# Symmetric Polynomial & CRT Based Algorithms for Multiple Frequency Determination from Undersampled Waveforms

Hanshen Xiao *†, Cas Cremers ‡, Hari Krishna Garg §
*MIT Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, USA
†Department of Mathematics, Tsinghua University, China
‡Department of Computer Science, University of Oxford, UK
§Department of Electrical and Engineering, National University of Singapore, Singapore
Email: *hsxiao@mit.edu, †xhs13@mails.tsinghua.edu.cn, ‡cas.cremers@cs.ox.ac.uk, §eleghk@nus.edu.sg

***Abstract*—Frequency estimation, especially with sampling rates below the Nyquist rate, has abundant applications in engineering. Recently, Chinese remainder theorem(CRT)-based frequency reconstruction from undersampled complex-value waveforms becomes one of the frontier focuses in the fields of signal processing, electromagnetism and optics etc. In this paper, we present several CRT-based algorithms for determining multiple frequencies via symmetric polynomials. The computational complexity of these algorithms is in the polynomial class (P).**

***Index Terms*—Chinese Remainder Theorem (CRT), Symmetric Polynomial, Frequency Determination, Dynamic Range.**

## I. INTRODUCTION

THE Chinese Remainder Theorem (CRT) has been widely used in digital signal processing [18], coding theory [14], [22] and cryptography [19], [20]. It provides a distributed number representation for a large integer in terms of its residues modulo several co-prime moduli. During the last two decades, Xia et. al. have contributed significantly to the CRT-based algorithms for determining multiple frequencies from undersampled complex-valued waveforms [1]-[11]. This work has applications in synthetic aperture radar (SAR) imaging of moving targets [17], polynomial phase detection [21] and so on. The problem can be stated as follows: given co-prime moduli, $m_1, m_2, \ldots, m_L$, reconstruct integers, $X_1, X_2, \ldots, X_N$, from the $L$ residue sets $R_l = \{\langle X_i \rangle_{m_l} = r_{il} | i = 1, 2, \ldots, N\}$ for $1 \leq l \leq L$, without knowing the corresponding relation between the residues and the integers. Let $\langle X \rangle_m$ denote the residue of $X$ modulo $m$; $X_i$, $i = 1, 2, \ldots, N$, represent frequencies to be determined and $m_l$, $l = 1, 2, \ldots, L$, represent the sampling frequencies in the model. Here $\{X_i\}$ and $\{m_l\}$ are both assumed to be arranged in an ascending order without loss of generality. The dynamic range in this paper is defined as the range for multiple integers/frequencies that can be uniquely computed from their residue sets.

Research concerning the problem falls into three categories:

a) *Exploring efficient algorithms.* Determination algorithms in general cases have been studied in [1], [3]. The main idea is to enumerate the $L$-dimensional sets of residues, which are constructed by selecting one residue from each set $R_l$, $l = 1, 2, \ldots, L$, and then to check whether the reconstructed integer by CRT is within the dynamic range. In order to reduce the computational complexity, a look-up table (LUT) is used in [1] with space complexity $O(NLC_G^N)$, where $G$ is the upper bound of $X_i$ and $C$ denotes the combinatorial number, which may be quite tedious when $N$ and $L$ are large. A search-based CRT, instead of LUT, is used in [3], where the time complexity is still exponential. In particular, $O(N^L) \approx O(N^{N \log_{\bar{m}}(\bar{X})})$ of CRT operations are required in [3], where $\bar{m}$ and $\bar{X}$ denote the average of moduli and integers to be determined, respectively. The total calculation amount of this search-based CRT algorithm is very intensive as numerous multiplication and matching operations are required. It is difficult to implement it in real-time signal processing systems due to the exponential growth of computational complexity with $N$ and $L$ increasing.

Computational algorithms for two integers or integers with small differences have been studied in [2], [5], [10], [11]. Compared to [1], [3], the algorithm in [2] is significantly more efficient. It only requires one CRT operation with an additional constraint that $X_N - X_1 < \frac{1}{2}m_1$. Recently, a new solution was proposed in [5] under a weaker constraint, $X_N - X_1 < m_1$, and some restrictions on the values of $N$ and $m_l$. The complexity in [5] is reduced to one CRT operation, the search range is within $O(N^L)$ and the dynamic range is given by $X_N < \prod_{l=1}^{L} m_l$. A special case of two integers is studied in [10], [11].

b) *Sharpening the dynamic range for given moduli.* Given sampling rates, the bigger dynamic range implies moving objects with higher velocities are detectable [3], [23]. To this end, an algorithm of sharpening dynamic ranges in general cases is proposed in [4]. Recently, the upper bound of a dynamic range for two integers is proved in [10] for given moduli.

c) *Developing robust CRT.* The contribution in [6]-[9], [24], [25] is to reduce the error-sensibility of traditional CRT since small errors in residues may lead to a great deviation in the CRT reconstruction. The works in [6]-[9],[24],[25] achieve error control via introducing remainder redundancy.

**Contributions.** We propose several theorems and algorithms based on symmetric polynomials that have polynomial time complexity to deal with different application cases. We propose

Theorem 1 and Algorithm 1 based on the Viete theorem to solve the problem in general cases. Moreover, another group of symmetric polynomials is developed in Theorem 2 and Algorithm 2, which further enlarges the dynamic range of Algorithm 1 when the maximum difference of the frequencies/integers, $X_N - X_1$, is relatively small. Corollary 1 is aimed at the two-integer case. Another special case, where $X_N - X_1 < m_L$, is dealt with in Corollary 2 and Algorithm 3.

This paper is organized as follows. In section II, some background assumptions and notations are briefly described. In section III, we present several algorithms dealing with the optimization of dynamic ranges and computational efficiency. We conclude in section IV.

## II. PRELIMINARIES

We begin with the problem of determining multiple-frequencies from multiple undersampled waveforms as introduced in [1]. We aim to determine $N$ integer frequencies $\{X_1, X_2, \dots, X_N\}$ in Hz in a superpositioned waveform $x(t)$, i.e.,

$$x(t) = \sum_{i=1}^{N} A_i e^{2\pi j X_i t} \tag{1}$$

where $A_i$ are nonzero complex coefficients, $1 \le i \le N$. Let $\{m_1, m_2, \dots, m_L\}$ be $L$ relatively co-prime sampling rates that may be much smaller than the frequencies and $j = \sqrt{-1}$. In this case the undersampled waveform becomes

$$x_{m_l}[n] = \sum_{i=1}^{N} A_i e^{\frac{2\pi j X_i n}{m_l}}, n \in \mathbb{Z} \tag{2}$$

under a sampling rate $f_s = m_l$ Hz. Applying the $m_l$-point Discrete Fourier Transform (DFT) to $x_{m_l}[n]$, we obtain

$$DFT_{m_l}(x_{m_l}[n]) = \sum_{i=1}^{N} A_i \delta(k - \langle X_i \rangle_{m_l}) \tag{3}$$

where $\delta(x) = 1$ when $x = 0$, otherwise it is 0.

If $\{A_i\}$, $i = 1, 2, \dots, N$, and $\langle X_i \rangle_{m_l}$, $l \in \{1, 2, \dots, L\}$, are different from each other, respectively, the detected peak values of amplitude-frequency response will be $\{A_i\}$. Indeed, the repeated residues with different sampling frequencies occur rarely in real systems when $m_1 \gg N$, which can be verified by simple probability analysis. Thus the corresponding relations between the residues and the amplitudes $A_i$ can be established when no two $A_i$ are the same. This can also be used to establish the relations between the frequencies and the residues. In cases where the difference of any two amplitudes $A_i$ is small enough, the corresponding relations may not be established as easily as that in above case. However, we may still be able to determine repeat times of residues in $R_l$, $l = 1, 2, \dots, L$, according to the peak values. For example, there are 3 frequencies, $\{X_1, X_2, X_3\}$, and we already get 3 distinct peaks in amplitude-frequency response as

$$\begin{aligned} \mathrm{Re}\{A_1\} = \mathrm{Re}\{A_2\} = \mathrm{Re}\{A_3\} = 1 \\ \mathrm{Im}\{A_1\} = \mathrm{Im}\{A_2\} = \mathrm{Im}\{A_3\} = 1 \end{aligned} \tag{4}$$

Here $\mathrm{Re}(A)$ and $\mathrm{Im}(A)$ denote the real and imaginary part of $A$ respectively, where $A$ is a complex number. Under a sampling rating $m_l$, $\alpha = \langle X_1 \rangle_{m_l} = \langle X_2 \rangle_{m_l}$ and $\beta = \langle X_3 \rangle_{m_l}$, it indicates that there are two frequencies with the same residue $\alpha$ modulo $m_l$, since the real parts of peaks in the amplitude-frequency response are 2 in $\alpha$ and turn to be 1 in $\beta$. The previous works assume that all sampling frequencies with same residues are such that their combined amplitude is non-zero. We now recall some well-known results.

**Lemma 1**. (Viete Theorem) Any $N$-degree polynomial

$$P(x) = a_N x^N + a_{N-1} x^{N-1} + \dots + a_1 x + a_0 \tag{5}$$

is known to have $N$ roots $\{X_1, X_2, \dots, X_N\}$ by the fundamental theorem of algebra and relations between roots and coefficients are:

$$\begin{cases} \sum_{i=1}^{N} X_i = -\frac{a_{N-1}}{a_N} = c_1 \\ \sum_{1 \le g < h \le N} X_g X_h = \frac{a_{N-2}}{a_N} = c_2 \\ \qquad \dots \\ \prod_{i=1}^{N} X_i = (-1)^N \frac{a_0}{a_N} = c_N \end{cases} \tag{6}$$

The converse theorem of Lemma 1 is also true.

**Lemma 2**. (Viete-Newton Theorem) Given $N$ integers $\{X_1, X_2, \dots, X_N\}$, let $S_k = \sum_{i=1}^{N} X_i^k$ $, k = 1, 2, \dots, N$, denote the power sum symmetric polynomials. To solve the equations $S_k = p_k$, where $p_k$ is a constant, $k = 1, 2, \dots, N$, is equivalent to solving

$$P(x) = x^N - c_1 x^{N-1} + \dots + (-1)^N c_N = 0 \tag{7}$$

where $c_0 = 1$ and

$$c_i = \frac{1}{i} \sum_{k=1}^{i} (-1)^{k-1} p_k c_{i-k}, 1 \le i \le N \tag{8}$$

## III. PROPOSED ALGORITHMS AND CORRESPONDING DYNAMIC RANGES

With the analysis in the section II, we always assume that each $R_l$ contains $N$ elements in the following, where some of them may be same. Inspired by Lemma 1, we develop Theorem 1 as follows.

**Theorem 1**. $X = \{X_1, X_2, \dots, X_N\}$ can be uniquely determined from the residue sets $R_l = \{\langle X_i \rangle_{m_l}, i = 1, 2, \dots, N\}, l = 1, 2, \dots, L$, if

$$M = \prod_{l=1}^{L} m_l > \max_{i \in \{1,2,\dots,N\}} C_N^i G^i \tag{9}$$

where $G$ is the upper bound of $X_i$ for $i = 1, 2, \dots, N$.

To prove Theorem 1, we firstly present Algorithm 1 below to determine the frequencies. Note that due to the symmetry, we need not to know the corresponding relations between residues and frequencies, i.e., $\langle c_1 \rangle_{m_l} = \langle \sum_{i=1}^{N} r_{il} \rangle_{m_l}$, $\langle c_2 \rangle_{m_l} = \langle \sum_{1 \le g < h \le N} r_{gl} r_{hl} \rangle_{m_l}, \dots, \langle c_N \rangle_{m_l} = \langle \prod_{i=1}^{N} r_{il} \rangle_{m_l}$. Now we prove the solution derived from Algorithm 1 is unique.

Proof. Assuming that there exists another solution with the same residue sets, following Algorithm 1, it would yield the same $\{c_i, i = 0, 1 \dots, N\}$. However, according to the converse

**Algorithm 1:**

```
1. Calculate the residues of $c_0 = 1, c_1 = \sum_{i=1}^{N} X_i, c_2 = \sum_{1 \le g < h \le N} X_g X_h, \ldots, c_N = \prod_{i=1}^{N} X_i$ modulo each $m_l$, $l = 1, 2, \ldots, L$.
2. Recover $c_0, c_1, \ldots, c_N$ with CRT.
3. Construct the polynomial $P(x) = \sum_{i=0}^{N} (-1)^i c_i x^{N-i}$.
4. Solve the equation $P(x) = 0$ and get $N$ distinct integer roots, $\{X_1, X_2, \ldots, X_N\}$, which are the frequencies.
```

theorem of Lemma 1, the roots of $P(x) = 0$ can be uniquely determined by the coefficients $\{c_i, i = 0, 1 \ldots, N\}$, which causes contradiction. Q.E.D.

Therefore we reduce the problem in polynomial time to solving an $N$-degree polynomial equation and the factorization of the polynomial, which have been extensively studied in [12], [13], [15]. The well-known LLL-algorithm [15] guarantees that the factorization can be solved in polynomial time. Solutions have been developed successfully with numerical analysis to find zeros of a polynomial as well, especially in our case that all roots of $P(x) = 0$ are distinct integers, like Newton-Raphson method with Steffensen Acceleration [12], [13]. Using such methods, Algorithm 1 can be ran in polynomial time.

**Example 1**. Assume there are 3 frequencies $\{32, 24, 28\}$ to be determined, where the residue sets of frequencies modulo $m_1 = 4, m_2 = 5, m_3 = 7, m_4 = 17$ and $m_5 = 19$ are $R_1 = \{0, 0, 0\}$, $R_2 = \{2, 4, 3\}$, $R_3 = \{4, 3, 0\}$, $R_4 = \{15, 7, 11\}$ and $R_5 = \{13, 5, 9\}$, respectively. Then we calculate the residue vectors of $\{c_1, c_2, c_3\}$ modulo $\{4, 5, 7, 17, 19\}$. For instance, the residue of $c_1$ modulo $m_1$ is $\langle 0 + 0 + 0 = 0 \rangle_4 = 0$ and the residue of $c_2$ modulo $m_3$ is $\langle 0 \times 3 + 0 \times 4 + 3 \times 4 = 12 \rangle_7 = 5$. Next $\{c_1, c_2, c_3\}$ are recovered with CRT, i.e., $c_1 = 84 \leftarrow (0, 4, 0, 16, 8), c_2 = 2336 \leftarrow (0, 1, 5, 7, 18)$ and $c_3 = 21504 \leftarrow (0, 4, 0, 16, 15)$. Finally, $\{32, 28, 24\}$ can be obtained by solving $x^3 - 84x^2 + 2336x - 21504 = 0$.

In many applications such as narrow-band communication, the maximum difference between any two frequencies, $d = X_N - X_1$, will be much smaller than any $X_i$ itself. Therefore, we develop another type of symmetric polynomial to sharpen the dynamic range. For brevity, let $\sum$ denote $\sum_{1 \le g < h \le N}$ in the following. Consider a group of symmetric polynomials below

$$\Gamma = \Big\{ \sum_{i=1}^{N} X_i, \ \sum (X_g - X_h)^{2\rho}, \sum (X_g + X_h)(X_g - X_h)^{2\rho} \ \Big| \ 1 \le \rho \le \Big\lfloor \frac{N}{2} \Big\rfloor \Big\} \tag{10}$$

Now we prove that $S_k = \sum_{i=1}^{N} X_i^k$, $k = 1, 2, \ldots, N$, can be derived iteratively with the elements in $\Gamma$. It is obvious that when $k = 1$, $S_1 = \sum_{i=1}^{N} X_i$ and when $k = 2$, $S_2 = \frac{\sum (X_g - X_h)^2 + S_1^2}{N}$. For general cases, we first introduce a well-known identity $\sum_{i=0}^{\theta} (-1)^i C_\theta^i = 0$, where $\theta$ is a positive integer. Especially, when $\theta$ is replaced by $2\rho$, we can obtain that $\sum_{i=0}^{\rho-1} (-1)^i C_{2\rho}^i + \frac{(-1)^\rho}{2} C_{2\rho}^\rho = 0$.

In the following, we prove the claim by induction and assume that $S_k$ $(1 \le k \le K - 1)$ have already been derived. Assume $K = 2\rho$, where $\rho$ is an integer larger than 1. Then $\sum (X_g - X_h)^{2\rho}$ can be rewritten as

$$\Big[\sum_{l=1}^{N} \big[(N-1)X_l^{2\rho} - C_{2\rho}^1 X_l^{2\rho-1}(S_1 - X_l) + \ldots + (-1)^{\rho-1} C_{2\rho}^{\rho-1} X_l^{\rho+1}(S_{\rho-1} - X_l^{\rho-1})\big]\Big] + (-1)^\rho C_{2\rho}^\rho \Big[\sum X_g^\rho X_h^\rho\Big]. \tag{11}$$

Replacing $C_{2\rho}^\rho \sum X_g^\rho X_h^\rho$ with $(C_{2\rho}^\rho (S_\rho^2 - S_{2\rho}))/2$, we get

$$\Big[\sum_{l=0}^{\rho-1} (-1)^{l+1} C_{2\rho}^l + (-1)^{\rho+1} \frac{C_{2\rho}^\rho}{2} + N\Big] S_{2\rho} + \Lambda = N S_{2\rho} + \Lambda \tag{12}$$

where $\Lambda$ is a parameter which can be expressed by $S_k$ $, 1 \le k \le K - 1$.

With the same idea for $K = 2\rho + 1$, we obtain

$$\sum (X_g + X_h)(X_g - X_h)^{2\rho} = \sum_{l=1}^{N} \big[(N-1)X_l^{2\rho+1} - C_{2\rho}^1 X_l^{2\rho}(S_1 - X_l) + \ldots + (-1)^{2\rho} C_{2\rho}^{2\rho} X_l (S_{2\rho} - X_l^{2\rho})\big] = \Big(N + \sum_{l=0}^{2\rho} (-1)^{l+1} C_{2\rho}^l\Big) S_{2\rho+1} + \Lambda' = N S_{2\rho+1} + \Lambda' \tag{13}$$

where $\Lambda'$ is a parameter which can be expressed by $S_k$ $, 1 \le k \le K - 1$.

Therefore, we can derive $S_k$, $1 \le k \le N$, iteratively. Using Lemma 2, the problem is converted to solve an $N$-degree polynomial equation similar to Algorithm 1. We conclude the above analysis as the following theorem:

**Theorem 2**. $X = \{X_1, X_2, \ldots, X_N\}$ can be uniquely determined from the residue sets $R_l = \{\langle X_i \rangle_{m_l}, i = 1, 2, \ldots, N\}, l = 1, 2, \ldots, L$, if

$$M = \prod_{l=1}^{L} m_l > 2 C_N^2 d^{N-1} G \tag{14}$$

where $d = \max_{1 \le g < h \le N} \{|X_g - X_h|\} = X_N - X_1$.

Proof. Similar to the proof of Theorem 1, we first develop the

**Algorithm 2:**

```
1. Calculate the corresponding residues of
   $\delta_1 = \sum_{i=1}^{N} X_i, \delta_2 = \sum_{1 \le g < h \le N} (X_g - X_h)^2$,
   $\ldots, \delta_N = \sum_{1 \le g < h \le N} (X_g - X_h)^{N-1}(X_g - X_h)$ (if $N$ is odd) or $\delta_N = \sum_{1 \le g < h \le N} (X_g - X_h)^N$ (if $N$ is even)
   modulo each $m_l$ $, l = 1, 2, \ldots, L$.
2. Recover $\delta_1, \delta_2, \ldots, \delta_N$ with CRT.
3. Calculate $p_k = S_k$ $, k = 1, 2, \ldots, N$ with
   $\delta_1, \delta_2, \ldots, \delta_N$ iteratively according to (11)-(13).
4. Calculate $c_i = \frac{1}{i} \sum_{k=1}^{i} (-1)^{k-1} p_k c_{i-k}$, $i = 1, 2, \ldots, N$
   and $c_0 = 1$. Solve the $N$-degree polynomial equation
   $P(x) = x^N - c_1 x^{N-1} + \ldots + (-1)^N c_N = 0$ and get $N$
   distinct roots $\{X_1, X_2, \ldots, X_N\}$.
```

Algorithm 2. The uniqueness is the same as that in Theorem 1, which we omit for brevity. Q.E.D.

In Theorem 2, assume $d \le \varepsilon m_1$, where $\varepsilon > 1$. The number of moduli (sampling frequencies), $L$, can be estimated as follows:

$$\begin{aligned} L &< \log_{m_1} 2C_N^2 d^{N-1} G \\ &\le \log_{m_1} G + \log_{m_1} N(N-1) + (\log_{m_1} \varepsilon + 1)(N-1) \end{aligned} \tag{15}$$

When $\varepsilon$ is relatively small compared to $m_1$, $|L - \log_{m_1} G|$ is $O(N)$, where $\log_{m_1} G$ can be regarded as the number of moduli required to achieve the basic requirement $G < \prod_{l=1}^{L} m_l$.

**Example 2.** Assuming that there are 3 frequencies $\{132, 127, 118\}$ to be determined, we have the following residue sets modulo $\{7, 11, 13, 15, 16\}$ as $R_1 = \{6, 1, 6\}$, $R_2 = \{0, 6, 8\}$, $R_3 = \{2, 10, 1\}$, $R_4 = \{12, 7, 13\}$, and $R_5 = \{4, 15, 6\}$, respectively. We therefore obtain the residues of $\delta_1, \delta_2, \delta_3$ in each modulus and recover them with CRT, i.e., $\delta_1 = 377 \leftarrow (6, 3, 0, 2, 9), \delta_2 = 302 \leftarrow (1, 5, 3, 2, 14)$ and $\delta_3 = 75320 \leftarrow (0, 3, 11, 5, 8)$. Calculate $p_1 = \delta_1 = 377, p_2 = \frac{p_1^2 + \delta_2}{3} = 47477$ and $p_3 = \frac{p_1 p_2 + \delta_3}{3} = 5991383$. At last, we obtain $c_1 = 377, c_2 = \frac{1}{2}(p_1 c_1 - p_2 c_0) = 47477$ and $c_3 = \frac{1}{3}(p_1 c_2 - p_2 c_1 + p_3 c_0) = 1978152$. This is equivalent to solving the 3-degree polynomial equation $P(x) = x^3 - 377x^2 + 47326x - 1978152 = 0$. Compared to Algorithm 1, the minimal requirement of $M$ has been reduced from 1978152 to 75320.

Based on Algorithm 2, we present two corollaries and their corresponding algorithms for some special cases, which are recently studied in references [11] and [5] respectively. First, we consider the two-integer case.

**Corollary 1**. For two integers $X_1$ and $X_2$, if $M = \prod_{l=1}^{L} m_l > \max\{2G, \frac{d^2}{4}\}$, where $d = X_2 - X_1$, $X_1$ and $X_2$ can be uniquely determined from their residue sets.

Proof. From the given conditions, we have $M > 2G$, $\delta_1 = X_1 + X_2$ and the residues of $\lfloor \frac{\delta_1}{2} \rfloor$ modulo each modulus. Let $\omega = \langle (X_1 - \lfloor \frac{\delta_1}{2} \rfloor)(X_2 - \lfloor \frac{\delta_1}{2} \rfloor) \rangle_M$ which is obtained with the residues of $(X_1 - \lfloor \frac{\delta_1}{2} \rfloor)(X_2 - \lfloor \frac{\delta_1}{2} \rfloor)$ by CRT. Noticing that $(X_1 - \lfloor \frac{\delta_1}{2} \rfloor)(X_2 - \lfloor \frac{\delta_1}{2} \rfloor) \le 0$ and $|X_1 - \lfloor \frac{\delta_1}{2} \rfloor| \cdot |X_2 - \lfloor \frac{\delta_1}{2} \rfloor| \le (\frac{X_1 - X_2}{2})^2 < M$, we have $(X_1 - \lfloor \frac{\delta_1}{2} \rfloor)(X_2 - \lfloor \frac{\delta_1}{2} \rfloor) = M - \langle (X_1 - \lfloor \frac{\delta_1}{2} \rfloor)(X_2 - \lfloor \frac{\delta_1}{2} \rfloor) \rangle_M = M - \omega$. The uniqueness follows from the fact that the nonnegative solution of

$$\begin{cases} X_1 + X_2 = \delta_1 \\ X_1 X_2 = M - \omega + \lfloor \frac{\delta_1}{2} \rfloor \delta_1 - \lfloor \frac{\delta_1}{2} \rfloor^2 \end{cases} \tag{16}$$

is unique. We omit the corresponding algorithm flow chart for brevity. Q.E.D.

The work in [5] assumes that $m_1 > d$. In the following, we expand on this case, by increasing $M$ while getting rid of constraints on $N$, $L$ and $\{m_l\}$, such as $\gcd(N, m_l) = 1$, etc. We present the corollary and corresponding scheme as follows.

**Corollary 2**. Assuming that $m_L > d = X_N - X_1$ and $M = \prod_{l=1}^{L} m_l > NG$, the multiple integers, $X_1, X_2, \ldots, X_N$, can be uniquely determined from their residue sets.

Proof. Similar to Theorem 1 and 2, we firstly propose Algorithm 3. $\delta_1 = \sum_{i=1}^{N} X_i$ can be recovered from the residues since $M > NG$. Note that $X_1 \le \lfloor \frac{\delta_1}{N} \rfloor \le X_N$ and $m_L > d$, then $|X_i - \lfloor \frac{\delta_1}{N} \rfloor| < m_L$ for $i = 1, 2, \ldots, N$.

**Algorithm 3:**

```
1. Calculate the residues of $\delta_1 = \sum_{i=1}^{N} X_i$ in each $m_l$ , $l = 1, 2, \ldots, L$, i.e., the sum of residues $r_{il}$ in $R_l$ denoted by $\delta_{1l} = \langle \sum_{i=1}^{N} r_{il} \rangle_{m_l}$.
2. Recover $\delta_1$ with CRT and calculate $\langle \lfloor \frac{\delta_1}{N} \rfloor \rangle_{m_L}$.
3. Select integers in $A = \{ r_{iL} - \langle \lfloor \frac{\delta_1}{N} \rfloor \rangle_{m_L}, r_{iL} - \langle \lfloor \frac{\delta_1}{N} \rfloor \rangle_{m_L} - m_L, r_{iL} - \langle \lfloor \frac{\delta_1}{N} \rfloor \rangle_{m_L} + m_L \mid i = 1, 2, \ldots, N \}$ whose absolute value is smaller than $m_L$. Denote those elements as $\xi[l]$ in an ascending order, $l = 1, 2, \ldots, 2N$.
4. Define $\Theta_k = \sum_{l=k}^{k+N-1} \xi[l]$ , $k = 1, 2, \ldots, N+1$. Then, use a binary search to find a $\gamma$ in $\{1, 2, \ldots, N+1\}$ such that $\Theta_\gamma = \delta_1 - \lfloor \frac{\delta_1}{N} \rfloor N$.
5. Compute $X_i = \lfloor \frac{\delta_1}{N} \rfloor + \xi[\gamma + i]$ for $i = 1, 2, \ldots, N$.
```

Considering the set $A = \{ r_{iL} - \langle \frac{\delta_1}{N} \rangle_{m_L}, r_{iL} - \langle \frac{\delta_1}{N} \rangle_{m_L} - m_L, r_{iL} - \langle \frac{\delta_1}{N} \rangle_{m_L} + m_L \mid i = 1, 2, \ldots, N \}$, which includes all the possible values of $X_i - \lfloor \frac{\delta_1}{N} \rfloor$. Select the elements from the set $A$ denoted by $\xi[l]$ such that $|\xi[l]| < m_L$. Indeed, if $r_{iL} = \langle \lfloor \frac{\delta_1}{N} \rfloor \rangle_{m_L}$, $r_{iL} - \langle \lfloor \frac{\delta_1}{N} \rfloor \rangle_{m_L}$ is within $[0, m_L)$, if $r_{iL} > \langle \lfloor \frac{\delta_1}{N} \rfloor \rangle_{m_L}$, $r_{iL} - \langle \frac{\delta_1}{N} \rangle_{m_L}$ and $r_{iL} - \langle \frac{\delta_1}{N} \rangle_{m_L} - m_L$ are selected and if $r_{iL} < \langle \lfloor \frac{\delta_1}{N} \rfloor \rangle_{m_L}$, $r_{iL} - \langle \frac{\delta_1}{N} \rangle_{m_L}$ and $r_{iL} - \langle \lfloor \frac{\delta_1}{N} \rfloor \rangle_{m_L} + m_L$ are selected. Without loss of generality, we omit the simple case of $r_{iL} = \langle \lfloor \frac{\delta_1}{N} \rfloor \rangle_{m_L}$. Let the selected elements $\xi[l]$, $l = 1, 2, \ldots, 2N$, be arranged in an ascending order. Define $\Theta_k = \sum_{l=k}^{k+N-1} \xi[l]$, $k = 1, 2, \ldots, N+1$. Clearly, $\Theta_k$ are also in an ascending order and $\Theta_{k+1} - \Theta_k = m_L$. Then we only need to find a $\gamma$ in $\{1, 2, \ldots, N+1\}$, such that $\Theta_\gamma = \delta_1 - \lfloor \frac{\delta_1}{N} \rfloor N$ and $\Theta_\gamma$ is just the sum of $\{X_i - \lfloor \frac{\delta_1}{N} \rfloor | i = 1, 2, \ldots, N\}$. The uniqueness is also clear due to the monotonicity of $\Theta_k$. Thus a binary search can be applied here to reduce the complexity to $O(\log_2 N)$. Q.E.D.

In such case, $L \approx \log_{m_1} NG = \log_{m_1} N + \log_{m_1} G$, when $N \ll m_1$, $\log_{m_1} N$ can be neglected.

**Example 3.** As a continuation of Example 2, notice that $d = 14 < m_5 = 16$, $\delta_1 = 377$ and $\lfloor \frac{\delta_1}{3} \rfloor = 125$ with its residue 13 modulo 16. Since $R_5 = \{4, 15, 6\}$, we obtain A={-25,-9,7,-14,2,18,-23,-7,9} and $\delta_1 - \lfloor \frac{\delta_1}{N} \rfloor N = 2$. Next we select $\xi[l]$ as $\{-14, -9, -7, 2, 7, 9\}$ and obtain $\Theta_k$, $k = 1, 2, 3, 4$. With a binary search, we first check $\Theta_2 = -9 - 7 + 2 \ne 2$. Then we check $\Theta_3 = -7 + 2 + 7 = 2$. Finally, we obtain $X_1 = 125 - 7 = 118$, $X_2 = 125 + 2 = 127$ and $X_3 = 125 + 7 = 132$.

## IV. CONCLUSION

In this paper, we studied several popular cases of CRT-based algorithms for determining multiple frequencies in undersampled complex-value waveforms. The proposed algorithms achieve improvements in the dynamic range and efficiency, based on symmetric polynomials.

## V. ACKNOWLEDGEMENTS

The work is supported by Initiative Scientific Research Program of Tsinghua University under Grant No. 2015THZ0 and National Key Technology Support Program of China (No. 2013BAD15B06).

## REFERENCES

[1] Xiang-Gen Xia, "On estimation of multiple frequencies in undersampled complex valued waveforms," in IEEE Transactions on Signal Processing, 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 Processing Lett., vol. 7, pp. 34-37, Feb. 2000.

[4] H. Liao and X. G. Xia, "A Sharpened Dynamic Range of a Generalized Chinese Remainder Theorem for Multiple Integers," in IEEE Transactions on Information Theory, vol. 53, no. 1, pp. 428-433, Jan. 2007.

[5] 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”[J]. Signal Processing Letters IEEE, 2015, 22:2199-2203.

[6] Xiang-Gen Xia and Guangcai Zhou, "Multiple frequency detection in undersampled waveforms," Signals, Systems Computers, 1997. Conference Record of the Thirty-First Asilomar Conference on, Pacific Grove, CA, USA, 1997, pp. 867-871 vol.1.

[7] 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”[J]. Signal Processing Letters, IEEE, 2005, 12(11): 768-771.

[8] Wang W, Xia X G. “A closed-form robust Chinese remainder theorem and its performance analysis”[J]. Signal Processing, IEEE Transactions on, 2010, 58(11): 5655-5666.

[9] W. Wang, X. Li, W. Wang and X. G. Xia, "Maximum Likelihood Estimation Based Robust Chinese Remainder Theorem for Real Numbers and Its Fast Algorithm," in IEEE Transactions on Signal Processing, vol. 63, no. 13, pp. 3317-3331, July1, 2015.

[10] Wei Wang; Xiaoping Li; Xiang-Gen Xia; Wenjie Wang, “The Largest Dynamic Range of a Generalized Chinese Remainder Theorem for Two Integers,” in Signal Processing Letters, IEEE , vol.22, no.2, pp.254-258, Feb. 2015

[11] Li Xiao; Xiang-Gen Xia, “A Generalized Chinese Remainder Theorem for Two Integers,” in Signal Processing Letters, IEEE, vol.21, no.1, pp.55-59, Jan. 2014

[12] Kincaid D R, Cheney E W. “Numerical analysis: mathematics of scientific computing”[M]. American Mathematical Soc., 2002.

[13] Kress R. “Numerical analysis, volume 181 of Graduate Texts in Mathematics”[J]. 1998.

[14] Hanshen Xiao, Hari Krishna Garg, Jianhao Hu, and Guoqiang Xiao, "New Error Control Algorithms for Residue Number System Codes," ETRI Journal, vol. 38, no. 2, Apr. 2016, pp. 326-336.

[15] Lenstra A K, Lenstra H W, LovÃąsz L. “Factoring polynomials with rational coefficients”[J]. Mathematische Annalen, 1982, 261(4): 515-534.

[16] Schnorr C P, Euchner M. “Lattice basis reduction: improved practical algorithms and solving subset sum problems”[J]. Mathematical programming, 1994, 66(1-3): 181-199.

[17] Li G, Xu J, Peng Y N, et al. “Bistatic linear antenna array SAR for moving target detection, location, and imaging with two passive airborne radars”[J]. Geoscience and Remote Sensing, IEEE Transactions on, 2007, 45(3): 554-565.

[18] Krishna H, Krishna B, Lin K Y, et al. “Computational Number Theory and Digital Signal Processing: Fast Algorithms and Error Control Techniques”[M]. CRC Press, 1994.

[19] Grossschadl J. “The Chinese remainder theorem and its application in a high-speed RSA crypto chip”[C]//Computer Security Applications, 2000. ACSAC’00. 16th Annual Conference. IEEE, 2000: 384-393.

[20] C.Ding, D.Pei, and A.Salomaa, “Chinese remainder theorem: applications in computing, coding, cryptography”[M], World Scientific Publishing, 1996.

[21] Xia, Xiang-Gen. "Dynamic range of the detectable parameters for polynomial phase signals using multiple-lag diversities in high-order ambiguity functions." Information Theory, IEEE Transactions on 47.4 (2001): 1378-1384.

[22] O. Goldreich, D. Ron and M. Sudan, "Chinese remaindering with errors," in IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1330-1338, Jul 2000.

[23] Li, Gang, et al. "Location and imaging of moving targets using nonuniform linear antenna array SAR." Aerospace and Electronic Systems, IEEE Transactions on 43.3 (2007): 1214-1220.

[24] L. Xiao, X. G. Xia and W. Wang, "Multi-Stage Robust Chinese Remainder Theorem," in IEEE Transactions on Signal Processing, vol. 62, no. 18, pp. 4772-4785, Sept.15, 2014.

[25] L. Xiao and X. G. Xia, "Error Correction in Polynomial Remainder Codes With Non-Pairwise Coprime Moduli and Robust Chinese Remainder Theorem for Polynomials," in IEEE Transactions on Communications, vol. 63, no. 3, pp. 605-616, March 2015.