冗余余数系统低复杂度快速纠错算法设计

肖翰珅[①] 胡剑浩*[②] 马 上[②]
[①](清华大学数学科学系 北京 100084)
[②](电子科技大学通信抗干扰技术国家级重点实验室 成都 611731)

摘 要：余数系统由于具有增强传输信息在并行系统中鲁棒性的优势，已被广泛应用在无线局域网(WLAN)以及码分多址通信技术(CDMA)等领域。而余数系统中的纠错检错是保证传输数据可靠性和高效性的关键问题。该文根据有限环上剩余类的性质提出溢出判定定理，不重复判断定理和唯一性区间搜索定理，并在此基础上进一步提出采用模运算代替传统中国剩余定理进行快速恢复的单错误纠错算法，将复杂度降低为$O(k/r)$；提出不重复判定纠错算法；并对于一般错误情形，设计通过比较算子实现的搜索纠错算法。其中搜索纠错算法能直接实现系统最大纠错能力，且避免依靠复杂模运算算子实现，系统吞吐率得以提高；与传统算法相比，计算复杂度由多项式级降低至对数级。

关键词：编码理论；中国剩余定理；冗余余数系统；纠错检错
中图分类号： TN919.3 **文献标识码**： A **文章编号**：1009-5896(2015)08-1944-06
DOI: 10.11999/JEIT141454

Low-complexity Error Correction Algorithms for Redundant Residue Number Systems

Xiao Han-shen[①] Hu Jian-hao[②] Ma Shang[②]
[①](*Department of Mathematics*, *Tsinghua University*, *Beijing* 100084, *China*)
[②](*National Key Laboratory of Science and Technology on Communications*, *University of Electronic Science and Technology of China*, *Chengdu* 611731, *China*)

Abstract: Redundant Residue Number System (RRNS) is widely used in communication systems for WLAN (Wireless LAN) and CDMA (Code Division Multiple Access) etc. due to its strong ability to enhance robustness of information in parallel processing environments. Error detection and correction of RRNS is an important guarantee for information reliability in communication systems. The overflow detection theorem, the unique theorem, and the searching theorem are proposed and proved in the paper based on properties of residue classes in finite rings. With the theorems, a single-error-correction algorithm using modular operations with reduced complexity $O(k/r)$ is proposed. The uniqueness test algorithm is proposed. Furthermore, for any general types of errors, the searching multiple-error-correction algorithm is proposed. The computational complexity of the searching multiple-error-correction algorithm is reduced from polynomial order to logarithmic order according to the analysis, and the method can reach the extreme correction capability efficiently with only comparison operations instead of complex modular arithmetic.

Key words: Coding theory; Chinese remainder theorem; Redundant Residue Number System (RRNS); Error detection and correction

1 引言

现代通信、雷达、多媒体技术的发展对数字信号处理(Digital Signal Processing, DSP)的要求日益增加。其主要表现在DSP算法复杂度增加的同时要求更高的处理速度、系统吞吐率和可靠性，更低的单位功耗和成本。这些需求在机载、移动和卫星等设备中的数字信号处理芯片设计上表现得尤为突出。研究表明，在未来的集成电路设计里，大规模的并行处理技术将取代传统的串行处理方式，以满足对集成电路处理能力和处理速度日益提高的要求。DSP算法的并行处理目前主要有两个研究领域：一是通过增加处理单元的数量并辅以相关调度机制

2014-11-20收到，2015-04-08改回，2015-06-09网络优先出版
国家自然科学基金(61101033, 61076096)，国家863计划项目(2011AA010201)，清华大学自主科研计划(20141081231)和国家高科技中央高校基本科研业务费(ZYGX 2011J118)资助课题
*通信作者：胡剑浩 jhhu@uestc.edu.cn

实现高速大容量的计算和处理，例如用两个解码器并行工作可以使解码速度提高 1 倍；二是采用并行数值表征系统代替传统的数值表征系统，从算法前端入手解决 VLSI 的速度、功耗和面积问题。后者利用数值表征系统的并行性，在算法的最前端考虑DSP 系统的并行实现，而余数系统(Residue Number System, RNS)就是一个并行数值表征系统。RNS 是一个古老的无权重数字表征系统，源于中国剩余定理(Chinese Remainder Theorem, CRT)，它将传统的多位数复杂运算用多个并行的较少位数的简单运算单元来实现；并且在进行乘、加运算时，各通道完全独立，只使用数据的余数表征向量的对应分量进行乘、加运算。这一并行的数值表征计算形式不仅可以有效地降低面积功耗，也决定了余数系统潜在的高速度。由于其高速、低复杂度和低功耗的特性，RNS 已被研究证明适用于如无线局域网[1]、码分多址通信技术、卷积和快速傅里叶变换等数字信号处理领域[2]。

冗余余数系统(Redundant Residue Number System, RRNS)通过向余数系统引入冗余的余数基，使得其表征的计算系统具有冗余性。具体体现为RRNS中各运算通道是互为冗余的，而且各通道计算是相互独立的；当部分余数分量出现错误时，该错误不会在各分量间扩散，此时仍可以通过余数分量间的冗余关系获得正确的运算结果。RRNS中所有余数分量(含冗余分量)可以同等地参与数据通道的相关计算和检错、纠错计算，而普通的纠错编码，需要在各级计算后重新进行编译码的操作。作为具有纠错能力的并行数值表征和计算系统，RRNS被广泛应用于正交信号处理[3,4]以及自适应多载波调制[5]等领域。

在现有工作中，基于RRNS的纠错编码一般有以下两种策略。第1种是基于计算余数向量特征值与设定值比对来完成：Yang等人[6]通过迭代增加冗余基，并利用中国剩余定理在低可靠度无线信道中进行数据还原以解决纠错问题；但是由于每一次增加冗余基的操作均需通过CRT还原数据，复杂度较高。文献[7,8]引入Hamming重量以及最小距离概念，提出了通过找出错误位并纠正，最终实现纠错检错的算法。但从文献[7]的单错误纠正算法到文献[8]双错误和单突发错误纠正算法的改进是较复杂的。第2种策略是通过还原数据比对来完成：文献[9]基于连分数以及欧几里得方法[10]，通过冗余校验基和信息基的组合有效地确定了余数向量的错误位，纠正后还原得到正确数据。文献[11]在文献[9,10]的基础上通过引入最大似然码(Maximum Likelihood Decoding, MLD)理论对算法进行了改进，不再遍历提取基的组合，但在计算码距时也引入了不少计算量。随后文献[12,13]设计了基于RRNS的高效集成电路数据通道抗辐照保护方法，使得RRNS的纠错算法更为广泛地用于解决通信可靠性问题，但是纠错的速度和高复杂度仍是现有RRNS纠错的瓶颈。

针对传统 RRNS 纠错算法复杂度高的问题，本文在 CRT 的基础上，利用有限环剩余类的性质，提出并证明了溢出判定定理、不重复判定定理和唯一性区间搜索定理，并在此基础上提出了 3 种分别针对单错误和多错误的低复杂度 RRNS 纠错算法，避免了枚举带来的算法复杂度随基的个数增加而指数上升的问题。实验证明：本文提出的单错误纠错算法利用模运算来避免多次运用 CRT 还原数据，并基于余数系统中基的无权重性，提出基的整体代换思想，将计算复杂度降低至 $O(k/r)$；基于定理 2 提出的不重复检测纠错算法在大型 RRNS 内具有优势；基于定理 3 提出的多错误搜索纠错算法只依靠比较算子实现，避免了传统算法中的复杂模运算，其计算复杂度从已有工作的 $O(k^t)$ 降低至 $O(\log k)$。

本文结构安排如下：在第 2 节中，介绍 RNS 和 RRNS 的定义，给出并证明支持所提出算法的必要定理及推论；在第 3 节中建立了 3 种 RRNS 纠错算法；在第 4 节中，对本文算法和已有的多种常用算法进行了复杂度比较与性能分析；最后给出了结论。

2　基本概念与数学推证

2.1 余数系统与中国剩余定理

余数系统(RNS)由一组两两互质的余数基 $\{m_1, m_2, \cdots, m_n\}$ 定义。一个整数 $\boldsymbol{X}$ 可由它对应的余数向量表示，记为 $\boldsymbol{\Phi}=(a_1,a_2,\cdots,a_n)$，其中 $a_i \equiv X(\mathrm{mod}\ m_i)=\langle X\rangle_{m_i}, i=1,2,\cdots,n$。此余数系统所能表示的整数 $\boldsymbol{X}$ 的范围为 $[0,M)$，其中 $M=\prod_{i=1}^{n} m_i$，M称为该余数系统(RNS)的动态范围。例如：在一个RNS中选取{2,3,5,7}作为基，则该RNS的动态范围为210，数19对应的余数表征向量为(1,1,4,5)。而 $\boldsymbol{X}$ 可以由下式(1)确定：

$$X=<\sum_{i=1}^{n} M_i <M_i^{-1}>_{m_i} a_i>_M \tag{1}$$

$M_i=M/m_i\left\langle M_i^{-1}\right\rangle_{m_i}$ 为 M_i 对 m_i 的模倒数。式(1)即为著名的中国剩余定理。

根据高斯模运算准则，任取[0,M]范围内的整数 (a,b,c)，其对应余数基 $\{m_1,m_2,\cdots,m_n\}$ 的余数向量分别为：$(a_1,a_2,\cdots,a_n),(b_1,b_2,\cdots,b_n)$ 和 $(c_1,c_2,\cdots,c_n)$，定义符号“Δ”表示加、减及乘法运算。则 $c=a\Delta b$ 的

计算在余数系统的表征下变为 $c_i = \langle a_i \Delta b_i \rangle_{m_i}, i = 1, 2, \cdots, n$。因此在进行乘加运算时可将传统的多位数(bit)的复杂运算用多个并行的较少位数的简单运算来实现。

2.2 冗余余数系统

含有冗余校验基的余数系统称为冗余余数系统(RRNS)。检错和纠错过程通常是基于冗余余数系统来实现的。设 $m_i (i = 1,2,\cdots,k,k+1,\cdots,k+r)$ 为 RRNS 的基，其中 $m_1 < m_2 < \cdots < m_{k+r}$，称 $m_1, m_2, \cdots, m_k$ 为信息基，$m_{k+1}, m_{k+2}, \cdots, m_{k+r}$ 为冗余校验基。此冗余余数系统的动态范围为 $[0, M_k)$，其中 $M_k = \prod_{i=1}^{k} m_i$。记 $n = k + r$，$M = \prod_{i=1}^{n} m_i$，定义 $[M_k, M)$ 为此冗余余数系统的非法范围。定义 RRNS(n,k)为一个共含有 $n = k + r$ 个基，其中有 k 个信息基，r 个冗余校验基的冗余余数系统。后文内容均在 RRNS(n,k)上讨论。

设接收向量为 $\boldsymbol{\Phi}' = (b_1, b_2, \cdots, b_n)$，其中 b_i 为 $\boldsymbol{\Phi}'$ 中基 m_i 对应的分量。在接收向量中，如果基 m_i 对应的分量未出错，则称该分量是正确的；否则，称它是错误的。余数系统作为一类 Reed-Solomon(RS)码，同样具有最小距离的定义：$d_{\min} = r + 1$(r 为冗余校验位的个数)。这意味着，一个有 r 个冗余校验基的 RRNS 至多可以检测出 r 个错误和纠正$[r/2]$个错误。

2.3 数学推证

一般地，每个余数向量代表一个剩余类，即集合 $\left\{ t\prod_{i=1}^{k} m_i + r \mid t,\ r \in N;\ r < \prod_{i=1}^{k} m_i \right\}$ 内的所有整数。但在 RNS 中，限定余数向量一一对应于模 M_k 的简系；任意选取一组余数基，如果这组基的乘积大于整数 X，则 X 可由在这组基意义下的余数向量唯一表示。因此，整数 X 在不同余数基的组合下可能对应不同的余数向量。下面从有限环上剩余类的角度给出本文算法的必要定理与证明。设 X 为原始余数向量 $\boldsymbol{\Phi} = (a_1, a_2, \cdots, a_n)$ 对应的正确数据，X' 为由接收向量 $\boldsymbol{\Phi}' = (b_1, b_2, \cdots, b_n)$ 还原的数据。

定理 1(溢出判定定理) 接收向量 $\boldsymbol{\Phi}'$ 中任一 $(l+t)$ 维分量子集 $\boldsymbol{\Phi}'_{l+t}$，其中 $l (l \geq k)$ 个分量 $\{a_{c_1}, a_{c_2}, \cdots, a_{c_l}\}$ 正确，$t (t \geq 1)$ 个分量 $\{a_{c_{l+1}}, a_{c_{l+2}}, \cdots, a_{c_{l+t}}\}$ 错误，则 $\boldsymbol{\Phi}'_{l+t}$ 还原出的数 $Y \notin [0, M_k)$。

证明

$$X \equiv Y \equiv a_{c_i} \bmod m_{c_i} (1 \leq i \leq l) \tag{2}$$

由基的互素性，Y 满足 $Y \equiv X \left(\bmod \prod_{i=1}^{l} m_{c_i} \right)$，其中 m_{c_i} 是正确分量对应的基。由 $t \geq 1$，则存在 j，基 m_j 对应分量错误，故 $X \neq Y$。这意味着

$$Y = X + h\prod_{i=1}^{l} m_{c_i} (h \geq 1) \tag{3}$$

故

$$Y - X \geq \prod_{i=1}^{l} m_{c_i} \geq \prod_{i=1}^{k} m_i = M_k \tag{4}$$

证毕

定理 1 为检错算法提供了依据，基于定理 1，可以构建定理 2 和定理 3。首先定义合成运算：任取两组余数基 $Q1$ 和 $Q2$, X 在 $Q1$ 和 $Q2$ 下对应的两个余数向量分别为 $\boldsymbol{\Phi}_1$ 和 $\boldsymbol{\Phi}_2$，记 $\boldsymbol{\Phi}_3 = \boldsymbol{\Phi}_1 * \boldsymbol{\Phi}_2$ 为 X 在余数基 $Q = Q1 \cup Q2$ 下的余数向量，$*$ 即为合成运算。

定理 2(不重复判定定理)：设接收向量 $\boldsymbol{\Phi}'$ 中有 s 个错误分量 $(1 \leq s \leq [r/2])$，则 $\boldsymbol{\Phi}'$ 中任意含有错误分量的 $(k+s-1)$ 维余数子向量 $\boldsymbol{\Phi}'_i (i = 1,2,\cdots,C_n^{k+s-1})$ 所还原出的数据若属于 $[0, M_k)$，则必定两两不同。

证明 反证之，若存在两个不同子向量 $\boldsymbol{\Phi}'_1 = (a_{u_1}, a_{u_2}, \cdots, a_{u_{k+s-1}})$ 和 $\boldsymbol{\Phi}'_2 = (a_{v_1}, a_{v_2}, \cdots, a_{v_{k+s-1}})$ 分别还原出的数 X_1 和 X_2 相同且均属于 $[0, M_k)$。记 $X_1 = X_2 = A$，则 A 对应余数向量为 $\boldsymbol{\Phi}'_A = \boldsymbol{\Phi}'_1 * \boldsymbol{\Phi}'_2$。又设 $\boldsymbol{\Phi}'_A$ 中正确的分量个数为 w，而 $\boldsymbol{\Phi}'_1$ 和 $\boldsymbol{\Phi}'_2$ 中至少有一个分量不同，因此

$$w \geq k + s - 1 - s + 1 = k \tag{5}$$

根据定理 1 有 $A \geq M_k$，而由假定 $A < M_k$，矛盾。因此 $X_1 \neq X_2$。 证毕

根据定理 2，接收向量分量中若有两个不同 $(k+s-1)$ 维子集对应相同的数值，则此值必为正确数值。

定义一个余数向量中非零分量的总数为此向量的重量。还原 RRNS(n,k)中所有向量重量不超过$[r/2]$的非零 n 维余数向量，记录其对应的整数于集合 U，则共有 $C_n^{[r/2]}$ 种基的组合方式。每种组合方式里，不妨记选中的基为 $\{m_{d_1}, m_{d_2}, \cdots, m_{d_{[r/2]}}\}$，令其余基对应分量均为 0，$m_{d_i} (i = 1,2,\cdots,[r/2])$ 对应分量任意取值，则一共可产生 $\prod_{i=1}^{[r/2]} m_{d_i} - 1$ 个非零 n 维余数向量。U 中元素个数记为$|U|$。当所有基之间相对差距较小时，可得到如式(6)$|U|$的估计式：

$$|U| = \left\lfloor C_n^{[r/2]} M^{[r/2]/n} \right\rfloor \tag{6}$$

下面举一例来说明 U 中元素的选取。

例 1 设定 RRNS(4,2) 中的信息基为{2,3} 而冗余基为{5,7}，则所有 U 中所包含的数值及其对应的表征向量为：105 ← (1,0,0,0)；70 ← (0,1,0,0)；140 ← (0,2,0,0)；126 ← (0,0,1,0)；42 ← (0,0,2,0)；168 ← (0,0,3,0)；84 ← (0,0,4,0)；120 ← (0,0,0,1)；30 ← (0,0,0,2)；150 ← (0,0,0,3)；60 ← (0,0,0,4)；

$180 \leftarrow (0,0,0,5)$; $90 \leftarrow (0,0,0,6)$。此时$|U|$=13。

定理 3(唯一性区间搜索定理)　设接收到的余数向量$\boldsymbol{\Phi}'$中有 s 个错误分量$(1 \le s \le [r/2])$，则存在唯一元素 F 属于 U 满足：

$$X' - M_k < F \le X' \tag{7}$$

证明　原向量$\boldsymbol{\Phi} = (a_1, a_2, \cdots, a_n)$，接收向量为$\boldsymbol{\Phi}' = (b_1, b_2, \cdots, b_n)$。设误差值$e = X' - X$，$e$ 对应表征向量为

$$\boldsymbol{\Phi}_{\boldsymbol{e}} = (b_1 - a_1, b_2 - a_2, \cdots, b_n - a_n) = (0, \cdots, 0, e_{d_1}, 0, \cdots, 0, e_{d_2}, 0, \cdots, 0, e_{d_s}, 0, \cdots, 0)(1 \le s \le [r/2]) \tag{8}$$

即$\boldsymbol{\Phi}_{\boldsymbol{e}}$在基$\{m_{d_1}, \cdots, m_{d_t}\}$下对应有非零分量。现在证明$e = F$。显然 e 满足$0 \le X' - e < M_k$。若还存在$e' \ne e$满足$0 \le X' - e' < M_k$。设e'对应的向量为

$$\boldsymbol{\Phi}_{e'} = (0, \cdots, 0, v_{f_1}, 0, \cdots, 0, v_{f_2}, 0, \cdots, 0, v_{f_t}, 0, \cdots, 0) \quad (1 \le t \le [r/2]) \tag{9}$$

且存在 i,j 满足$d_i \ne f_j (1 \le i \le s, 1 \le j \le t)$。考虑到$X' - e'$的表示向量$\boldsymbol{\Omega}$=$(b_1, \cdots, b_{f_1} - v_{f_1}, \cdots, b_{f_2} - v_{f_2}, \cdots, b_{f_s} - v_{f_s}, \cdots, b_n)$至少含有一个错误分量，且正确分量个数不少于

$$n - 2[r/2] \ge k \tag{10}$$

根据定理 1，$X' - e' \ge M_k$，与$0 \le X' - e' < M_k$的假设矛盾。　　证毕

3　算法描述

3.1 检错算法

根据定理 1，在 n 元接收向量$\boldsymbol{\Phi}'$错误分量个数不多于 r 的前提下，利用 CRT 还原出来的数据如果在动态范围内，则数据无错；若不然，则说明原余数向量中存在错误分量。

3.2 对 $s(1 \le s \le [r/2])$个错误情形的纠错方法

3.2.1 基替换单错误纠错算法步骤　对于存在一个错误的情形，纠错算法如下：

步骤 1　利用 CRT，还原出接收到的 n 元余数向量$\boldsymbol{\Phi}'$对应数X'；

步骤 2　取出 k+1 个基的乘积记为V_1；

步骤 3　用V_1模X'得到余数R_i：当R_i在动态范围内时，则该数即为所求；如果R_i超过动态范围，则说明剩余的$r-1$个基对应的分量是正确的，因此我们将这$r-1$个基合并成一个替换基记为$\Delta_1 = \{m_{c_1}, m_{c_2}, \cdots, m_{c_{r-1}}\}$；

步骤 4　从步骤 2 中的 k+1 个基中任意剔除$r-1$个基，再将替换基$\Delta_1 = \{m_{c_1}, m_{c_2}, \cdots, m_{c_{r-1}}\}$与剩下的$k-r+2$个基合并成一个新的 k+1 元基的组合，其乘积记为V_2，再用V_2模X'，得到余数R_2：若在动态范围内，该数为所求；若不然，则表明步骤 2 中从k+1 个基中剔除的$r-1$个基的对应分量是正确的，因此又将此$r-1$个基加入替换基$\Delta_2 = \{m_{c_1}, m_{c_2}, \cdots, m_{c_{r-1}}, m_{c_r}, m_{c_{r+1}}, \cdots, m_{c_{2r-2}}\}$。以此类推，则至多重复$[k/r-1]+2$次即可完成纠错过程。

例 2　在 RRNS 中，信息基为{2,3,5}，校验基为{7,11}。X=13，其对应的余数表示向量为$\boldsymbol{\Phi} = (1,1,3,6,2)$。假设基 3 对应的分量发生错误，接收向量$\boldsymbol{\Phi}' = (1,0,3,6,2)$，根据 CRT 还原出$X'$=783。任意选取 4 个基{2,3,5,7}计算其乘积为：210。X'=783 模 210 得余数 153，超过动态范围，说明{2,3,5,7}中存在基对应错误分量，而基 11 对应的分量是正确的。从{2,3,5,7}中选取一个基 2 用基 11 替换，得到一组新的 4 个基的组合{11,3,5,7}，其乘积为 1155。用X'=783 模 1155，得到余数 783 超过动态范围，说明上一次选择的 4 个基中仍有基对应错误分量，于是再从中选取一个未作过替换基的元素 3 用 2 替换，又得到一组新的 4 个基的组合{2,5,7,11}，其乘积为 770，用X'=783 模 770 得到余数 13，在动态范围内，停止纠错过程，输出正确的数据为 13。

3.2.2 不重复检测多错误纠错算法步骤　一般地，基于定理 2，对错误分量个数为 s 的情况，纠错算法如下：

步骤 1　利用 CRT，还原出接收到的 n 元余数向量$\boldsymbol{\Phi}'$对应数X'；

步骤 2　任取$k+s-1$个基的乘积记为$S_i (i = 1, 2, \cdots, C_{k+r}^{k+s-1})$；

步骤 3　记$T_i = < X' >_{S_i}$，如果T_i超出动态范围则舍去，如果未超出，则进行记录；

步骤 4　数据验证：若存在 i<j，使得$T_i = T_j$，则$T_i = T_j = X$，输出 X 作为恢复数据，停止；若不存在，则重新进入步骤 2。

下面举一个纠正一个错误的例子。

例 3　在选择{2,3,5,11,13}作为基的 RRNS 中，{2,3,5}为信息基，{11,13}作为冗余校验基。X=23，对应的余数表征向量为$\boldsymbol{\Phi} = (1,2,3,1,10)$。假定基 11 对应的元素出现错误，得到错误的接收向量$\boldsymbol{\Phi}' = (1,2,3,0,10)$，根据 CRT 还原出$X' = 803$。{2,3,5,11,13}中 3 个基的乘积分别为：30,66,78,110,130,165,195,715。X'模这些乘积分别得到以下余数：23,14,23,33,23,143,23,88。当 23 出现两次时即可停止纠错过程，输出正确数据：23。

3.2.3 未知错误个数情况下的多错误搜索纠正算法

基于定理 3，算法如下：

步骤 1　利用 CRT，还原出接收到的 n 元余数向量$\boldsymbol{\Phi}'$对应数X'；

步骤 2　计算$S = X' - M_k$；

步骤 3　若可以在 U 中找到唯一属于$(S, X']$的

错误差值 F，进入步骤 4。如果不存在 F，则接收向量存在多于$\lfloor r/2 \rfloor$个错误，报错；

步骤 4　$X = X' - F$，输出 X。

在步骤 3 检索数据的过程中，采用二分法进行数据检索，那么至多进行$\lceil \log_2 \| U \| \rceil + 2$次检索，即可确定是否存在对应误差值。

4　算法性能分析

4.1 单错误纠错算法性能分析

文献[7]首先恢复信息基分量集合所对应的数，然后判断错误分量对应基是在信息基中还是在冗余校验基中，之后利用不同的冗余校验基进行 CRT 还原，找到错误元素纠正并恢复达到纠错目标；文献[14]在动态范围内选取常数 m 的所有倍数作为发送数据，因此在该系统中没有冗余基，之后通过误差范围的检验确定错误位，并进行数据还原。以下给出单错误纠错算法的性能比较，如表 1 所示。从表 1 中可以看出，本文算法在复杂度上具有明显优势。

表 1 单错误纠错算法计算复杂度分析

	文献[7]	文献[14]	本文单错误纠错算法
CRT 数据还原次数	2+r	1	1
模运算次数	r+k	3(k+r)	$\left\lceil \frac{k+1}{r-1} \right\rceil$+2
大小比较次数	$r + k \times C_r^2$	3(k+r)	$\left\lceil \frac{k+1}{r-1} \right\rceil$+2
计算复杂度	2+3r+k+$k \times C_r^2$	1+6(k+r)	$2\left\lceil \frac{k+1}{r-1} \right\rceil$+5

4.2 唯一性判断纠错算法性能分析

下面给出唯一性判断纠正算法在 RRNS(n,k)中纠正一个错误的情况下算法的性能分析，唯一判断纠错算法更有利于在基较多的情况下应用，记$\alpha = C_n^k, \beta = C_{n-1}^{k-1}$，则运算次数的期望为

$$E = (\alpha - \beta)(\alpha - \beta - 1)\sum_{i=1}^{\beta} \frac{C_{i+1}^1 \prod_{j=0}^{i-1} \beta - j}{\prod_{j=0}^{i+1} \alpha - j} \tag{11}$$

算法复杂度为$C_{n-1}^{k-1} + 2$，因此对于较大 n 的 RRNS，本文提出的唯一判断纠错算法具有较大优势。

4.3 多错误搜索纠正算法性能分析

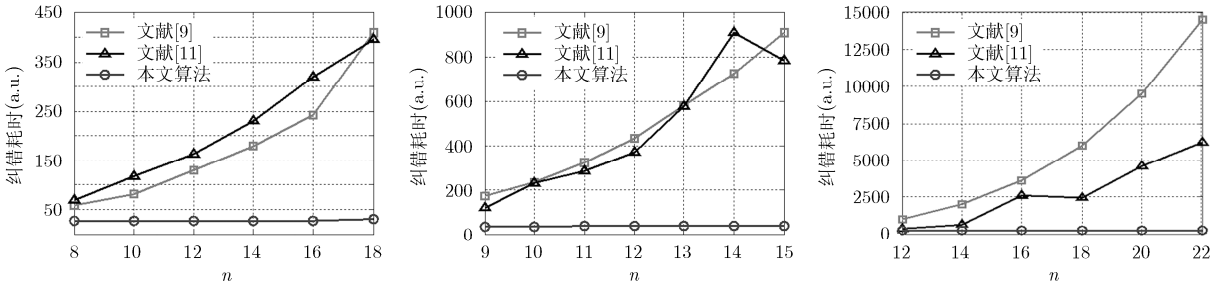
文献[9,11]中提出的算法是目前最主要的两种适用于一般情形下的多错误纠错算法。文献[9]利用欧几里德方法和连分数理论判断接收向量中所选择的分量子集是否全为正确分量。其实质上可以通过模运算实现，如文献[11]中所示：第 1 步首先验证接收向量中所有 $n-1$ 维分量的组合对应的数据是否出错，若有错则进行第 2 步：检验所有 $n-2$ 维分量的组合对应的数据是否出错。以此类推，直到找出一个完全由正确分量组成的子集；若验证完所有 $n-[r/2]$个分量的组合发现均有错，则说明错误分量多于[r/2]个，超出系统纠错范围。文献[12]在其基础上引入了最大似然码理论，在分量组合的选取上取得了明显优化：首先，假设存在 t 个错误，并通过实验找到 f 个 k 维分量组合$\{U_1, U_2, \cdots, U_f\}$，其分别对应的 r 维补集，记为$\{U_1', U_2', \cdots, U_f'\}$，满足接收向量中任意 t 维分量子集 V，均存在 i, $1 \le i \le f$ 使得$V \subseteq U_i'$。f即为满足上述要求的最小整数。因此 f 是与 n, k, t 相关的实验数据，并且显然有$f \ge [C_n^t / C_r^t]$。之后逐次恢复U_i并进行码距判定直至找到完全由正确分量构成的组合。但码距判断会引入新的模运算与比较运算量。因此，大数取模运算将成为上述算法的瓶颈之一。

现阶段取模运算通常利用试减算法实现，一般地，在二进制表示下，设被模数是位长为 p 的整数 A，模数是位长为 q 的整数 B，则模运算通过迭代地将 B 进行移位，并用 A 不断试减 B 的倍数，直至结果属于[0,B]，得到余数。因此 A 模 B 所需减法运算的时间复杂度为$O(p-q)$，比较运算的时间复杂度为$O(p-q)$。

而本文提出的搜索纠错算法基于定理 3，采用二分法搜索，仅通过比较算子实现，不仅避免了复杂的模运算，提高了系统整体吞吐率而且复杂度为对数级，远低于文献[9,11]所需的运算次数。因此在最开始即可只付出极小代价而直接达到纠错系统的最大纠错能力。具体计算复杂度如表 2 所示，从表 2 中看出，本文算法在复杂度上远低于文献[9,11]的多项式级。为了进一步分析本文算法的性能，本文分别对 r=4, 6 和 8，即分别具有 2, 3, 4 个错误纠错能力的余数系统的纠错性能进行实验。对 r=4, RRNS(n,$n-4$)，设定$M = 2^{10n}$，计算复杂度对比如图 1(a)所示；对$r = 6$,RRNS(n,$n-6$)，设定$M = 2^{11n}$，计算复杂度对比如图 1(b)所示；对 r=8, RRNS(n,$n-8$)，设定$M = 2^{12n}$，计算复杂度对比如图 1(c)所示。从图 1 中可以看出本文算法复杂度

表 2 搜索算法与传统算法计算复杂度对比

	文献[9]	文献[11]	本文搜索纠错算法
模运算次数	C_n^{n-t}	$f(r+1)$	0
比较运算次数	C_n^{n-t}	$f(r+2)$	$\lceil \log_2 \| U \| \rceil$+2
加减运算次数	0	0	2
计算复杂度	$2\,C_n^{n-t}$	$f(2r+3)$	$\lceil \log_2 \| U \| \rceil$+4



(a)搜索算法RRNS(n,n–4)计算复杂度对比　(b)搜索算法RRNS(n,n–6)计算复杂度对比　(c)搜索算法RRNS(n,n–8)计算复杂度对比

图 1 与传统算法计算复杂度对比

不仅明显小于文献[9,11]中的算法，并且随着 n 的增大而优势更加显著。

5 结束语

本文基于中国剩余定理和有限环上剩余类的观点提出了溢出判定定理，不重复判断定理和唯一性区间搜索定理，构建了 3 种适用于不同情况的易于硬件实现的低复杂度纠错算法，解决了传统算法中反复利用 CRT 进行数据还原而引入大量复杂的乘，加算子的问题。其中多错误搜索纠错算法仅依靠比较算子和二分法搜索实现，避免了复杂的大数取模运算，将计算复杂度由传统算法的多项式级降低为对数级，且通过实验证明只需付出极小代价即可达到算法环境下的最大纠错能力，纠错性能远高于传统算法。

参 考 文 献

[1] Madhukumar A S, Chin F, and Premkumar A B. Incremental redundancy and link adaptation in wireless local area networks using residue number systems[J]. *Wireless Personal Communication*, 2003, 55(27): 321–336.

[2] Pham Duc-Minh, Premkumar A B, and Madhukumar A S. Error detection and correction in communication channels using inverse gray RSNS Codes[J]. *IEEE Transactions on Communications*, 2011, 59(4): 975–986.

[3] Yang L L and Hanzo L. A residue number system based parallel communication scheme using orthogonal signaling-part I: system outline[J]. *IEEE Transactions on Vehicular Technology*, 2002, 51(6): 1534–1546.

[4] Yang L L and Hanzo L. A residue number system based parallel communication scheme using orthogonal signaling-part II: multipath fading channels[J]. *IEEE Transactions on Vehicular Technology*, 2002, 51(6): 1547–1559.

[5] Keller T, Liew T H, and Hanzo L. Adaptive redundant residue number system coded multicarrier modulation[J]. *IEEE Journal on Selected Areas in Communications*, 2000, 18(11): 2292–2301.

[6] Yang Lie-liang and Hanzo L. Redundant residue number system based error correction codes[C]. IEEE 54th Vehicular Technology Conference, Atlantic, USA, 2001, 3: 1472–1476.

[7] Krishna H, Lin K Y, and Sun Jenn-dong. A coding theory approach to error control in redundant residue number systems. I. theory and single error correction[J]. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 1992, 39(1): 8–17.

[8] Sun Jenn-dong and Krishna H. A coding theory approach to error control in redundant residue number systems. II. Multiple error detection and correction[J]. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 1992, 39(1): 18–34.

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

[10] Mandelbaum D M. On a class of arithmetic codes and a decoding algorithm (Corresp.)[J]. *IEEE Transactions on Information Theory*, 1976, 22 (1): 85–88.

[11] Goh V T and Siddiqi M U. Multiple error detection and correction based on redundant residue number systems[J]. *IEEE Transactions on Communications*, 2008, 56(3): 325–330.

[12] Lei Li and Hu-Jian-hao. Joint redundant residue number systems and module isolation for mitigating single event multiple bit upsets in datapath[J]. *IEEE Transactions on Nuclear Science*, 2010, 57(6): 3779–3786.

[13] Lei Li and Hu-Jian-hao. Redundant residue number systems based radiation gardening for datapath[J]. *IEEE Transactions on Nuclear Science*, 2010, 57(4): 2332–2343.

[14] Pontarelli S, Cardarilli G C, Re M, *et al*.. A novel error detection and correction technique for RNS based FIR filters[C]. IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems (DFTVS), Boston, USA, 2008: 436–444.

肖翰珅：　男，1995年生，博士生，研究方向为通信编码理论、数学模型.

胡剑浩：　男，1971 年生，教授，博士生导师，研究方向为余数系统、Internet 无线接入技术、拥塞控制、流量控制.

马　上：　男，1978 年生，副教授，研究方向为 VLSI 设计和无线通信.