中国科学 E 辑：信息科学 2008 年 第 38 卷 第 4 期：647 ~ 656
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE IN CHINA PRESS

一种基为$\{2^n-1, 2^n+1, 2^{2n}+1\}$的余数系统奇偶检测方法及其应用

马上*，胡剑浩，张林，凌翔

电子科技大学通信抗干扰技术国家重点实验室，成都 610054
* E-mail: mashang@uestc.edu.cn

收稿日期: 2006-12-25; 接受日期: 2007-05-11
国家自然科学基金重大项目(批准号: 60496313)资助

摘要 余数系统(RNS)的并行运算特性使之在乘、加运算时模块间无进位传播，具有良好的时延和功耗特性，在乘加密集型的数字信号处理(DSP)系统中得到了广泛关注. 当余数基为奇数时，可用奇偶检测完成余数系统中的大小比较、符号检测和溢出检测. 结合中国剩余定理(CRT)和混合基转换(MRC)提出了余数基为$\{2^n-1, 2^n+1, 2^{2n}+1\}$的一种奇偶检测电路实现方法，并给出相关定理及其证明. 该检测方法由两个模加法器和一个超前进位链构成，减小了电路复杂度. 还给出了基于奇偶检测的 RNS 大小比较、符号检测和溢出检测电路实现方法，做到了电路模块化，从而易于实现基于 RNS 的算术逻辑单元(ALU)和 DSP 系统.

关键词
超大规模集成电路
余数系统
奇偶检测
大小比较
符号检测
溢出检测

随着集成电路工艺的发展及信息处理系统需求的增长, VLSI的集成度越来越高，其面积、功耗和速度之间的矛盾越来越突出. 研究表明，在未来的集成电路设计中，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日益提高的要求 [1]. 并行处理有两个研究领域: 通过增加处理单元的数量并辅以相关调度机制实现高速大容量的计算和处理，这种方法在商用计算机系统中已经取得了巨大成功，但并未改善处理单元的能力、速度和功 耗，仅以规模的代价换取性能的提升，依然会成为复杂系统和高速信号处理系统的瓶颈之一；另一种方法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.

余数系统(residue number system, RNS)是一个古老的数值表征系统, “今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何?”就是它最早的命题，记载于中国南北朝时期的《孙子算经》中，于 12 世纪末流传到欧洲国家，被称为“中国剩余定理”(Chinese

remainder theorem, CRT), 它是一个非权重数值表征系统. 在RNS中, 一个大整数X被划分为几个独立并行运算的小整数, 在乘法和加法运算中, 各并行模块之间无进位传播, 从而减小了芯片关键路径时延, 因此在具有大量乘加运算的DSP系统中得到了广泛应用和研究[2,3]. 以16抽头结合RNS和符号位(sign digit, SD)数值表征方法的FIR数字滤波器为例, 在字长为48 bit和64 bit时"面积×时延×功耗"特性几乎提高了7倍[3]. 同时由于其本身的冗余特性, 使得RNS在通信系统和图像处理中也得到了广泛关注[4,5]. 然而RNS的一些基本问题还未得到较好解 决, 尤其在大小比较、溢出检测、奇偶检测、除法运算以及余数基扩展等方面最为困难, 因此限制了RNS在通用微处理器和DSP系统中的大规模应用.

由于RNS的非权重特性, 当余数基为奇数时它所表示的二进制整数奇偶性不再显而易见, 但此时RNS中的诸多基本问题, 如大小比较、符号检测、溢出检测都可以通过奇偶检测得到解决, 同时奇偶检测也是余数系统除法运算和缩放运算的关键问题之一[6,7]. 文献[6]将CRT展开成权重系统求和再减去一个未知变量的形式, 利用分数CRT(fractional CRT)求展开式中的未知变量的奇偶性, 进而求得RNS的奇偶性. 在实现时采用查找表以避免乘法和除法运算, 为了满足计算的正确性, 每个查找表的位宽均大于RNS所能表示动态范围的位宽. 文献[8]基于Montgomery缩减算法(Montgomery reduction method, MRM)给出了余数基为$\{2^r-(2^{l_1}\pm1), 2^r-(2^{l_2}\pm1),\cdots,(2^{l_L}\pm1)\}$的余数系统奇偶检测方法, 该方法在CRT中引入一个缩放因子, 然后将CRT展开成与文献[6]相同的形式, 针对该余数基利用一个Wallace加法树计算未知变量以避免除法运算, 同时在计算过程中也使用了查找表. 文献[6]同文献[8]基本思路是一致的, 不同在于后者使用MRM技术以便于实现动态范围较大的RNS的奇偶检测. 目前, 有关RNS奇偶检测实现基本以此为出发点, 其关键在于求未知变量的奇偶性, 但无论利用查找表还是除法器都会占用较多硬件资源.

本文结合CRT和混合基转换(mixed radix conversion, MRC), 给出了一种余数基为$\{2^n-1, 2^n+1, 2^{2n}+1\}$的RNS奇偶检测算法及必要的定理和证明, 该算法仅需要一个模2^n-1加法器、一个模$2^{2n}-1$加法器及一个超前进位链, 减小了电路复杂度. 同时本文还给出了基于奇偶检测的RNS大小比较、符号检测和溢出检测方法, 同其他方法相比, 不仅减小了电路规模和复杂度, 而且在实现大小比较、溢出检测和符号检测时易于做到电路的通用性, 可简化基于RNS的算术逻辑单元(arithmetic logic unit, ALU)和DSP系统的设计.

1 余数系统基本理论及余数基的选择

1.1 余数系统定义

一个余数系统由一组互质的余数基$\{p_1,p_2,\cdots,p_n\}$定义(n>1, GCD$(p_i,p_j)=1$, $i\neq j$, $i,j=1,2,\cdots,n$), 二进制整数X由它对该余数基的余数向量表示, 记为$RNS\{x_1,x_2,\cdots,x_n\}$, 其中$x_i$为整数$X$模$p_i$的余数, 记为

$$x_i = X \bmod p_i = \langle X \rangle_{p_i}, \quad i=1,2,\cdots,n. \tag{1}$$

它所能表示的整数 X 的动态范围为 $[0,P)$, 其中 $P=p_1\times p_2\times\cdots\times p_n$. 对于有符号数的定义同二进制系统类似, 即 $0\leqslant X\leqslant(P-1)/2$ 时表示正数, $(P-1)/2<X\leqslant P-1$ 时表示负数.

1.2 中国剩余定理

CRT 是 RNS 的基本定理之一, 它在 RNS 的后向转换(residue to binary , R/B)电路、大小比较、溢出检测等方面具有重要作用, $RNS\{x_1,x_2,\cdots,x_n\}$ 表示的整数 X 由(2)式计算:

$$X=RNS\{x_1,x_2,\cdots,x_n\}=\left\langle\sum_{i=0}^{k-1}P_i\left\langle P_i^{-1}\right\rangle_{p_i}x_i\right\rangle_P, \tag{2}$$

其中 $P_i=P/p_i, i=1,2,\cdots,n$, $\left\langle P_i^{-1}\right\rangle_{p_i}$ 称为 P_i 模 p_i 的模倒数, 满足 $\left\langle P_i^{-1}\times P_i\right\rangle_{p_i}=1$.

1.3 混合基转换

任意一个余数基为 $\{p_n,\cdots,p_2,p_1\}$ 的 RNS 同一个混合基系统(mixed radix system, MRS)相对应, 记为 $MRS(z_n,\cdots,z_2,z_1)$, 它是一个权重系统, 其权重分别为 $(p_{k-1}\cdots p_2p_1)\cdots(p_2p_1)(p_1)$ (1), 若 p_i 互质, 则同与之对应的 RNS 具有相同的动态范围, 整数 X 用 MRS 可表示为

$$X=MRS(z_{k-1},\cdots,z_2z_1)=z_{k-1}(p_{k-2}\cdots p_2p_1)+\cdots+z_2(p_1)+z_1. \tag{3}$$

利用 MRS 可将 RNS 转换到权重系统, 因此混合基转换常用于解决 R/B 转换、大小比较等问题中, 但求解 z_i 时是一个严格的迭代过程.

1.4 余数基选择

余数基的形式在很大程度上决定电路的复杂度, 一种常见的三模余数基是 $\{2^n-1,2^n,2^n+1\}$ [9], 该余数基兼顾了R/B转换电路和模加法器的实现, 但不满足余数基为奇数的条件, 因此不能利用RNS的奇偶性解决大小比较、符号检测等问题, 同时在表示有符号整数时, 在后向R/B完成后必须做符号判断及其他额外处理才能同二进制有符号数表示方法相对应. 本文选择形如 $\{2^n-1,2^n+1,2^{2n}+1\}$ 的余数基, 其动态范围为 $2^{4n}-1$. 这种形式的余数基具有以下优点:

- 可直接同用反码表示的有符号数二进制系统相对应, 这使得在完成 R/B 转换后, 不再需要做符号判断及调整;
- 该余数基在实现后向转换电路时无乘法操作, 直接移位连接即可; 实现RNS动态范围扩展时, 具有相同的电路结构 [10];
- 余数基中各分量的形式简单, 目前的研究最成熟, 尤其是对于形如 2^k-1 和 2^k+1 的模加法运算都有优化的实现方法 [11~13].

2 奇偶检测算法及电路设计

奇偶性是整数的基本信息之一, 由于 RNS 的非权重特性, 当余数基的所有元素均为奇数时, 在封闭的 RNS 中很难直接判断它所表示的二进制数的奇偶性. 下面结合 CRT 和 MRC, 给

出了基为 $\{2^n-1, 2^n+1, 2^{2n}+1\}$ 的余数系统的奇偶检测算法及必要的定理和证明.

2.1 有关奇偶检测中的几个定理及证明

定理 1 若余数基为 $\{p_1, p_2\}$, 二进制整数 X 的 RNS 表示为 $RNS\{x_1, x_2\}$, 则 $X = x_1 + \langle k_0(x_2 - x_1)\rangle_{p_2} p_1$, 其中 $k_0 = \langle p_1^{-1}\rangle_{p_2}$.

证明 令对应的混合基系统表示为 $MRS\{z_1, z_2\}$, 则由(3)式可得

$$X = z_1 + z_2 p_1,$$

$$x_1 = \langle X\rangle_{p_1} = \langle z_1 + z_2 p_1\rangle_{p_1} = z_1,$$

$$X - x_1 = RNS\{x_1, x_2\} - RNS\{x_1, \langle x_1\rangle_{p_2}\} = RNS\{0, \langle x_2 - x_1\rangle_{p_2}\}.$$

利用(2)式, 则

$$RNS\{0, \langle x_2 - x_1\rangle_{p_2}\} = \langle p_1 \langle x_2 - x_1\rangle_{p_2} \langle p_1^{-1}\rangle_{p_2}\rangle_{p_1 p_2}.$$

由于 $\langle a p_1\rangle_{p_1 p_2} = \langle a\rangle_{p_2} p_1$, 令 $k_0 = \langle p_1^{-1}\rangle_{p_2}$, 则

$$X = x_1 + \langle k_0(x_2 - x_1)\rangle_{p_2} p_1.$$

证毕.

若余数基为 $\{p_1, p_2, p_3\}$, RNS表示的整数X为 $RNS\{x_1, x_2, x_3\}$, 可认为先由余数基 $\{p_1, p_2\}$ 决定一个在 $[0, p_1 p_2)$ 内的整数 x_{12}, 然后再由 $\{x_{12}, p_3\}$ 决定整数X, 这实质就是CRT-II[14]所阐述的内容, 即

$$X = x_3 + \langle k_1(x_{12} - x_3)\rangle_{p_1 p_2} P_3, \tag{4}$$

其中 $x_{12} = x_1 + \langle k_0(x_2 - x_1)\rangle_{p_2} p_1$, $\langle k_1 p_3\rangle_{p_1 p_2} = 1$.

定理 2 当 $p_1 = 2^n + 1$, $p_2 = 2^n - 1$时, $\langle p_1^{-1}\rangle_{p_2} = \langle p_2^{-1}\rangle_{p_1} = 2^{n-1}$.

证明

$$\langle \langle p_1^{-1}\rangle_{p_2} p_1\rangle_{p_2} = \langle 2^{n-1}(2^n + 1)\rangle_{2^n - 1} = \langle 2^{n-1}(2^n - 1) + 2^n\rangle_{2^n - 1} = 1,$$

$$\langle \langle p_2^{-1}\rangle_{p_1} p_2\rangle_{p_1} = \langle 2^{n-1}(2^n - 1)\rangle_{2^n + 1} = \langle 2^{n-1}(2^n + 1) - 2^n\rangle_{2^n + 1} = 1.$$

定理 3 若 $0 \leqslant a < 2^n - 1$, 其二进制表示为 $a_{n-1}a_{n-2}\cdots a_i a_{i-1}\cdots a_0$, 则 $\langle 2^{n-i} a\rangle_{2^n - 1}$ $(i = 1, 2, \cdots, n-1)$的结果为 $a_{i-1}\cdots a_0 a_{n-1}\cdots a_i$, 即循环右移 i bit.

证明

$$2^{n-i}a=\underbrace{a_{n-1}a_{n-2}\cdots a_i a_{i-1}\cdots a_0}_{n\text{ bit}}\underbrace{00\cdots0}_{n-i\text{ bit}}=\underbrace{a_{n-1}a_{n-2}\cdots a_i}_{n-i\text{ bit}}\underbrace{a_{i-1}\cdots a_0 00\cdots0}_{n\text{ bit}},$$

$$\left\langle 2^{n-i}a\right\rangle_{2^n-1}=\left\langle \underbrace{a_{n-1}a_{n-2}\cdots a_i}_{n-i\text{ bit}}\underbrace{a_{i-1}\cdots a_0 00\cdots0}_{n\text{ bit}}\right\rangle_{2^n-1}=\underbrace{a_{n-1}a_{n-2}\cdots a_i}_{n-i\text{ bit}}+\underbrace{a_{i-1}\cdots a_0 00\cdots0}_{n\text{ bit}}$$
$$=a_{i-1}\cdots a_0 a_{n-1}\cdots a_i.$$

证毕.

2.2 奇偶检测算法

令 $\{p_1,p_2,p_3\}=\{2^n+1,2^n-1,2^{2n}+1\}$, 则 $p_1p_2=2^{2n}-1$, $P=2^{4n}-1$, 由定理 1 和 2 及(4)式可得

$$k_0=2^{n-1},k_1=2^{2n-1}. \tag{5}$$

令 $C=\left\langle x_{12}-x_3\right\rangle_{p_1p_2}$, C 的二进制表示为 $C_{2n-1}\cdots C_1C_0$, 令 $P(X)$ 表示 X 的奇偶性, 则

$$P(X)=P(x_3)\text{xor}P(\left\langle k_1(x_{12}-x_3)\right\rangle_{p_1p_2}\ p_3). \tag{6}$$

因为 p_3 为奇数, 由(4)和(5)式及定理 3 可得

$$P(X)=LSB(x_3)\text{xor}C_1, \tag{7}$$

因此, 求 X 的奇偶性关键在于计算 C 的第 2 个比特值. 由(4)式及定理 1 可得

$$\begin{aligned}C&=\left\langle x_1-x_3+\left\langle k_0(x_2-x_1)\right\rangle_{p_2}\ p_1\right\rangle_{p_1p_2}\\&=\left\langle\left\langle x_1-x_3\right\rangle_{p_1p_2}+\left\langle k_0(x_2-x_1)\right\rangle_{p_2}\ p_1\right\rangle_{p_1p_2}.\end{aligned} \tag{8}$$

令 $A=\left\langle x_1-x_3\right\rangle_{p_1p_2}$, $B=\left\langle k_0(x_2-x_1)\right\rangle_{p_2}\ p_1$, $B'=\left\langle x_2-x_1\right\rangle_{p_2}$, 并考虑到

$$\left\langle k_0(x_2-x_1)\right\rangle_{p_2}<2^n-1,\ p_1=2^n+1,$$

应用定理 2 和 3 可得

$$B=\underbrace{B'_0B'_{n-1}B'_{n-2}\cdots B'_1B'_0B'_{n-1}B'_{n-2}\cdots B'_1}_{2n\text{ bit}}, \tag{9}$$

因此, (8)式无乘法操作, 仅需要模加法器即可实现, 其电路如图 1 所示.

2.3 设计优化

若整数 x 的二进制表示为 $x_{k-1}x_{k-2}\cdots x_0$, 结合文献 [15]的方法, 可以证明 $\left\langle -x\right\rangle_{2^k-1}=\left\langle \overline{x}_{k-1}\overline{x}_{k-2}\cdots\overline{x}_0\right\rangle_{2^k-1}$, $\overline{x}_i\ (i=0,1,\cdots,k-1)$ 表示对 x 按位取反. 考虑到 $x_3=\left\langle X\right\rangle_{2^{2n}+1}$, 它可能为 2^{2n}, 将此特殊情形考虑进去, 则

$$\left\langle -x_3\right\rangle_{2^{2n}-1}=\left\langle \overline{x}_{3,2n-1}\overline{x}_{3,2n-2}\cdots\overline{x_{3,0}\ \text{or}\ x_{3,2n}}\right\rangle_{2^{2n}-1}.$$

由于 $p_1p_2=2^{2n}-1$, $p_2=2^n-1$, 因此图 1 中的模减法器均可用模 2^k-1 形式的模加法器代替

实现, 对于模 2^k-1 加法器实现时较简单 [13].

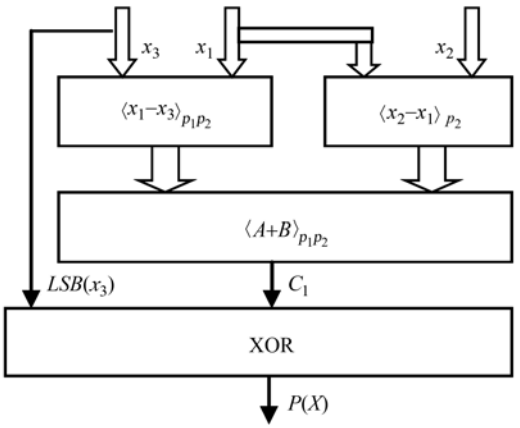

图 1　奇偶检测电路

此外, 图 1 中求 $P(X)$ 时并不需要完整的 C 值, 只需要知道它的第 2 个比特 C_1 的值. 令 $Carr$ 为 $A+B$ 的进位, 由前面的分析知道 C_1 只同 $Carr$, A_1, A_0, B_1 和 B_0 相关,

$$C_1=(A_1\text{xor}B_1)\text{xor}((A_0\text{and}B_0)\text{or}(A_0\text{and}Carr)\text{or}(B_0\text{and}Carr)). \tag{10}$$

由(7)及(10)式可得 X 的奇偶性为

$$P(X)=LSB(x_3)\text{xor}(A_1\text{xor}B_1)\text{xor}((A_0\text{and}B_0)\text{or}(A_0\text{and}Carr)\text{or}(B_0\text{and}Carr)). \tag{11}$$

经以上分析, 可由两个模加法器获得 A_0, A_1, B_0 和 B_1 的值, 而 $Carr$ 可以由一个超前进位链计算得到, 因此图 1 可优化如图 2 所示, 其中 $x'_2=\overline{x}_{2,n-1}\overline{x}_{2,n-2}\cdots\overline{x}_{2,0}$, $x'_3=\overline{x}_{3,2n-1}\overline{x}_{3,2n-2}\cdots\overline{x}_{3,0}$ or $x_{3,2^{2n}}$.

可以看出, 这种方法实现余数基为 $\{2^n-1,2^n+1,2^{2n}+1\}$ 的奇偶检测电路时仅需两个宽度分别为 n 和 $2n$ bit 的模加法器, 一个 $2n$ bit 的超前进位链及少量的组合逻辑. 同时, 两个模加法器具有模 2^k-1 的形式, 简化了电路复杂度.

2.4　性能分析

文献 [6]利用分数CRT实现RNS的奇偶检测具有一定的通用性, 但需要较多的查找表来代替除法运算, 在RNS的动态范围很大时难于硬件实现. 若实现 $\{2^n-1,2^n+1,2^{2n}+1\}$ 的奇偶检测, 分数CRT需要 $(4n+2)\cdot(\log_2 nP+2)$ bit的存储器和两个宽度为 $\log_2 nP$ 的加法器. 文献 [8]的基本思路同分数CRT是一致的, 但针对特殊的余数基利用MRM引入一个缩减因子来优化大动态范围下的奇偶检测运算, 使得所需要的存储器深度较小, 但需要更多的逻辑实现奇偶检测, 若不仔细选择余数基和缩减因子, 还需要模乘法运算 [8]. 本文提出的方法同利用分数CRT实现的方法所占用硬件资源的比较如表 1 所示, 可见本文的方法仅利用模加法器和超前进位链即可实现RNS的奇偶检测, 避免了使用查找表和除法操作. 同时, 本文提出的方法对三模余数系统及

三模以上的余数系统的奇偶检测具有一定的通用性, 针对具体的余数基形式可以根据(4)式及本文推导 $\{2^n-1, 2^n+1, 2^{2n}+1\}$ 奇偶性类似的过程加以优化, 需要注意的是, 当余数基个数增加时将会增加相应的处理延迟.

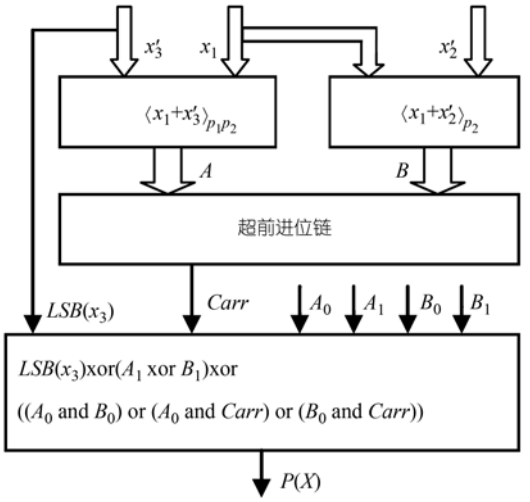

图 2 优化后的奇偶检测电路

表 1 实现余数基为$\{2^n-1, 2^n+1, 2^{2n}+1\}$奇偶检测的资源占用比较

硬件资源	本文的方法	分数CRT[6]
ROM	无	$(4n+2)\cdot(\log_2 nP+2)$
加法器	2 个($2n$ bit 模加法器)	2 个($\log_2 nP$ bit)
超前进位链	1 个($2n$ bit)	无

3 奇偶检测的应用

在RNS中, 大小比较、符号检测和溢出检测最为困难, 学者们针对这些问题做了广泛研究, 但基本都是在一定程度上将RNS转换到权重系统来获得必要的权重信息. 在大小比较中, 商和技术(sum of quotients techniques, SQT)利用MRC获得整数X在RNS所定义的n维空间中的权重标号作为大小判断的依据(即对角函数), 但余数基是冗余的, Dimauro等人对SQT进行了改进, 消除了SQT所引人的冗余动态范围[16]; 文献[17]提出了基于CRT-II的方法进行大小比较, 减小了模操作, 但需要比较电路. 对于符号检测, 文献[18]给出了一种便于符号检测的余数基选择方法, 但要求其中一个余数基为 2; 文献[19]介绍了一种利用核函数进行符号检测和实现RNS后向转换电路的方法, 这种方法关键在于提取合适的核函数. 对于RNS运算溢出的处理, 第 1 种方法是在运算过程中进行缩放, 以保证运算不溢出, 文献[17]介绍了一种基于核函数的方法, 而文献[20]给出了一种实现 2^n缩放的方法, 在实现 2^n缩放时奇偶检测是其核 心; 另一种是检测运算过程中是否产生溢出, 文献[21]通过引入一个索引参数的方法判断RNS加法运算是否

溢出, 但计算索引值时较困难; 文献 [22]则给出了基于查找表实现RNS的溢出检测的方法.

在大小比较、符号检测及溢出检测中, 以上的方法针对具体应用做了适当优化, 在特定余数基形式下解决某个问题时具有较好的性能, 但若要在通用微处理器中完成这些基本的算术运算, 则需要针对每个问题设计专门的优化电路, 将会增加电路复杂度、芯片面积和功耗, 难于做到基于 RNS 的 ALU 的通用实现及在 DSP 系统中的大规模应用. 当余数基为奇数时, RNS 的大小比较、符号检测及溢出检测等问题都可用 RNS 的奇偶检测电路来解决, 因此易于实现通用的 RNS 算术逻辑单元和通用化的 DSP 模块.

若 P 为奇数, 两个整数进行加法或减法时的运算溢出会违背奇偶运算规则(例如运算溢出时: 奇数减奇数为奇数, 奇数减偶数为偶数, 偶数减偶数为奇数, 偶数减奇数为偶数). 利用这一特性可实现 RNS 的大小比较、符号检测及溢出检测. 当 P 为偶数时, 则 p_i 中至少一个为偶数, 此时整数 $\{x_1,x_2,\cdots,x_n\}$ 的奇偶性显而易见, 但运算溢出时仍满足奇偶变化规则, 不再满足以上规则.

3.1 基于奇偶检测的大小比较方法

对于无符号整数的大小比较, 可按以下步骤进行:

1) 检测 x 和 y 的奇偶性, 计算 $z=\langle x-y\rangle_P$;

2) 检测 z 的奇偶性;

3) 若 z 的奇偶性满足奇偶变化规则, 则 x 大于 y, 否则 x 小于 y.

若进行有符号数的大小比较, 则在奇偶检测前将 RNS 所表示的数环作 $(P-1)/2$ 的旋转, 即 x 和 y 分别加上 $(P-1)/2$ 后再进行以上步骤.

3.2 符号检测

1) 检测 x 的奇偶性, 计算 $y=\langle x+(P-1)/2\rangle_P$;

2) 检测 y 的奇偶性;

3) 若 y 的奇偶性满足奇偶变化规则, 则 x 为正数, 否则为负数.

3.3 加法运算的溢出检测

根据溢出的定义, 当两个同号的有符号数 x 和 y 相加结果的符号发生变化时, 表明运算溢出. 利用 3.2 节的符号检测方法, 溢出检测的步骤如下:

1) 判断 x 和 y 的符号, 计算 $z=\langle x+y\rangle_P$;

2) 判断 z 的符号;

3) 根据 x, y, z 的符号判断是否产生溢出.

具体应用中, 若在 RNS 前向转换时从二进制系统中提取出奇偶信息, 并在 RNS 的 ALU 寄存器中用一个比特来存储, 则可减小基于奇偶检测的 RNS 大小比较、符号检测和溢出检测电路的规模.

4 结论

本文首先结合 CRT 和 MRC, 给出了一种余数基为 $\{2^n-1, 2^n+1, 2^{2n}+1\}$ 的 RNS 奇偶检测电路实现方法, 并给出了必要的定理及其证明, 同利用分数 CRT 实现相同余数基的奇偶检测相比, 电路复杂度大大减小. 其次, 针对目前 RNS 的大小比较、符号检测和溢出检测较难做到电路模块化的问题, 本文给出了基于奇偶检测的 RNS 大小比较、符号检测和溢出检测算法, 将 RNS 中的 3 个基本问题(大小比较、符号检测和溢出检测)的解决建立在奇偶检测之上, 无需针对每一问题设计专门电路, 简化了 RNS 算术逻辑单元及 DSP 系统的设计, 便于电路的模块化实现.

参考文献

1 Dally W J, Lacy S. VLSI Architecture: past, present, and future. In: Proceedings of the 20th Anniversary Conference on Advanced Research in VLSI. Atlanta: IEEE Press, 1999. 232—241

2 Liu Y, Lai E M-K. Design and implementation of an RNS-based 2-D DWT processor. IEEE Trans on Consum Electr, 2004, 50(1): 376—385 [DOI]

3 Lindahl A, Bengtsson L. A low-power FIR filter using combined residue and radix-2 signed-digit representation. In: Proceedings of the 8th Euromicro Conference on Digital System Design. New York: IEEE Press, 2005. 42—47

4 Yang L L, Hanzo L. A residue number system based parallel communication scheme using orthogonal signaling: part I—system outline. IEEE Trans Veh Technol, 2002, 51(6): 1534—1546 [DOI]

5 Wang W, Swamy M N S, Ahamad M O. RNS application for digital image processing. In: Proceedings of the 4th IEEE International Workshop on System-on-Chip for Real-Time Applications. New York: IEEE Press, 2004. 77—80

6 Lu M, Chiang J S. A novel division algorithm for the residue number system. IEEE Trans Comput, 1992, 41(8): 1026—1032 [DOI]

7 Burgess N. Scaling an RNS number using the core function. In: Proceedings of the 16th IEEE Symposium on Computer Arithmetic. New York: IEEE Press, 2003. 262—269

8 Suk J-H, Youn J-S, Kim H-G, et al. A parity checker for a large residue numbers based montgomery reduction method. IEICE Transactions on Electronics, 2005 E88-C(9): 1880—1885 [DOI]

9 Wang W, Swamy M N S, Omair Ahmad M, et al. A study of the residue-to-binary converters for the three-moduli sets. IEEE Trans Circuits Syst I-Regul Pap, 2003, 50(2): 235—243 [DOI]

10 Wang W, Swamy M N S, Ahmad M O, et al. A parallel residue-to-binary converter for the moduli set $\{2^m-1, 2^{2^0 m}+1, 2^{2^1 m}+1, \cdots, 2^{2^k m}+1\}$. VLSI Des, 2002, 2(14): 183—191

11 Efstathiou C. Fast parallel-prefix modulo 2^n+1 adders. IEEE Trans Comput, 2004, 53(9): 1211—1216 [DOI]

12 Patel R A, Benaissa M, Powell N, et al. ELMMA: a new low power high-speed adder for RNS. SIPS 2004: 95—100

13 Wang Y K. New Chinese remainder theorems. In: Proceedings of the 32nd Asilomar Conference on Signals, Systems and Computers, vol 1. Pacific Grove: IEEE Press, 1998. 165—171

14 Wang W, Swamy M N S, Ahmad M O, et al. A high-speed residue-to-binary converter for three-moduli $(2^k, 2^k-1, 2^{k-1}-1)$ RNS and a scheme for its VLSI implementation. IEEE Trans Circuits Syst II- Express Briefs, 2000, 47(12): 1576—1581 [DOI]

15 Hiasat A A. High-speed and reduced-area modular adder structures for RNS. IEEE Trans Comput, 2002, 51(1): 84—89 [DOI]

16 Dimauro G, Impedovo S, Pirlo G. A new technique for fast number comparison in the residue number system. IEEE Trans Comput, 1993, 42(5): 608—612 [DOI]
17 Wang Y K. A new algorithm for RNS magnitude comparison based on new Chinese remainder theorem II. In: Proceedings of the 9th Great Lakes Symposium on VLSI. New York: IEEE Press, 1999. 362—365
18 Setiaarif E, Siy P. A new moduli set selection technique to improve sign detection and number comparison in residue number system (RNS). In: NAFIPS 2005—2005 Annual Meeting of the North American Fuzzy Information Processing Society. 766—768
19 Abtahi M, Siy P. The non-linear characteristic of core function of RNS numbers and its effect on RNS to binary conversion and sign detection algorithms. In: NAFIPS 2005—2005 Annual Meeting of the North American Fuzzy Information Processing Society. 731—736
20 Cardarilli G C, Nannarelli A, Re M. Programmable power-of-two RNS scaler and its application to a QRNS polyphase filter. In: Proceedings of 2005 IEEE International Symposium on Circuits and Systems (ISCAS). Kobe: IEEE Press, 2005. 1002—1005
21 Rao T R N, Trehan A K. Binary logic for residue arithmetic using magnitude index. IEEE Trans Comput, 1970, C19(8): 752—757
22 Sasaki A. The basis for implementation of additive operations in the residue number system. IEEE Trans Comput, 1968, C-17(11): 1066—1073