广义稳健的中国剩余定理及其在欠采样率下频率估计中的应用

梁 红　张 琦　杨长生
(西北工业大学航海学院　西安　710072)

摘　要：该文针对传统中国剩余定理在余数有误差时重构整数不稳健性的缺陷，提出了采用一组非互质的模数和相应的有误差的余数估计任意正整数的广义稳健中国剩余定理，给出了详细的定理证明，得出了算法重构整数公式和误差上限表达式。将该定理用于欠采样下信号频率估计，仿真实例验证了所提算法的稳健性和实际工程应用前景。

关键词：信号处理；中国剩余定理；广义稳健中国剩余定理；欠采样；频率估计
中图分类号：TN911.7　　**文献标识码**：A　　**文章编号**：1009-5896(2010)08-1802-04
DOI: 10.3724/SP.J.1146.2009.00718

A Generalized Robust Chinese Remainder Theorem and Its Application to Frequency Estimation with Undersampling

Liang Hong　Zhang Qi　Yang Chang-sheng
(*College of Marine*, *Northwestern Polytechnical University*, *Xi'an* 710072, *China*)

Abstract: The Chinese remainder theorem 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 this paper, a Generalized Robust Chinese Remainder Theorem (GRCRT) is presented when moduli are not pair-wisely co-prime and the remainders have errors. The new theorem is proofed in detail; The formulas of the estimated integer and estimation error upper bound are provided. The RCRT is then applied to determine the frequency when the signal waveforms are undersampled. Simulation results show that new algorithm is robust with considering residue errors and can use to the area of digital signal processing and will have more applications to other areas.

Key words: Signal Processing; Chinese Remainder Theorem (CRT); Generalized Robust Chinese Remainder Theorem (GRCRT); Undersampled; Frequency estimation

1　引言

近几十年来中国剩余定理(Chinese Remainder Theorem，CRT)在数字信号处理、编码、密码学、计算机等领域获得了广泛的应用[1−3]。传统的 CRT 利用一组两两互质的模数及相应的余数来估计一个整数，但是只有未知的整数小于这组模数的最小公倍数时，才能唯一确定一个整数。而且传统 CRT 算法不稳健，即余数的极小误差就可能引起被估计整数相当大的误差。而在许多应用场合，余数的估计是存在误差的，这一点限制了它在许多领域的应用。例如，在数字信号处理中可以采用几次欠采样(欠采样频率对应 CRT 中模数)获得的样本估计频率(CRT 中的余数)，如果这些频率估计有很小的误差(在低信噪比下)，则利用 CRT 重构算法估计信号真实频率就会产生相当大的误差。为了解决这一问题，文献[4–6]等提出的广义 CRT 方法利用足够大的模数/余数来修正余数的误差；文献[7]从相位解卷积出发，提出了稳健的 CRT(Robust Chinese Remainder Theorem, RCRT)重构算法，采用了一组非互质的模数及相应的有误差的余数来估计整数，无需修正余数误差，控制了 CRT 重构算法产生的整数估计误差，但是该算法的缺陷在于被估计的整数局限于与模数相关的离散点，大大限制了在实际工程中的应用。本文在该算法的基础上，提出了广义的 RCRT(Generalized RCRT，GRCRT)重构算法，给出了严格的数学证明，并详细分析了传统 CRT 与 GRCRT 重构算法的误差，纠正了文献[7]中给出的传统 CRT 估计误差下限公式，最后用信号处理中的算例验证了 GRCRT 的稳健性及工程实用性。

2　问题的提出

设 N 为正整数；$M=\{M_1,M_2,\cdots,M_L\}$ 为一组正整数，不失一般性，假定 $M_i(1\le i\le L)$ 两两互质，

2009-05-12 收到，2010-05-18 改回
国家自然科学基金(60702067)资助课题
通信作者：梁红　Lianghong@nwpu.edu.cn

且 $M_1 < M_2 < \cdots < M_L$；$\boldsymbol{r}$ 为 N 对模数 M_i 后的余数集合

$$\boldsymbol{r}(N) \triangleq \{r_i : i = 1,2,\cdots,L\} \tag{1}$$

其中

$$r_i \equiv N \bmod M_i, \quad i = 1,2,\cdots,L \tag{2}$$

传统的CRT给出了已知 M_i 和 r_i 求自然数N的公式：

$$N = \sum_{i=1}^{L} r_i Q_i N_i + K(N)Q \tag{3}$$

式中 N_i 为正整数，并且 $Q_i N_i \equiv 1 \mod M_i$；$Q_i \triangleq M_1 \cdots M_{i-1} M_{i+1} \cdots M_L$，$Q = \prod_{i=1}^{L} M_i$，$K(N)$ 为任意整数。一般情况下，我们要求的是符合条件的最小自然数N，此时 $K(N)$ 就是确定的整数。如果能得到余数的准确估计，则传统的CRT就提供了很好的求解自然数N的方法。但在许多应用场合，我们获得的 r_i 是有误差的，即

$$\tilde{\boldsymbol{r}}(N) \triangleq \{\tilde{r}_i = r_i + \varepsilon_i : i = 1,2,\cdots,L\} \tag{4}$$

ε_i 为估计的误差，可正可负。利用式(3)估计得到 $\widehat{N}$，其估计误差的绝对值为

$$\left|N - \widehat{N}\right| = \left|\sum_{i=1}^{L} \varepsilon_i N_i Q_i + (K'(\widehat{N}) - K(N))Q\right| \tag{5}$$

$K'(\widehat{N})$ 为任意整数，一般 $K'(\widehat{N})$ 等于使 $\widehat{N}$ 等于模 M_i 后余数为 $\tilde{r}_i$ 的最小自然数的整数，一般情况下 $K(N) \neq K'(\widehat{N})$。可见，整数$N$估计的误差不仅与余数误差有关，而且与模数及除法次数有关，采用的除法次数越多，模数越大，则该方法可能达到的误差就越大。也就是说传统CRT算法中，余数的很小误差就可能引起很大的被估计整数误差。因为 $\varepsilon_i, K(N)$ 和 $K'(\widehat{N})$ 均可正可负，且为整数，式(5)估计误差的下限是1。文献[7]中式(25)给出的重构自然数 N 的公式本身没有错误，与本文式(3)只是表达形式不一致而已，但是文献[7]作者在推导估计误差下限时没有考虑到无误差时重构整数 N 要求的N_i(文献[7]中式(25)中出现)与有误差时重构整数 $\widehat{N}$ 要求的N_i可能是不相等的，因而文献[7]中式(26)给出的传统CRT估计误差最小值的表达式 $\tau\, \Gamma_1\Gamma_2 \cdots \Gamma_{L-1}$(其中 τ 为所有余数误差绝对值中的最大值，Γ_i 与本文中的 M_i 的定义相同)是错误的。因为 τ 最小值为1，余数定理中 $L \geq 2$，该表达式的最小值为 Γ_1，是不可能为1的。可以举例说明：已知模数 $M_1 = 30$，$M_2 = 31$，相应的无误差的余数为 $r_1 = 10$，$r_2 = 8$，利用传统的CRT估计的最小自然数为 N 为70；如果余数的估计存在误差，其值分别为 $\tilde{r}_1 = 9$，$\tilde{r}_2 = 7$，则利用传统的CRT估计的最小自然数为 $\widehat{N}$ 为69，估计误差的绝对值为1。如果根据文献[7]中式(26)给出的传统CRT估计误差最小值的表达式 $\tau\, \Gamma_1\Gamma_2 \cdots \Gamma_{L-1}$，在此例中误差的最小值为30，这与实际情况是不符的。

根据以上分析提出了以下问题：假定有一组误差在一个合理范围内的余数集合及相对应的准确已知的模数集合，如何找到一种方法能稳健地重构估计参数N? 与此相关需要解决的就是如何确定N的范围和余数的误差范围，从而唯一地确定整数N。文献[7]提出了稳健的CRT重构方法，但是定理要求估计的数N是一组两两互质数乘积的正整数倍，在实际应用中该条件不容易满足。本文就是在文献[7]的基础上，提出一种广义的RCRT算法，有效地解决了这一问题，扩大了CRT的工程应用领域。

3　广义稳健的中国剩余定理

给定模数和相应的余数，利用传统的 CRT，一个整数可以表示为

$$N = n_i M_i + r_i, \quad 1 \leq i \leq L \tag{6}$$

如果余数的估计为 $\tilde{r}_i$，则式(6)可写成

$$N = n_i M_i + \tilde{r}_i + \varepsilon_i, \quad 1 \leq i \leq L \tag{7}$$

其中 n_i 为正整数，$0 \leq \tilde{r}_i \leq M_i - 1$，$\varepsilon_i$ 为估计的误差，$|\tilde{r}_i - r_i| = |\varepsilon_i| \leq \tau$。我们需要通过 M_i 和 $\tilde{r}_i$ 唯一地确定 N 的值，也就是要准确地估计式(7)中的 $n_i\,(1 \leq i \leq L)$。

受文献[7]的启发，对模数进行合理的约束，使 M_i 满足：

$$M_i = M\Gamma_i, \quad 1 \leq i \leq L \tag{8}$$

其中 M 是正的整常数，Γ_i 和 Γ_j 互质，$\Gamma_1 < \Gamma_2 < \cdots \Gamma_L$，$1 \leq i \neq j \leq L$。在实际应用中可以通过选择互质的一组数的整数倍作为模数 M_i，这样的假设也是合理的。

对 $1 < i < L$，定义：

$$\gamma_i \triangleq \Gamma_1 \cdots \Gamma_{i-1}\Gamma_{i+1} \cdots \Gamma_L \tag{9}$$

对 $2 \leq i \leq L$，定义：

$S_i \triangleq$

$$\left\{(\overline{n}_1, \overline{n}_i) = \arg\min_{\substack{\overline{n}_1 = 0,1,\cdots,\gamma_1 - 1 \\ \overline{n}_i = 0,1,\cdots,\gamma_i - 1}} \left|\widehat{n}_i M_i + \tilde{r}_i - \widehat{n}_1 M_1 - \tilde{r}_1\right|\right\} \tag{10}$$

$S_{i,1}$ 表示满足式(10)的所有 $(\overline{n}_1, \overline{n}_i)$ 中的第 1 个元素 $\overline{n}_1$ 的集合，即

$$S_{i,1} \triangleq \{\overline{n}_1 : (\overline{n}_1, \overline{n}_i) \in S_i\} \tag{11}$$

定义

$$S \triangleq \bigcap_{i=2}^{L} S_{i,1} \tag{12}$$

根据上述定义，可以得到以下定理。

定理 假设模数满足式(8)条件，Γ_i 和 Γ_j 互质，$1 \le i \ne j \le L$。如果

$$0 \le N < M\Gamma_1\Gamma_2\cdots\Gamma_L \tag{13}$$

且

$$M > 4\tau \tag{14}$$

则由式(12)定义的集合 S 仅包含一个元素 n_1，即 $S=\{n_1\}$，如 $(n_1,\overline{n}_i)\in S_i$，表明对任意 $1\le i\le L$ 有 $n_i\ (1\le i\le L)$ 是式(7)的唯一解。

定理的详细证明见附录。文献[8,9]提供了求解 n_i 的简化算法。当获得了式(6)或式(7)中的 n_i 的准确值后，则整数 N 的估计值为

$$\widehat{N}=\frac{1}{L}\sum_{i=1}^{L}(n_iM_i+\tilde{r}_i) \tag{15}$$

估计的误差上限为

$$\left|N-\widehat{N}\right|=\frac{1}{L}\sum_{i=1}^{L}|\varepsilon_i|\le\tau \tag{16}$$

可见利用 GRCT 估计整数 N 的误差仅与余数的估计误差 ε_i 有关，最大不会超过 $M\Gamma_L$。而由式(5)给出的传统 CRT 估计的误差不仅与余数误差有关，而且与模数及除法次数有关，可以达到相当大的数量级。另外，GRCRT 的模数为 $\Gamma_iM\ (1\le i\le L)$，有公倍数 M，这一点不满足传统 CRT 重构定理的条件，因而本文提出的 GRCRT 方法提供了利用非相互互质的模数和相应的余数估计小于 $M\Gamma_1\Gamma_2\cdots\Gamma_L$ 的任意正整数方法，而文献[7]给出的是重构 $n_0\prod_{i=1}^{L}\Gamma_i$ (n_0 为非负整数)的方法，限制了算法在实际中的应用。

4 欠采样下利用 GRCRT 估计信号频率

在实际的信号处理中，至少有 3 种情形下需要处理的样本是不满足 Nyquist 采样定理要求的，即获得的是欠采样样本。一是为了满足实时处理的需要，采样频率不能太高；二是考虑硬件处理的复杂度；三是信号频率发生变化。在这些情况下如采用样本满足 Nyquist 采样定理下的算法进行信号的参数估计就不能获得准确的估值，这就需要寻求新的方法。本节利用本文提出的 GRCRT 算法，对欠采样下最常见的单频信号的频率进行估计，并给出仿真结果。过程如下：首先确定欠采样频率 M_i(对应于定理中的模数，$1\le i\le L$)，L 为欠采样次数，获得欠采样下信号样本，采用 FFT 估计在 M_i 采样率下频率(对应于定理中的余数 $\tilde{r}_i$)，再利用本文提出的定理求出 n_i，最后利用式(15)估计信号真实频率(相当于定理中的 $\widehat{N}$)。在仿真中复信号形式：

$$x(t)=Ae^{j2\pi f_0t+\theta}+w(t) \tag{17}$$

其中 $f_0=120$ kHz，θ 在 $[0,2\pi]$ 之间均匀分布，$w(t)$ 为复高斯白噪声，均值为 0，方差为 1，样本数为 6000。仿真中选取第 3 节中的参数：$L=2$，$\Gamma_1=17$，$\Gamma_2=18$，M 取一确定正整数。也就是采用两次欠采样频率为 M_1 和 M_2(模数)下获得的样本进行 FFT 运算，得到两次频率的估计，相当于 GRCRT 中的余数 $\tilde{r}_i\ (i=1,2)$，再利用本文提出的定理获得信号频率 f_0 的估计。为了验证 M 的取值对算法性能的影响，仿真中 M 取 400，800，1000，图 1 为 M 变化时信噪比与检测概率的曲线(估计的相对误差小于 0.5%时，该次检测有效)，结果表明，M 越大，采样频率越高，在低信噪比下的检测概率就越高。图 2 为 M 变化时信噪比与估计的均方误差曲线，图中结果表明，在很低的信噪比下，由于余数估计的误差超过定理中 $M>4\tau$ 的限制，式(7)中的 n_i 得不到唯一解，故 SNR <-24 dB 时曲线有交叉，估计的均方误差也相当大；SNR ≥ -22 dB 时，FFT 估计频率的精度很高，信号频率估计的均方误差接近零。图 1 和图 2 均是 10000 次 Monte-carlo 试验的结果。

需要说明的余数估计的误差与采用的估计频率算法有关，该例子中与 FFT 估计频率的误差有关(采样频率，采样点数，信噪比等因素有关)。

传统 CRT 算法中余数的极小误差就可能在重构被估计整数时引起很大的误差。为了证明这一点，本文在欠采样情况下进行了仿真实验，利用两次欠采样获得的样本，采用 FFT 估计频率(余数)，再利用传统 CRT 估计信号真实频率。信号形式同前，$f_0=120$ kHz，为了与 GRCRT 算法中 $M=1000$ 的情况做比较，选取欠采样频率 $M_1=17011$，$M_2=17989$ (传统 CRT 的模数必须互质，M_1 为与 1000×17 接近的质数，M_2 是与 1000×18 接近的质数)，经过 10000 次 Monte-carlo 实验得到图 3 所示的 SNR 与估计的均方误差曲线。可见在 SNR ≥ -10 dB 时由于估计的 $\tilde{r}_1=924$，$\tilde{r}_2=12065$，而实际余数为 $r_1=923$，$r_2=12066$，余数估计误差 $|\varepsilon_i|=1$，导致实际估计信号频率的均方误差达到 10^{16} 数量级。说明在欠采样情况下，采样传统 CRT 算法不稳健，不能估计信号的真实频率。

5 结论

本文提出了解余数有误差的广义稳健中国剩余定理，并给出了详细的定理证明，得出算法估计的误差仅与余数估计的误差有关，克服了传统 CRT 算法极小的余数误差带来相当大整数估计误差的局限。与文献[7]不同，本文算法估计的整数不局限于与采样频率有关的离散点，文献[7]仅是本文提出定理的特例。同时指出了文献[7]中传统 CRT 算法估

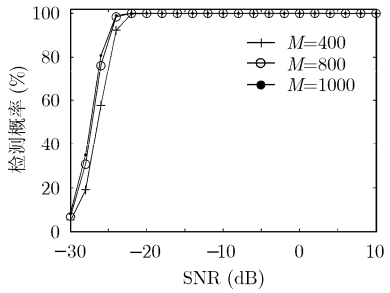

图 1 M 变化时，信噪比与检测概率之间的关系曲线

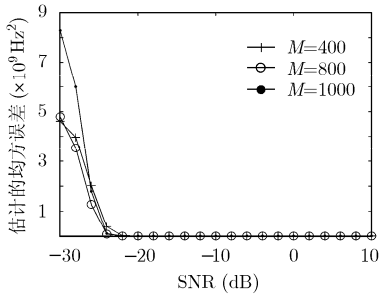

图 2 M 变化时，信噪比与估计的均方误差之间的关系曲线

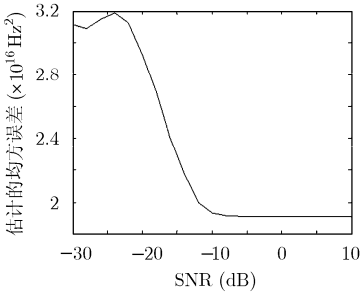

图 3 传统 CRT 算法下信噪比与估计频率的均方误差关系曲线

计误差最小值表达式的错误。用信号处理中的仿真实验比较了 GRCRT 算法和传统 CRT 算法估计信号频率的误差，验证了所提算法的稳健性。算法适用于任意余数估计有误差，对整数估计可以有误差的场合，不仅可以应用于数字信号处理中的雷达、声纳、生物医学等方面，还可推广应用其他相关领域。

附录　定理的证明

由式(6)和式(13)可得，$n_i < \dfrac{M\Gamma_i\gamma_i - r_i}{M_i} = \gamma_i - r_i/M_i$。因为 $r_i < M_i$，所以 $n_i < \gamma_i$，即式(7)中的真实解 n_i 落在 $[0,\gamma_i)$ 内，$1 \le i \le L$。因此，对于 $2 \le n_i \le L$ 和任意 $(\overline{n}_1,\overline{n}_i) \in S_i$，有

$$\left|\overline{n}_i M_i + \tilde{r}_i - \overline{n}_1 M_1 - \tilde{r}_1\right| \le \left|n_i M_i + \tilde{r}_i - n_1 M_1 - \tilde{r}_1\right| \tag{A1}$$

设 $\mu_i = \overline{n}_i - n_i$，$1 \le i \le L$。将式中 $(n = n_i M_i + \tilde{r}_i + \varepsilon_i, 1 \le i \le L)$ $\tilde{r}_i = n - n_i M_i - \varepsilon_i$ 代入式(A1)的两边，得

$$\left|\mu_i M\Gamma_i - \mu_1 M\Gamma_1 - (\varepsilon_i - \varepsilon_1)\right| \le \left|\varepsilon_i - \varepsilon_1\right|$$

再利用式(14)，得

$$\left|\mu_i\Gamma_i - \mu_1\Gamma_1\right| \le \frac{2\left|\varepsilon_i - \varepsilon_1\right|}{M} \le \frac{4\tau}{M} < 1 \tag{A2}$$

因为 μ_i, Γ_i, μ_1 和 Γ_1 是整数，式(A2)表明

$$\mu_i\Gamma_i = \mu_1\Gamma_1, \quad i = 2,3,\cdots,L \tag{A3}$$

因为 Γ_i 和 Γ_1 互质，式(A3)意味着

$$\mu_1 = m_i\Gamma_i, \quad \mu_i = m_i\Gamma_1$$

即对于 $|m_i| < \min(\gamma_i,\gamma_1)$ 有

$$\overline{n}_1 = n_1 + m_i\Gamma_i, \quad \overline{n}_i = n_i + m_i\Gamma_1 \tag{A4}$$

将式(A4)代入式(A1)，即得

$$\left|\overline{n}_i M_i + \tilde{r}_i - \overline{n}_1 M_1 - \tilde{r}_1\right| = \left|n_i M_i + \tilde{r}_i - n_1 M_1 - \tilde{r}_1\right| \tag{A5}$$

这就意味着 $(n_1,n_i) \in S_i$，$i = 2,3,\cdots,L$，这就证明了 $n_1 \in S$。式(A4)还表明

$$S_i = \left\{(n_1 + m_i\Gamma_i, n_i + m_i\Gamma_1) \ \middle| \ |m_i| < \min(\gamma_i,\gamma_1)\right\} \tag{A6}$$

如果 $\overline{n}_1 \in S$ 成立，则 $\overline{n}_1 \in S_{i,1}$ $(i = 2,3,\cdots,L)$，结合式(11) $S_{i,1}$ 的定义式和式(A6)，可得 $\overline{n}_1 - n_1 = m_i\Gamma_i$，$|m_i| < \min(\gamma_i,\gamma_1)$ $(i = 2,3,\cdots,L)$。也就是说 $\overline{n}_1 - n_1$ 可以整除所有的 Γ_i $(i = 2,3,\cdots,L)$，结合式(9)，可得 $\overline{n}_1 - n_1$ 是 γ_1 的整数倍。由于 $0 \le \overline{n}_1, n_1 \le \gamma_1 - 1$，所以 $\overline{n}_1 - n_1 = 0$。$S = \{n_1\}$ 得证。同时 $\overline{n}_1 = n_1$ 意味着式(A6)中的 $m_i = 0$，代入式(A4)有 $\overline{n}_i = n_i$ $(i = 2,3,\cdots,L)$。定理得证。

参 考 文 献

[1] Krishna B, Krishna H C, and Lin K Y. Computational Number Theory and Digital Signal Processing: Fast Algorithms and Error Control Techniques[M]. CRC Press, Boca Raton, FL, USA, 1994: 1–5.

[2] Grossschadl J. The Chinese Remainder Theorem and its application in a high-speed RSA crypto chip[C]. 16th Annual Conference on Computer Security Applications, New Orleans, USA, 2000: 384–393.

[3] Ding C, Pei D, and Salomaa A. Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography[M]. Singapore, World Scientific, 1996: 2–10.

[4] Goldreich O, Ron D, and Sudan M. Chinese remaindering with errors[J]. *IEEE Transactions on Information Theory*, 2000, 46(7): 1330–1338.

[5] Guruswami V, Sahai A, and Sudan M. 'Soft-decision' decoding of Chinese remainder codes. in Proc[C]. 41st IEEE Symp. Foundations Computer Science, Redondo Beach, CA, 2000: 159–168.

[6] Xia X G and 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]. *IEEE Signal Processing Letters*, 2005, 12(11): 768–771.

[7] Xia X G and Wang G. Phase unwrapping and a robust Chinese remainder theorem[J]. *IEEE Signal Processing Letters*, 2007, 14(4): 247–250.

[8] Li G, Xu J, Peng Y N, and Xia X G. An efficient implementation of robust phase- unwrapping algorithm[J]. *IEEE Signal Processing Letters*, 2007, 14(6): 393–396.

[9] Li X and Xia X G. A fast robust Chinese remainder theorem based phased unwrapping algorithm[J]. *IEEE Signal Processing Letters*, 2008, 15(10): 665–668.

梁　红：　女，1969 年生，副教授，研究方向为信号检测、参量估计及自适应信号处理.

张　琦：　女，1987 年生，硕士生，研究方向为水下信号处理.

杨长生：　男，1978 年生，博士后，研究方向为宽带信号处理.