rfloor$.

Subcase (c): Likewise, since $r_i^c + \Delta_{i,l} \in [\frac{3\Gamma}{4}, \Gamma)$, we have $\tilde{r}_{i,l}^c = \langle r_i^c + \Delta_{i,l} \rangle_\Gamma \in [\frac{3\Gamma}{4}, \Gamma)$. Therefore, based on (A6), we have $q_i \equiv \frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma} + 1$. From (7), one can obtain $\frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma}$ are residues of $\lfloor \frac{X_i}{\Gamma} \rfloor$ modulo M_l, which leads to $q_i = \lfloor \frac{X_i}{\Gamma} \rfloor + 1$.

Subcase (d): Since $r_i^c + \Delta_{i,l} \in (-\frac{\Gamma}{4}, 0)$, we have $\tilde{r}_{i,l}^c = \langle r_i^c + \Delta_{i,l} \rangle_\Gamma \in (\frac{3\Gamma}{4}, \Gamma)$. Therefore, based on (A6), we have $q_i \equiv \frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma} + 1$. From (7), one can obtain $\frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma}$ are residues of $\lfloor \frac{X_i}{\Gamma} \rfloor - 1$ modulo M_l. Thus, we have $q_i = \lfloor \frac{X_i}{\Gamma} \rfloor$.

Subcase (e): Since $r_i^c + \Delta_{i,l} \in (\Gamma, \frac{5\Gamma}{4})$, we have $\tilde{r}_{i,l}^c = \langle r_i^c + \Delta_{i,l} \rangle_\Gamma \in (0, \frac{\Gamma}{4})$. Therefore, based on (A6), we have $q_i \equiv \frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma}$. From (7), one can obtain $\frac{\tilde{r}_{i,l} - \tilde{r}_{i,l}^c}{\Gamma}$ are residues of $\lfloor \frac{X_i}{\Gamma} \rfloor + 1$ modulo M_l, which results in $q_i = \lfloor \frac{X_i}{\Gamma} \rfloor + 1$.

Since $|\Delta_{i,l}| < \Gamma/4$, only subcases (b) and (d) or subcases (c) and (e) can occur simultaneously. Clearly, subcases (b) and (d) result in the same q_i, i.e., $q_i = \lfloor \frac{X_i}{\Gamma} \rfloor$. Similarly, subcases c) and e) lead to the same q_i, where $q_i = \lfloor \frac{X_i}{\Gamma} \rfloor + 1$. Based on the discussions above, we start to consider the residue pair $\{r_1^c, r_2^c\}$. Since $r_2^c = \Gamma - r_1^c$, $\{r_1^c, r_2^c\}$ must fall into one the four subcases:

(1) $r_1^c \in (0, \frac{\Gamma}{4}), r_2^c \in (\frac{3\Gamma}{4}, \Gamma)$
(2) $r_1^c \in (\frac{3\Gamma}{4}, \Gamma), r_2^c \in (0, \frac{\Gamma}{4})$
(3) $r_1^c \in (\frac{\Gamma}{4}, \frac{\Gamma}{2}), r_2^c \in (\frac{\Gamma}{2}, \frac{3\Gamma}{4})$

(4) $r_1^c \in (\frac{\Gamma}{2}, \frac{3\Gamma}{4}), r_2^c \in (\frac{\Gamma}{4}, \frac{\Gamma}{2})$

Subcase (1): Since $r_1^c \in (0, \frac{\Gamma}{4})$ and $|\Delta_{i,l}| < \frac{\Gamma}{4}$, $r_1^c + \Delta_{i,l}$ may fall into subcases (b) and (d), leading to $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$. In the same way, since $r_2^c \in (\frac{3\Gamma}{4}, \Gamma)$, $r_2^c + \Delta_{i,l}$ can fall into subcases (c) and (e), resulting in $q_2 = \lfloor \frac{X_2}{\Gamma} \rfloor + 1$. Based on the fact that $x_1 = -x_2$, we have $q_2 = \lfloor \frac{X_2}{\Gamma} \rfloor + 1 = -\lfloor \frac{X_1}{\Gamma} \rfloor$, i.e., $q_1 = -q_2 = \lfloor \frac{X_1}{\Gamma} \rfloor$.

Subcase (2): Subcase (2) is obviously symmetric with subcase (1) on the circle of length Γ. The proof is very similar to that of subcase (1). It is clear that $r_1^c + \Delta_{i,l}$ can fall into subcases (c) and (e), leading to $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1$. $r_2^c + \Delta_{i,l}$ may fall into subcases (b) and (d), leading to $q_2 = \lfloor \frac{X_2}{\Gamma} \rfloor$. Replacing x_2 with $-x_1$, we have $q_2 = \lfloor \frac{X_2}{\Gamma} \rfloor = -\lfloor \frac{X_1}{\Gamma} \rfloor - 1$. Thus, $q_1 = -q_2 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1$.

Subcase (3): Since $r_1^c \in (\frac{\Gamma}{4}, \frac{\Gamma}{2})$ and $|\Delta_{i,l}| < \frac{\Gamma}{4}$, $r_1^c + \Delta_{i,l}$ may fall into subcases (b) and (d). Then, we have $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$. For $r_2^c \in (\frac{\Gamma}{2}, \frac{3\Gamma}{4})$, $r_2^c + \Delta_{i,l}$ can fall into subcases (c) and (e), resulting in $q_2 = \lfloor \frac{X_2}{\Gamma} \rfloor + 1$. Therefore, we have $q_2 = \lfloor \frac{X_2}{\Gamma} \rfloor + 1 = -\lfloor \frac{X_1}{\Gamma} \rfloor$, i.e., $q_1 = -q_2 = \lfloor \frac{X_1}{\Gamma} \rfloor$.

Subcase (4): Subcase (4) is clearly symmetric with subcase 3) on the circle of length Γ. Clearly, $r_1^c + \Delta_{i,l}$ can fall into subcases (c) and (e), leading to $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1$. $r_2^c + \Delta_{i,l}$ may fall into subcases (b) and (d), which means $q_2 = \lfloor \frac{X_2}{\Gamma} \rfloor$. Replacing x_2 with $-x_1$, we have $q_2 = \lfloor \frac{X_2}{\Gamma} \rfloor = -\lfloor \frac{X_1}{\Gamma} \rfloor - 1$. Thus, $q_1 = -q_2 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1$.

In a nutshell, when Operation 2 is the appropriate operation, $q_2 = -q_1$. If $r_1^c \in [0, \Gamma/2)$, $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$. Otherwise, $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1$. Q.E.D. □

Appendix C. Proof of Theorem 1

Proof. At a high level, the proof is developed in two parts. First, we verify that q_1 has a unique solution when $X_1 \in [0, \lfloor \sqrt{M} \rfloor \Gamma - \frac{\Gamma}{2})$. Second, the reconstruction error is discussed under Operations 1 and 2, respectively.

Now, we discuss the uniqueness of the solution to q_i. If Operation 1 is implemented, we have $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$ based on Lemma 2. Since $x_1 < \lfloor \sqrt{M} \rfloor \Gamma - \frac{\Gamma}{2}$, we have

$$q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor < \lfloor \frac{\lfloor \sqrt{M} \rfloor \Gamma - \frac{\Gamma}{2}}{\Gamma} \rfloor = \lfloor \sqrt{M} \rfloor - 1. \tag{A7}$$

From Algorithm 1, q_1 is determined by (14) when Operation 1 is implemented. Clearly, $q_1^2 + q_1$ in (14) satisfies $q_1^2 + q_1 < M$, which guarantees that $q_1^2 + q_1$ can be uniquely determined via CRT. Once $q_1^2 + q_1$ is known, q_1 can be uniquely determined by solving a quadratic equation.

If Operation 2 is applied on $\tilde{r}_{i,l}^c$ and $r_1^c \in [0, \frac{\Gamma}{2})$, we have $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$ based on Lemma 2, where $X_1 \leq (\lfloor \sqrt{M} \rfloor - 1)\Gamma + r_1^c$, .i.e.,

$$q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor \leq \lfloor \frac{(\lfloor \sqrt{M} \rfloor - 1)\Gamma + r_1^c}{\Gamma} \rfloor = \lfloor \sqrt{M} \rfloor - 1. \tag{A8}$$

If $r_1^c \in (\frac{\Gamma}{2}, \Gamma)$ and Operation 2 is applied, we obtain $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1$ based on Lemma 2. Correspondingly, $X_1 \leq (\lfloor \sqrt{M} \rfloor - 2)\Gamma + r_1^c$, which leads to

$$q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1 \leq \lfloor \frac{(\lfloor \sqrt{M} \rfloor - 2)\Gamma + r_1^c}{\Gamma} \rfloor + 1 = \lfloor \sqrt{M} \rfloor - 1. \tag{A9}$$

From Algorithm 1, q_1 is calculated by (13) when Operation 2 is implemented. Since $q_1 \leq \lfloor \sqrt{M} \rfloor - 1$, we obtain $q_1^2 < M$ in (13), which means q_1 can be uniquely recovered.

In the following, we continue to the second part of the proof, i.e., we discuss the robustness of reconstruction using the unique q_1, where $q_1 \neq q_2$. Once q_1 is determined, we can obtain the corresponding $\hat{r}_{1,l}^c$ from (11) and further reconstruct $\hat{X}_1$ from (15). There

are two scenarios for the reconstruction error: (i) Operation 1 is the appropriate operation and applied; (ii) Operation 2 is the appropriate operation and implemented.

When Operation 1 is applied: In this case, $\hat{r}^c_{1,l} = \tilde{r}^c_{1,l}$ based on (9). Then, we discuss $\tilde{r}^c_{1,l} = \langle r^c_1 + \Delta_{1,l} \rangle_\Gamma$, where $r^c_1 + \Delta_{1,l}$ must fall into one of the three subcases:

(a) $r^c_1 + \Delta_{1,l} \in (0, \Gamma)$
(b) $r^c_1 + \Delta_{1,l} \in (-\frac{\Gamma}{4}, 0)$
(c) $r^c_1 + \Delta_{1,l} \in (\Gamma, \frac{5\Gamma}{4})$

If $r^c_1 + \Delta_{1,l}$ satisfies subcase (b), we have $\min_{il} d(0, \tilde{r}^c_{i,l}) < \frac{\Gamma}{4} < \min_{il} d(\frac{\Gamma}{2}, \tilde{r}^c_{i,l})$, a contradiction to the fact that Operation 1 is the appropriate operation. Likewise, when $r^c_1 + \Delta_{1,l}$ falls into subcase (c), we have $\min_{il} d(0, \tilde{r}^c_{i,l}) < \frac{\Gamma}{4} < \min_{il} d(\frac{\Gamma}{2}, \tilde{r}^c_{i,l})$, which contradicts the fact that Operation 1 is the appropriate operation. Therefore, only subcase a) can happen, i.e., $r^c_1 + \Delta_{1,l} \in (0, \Gamma)$. Thus,

$$\tilde{r}^c_{1,l} = \langle r^c_1 + \Delta_{1,l} \rangle_\Gamma = r^c_1 + \Delta_{1,l}.$$

Since Operation 1 is applied on $\tilde{r}^c_{1,l}$, we have $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$ based on Lemma 2. Then, reconstructing X_1 from (15), we have $|\hat{X}_1 - X_1|$ is equal to

$$|\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \frac{\sum_{l=1}^{L} \hat{r}^c_{1,l}}{L} - X_1| = |\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \frac{\sum_{l=1}^{L} (r^c_1 + \Delta_{1,l})}{L} - X_1| = |\frac{\sum_{l=1}^{L} \Delta_{1,l}}{L}| < \frac{\Gamma}{4}. \quad \text{(A10)}$$

When Operation 2 is applied: In this case, $\hat{r}^c_{1,l} = \tilde{r}^c_{1,l}$ when $\tilde{r}^c_{1,l} \in [0, \Gamma/2)$; otherwise $\hat{r}^c_{1,l} = \tilde{r}^c_{1,l} - \Gamma$ based on (9). Similarly, we discuss $\tilde{r}^c_{1,l} = \langle r^c_1 + \Delta_{1,l} \rangle_\Gamma$, where $r^c_1 + \Delta_{1,l}$ must fall into one of the five subcases:

(a) $r^c_1 + \Delta_{1,l} \in (\frac{\Gamma}{4}, \frac{3\Gamma}{4})$
(b) $r^c_1 + \Delta_{1,l} \in [0, \frac{\Gamma}{4}]$
(c) $r^c_1 + \Delta_{1,l} \in [\frac{3\Gamma}{4}, \Gamma)$
(d) $r^c_1 + \Delta_{1,l} \in (-\frac{\Gamma}{4}, 0)$
(e) $r^c_1 + \Delta_{1,l} \in (\Gamma, \frac{5\Gamma}{4})$

If $r^c_1 + \Delta_{1,l}$ satisfies subcase (a), we have $\min_{il} d(0, \tilde{r}^c_{i,l}) > \frac{\Gamma}{4} > \min_{il} d(\frac{\Gamma}{2}, \tilde{r}^c_{i,l})$, a contradiction to that Operation 2 is the appropriate operation, which means that subcase (a) cannot happen. As proved in Appendix B, when $r^c_1 + \Delta_{1,l}$ falls into subcase (b) or (d), we have $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$. When $r^c_1 + \Delta_{1,l}$ falls into subcase (c) or (e), we obtain $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1$. Based on these conclusions, we discuss the reconstruction error: (i). only one subcase occurs; (ii). subcases (b) and (d) or subcases (c) and (e) happen simultaneously.

Subcase (b): Since $r^c_1 + \Delta_{1,l} \in [0, \frac{\Gamma}{4}]$ and Operation 2 is applied, we have $\hat{r}^c_{1,l} = \tilde{r}^c_{1,l} = \langle r^c_1 + \Delta_{1,l} \rangle_\Gamma = r^c_1 + \Delta_{1,l}$. Since $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$, $|\hat{X}_1 - X_1|$ is equal to

$$|\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \frac{\sum_{l=1}^{L} \hat{r}^c_{1,l}}{L} - X_1| = |\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \frac{\sum_{l=1}^{L} (r^c_1 + \Delta_{1,l})}{L} - X_1| = |\frac{\sum_{l=1}^{L} \Delta_{1,l}}{L}| < \frac{\Gamma}{4}. \quad \text{(A11)}$$

Subcase (c): Since $r^c_1 + \Delta_{1,l} \in [\frac{3\Gamma}{4}, \Gamma)$ and Operation 2 is applied, we have $\hat{r}^c_{1,l} = \tilde{r}^c_{1,l} - \Gamma = \langle r^c_1 + \Delta_{1,l} \rangle_\Gamma - \Gamma = r^c_1 + \Delta_{1,l} - \Gamma$. Since $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1$, $|\hat{X}_1 - X_1|$ is equal to

$$|(\lfloor \frac{X_1}{\Gamma} \rfloor + 1)\Gamma + \frac{\sum_{l=1}^{L} \hat{r}^c_{1,l}}{L} - X_1| = |\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \Gamma + \frac{\sum_{l=1}^{L} (r^c_1 + \Delta_{1,l} - \Gamma)}{L} - X_1| = |\frac{\sum_{l=1}^{L} \Delta_{1,l}}{L}| < \frac{\Gamma}{4}. \quad \text{(A12)}$$

Subcase (d): Since $r^c_1 + \Delta_{1,l} \in (-\frac{\Gamma}{4}, 0)$ and Operation 2 is applied, we have $\hat{r}^c_{1,l} = \tilde{r}^c_{1,l} - \Gamma = \langle r^c_1 + \Delta_{1,l} \rangle_\Gamma - \Gamma = r^c_1 + \Delta_{1,l}$. Since $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$, $|\hat{X}_1 - X_1|$ is equal to

$$|\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \frac{\sum_{l=1}^{L} \hat{r}^c_{1,l}}{L} - X_1| = |\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \frac{\sum_{l=1}^{L} (r^c_1 + \Delta_{1,l})}{L} - X_1| = |\frac{\sum_{l=1}^{L} \Delta_{1,l}}{L}| < \frac{\Gamma}{4}. \quad \text{(A13)}$$

Subcase (e): Since $r_1^c + \Delta_{1,l} \in (\Gamma, \frac{5\Gamma}{4})$ and Operation 2 is applied, we have $\hat{r}_{1,l}^c = \tilde{r}_{1,l}^c = \langle r_1^c + \Delta_{1,l} \rangle_\Gamma = r_1^c + \Delta_{1,l} - \Gamma$. Since $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1$, $|\hat{X}_1 - X_1|$ is equal to

$$|(\lfloor \frac{X_1}{\Gamma} \rfloor + 1)\Gamma + \frac{\sum_{l=1}^{L} \hat{r}_{1,l}^c}{L} - X_1| = |\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \Gamma + \frac{\sum_{l=1}^{L} (r_1^c + \Delta_{1,l} - \Gamma)}{L} - X_1| = |\frac{\sum_{l=1}^{L} \Delta_{1,l}}{L}| < \frac{\Gamma}{4}. \quad \text{(A14)}$$

Subcase (b) and (d) happen simultaneously: Based on the discussions above, we have $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor$ and $\hat{r}_{1,l}^c = r_1^c + \Delta_{1,l}$. Therefore, $|\hat{X}_1 - X_1|$ is equal to

$$|\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \frac{\sum_{l=1}^{L} \hat{r}_{1,l}^c}{L} - X_1| = |\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \frac{\sum_{l=1}^{L} (r_1^c + \Delta_{1,l})}{L} - X_1| = |\frac{\sum_{l=1}^{L} \Delta_{1,l}}{L}| < \frac{\Gamma}{4}. \quad \text{(A15)}$$

Subcase (c) and (e) happen simultaneously: Likewise, based on the discussions above, we have $q_1 = \lfloor \frac{X_1}{\Gamma} \rfloor + 1$ and $\hat{r}_{1,l}^c = r_1^c + \Delta_{1,l} - \Gamma$. As a result, $|\hat{X}_1 - X_1|$ is equal to

$$|(\lfloor \frac{X_1}{\Gamma} \rfloor + 1)\Gamma + \frac{\sum_{l=1}^{L} \hat{r}_{1,l}^c}{L} - X_1| = |\lfloor \frac{X_1}{\Gamma} \rfloor \Gamma + \Gamma + \frac{\sum_{l=1}^{L} (r_1^c + \Delta_{1,l} - \Gamma)}{L} - X_1| = |\frac{\sum_{l=1}^{L} \Delta_{1,l}}{L}| < \frac{\Gamma}{4}. \quad \text{(A16)}$$

Thus, the reconstruction error is bounded by $\frac{\Gamma}{4}$. Q.E.D. □

References

1. Chessa, S.; Maestrini, P. Robust distributed storage of residue encoded data. *IEEE Trans. Inf. Theory* **2012**, *58*, 7280–7294. [CrossRef]
2. Xiao, L.; Xia, X.-G.; Huo, H. Towards robustness in residue number systems. *IEEE Trans. Signal Process.* **2017**, *65*, 1497–1510. [CrossRef]
3. Goldreich, O.; Ron, D.; Sudan, M. Chinese remaindering with errors. *IEEE Trans. Inf. Theory* **2006**, *46*, 1330–1338. [CrossRef]
4. Xiao, H.; Garg, H.K.; Hu, J.; Xiao, G. New error control algorithms for residue number system codes. *ETRI J.* **2016**, *38*, 326–336. [CrossRef]
5. Ding, C.; Pei, D.; Salomaa, A. *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*; World Scientific Publishing Company: Singapore, 1996.
6. Krishna, H.; Krishna, B.; Lin, K.Y.; Sun, J.D. *Computational Number Theory and Digital Signal Processing: Fast Algorithms and Error Control Techniques*; CRC Press: Boca Raton, FL, USA, 1994.
7. Li, C.; Tan, C.W.; Li, J.; Chen, S. Fault-tolerant computation meets network coding: Optimal scheduling in parallel computing. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6.
8. Xia, X.G.; Wang, G. Phase unwrapping and a robust chinese remainder theorem. *IEEE Signal Process. Lett.* **2007**, *14*, 247–250. [CrossRef]
9. Li, X.; Xia, X.-G. A fast robust chinese remainder theorem based phase unwrapping algorithm. *IEEE Signal Process. Lett.* **2008**, *15*, 665–668. [CrossRef]
10. Xiao, L.; Xia, X.-G.; Wang, Y.-P. Exact and robust reconstructions of integer vectors based on multidimensional chinese remainder theorem (md-crt). *IEEE Trans. Signal Process.* **2020**, *68*, 5349–5364. [CrossRef]
11. Li, W.; Wang, X.; Moran, B. An enhanced lattice algorithm for range estimation using noisy measurement with phase ambiguity. *IEEE Trans. Signal Process.* **2022**, *70*, 890–902. [CrossRef]
12. Xiao, L.; Xia, X.; Wang, W. Multi-stage robust chinese remainder theorem. *IEEE Trans. Signal Process.* **2014**, *62*, 4772–4785. [CrossRef]
13. Xiao, L.; Xia, X.G. Frequency determination from truly sub-nyquist samplers based on robust chinese remainder theorem. *Signal Process.* **2018**, *150*, 248–258. [CrossRef]
14. Wang, W.; Li, X.; Wang, W.; Xia, X.-G. Maximum likelihood estimation based robust chinese remainder theorem for real numbers and its fast algorithm. *IEEE Trans. Signal Process.* **2015**, *63*, 3317–3331. [CrossRef]
15. Li, X.; Huang, T.; Liao, Q.; Xia, X.-G. Optimal estimates of two common remainders for a robust generalized chinese remainder theorem. *IEEE Trans. Signal Process.* **2019**, *67*, 1824–1837. [CrossRef]
16. Xia, L.; Xia, X.-G. A new robust chinese remainder theorem with improved performance in frequency estimation from undersampled waveforms. *Signal Process. Off. Publ. Eur. Assoc. Signal Process. (EURASIP)* **2015**, *117*, 242–246. [CrossRef]
17. Xiao, H.; Du, N.; Wang, Z.; Xiao, G. Wrapped ambiguity gaussian mixed model with applications in sparse sampling based multiple parameter estimation. *Signal Process* **2021**, *179*, 107825. [CrossRef]
18. Xia, X.G. On estimation of multiple frequencies in undersampled complex valued waveforms. *Signal Process. IEEE Trans.* **1999**, *47*, 3417–3419. [CrossRef]
19. Zhou, G.; Xia, X.G. Multiple frequency detection in undersampled complex-valued waveforms with close multiple frequencies. *Electron. Lett.* **1997**, *33*, 1294–1295. [CrossRef]
20. Wang, W.; Xia, X.-G. A closed-form robust chinese remainder theorem and its performance analysis. *IEEE Trans. Signal Process.* **2010**, *58*, 5655–5666. [CrossRef]

21. Xiao, H.; Huang, Y.; Ye, Y.; Xiao, G. Robustness in chinese remainder theorem for multiple numbers and remainder coding. *IEEE Trans. Signal Process.* **2018**, *66*, 4347–4361. [CrossRef]
22. Xiao, L.; Xia, X.-G. A generalized chinese remainder theorem for two integers. *IEEE Signal Process. Lett.* **2014**, *21*, 55–59. [CrossRef]
23. Li, X.; Xia, X.-G.; Wang, W.; Wang, W. A robust generalized chinese remainder theorem for two integers. *IEEE Trans. Inf. Theory* **2016**, *62*, 7491–7504. [CrossRef]
24. Xiao, H.; Zhang, Y.; Xiao, G. On the foundation of sparse sensing (part i): Necessary and sufficient sampling theory and robust remaindering problem. *arXiv* **2021**, arXiv:2108.10423.
25. Xiao, H.; Zhou, B.; Xiao, G. On the foundation of sparse sensing (part ii): Diophantine sampling and array configuration. *arXiv* **2021**, arXiv:2108.10425.
26. Xia, X.G. An efficient frequency-determination algorithm from multiple undersampled waveforms. *IEEE Signal Process. Lett.* **2000**, *7*, 34–37. [CrossRef]
27. Xia, X.G.; Liu, K. 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.* **2005**, *12*, 768–771. [CrossRef]
28. Li, G.; Xu, J.; Peng, Y.-n.; Xia, X.-g. Detection, location and imaging of fast moving targets using non-uniform linear antenna array sar. In Proceedings of the 2006 8th International Conference on Signal Processing, Guilin, China, 16–20 November 2006; Volume 4.
29. Maroosi, A.; Bizaki, H.K. Digital frequency determination of real waveforms based on multiple sensors with low sampling rates. *IEEE Sens. J.* **2012**, *12*, 1483–1495. [CrossRef]
30. Xiao, L.; Xia, X.-G.; Huo, H. New conditions on achieving the maximal possible dynamic range for a generalized chinese remainder theorem of multiple integers. *IEEE Signal Process. Lett.* **2015**, *22*, 2199–2203. [CrossRef]
31. Xiao, H.; Cremers, C.; Garg, H.K. Symmetric polynomial amp; crt based algorithms for multiple frequency determination from undersampled waveforms. In Proceedings of the 2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Washington, DC, USA, 7–9 December 2016; pp. 202–206.
32. Wang, W.; Li, X.; Xia, X.-G.; Wang, W. The largest dynamic range of a generalized chinese remainder theorem for two integers. *IEEE Signal Process. Lett.* **2015**, *22*, 254–258. [CrossRef]
33. Xiao, H.; Xiao, G. Notes on crt-based robust frequency estimation. *Signal Process.* **2017**, 133, 13–17. [CrossRef]
34. Xiao, H.; Xiao, G. On solving ambiguity resolution with robust chinese remainder theorem for multiple numbers. *IEEE Trans. Veh. Technol.* **2019**, *68*, 5179–5184. [CrossRef]