

# 鲁棒的闭式中国余数定理及其在欠采样 频率估计中的应用

王文杰 李小平

(西安交通大学智能网络与网络安全教育部重点实验室, 西安 710049)

**摘 要:** 中国余数定理在数字信号处理等领域有着广泛的应用。传统的中国余数定理要求待恢复的数及余数都为整数, 且对噪声极其敏感。为了在余数含有误差时鲁棒的恢复原来的数, 一种鲁棒的中国余数定理最近被提出。但是现有的算法都是基于搜索的, 因此所需的运算量极大。为了克服这一缺陷, 本文提出了鲁棒的闭式中国余数定理, 在此基础上给出了重建原来数的算法。最后, 将该方法应用于欠采样下信号频率的估计中。仿真的结果表明, 在相同信噪比下, 所给算法和现有的搜索算法的估计性能一样的, 但是所给出的算法所需的运算量大幅的减少, 且解的形式更为简洁。

**关键词:** 信号处理; 中国余数定理; 鲁棒的; 欠采样; 频率估计

**中图分类号:** TP911.7    **文献标识码:** A    **文章编号:** 1003-0530(2013)09-1206-06

## The Closed-Form Robust Chinese Remainder Theorem and Its Application in Frequency Estimation with Undersampling

WANG Wen-jie LI Xiao-ping

(Ministry of Education Key Lab for Intelligent Networks and Network Security, Xi'an  
Jiaotong University, Xi'an 710049, China)

**Abstract:** The Chinese remainder theorem is widely used in many fields such as signal processing. It tells us that an integer can be reconstructed by its corresponding remainders. As we know, it is not robust in the sense that a small error in its remainders may cause a large error in the determined integer by the CRT. In order to resist the error sensitivity, a robust CRT was proposed recently. However, all of the methods in the literatures were searching based which required a heavy computational load. In this paper, a Closed-form robust Chinese Remainder Theorem is presented to solve the robust estimation problem. Furthermore, we give the algorithm to reconstruct the original number. In order to verify the effectiveness of the method, we applied it to the frequency determination when the signal waveforms are undersampled. Simulation results show that the proposed algorithm has the same performance but less computational complexity. Moreover, it has a more concise expression.

**Key words:** Signal Processing; Chinese Remainder Theorem; Robust; Undersampled; Frequency estimation

### 1 引言

中国余数定理 (Chinese remainder theorem, CRT) 是数论中的一个古老话题<sup>[1]</sup>。它告诉我们, 如

果一个整数小于一组两两互质的数的最小公倍数, 则该数可由其取模运算后的余数唯一地确定下来。由于其“化整为零”的特点, 使得该定理在数字信号处理<sup>[2-3]</sup>、编码<sup>[4-5]</sup>、密码学<sup>[6]</sup>及计算机<sup>[7-8]</sup>等领域获

收稿日期: 2013-05-01; 修回日期: 2013-08-03

基金项目: 国家自然科学基金(编号: 61172092, 61171108)

得了广泛的应用。然而, CRT 对误差特别敏感, 即极小的余数误差使得恢复的数与原来的数相差很大。正是这一缺陷, 限制了其在实际系统中的应用, 如在雷达<sup>[9-10]</sup>、RIPS<sup>[11]</sup>等系统中, 由于不可避免的存在噪声, 从实际中得到的数据往往带有误差且为实数。因而, 传统的 CRT 无法解决这些实际的问题。

为了克服这一缺陷, 文献[12]提出了一种鲁棒的中国余数定理方法, 即利用余数的冗余来鲁棒的恢复原来的数。该方法的基本原理为: 假设所有的模含有不为 1 的最大公约数, 且除去该最大公约数后所得的余数两两互质。若所有余数的误差在某个范围时, 则被回复数的误差也会控制在一定范围内。该文献给出了这个最大的误差范围, 即误差的界为最大公约数的四分之一; 同时给出了搜索算法。但所给该算法是一个二维的搜索, 运算量是很大的, 尤其是当被恢复的数很大时, 这种二维的搜索变得更难实现。为了减少繁重的运算, 文献[13-14]给出了快速的搜索算法, 大大降低了运算量。由于鲁棒的中国余数定理既克服了传统 CRT 要求被恢复的数以及余数都为整数的条件限制, 又具有鲁棒性, 使得其在雷达系统<sup>[15-17]</sup>、测距<sup>[18-19]</sup>、角度估计<sup>[20]</sup>以及欠采样频率估计<sup>[21-22]</sup>等问题中有着广泛的应用。

尽管文献[21]给出的快速算法将二维的搜索降为一维的搜索, 大大降低了运算量, 但该算法的运算量与所取模的个数以及模的大小都有关。当所取模的个数较多或数值较大时, 都会使得搜索量加大。为了避免多余的搜索, 本文提出了一种鲁棒的中国余数定理的闭式求解方法( closed-form robust CRT, CRCRT)。该方法通过差分运算得到了余数问题的闭式解, 无需搜索, 因而大大减少了运算量。为了验证该方法的效果, 我们将其应用到频率估计中。仿真的结果表明, 与所给出的快速搜索算法( fast searching CRT, FSCRT) 相比, 所给的算法不仅有更小的运算量, 还有着更简洁的闭式估计表达式。

## 2 中国余数定理及其推广

我们首先给中国余数定理及其推广的形式。

设  $N$  为一正整数, 若  $N$  关于模  $M_1, M_2, \dots, M_L$  的余数分别为  $r_1, r_2, \dots, r_L$ , 即

$$N \equiv r_i \pmod{M_i} \quad (1)$$

其中  $0 \leq r_i < M_i, i=1, 2, \dots, L$ 。则当  $N < lcm(M_1, M_2, \dots, M_L)$  时, 其中  $lcm(\cdot)$  表示最小公倍数, 整数  $N$  可由其余数唯一的确定<sup>[1]</sup>。本文考虑模  $M_1, M_2, \dots, M_L$  有最大公约数  $M$ , 且除去最大公约数  $M$  后的数是两两互质的情况, 即  $M_i = M\Gamma_i, i=1, 2, \dots, L$ , 且  $\gcd(\Gamma_i, \Gamma_j) = 1, i \neq j$ ,  $\gcd(\cdot)$  表示最大公约数。下面我们来讨论此推广的中国余数定理。

注意到 (1) 可等价的写为:

$$N = n_i M \Gamma_i + r_i, i=1, 2, \dots, L \quad (2)$$

其中  $n_i$  为一整数, 也称为模糊倍数。

由上式可知,  $r_i$  关于模  $M$  后的余数为同一常数, 记为  $r^c$ 。于是  $r_i - r^c$  为  $M$  的一整倍数, 不妨设为  $q_i$ , 于是有

$$r_i = M q_i + r^c \quad (3)$$

将上式代入(2)可得

$$N = (n_i \Gamma_i + q_i) M + r^c \quad (4)$$

记  $N_0 = n_i \Gamma_i + q_i, i=1, 2, \dots, L$ , 则(4)可表示为:  $N = M N_0 + r^c$ 。

上述推广的中国余数定理是在余数没有误差的情况下得到的, 下面我们着重分析当余数有误差时, 如何得到原来数的鲁棒估计。

## 3 鲁棒的闭式中国余数定理

设第  $i$  个余数的误差为  $\Delta r_i$ , 则含有误差的余数  $\hat{r}_i$  为

$$\hat{r}_i = r_i + \Delta r_i, i=1, 2, \dots, L \quad (5)$$

于是鲁棒的估计问题即为, 如何从余数  $\hat{r}_1, \hat{r}_2, \dots, \hat{r}_L$  中鲁棒的恢复原来数  $N$ 。由(2)可以看出  $n_i M \Gamma_i \gg r_i$ , 因此, 模糊倍数  $n_i$  的估计值决定了原来数的估计。为了得到鲁棒的估计值  $\hat{N}$ , 模糊倍数  $n_i$  要估计正确。下面我们从  $\hat{r}_i$  来得到这些估计值  $\hat{n}_i$ 。

由于  $N_0 = n_i \Gamma_i + q_i, i=1, 2, \dots, L$ , 将其写成一个等式组即为,

$$\begin{cases} N_0 = n_1 \Gamma_1 + q_1 \\ N_0 = n_2 \Gamma_2 + q_2 \\ \vdots \\ N_0 = n_L \Gamma_L + q_L \end{cases} \quad (6)$$

将上方程组的后  $L-1$  项减去第一项, 得

$$\begin{cases} n_1\Gamma_1 - n_2\Gamma_2 = q_{2,1} \\ n_1\Gamma_1 - n_3\Gamma_3 = q_{3,1} \\ \vdots \\ n_1\Gamma_1 - n_L\Gamma_L = q_{L,1} \end{cases} \quad (7)$$

其中  $q_{i,1} = q_i - q_1 \quad i=2, 3, \dots, L$ 。

通过上方程组可以得到模糊数  $n_i$  的表达式,进而可以得到  $N$  的值。下面的定理给出这一结论。为了方便,我们记  $x$  关于模  $M$  的余数为  $\langle x \rangle_M$ 。

引理 1

由方程组(7)确定的解为:

$$\begin{cases} n_1 = q_{i,1} \overline{\Gamma_{i,1}} + k\Gamma_i \\ n_i = \frac{n_1\Gamma_1 - q_{i,1}}{\Gamma_i} \end{cases} \quad (8)$$

其中  $k$  为某一整数,  $\overline{\Gamma_{i,1}}$  为  $\Gamma_1$  关于  $\Gamma_i$  的模逆,  $i=2, 3, \dots, L$ 。

证明: 考虑方程组(7)中第  $i$  个方程:

$$n_1\Gamma_1 - n_i\Gamma_i = q_{i,1} \quad (9)$$

由于  $\Gamma_1, \Gamma_2, \dots, \Gamma_L$  是两两互质的,故  $\Gamma_1$  关于  $\Gamma_i$  的模逆是存在的。设其为  $\overline{\Gamma_{i,1}}$ , 于是

$$\langle \overline{\Gamma_{i,1}} \cdot \Gamma_1 \rangle_{\Gamma_i} = 1 \quad (10)$$

(9) 两边同乘以  $\overline{\Gamma_{i,1}}$  可得

$$n_1\Gamma_1 \overline{\Gamma_{i,1}} - n_i\Gamma_i \overline{\Gamma_{i,1}} = q_{i,1} \overline{\Gamma_{i,1}} \quad (11)$$

(11) 关于  $\Gamma_i$  取模可得  $n_1 = \langle q_{i,1} \overline{\Gamma_{i,1}} \rangle_{\Gamma_i}$ 。这意味着存在某一整数  $k$ , 使得  $n_1 = q_{i,1} \overline{\Gamma_{i,1}} + k\Gamma_i$ 。

将所求得的  $n_1$  代入(9), 即可得  $n_i = \frac{n_1\Gamma_1 - q_{i,1}}{\Gamma_i} \quad i=2, 3, \dots, L$ 。

由引理 1 可看出,为了求得  $n_i$ , 首先得求解出  $q_{i,1}$ , 其中  $i=2, 3, \dots, L$ 。由(3)可得,

$$r_i - r_1 = M(q_i - q_1)$$

也即是,

$$q_{i,1} = \frac{r_i - r_1}{M}$$

在余数有错误的情况下,记  $q_{i,1}$  的估计值  $\hat{q}_{i,1}$  为

$$\hat{q}_{i,1} = \left[ \frac{\hat{r}_i - \hat{r}_1}{M} \right] \quad (12)$$

其中,  $[\cdot]$  表示取圆整运算,任意实数  $x$  的圆整运算满足关系:  $-\frac{1}{2} \leq x - [x] < \frac{1}{2}$ 。

得到  $q_{i,1}$  的估计值  $\hat{q}_{i,1}$  后,可以求得模糊数  $n_i$  的估计值  $\hat{n}_i$ , 下面的定理给出了这一结果。

定理 1

记  $\Gamma = \Gamma_1 \cdots \Gamma_L$ ,  $\gamma_i = \Gamma / \Gamma_i$ , 则在(12)的条件下  $n_i$  的估计值  $\hat{n}_i$  为:

$$\begin{cases} \hat{n}_1 = \left\langle \sum_{i=2}^L \hat{\xi}_{i,1} b_{i,1} \frac{\gamma_1}{\Gamma_i} \right\rangle_{\gamma_1} \\ \hat{n}_i = \frac{\hat{n}_1\Gamma_1 - \hat{q}_{i,1}}{\Gamma_i} \end{cases} \quad (13)$$

其中  $b_{i,1}$  为  $\frac{\gamma_1}{\Gamma_i}$  关于  $\Gamma_i$  的模逆,  $\hat{\xi}_{i,1} = \hat{q}_{i,1} \overline{\Gamma_{i,1}}, i=2, 3, \dots, L$ 。

证明: 当余数为  $\hat{r}_1, \hat{r}_2, \dots, \hat{r}_L$  时,在(12)的条件下,定理 1 的结论中的  $q_{i,1}$  为对应的估计值  $\hat{q}_{i,1}$ 。因此  $n_i$  的估计值  $\hat{n}_i$  为:

$$\hat{n}_1 = \hat{q}_{i,1} \overline{\Gamma_{i,1}} + k\Gamma_i \quad (14)$$

$$\hat{n}_i = \frac{\hat{q}_{i,1} \overline{\Gamma_{i,1}} \Gamma_1 - \hat{q}_{i,1}}{\Gamma_i} + k\Gamma_1 \quad i=2, 3, \dots, L \quad (15)$$

由(14)可知  $\hat{n}_1 = \langle \hat{q}_{i,1} \overline{\Gamma_{i,1}} \rangle_{\Gamma_i}$ , 记  $\hat{\xi}_{i,1} = \hat{q}_{i,1} \overline{\Gamma_{i,1}}$ , 于是

$$\hat{n}_1 = \langle \hat{\xi}_{i,1} \rangle_{\Gamma_i} \quad i=2, 3, \dots, L \quad (16)$$

于是  $\hat{n}_1$  可由  $L-1$  个余数  $\langle \hat{\xi}_{2,1} \rangle_{\Gamma_2}, \langle \hat{\xi}_{3,1} \rangle_{\Gamma_3}, \dots, \langle \hat{\xi}_{L,1} \rangle_{\Gamma_L}$  确定下来。记  $\gamma_1 = \Gamma_2\Gamma_3 \cdots \Gamma_L$ ,  $\frac{\gamma_1}{\Gamma_i}$  关于模  $\gamma_1$  的模逆记为  $b_{i,1}$ , 则由中国余数定理可得  $\hat{n}_1$  的值为

$$\hat{n}_1 = \left\langle \sum_{i=2}^L \hat{\xi}_{i,1} b_{i,1} \frac{\gamma_1}{\Gamma_i} \right\rangle_{\gamma_1} \quad (17)$$

将其代入(15)可得:  $\hat{n}_i = \frac{\hat{n}_1\Gamma_1 - \hat{q}_{i,1}}{\Gamma_i} \quad i=2, 3, \dots, L$ 。

定理 1 给出了从有误差的余数中估计模糊数的方法,当模糊数  $n_1, n_2, \dots, n_L$  全部估计出以后,可以得到原来数  $N$  的估计值  $\hat{N}$ :

$$\hat{N} = \frac{1}{L} \sum_{i=1}^L \hat{n}_i M \Gamma_i + \hat{r}_i \quad (18)$$

下面我们给出鲁棒的闭式中国余数定理的算法。

步骤 1: 利用(12),从带有误差的余数  $\hat{r}_1, \hat{r}_2, \dots, \hat{r}_L$  中计算  $\hat{q}_{i,1} \quad i=2, 3, \dots, L$ 。

步骤 2: 计算  $\hat{\xi}_{i,1}$ :

$$\hat{\xi}_{i,1} = \hat{q}_{i,1} \overline{\Gamma_{i,1}} \quad i=2, 3, \dots, L$$

其中  $\overline{\Gamma_{i,1}}$  为  $\Gamma_1$  关于  $\Gamma_i$  的模逆。

步骤 3: 计算  $\hat{n}_1$ :

$$\hat{n}_1 = \left\langle \sum_{i=2}^L \hat{\xi}_{i,1} b_{i,1} \frac{\gamma_1}{\Gamma_i} \right\rangle_{\gamma_1}$$

其中  $b_{i,1}$  为  $\frac{\gamma_1}{\Gamma_i}$  关于模  $\gamma_1$  的模逆。

步骤 4: 计算  $\hat{n}_i$ :

$$\hat{n}_i = \frac{\hat{n}_1 \Gamma_1 - \hat{q}_{i,1}}{\Gamma_i} \quad i=2, 3, \dots, L$$

步骤 5: 由 (18) 计算出  $\hat{N}$ 。

最后, 我们给出鲁棒的估计出原来数  $N$  的充分必要条件。

定理 2

记  $\Gamma = \Gamma_1 \Gamma_2 \cdots \Gamma_L$ ,  $\Gamma_1, \Gamma_2, \dots, \Gamma_L$  两两互质。若  $0 \leq N < lcm(M_1, M_2, \dots, M_L) = M\Gamma$ , 则  $\hat{n}_j = n_j$ ,  $j=1, 2, \dots, L$  当且仅当  $-\frac{M}{2} \leq \Delta r_i - \Delta r_1 < \frac{M}{2}$ ,  $i=2, 3, \dots, L$ 。

证明: 由 (5) 及 (12) 可得,

$$\hat{q}_{i,1} = q_{i,1} + \left[ \frac{\Delta r_i - \Delta r_1}{M} \right] \quad (19)$$

充分性:

由于  $-\frac{M}{2} \leq \Delta r_i - \Delta r_1 < \frac{M}{2}$ ,  $i=2, 3, \dots, L$ , 故有

$$\left[ \frac{\Delta r_i - \Delta r_1}{M} \right] = 0。从而 \hat{q}_{i,1} = q_{i,1}。也即是 \hat{\xi}_{i,1} = \xi_{i,1}。$$

由 (17) 可得  $\hat{n}_1 = \left\langle \sum_{i=2}^L \xi_{i,1} b_{i,1} \frac{\gamma_1}{\Gamma_i} \right\rangle_{\gamma_1}$ , 即  $\hat{n}_1 = n_1$ 。由

(13) 可得  $\hat{n}_i = n_i$ ,  $i=2, 3, \dots, L$ 。

必要性:

假设至少存在一个  $\Delta r_j$ ,  $j \in \{2, 3, \dots, L\}$ , 不满足  $-\frac{M}{2} \leq \Delta r_j - \Delta r_1 < \frac{M}{2}$ 。于是,  $\left[ \frac{\Delta r_j - \Delta r_1}{M} \right] \neq 0$ 。由

(19) 可得  $\hat{q}_{j,1} \neq q_{j,1}$ 。下面分两种情况讨论:

(1) 若  $\left[ \frac{\Delta r_j - \Delta r_1}{M} \right] \neq k\Gamma_j$

在此情况下  $\hat{q}_{j,1} \neq q_{j,1} + k\Gamma_j$ 。由 (16) 可知  $\hat{n}_1$  关于模  $\Gamma_j$  的余数为  $\langle \hat{q}_{j,1} \overline{\Gamma_{j,1}} \rangle_{\Gamma_j}$ 。而  $n_1$  关于模  $\Gamma_j$  的余数为  $\langle q_{j,1} \overline{\Gamma_{j,1}} \rangle_{\Gamma_j}$ 。由于  $\langle \hat{q}_{j,1} \overline{\Gamma_{j,1}} \rangle_{\Gamma_j} \neq \langle q_{j,1} \overline{\Gamma_{j,1}} \rangle_{\Gamma_j}$ , 由中国余数定理可知  $\hat{n}_1 \neq n_1$ 。

(2)  $\left[ \frac{\Delta r_j - \Delta r_1}{M} \right] = k\Gamma_j$

在此情况下  $\hat{q}_{j,1} = q_{j,1} + k\Gamma_j$ 。由于  $\hat{n}_1$  与  $n_1$  关于  $\Gamma_i$  同模, 所以  $\hat{n}_1 = n_1$ 。由引理 2 可得,

$$\hat{n}_j = \frac{\hat{n}_1 \Gamma_1 - \hat{q}_{j,1}}{\Gamma_j} = n_j - k \quad (20)$$

从而  $\hat{n}_j \neq n_j$ 。

#### 4 欠采样下信号频率的估计

本节利用本文提出的 CRCRT 算法, 对欠采样下单频率的信号进行频率估计。

假设频率为  $f_0$  的复信号为:

$$S(t) = A \exp(j2\pi f_0 t) + \omega(t) \quad (21)$$

其中  $\omega(t)$  为高斯白噪声。

由 Nyquist 采样定理可知, 为了估计频率  $f_0$ , 采样的频率不能小于  $2f_0$ 。通常频率  $f_0$  较大, 因此高的采样率给硬件带来了诸多的不便。为了降低采样速率, 我们在欠采样的情况下对原频率进行估计。现假设用  $L$  次采样, 频率分别为  $M_1, M_2, \dots, M_L$ 。由中国余数定理可知, 能唯一的确定出原信号的频率而不产生模糊的最大频率为  $lcm(M_1, M_2, \dots, M_L)$ 。在不超过最大频率的条件下, 将获得欠采样下信号的样本用 FFT 来求得在  $M_i$  采样率下的估计值(对应于定理中的带误差的余数  $\hat{r}_i$ )。最后, 利用鲁棒的中国余数定理估计出原频率的值。本文用 CRCRT 和 FSCRT 两种鲁棒的方法来估计信号的真实频率。下面给出仿真的条件及结果。

图 1 和 2 取采样点数  $L=3$ , 采样率分别为  $M_1=11M$ ,  $M_2=13M$ ,  $M_3=17M$ , 其中  $M$  为最大公约数, 本实验取 100 以及 200。每个信噪比下, 运行的次数为 10000。我们用相对误差的均值以及正确估计的概率来衡量算法的性能。如果估计的误差不超过真实值的 0.1%, 则认为估计是正确的。从误差均值及正确估计的概率随信噪比的变化曲线的结果可以看出: 当采样率有相同的最大公约数  $M$  时, CRCRT 算法和 FSCRT 的均值误差和正确估计的概率几乎是一样的。也就是说, 这两种方法几乎有这相同的性能。另外, 从图中也可以看出,  $M=200$  时的性能好于  $M=100$  的, 也就是说, 最大公约数大的余数组, 对应的估计性能好。这一结论也符合事实, 由 (12) 可以看出,  $M$  越大, 就能容忍的误差的范围也就越大。经过欠采样后, 采样率由原来的最大 243100 降为 1700, 大大降低了采样率。

图3给出了两种算法的运行时间随着采样点个数变化时的曲线。在实验中,取 $M=100$ , $\Gamma_1$ 到 $\Gamma_6$ 分别为7、11、13、17、19、23,运行的次数为1000。从图中可以看出,FSCRT的运行时间随着采样点数呈线性增加,而CRCRT的运行时间基本不随采样点数的增加而增加。因而,与FSCRT算法相比,CRCRT算法更快。随着采样的个数增多,且采样率的变大,这种运算的优势更加明显。

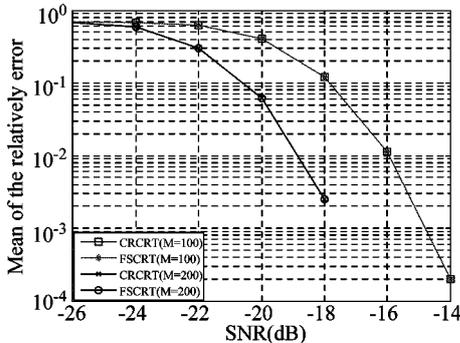


图1 相对误差均值随信噪比变化的曲线

Fig. 1 Mean of the relatively error versus SNR

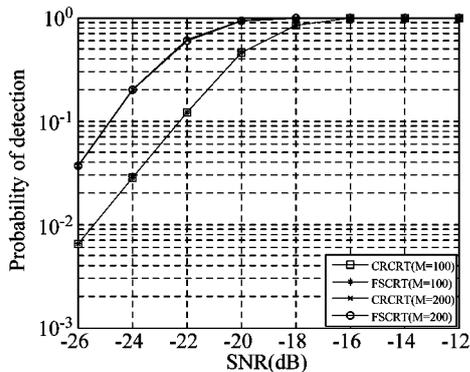


图2 正确估计的概率随信噪比变化的曲线

Fig. 2 The probability of the correct estimation versus SNR

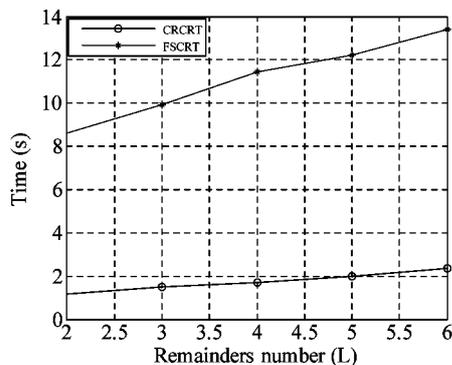


图3 运算时间随采样点个数的变化曲线

Fig. 3 Running time versus the number of sampling

## 5 结论

本文给出了一种鲁棒的中国余数定理的新的算法,解决了当余数含有误差且不为整数时,快速的估计出原来的数这一问题。不同于已有鲁棒的恢复方法,本文给出的基于差分思想的鲁棒闭式中国余数定理不需要大量的搜索,且有着更为简洁的数学表达式。为了验证所给方法的有效性,将其应用于欠采样下信号频率的估计中,并将该方法和现有的FSCRT做了对比。仿真的结果表明,所给算法和搜索算法相比,有几乎相同的性能,但是所给出的算法所需的运算量大幅减小。

## 参考文献

- [1] Rosen K H. Elementary Number Theory and Its Applications [M]. fifth ed. Addison-Wesley, 2010.
- [2] McClellan J H, Rader C M. Number Theory in Digital Signal Processing [M]. Englewood Cliffs, NJ: Prentice-Hall, 1979.
- [3] 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.
- [4] Goldreich O, Ron D, Sudan M. Chinese remaindering with errors [J]. Information Theory, IEEE Transaction on, 2000, 46(7): 1330-1338.
- [5] Guruswami V, Sahai A, Sudan M. "Soft-decision" decoding of Chinese remainder codes [C]. Foundations of Computer Science, 2000. Proceedings 41st Annual Symposium on. IEEE, 2000: 159-168.
- [6] Ding C, Pei D, Salomaa A. Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography [M]. Singapore: World Scientific, 1999.
- [7] Yen S M, Lim S, Moon S. RSA speedup with Chinese remainder theorem immune against hardware fault cryptanalysis [J]. Computers, IEEE Transactions on, 2003, 52(4): 461-472.
- [8] Sarkar S, Kisku B, Misra S, Obaidat M S. Chinese remainder theorem based RSA-threshold cryptography in MANET using verifiable secret sharing scheme [C]. Wireless and Mobile Computing, Networking and Communications, 2009. IEEE International Conference on, IEEE, 2009: 258-262.

- [9] Jorgensen D P , Shepherd T R , Goldstein A S. A dual-pulse repetition frequency scheme for mitigating velocity ambiguities of the NOAA P-3 airborne Doppler radar [J]. *Journal of Atmospheric and Oceanic Technology* , 2000 , 17( 5) : 585-594.
- [10] Ruegg M , Meier E , Nuesch D. Capabilities of dual-frequency millimeter wave SAR with monopulse processing for ground moving target indication [J]. *Geoscience and Remote Sensing , IEEE Transactions on* , 2007 , 45( 3) : 539-553.
- [11] Maroti M , Kusy B , Balogh G , Volgyesi P , Molnar K , Nadas A , Dora S , Ledecz A. Radio interferometric geolocation [C]. *Proceedings of the 3rd international conference on Embedded networked sensor systems. ACM* , 2005: 1-12.
- [12] Xia X G , Wang G. Phase unwrapping and a robust Chinese remainder theorem [J]. *Signal Processing Letters , IEEE* , 2007 , 14( 4) : 247-250.
- [13] Li G , Xu J , Peng Y N , Xia X G. An efficient implementation of a robust phase unwrapping algorithm [J]. *Signal Processing Letters , IEEE* , 2007 , 14( 6) : 665-668.
- [14] Li X , Xia X G. A fast robust Chinese remainder theorem based phase unwrapping algorithm [J]. *Signal Processing Letters , IEEE* , 2008 , 15: 665-668.
- [15] Li G , Xu J , Peng Y N , Xia X G. Location and imaging of moving targets using nonuniform linear antenna array SAR [J]. *Aerospace and Electronic Systems , IEEE Transactions on* , 2007 , 43( 3) : 1214-1220.
- [16] Li G , Xu J , Peng Y N , Xia X G. Moving target location and imaging using dual-speed velocity SAR [J]. *IET-Radar , Sonar & Navigation* , 2007 , 1( 2) : 158-163.
- [17] Li G , Xu J , Peng Y N , Xia X G. 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] Li W C , Wang X Z , Wang X M , Moran B. Distance estimation using wrapped phase measurements in noise [J]. *Signal Processing , IEEE Transactions on* , 2013 , 61( 7) : 1676-1688.
- [19] Wang C , Yin Q Y , Wang W J. An efficient ranging method for wireless sensor networks [C]. *Acoustics Speech and Signal Processing ( ICASSP )* , 2010. *IEEE International Conference on. IEEE* , 2010: 2846-2849.
- [20] Xia X G. On estimation of multiple frequencies in under-sampled complex valued waveforms [J]. *Signal Processing , IEEE Transactions on* , 1999 , 47 ( 12) : 3417-3419.
- [21] Li X W , Liang H , Xia X G. A robust Chinese remainder theorem with its applications in frequency estimation from undersampled waveforms [J]. *Signal Processing , IEEE Transactions on* , 2009 , 57( 11) : 4314-4322.
- [22] 叶丰 , 罗景青 , 陈明建 , 唐希雯. 基于低速采样的多正弦波信号的频率估计 [J]. *信号处理* , 2011 , 27( 6) : 883-889.
- Ye F , Luo J Q , Chen M J , Tang X W. Multiple frequencies estimation of sinusoidal signals with sub-sampling [J]. *Signal Processing* , 2011 , 27( 6) : 883-889. ( in Chinese)

#### 作者简介



王文杰 男, 1971 年出生于山西, 2001 年获得西安交通大学信息与通信工程专业博士学位。现为西安交通大学教授、博士生导师。主要研究方向为 MIMO 和 OFDM 系统、数字信号处理、无线传感器网络等。E-mail: wjwang@xjtu.edu.cn



李小平 男, 1984 年生, 西安交通大学博士研究生, 主要研究方向为阵列信号处理。E-mail: lixiaoping@stu.xjtu.edu.cn