中国科学: 信息科学 2016 年 第 46 卷 第 6 期: 800–810
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
论 文

一种余数基性能评估及多通道余数基构建方法

马上*, 汪陈浩, 胡剑浩, 姚毅

电子科技大学通信抗干扰技术国家级重点实验室, 成都 611731
* 通信作者. E-mail: mashang@uestc.edu.cn

收稿日期: 2015–09–07; 接受日期: 2016–01–28; 网络出版日期: 2016–05–26
国家自然科学基金 (批准号: 61571083) 和中央高校基本业务费 (批准号: ZYGX2014J009) 资助项目

摘要 余数系统由于其优良的并行计算特性, 在乘加密集型的数字信号处理系统中得到了深入研究和关注. 余数基的选择和构建是余数系统应用中的核心问题之一, 它是 VLSI 实现复杂度的关键因素. 目前的研究已经提出了多种具体的余数基形式, 但构建方法种类繁多, 且在构建过程中具有较大的随意性. 传统的评估方法均为面向特定应用的电路实现进行评估, 忽略了余数基形式带来的内在影响. 本文从余数基的基本运算单元、动态范围利用率、通道间平衡性、余数基并行度这 4 个方面对余数基实现性能进行抽象, 同具体的电路实现性能评估一起作为描述余数系统性能的参数, 以避免通常的 VLSI 实现性能评估只能针对具体实现结构和电路的弊端, 为余数基的构建提供建议. 基于此, 本文通过引入一个新的余数基分量, 提出了一种多通道余数基构建方法, 所构建的余数基具有良好的动态范围利用率、平衡性和并行度.

关键词 余数系统 性能评估 动态范围利用率 平衡度 并行度

1 引言

余数系统 (residue number system, RNS) 是一个古老的数字表征系统, 最早记载于中国南北朝时期的《孙子算经》中, “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, 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). RNS 是一个非权重数值表征系统, 在 RNS 中一个大整数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. 它最早被应用于密码系统中, 后来由于其乘加运算的无进位传播、并行计算等特性, 在乘加密集型的数字信号处理系统中得到了广泛关注和研究 [1,2].

在基于 RNS 的应用中, 余数基的具体形式是决定其实现复杂度的主要因素. 这是由于在余数系统中基本运算单元 —— 模加法和模乘法运算的复杂度与余数基的具体形式密切相关. 此外, 其他运算, 如前后向转换、数值缩放及符号检测等的复杂度均依赖于余数基的形式. 目前, 已经提出了多种余数基. 例如, 文献 [3] 给出了 4 种三通道余数基的性能分析, 它们分别是 $\{2^n-1, 2^n, 2^n+1\}$, $\{2n-1, 2n, 2n+1\}$, $\{2^n-1, 2^n, 2^{n-1}-1\}$, $\{2^n-1, 2^n+1, 2^{2n}+1\}$. 文献 [4,5] 则分别提出了具有 $\{2^{n+1}-1, 2^n, 2^n-1\}$ 和 $\{2^{kn}-1, 2^n-1, 2^n+1\}$ 形式的三通道余数基. 对于四通道及以上的余数基, 大

引用格式: 马上, 汪陈浩, 胡剑浩, 等. 一种余数基性能评估及多通道余数基构建方法. 中国科学: 信息科学, 2016, 46: 800–810, doi: 10.1360/N112014-00217

多利用 $\{2^n\}$, $\{2^n-1\}$ 和 $\{2^n+1\}$ 分量来构建. 文献 [6,7] 分别提出了基为 $\{2^n-1, 2^n, 2^n+1, 2^{2n}+1\}$ 和 $\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$ 的四通道余数基, 文献 [8] 给出了形如 $\{2^n-1, 2^n, 2^n+1, 2^{n+1}+1\}$ 和 $\{2^n-1, 2^n, 2^n+1, 2^{n-1}+1\}$ 的余数基. 而文献 [9] 提出了形如 $\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1, 2^{n-1}-1\}$ 的五通道余数基, 文献 [10] 则给出了具有 $\{2^m-1, 2^{2^0 m}+1, 2^{2^1 m}+1, \ldots, 2^{2^k m}+1\}$ 形式的多通道余数基.

可见, 在余数基构建中绝大多数研究均选择 $\{2^n\}$ 和 $\{2^n \pm 1\}$ 作为余数基分量, 这主要是由于目前的 VLSI 实现基础为二进制逻辑, 这可以充分利用其模运算低复杂度的特性. 同时, 这些余数基的构建通常考虑的是模加法运算和 R/B (residue to binary) 转换的实现复杂度. 由于余数基构建的随意性, 如何选择高效的余数基是实际应用中的一个重要问题, 因此需要对余数基的性能进行评估. 通常, 对于 VLSI 电路的面积、时延和功耗性能的评估采用单位门模型或者直接利用 VLSI 设计工具进行评估和分析. 基于单位门模型的分析方法是电路设计研究中常用的分析方法之一, 虽然所得到的性能参数的精准性不及直接 VLSI 实现, 但由于单位门模型是在 RTL 级别对复杂度和性能进行分析评估, 因此易于实现具有通用逻辑结构的 VLSI 电路的性能分析, 并可消除具体实现和优化技术差异对分析所得到的性能参数的影响, 可对算法或电路实现结果作出趋势性的评估. 然而, 这两种评估方法均只能针对具体的电路和 VLSI 实现进行性能评估, 不能揭示余数基本身所带来的内在影响. 因此, 针对余数系统不仅需要具体电路实现的评估, 而且需要从其他方面来探讨其评估方法, 合理的性能评估方法可以在工程实践中发挥指导作用.

目前已有少量文献针对余数基的构建和性能这一问题进行了探讨. 文献 [3] 对常见的 4 种三通道余数基进行了性能分析, 结果表明形式为 $\{2^n-1, 2^n, 2^n+1\}$ 的余数系统在完成 R/B 转换时具有最优的实现性能. 鉴于目前的余数基分量通常具有 $\{2^n\}$ 和 $\{2^n \pm 1\}$ 的形式, 文献 [11] 针对基于这 3 个分量所构建的余数基进行了性能分析, 并给出了在不同动态范围下选择构造这类余数基的基本指导意见. 其分析结果表明, 当动态范围小于 22 bit 时, $\{2^n-1, 2^n, 2^n+1\}$ 具有最优的 R/B 性能, 而动态范围大于 22 bit 时, $\{2^{n_1}, 2^{n_1}\pm 1, 2^{n_2}\pm 1, \ldots, 2^{n_l}\pm 1\}$ 具有最优的性能. 然而, 基于余数系统的实现在不同的应用场合下对各种运算具有不同的侧重点, 仅基于 R/B 转换进行性能分析是不全面, 也是不公平的.

在 RNS 构建中, 其基本要求为在一定的动态范围条件下各余数基分量互质, 其次则应首先考虑模加法器的实现复杂度, 这是因为模加法器是构成 RNS 其他运算模块的基本单元且实现复杂度与余数基形式密切相关. 另一方面, 为了充分发挥 RNS 的并行特性, 在大动态范围时应降低各通道的位宽 (即增加余数通道个数), 并应尽量保持各通道间复杂度的平衡性 (即各通道位宽应大致相同) 以避免因某一通道的处理位宽过大而成为整个系统的处理瓶颈. 此外, 由于需满足互质的基本要求, 使得基于二进制逻辑的余数系统 VLSI 实现不能完全利用其动态范围, 这要求 RNS 在特定二进制位宽占用下所能表示的动态范围应尽可能大. 简言之, 在构建余数基时应主要考虑以下几个因素:

- 各余数基分量互质;
- RNS 动态范围及其利用率;
- 模加法器实现复杂度;
- RNS 并行特性;
- 通道间复杂度的平衡性.

根据已有的研究情况来看, 目前还没有一种余数基能很好地兼顾以上问题, 这使得如何衡量和评价这些余数基的性能显得尤为重要. 本文提出了衡量余数基通道间平衡性和并行性的定义方法, 并从 RNS 动态范围利用率、并行度、通道间平衡性和模加法器实现复杂度的角度分析了常见余数基的性

能, 为余数基的选择提供一种可供参考的依据.

此外, 由于目前的余数基分量大多以 $\{2^n\}$ 和 $\{2^n \pm 1\}$ 为余数基分量, 为了满足基分量之间的互质要求, 很难构建多通道余数系统. 针对这一问题, 本文通过引入一个新的余数基分量 $\{2^n - 2^k - 1\}$, 并提出了一种具有优良平衡性、高效模加法器实现、高态范围利用率及高并行度的余数基构建方法, 其基本形式为 $\{2^n, 2^n - 1, 2^n - 2^1 - 1, \ldots, 2^n - 2^k - 1, \ldots, 2^n - 2^{n-2} - 1\}$ $(1 \leqslant k \leqslant n-2)$, 它可以轻易地构建六通道以上的余数系统. 针对新引入的余数基分量, 文献 [12] 给出了其基本运算单元 —— 模加法器的实现方法, 从而为这一类余数基的应用奠定基础.

2 基本运算单元复杂度

与普通二进制系统加法运算不同在于, 模加法运算无最终进位输出. 对于两个整数 A, B $(A, B \in [0, m))$ 进行模加法运算定义为

$$C = \langle A + B \rangle_m = \begin{cases} A + B, & A + B < m, \\ A + B - m, & A + B \geqslant m. \end{cases} \tag{1}$$

即 A 和 B 的和若小于 m 则直接取其和作为模加法运算结果, 否则减去 m 作为模加法运算的最终结果. 在基于二进制的实现中, 模加法的等价的运算如下:

$$C = \langle A + B \rangle_m = \begin{cases} A + B, & A + B + T < 2^n, \\ \langle A + B + T \rangle_{2^n}, & A + B + T \geqslant 2^n, \end{cases} \tag{2}$$

其中, $T = 2^n - m$, n 为模加法器的位宽, $n = \lceil \log_2 m \rceil$. 上式表明, 若 $A + B + T$ 的进位输出为 “1”, 则模加法的结果为 $A + B + T$ 的低 n bit, 反之则为 $A + B$, 这是目前绝大多数模加法器设计所遵循的基本原则.

早期的模加法器设计要么利用一个普通二进制加法器进行两次加法运算或者采用两个普通二进制加法器并行进行计算来实现 [13,14], 但它们的时延或面积通常都为对应位宽二进制加法器的两倍以上. 因此, 后来的研究多基于普通二进制加法器的并行前缀结构 [12,15,16], 这种设计方法结合 $A+B+T$ 的特点和普通二进制加法器的前缀运算结构, 可以做到较好的面积和时延性能. 另外一类设计方法则针对具体的模加法形式进行优化设计, 例如研究最多的模 $2^n - 1$ 加法器和模 $2^n + 1$ 加法器.

对于模 2^n 加法器, 实际上就是无进位的普通二进制加法器, 其实现复杂度被认为与普通二进制加法器相同.

针对模 $2^n - 1$ 加法器, 最常用的方法为端回进位方式, 其实现结构为将两个加数的结果再加上它们的进位输出作为最后的模运算结果. 具体实现中, 仅需要增加一级普通二进制加法器所采用的并行前缀结构 [16,17]. 因此, 模 $2^n - 1$ 加法器具有与普通二进制加法器最接近的实现性能.

对于模 $2^n + 1$ 加法器, 一种是消 “1” 法表示并使用端回进位加法器实现 [18,19], 另一种是进位保留加法器并使用端回进位加法器实现 [20,21]. 消 “1” 法将加数作减 “1” 表示, 然后可以得到与模 $2^n - 1$ 加法器类似的表达式, 从而可以利用端回进位方式来实现, 但这种方法需要将加数和计算结果与普通二进制之间进行转换, 即需要额外的加 1 和减 1 操作. 第 2 种方法利用进位保留的方式对加数进行预处理, 然后根据进位决定是否再进行最后一级的类似模 $2^n - 1$ 加法器的前缀运算. 显然, 这两种方法均需要进行额外的前后级处理, 因此其实现性能较模 $2^n - 1$ 加法器复杂, 一般认为其复杂度约为模 $2^n - 1$ 加法器的 1.5 倍.

表 1 常见三通道余数基动态范围利用率

Table 1 The DUR performance of common used 3-channel moduli sets

Moduli sets	n=4	n=8	n=16	n=24	n=32
$R_1=\{2^n-1,2^n,2^n+1\}$	0.9226	0.9600	0.9796	0.9863	0.9897
$R_2=\{2n-1,2n,2n+1\}$	0.8977	0.9226	0.9374	0.9308	0.9473
$R_3=\{2^n-1,2^n+1,2^{2n}+1\}$	0.8889	0.9412	0.9697	0.9796	0.9846
$R_4=\{2^{n-1}-1,2^n-1,2^n\}$	0.9740	0.9993	1.000	1.000	1.000
$R_5=\{2^n-1,2^n,2^{2n+1}+1\}$	0.9394	0.9704	0.9848	0.9898	0.9923
$R_6=\{2^n,2^{2n}-1,2^{2n}+1\}$	0.9479	0.9755	0.9877	0.9917	0.9938

对于非 2^n-1 和非 2^n+1 的模加法器的研究, 通常伴随着余数基的选择出现. 例如, Patel 等在文献 [22] 中提出了一种基于进位修正的模 $2^n-\left(2^{n-2}+1\right)$ 加法器实现结构, 在其进位计算模块中仅计算 $A+B+T$ 的进位信息, 但其实现复杂度较模 2^n+1 加法器高.

总之, 结合我们在文献 [12] 中的研究, 模 2^n 模加法器无疑具有最低复杂度, 其次是模 2^n-1 模加法器, 模 2^n+1 模加法器在三者中具有最高复杂度. 其他形式的模加法器复杂度通常较这 3 种模加法器高, 模 $2^n-\left(2^{n-2}+1\right)$ 加法器的复杂度则低于模 2^n-2^k-1 加法器的复杂度.

3 动态范围利用率

由于余数基分量互质条件的限制, 在二进制逻辑表达下余数系统占用位宽与动态范围的不匹配, 产生了动态范围利用率问题. 令余数基为 $\{m_1,m_2,\ldots,m_L\}$, 则其动态范围为 $D_{\rm RNS}=\prod_{i=1}^{L}m_i$, 占用的二进制位宽为 $W=\sum_{i=1}^{L}\lceil\log_2 m_i\rceil$. 其中, $\lceil x\rceil$ 表示大于 x 的最小整数.

余数系统动态范围利用率指余数系统实际所能表示的动态范围的位宽与表示其各通道数字所占用的二进制总位宽之间的比值, 即

$$\mathrm{DUR}_W=\frac{\log_2 D_{\rm RNS}}{W}=\frac{\log_2\prod_{i=1}^{L}m_i}{\sum_{i=1}^{L}\lceil\log_2 m_i\rceil}=\frac{\sum_{i=1}^{L}\log_2 m_i}{\sum_{i=1}^{L}\lceil\log_2 m_i\rceil}. \tag{3}$$

根据该定义, 在构建余数基时, 总是期望余数基的动态范围接近其所占用的二进制位宽所能表示的动态范围, 最大的动态范围利用率为 1. 常见三通道、四通道和五通道余数基的动态范围利用率计算结果如表 1∼3 所示. 我们在构建余数基时需要考虑到该参数的大小, 较低的动态范围利用率则意味着更多的硬件资源浪费. 例如, 表 1 中的余数基 R_1, 实际所能表示的整数动态范围约为其所占用位宽所能表示动态范围的一半.

4 平衡性

为了不因某个计算通道复杂度过高而成为整个系统的瓶颈, 在构建余数基时总是期望各个余数通道具有相近的复杂度. 例如, 文献 [10] 虽然给出了一种多通道余数基构建方法, 但是该方法所构建的余数基各通道位宽相差很大, 因此实用性较低. 余数系统通道间平衡性包括两个方面, 时延的平衡性和面积的平衡性. 对于余数系统的各个并行运算通道, 其基本运算单元均为模加法和模乘法, 而模加法和模乘法运算的时延通常与运算位宽呈对数关系, 因此位宽 (或复杂度) 可以代表通道间的平衡性.

表 2　常见四通道余数基动态范围利用率

Table 2　The DUR performance of common used 4-channel moduli sets

Moduli sets	n=4	n=8	n=16	n=24	n=32
$R_7=\{2^n-1,2^n,2^n+1,2^{n+1}-1\}$	0.9416	0.9705	0.9848	0.9898	0.9923
$R_8=\{2^n-1,2^n,2^n+1,2^{n-1}-1\}$	0.9251	0.9684	0.9844	0.9896	0.9922
$R_9=\{2^n-1,2^n,2^n+1,2^{n-1}+1\}$	0.8920	0.9397	0.9692	0.9794	0.9845
$R_{10}=\{2^n-1,2^n,2^n+1,2^{2n}+1\}$	0.9091	0.9524	0.9756	0.9836	0.9877
$R_{11}=\{2^n-1,2^n,2^n+1,2^{2n+1}-1\}$	0.9542	0.9762	0.9878	0.9918	0.9938
$R_{12}=\{2^n-1,2^{2n},2^n+1,2^{2n+1}-1\}$	0.9612	0.9800	0.9898	0.9932	0.9948
$R_{13}=\{2^n-1,2^n+1,2^{2n}-2,2^{2n+1}-3\}$	0.9606	0.9800	0.9898	0.9932	0.9948

表 3　常见五通道余数基动态范围利用率

Table 3　The DUR performance of common used 5-channel moduli sets

Moduli sets	n=4	n=8	n=16	n=24	n=32
$R_{14}=\left\{\begin{matrix}2^n-1,2^n,2^n+1,\\2^{n-1}-1,2^{n+1}+1\end{matrix}\right\}$	0.9021	0.9522	0.9756	0.9836	0.9877
$R_{15}=\left\{\begin{matrix}2^n,2^{n/2}-1,2^{n/2}+1,\\2^n+1,2^{2n-1}-1\end{matrix}\right\}$	0.8938	0.9459	0.9726	0.9817	0.9862
$R_{16}=\left\{\begin{matrix}2^n-1,2^n,2^n+1,\\2^n-2^{(n+1)/2}+1,\\2^n+2^{(n+1)/2}+1\end{matrix}\right\}$	0.9091	0.9524	0.9756	0.9836	0.9877

这里首先给出余数系统的平均位宽的定义, 令 L 和 W 分别表示余数通道的个数和总位宽, $\overline{W}$ 表示余数系统的平均位宽, 则

$$\overline{W}=\frac{W}{L}=\frac{\sum_{i=1}^{L}\lceil\log_2 m_i\rceil}{L}. \tag{4}$$

每个余数基分量与平均位宽偏离之和的平均比率为

$$Bq'=\frac{\sum_{i=1}^{L}\left|\left(\lceil\log_2 m_i\rceil-\overline{W}\right)/\overline{W}\right|}{L}. \tag{5}$$

从上式可以看出, 若 Bq' 的值越大则偏离程度越大, 即余数系统通道间平衡性越差. 为了直观描述该参数与系统平衡性的关系 (即平衡性的计算值越大说明平衡性越好), 我们将余数系统的平衡度定义如下:

$$BQ=\frac{1}{Bq'+1}=\frac{1}{\frac{\sum_{i=1}^{L}\left|\left(\lceil\log_2 m_i\rceil-\overline{W}\right)/\overline{W}\right|}{L}+1}=\frac{L\overline{W}}{\sum_{i=1}^{L}\left|\lceil\log_2 m_i\rceil-\overline{W}\right|+L\overline{W}}. \tag{6}$$

因此, 本文所提出的余数基平衡性定义了各个通道与平均位宽的平均偏离程度, 该定义方式使得余数系统的平衡度最大值为 1, 且 BQ 越大则余数系统通道间平衡性越好. 利用余数系统平衡度的定义可以对常用余数基进行其平衡性的分析, 由此可以估计出其通道间的平衡性能, 如表 4~6 所示.

5　并行度

由于并行度与系统的实际实现有较为密切的联系, 例如系统需要频繁地进行缩放、符号检测等需

表 4 常见三通道余数基平衡性

Table 4 The BQ performance of common used 3-channel moduli sets

Moduli sets	n=4	n=8	n=16	n=24	n=32
$R_1=\{2^n-1,2^n,2^n+1\}$	0.9070	0.9494	0.9735	0.9821	0.9864
$R_2=\{2n-1,2n,2n+1\}$	0.8824	0.9070	0.9231	1.000	0.9344
$R_3=\{2^n-1,2^n+1,2^{2n}+1\}$	0.7500	0.7500	0.7500	0.7500	0.7500
$R_4=\{2^{n-1}-1,2^n-1,2^n\}$	0.8919	0.9452	0.9724	0.9816	0.9862
$R_5=\{2^n-1,2^n,2^{2n+1}+1\}$	0.6923	0.7183	0.7333	0.7387	0.7414
$R_6=\{2^n,2^{2n}-1,2^{2n}+1\}$	0.7778	0.7834	0.7864	0.7874	0.7879

表 5 常见四通道余数基平衡性

Table 5 The BQ performance of common used 4-channel moduli sets

Moduli sets	n=4	n=8	n=16	n=24	n=32
$R_7=\{2^n-1,2^n,2^n+1,2^{n+1}-1\}$	0.9000	0.9444	0.9706	0.9800	0.9848
$R_8=\{2^n-1,2^n,2^n+1,2^{n-1}-1\}$	0.8889	0.9412	0.9697	0.9796	0.9846
$R_9=\{2^n-1,2^n,2^n+1,2^{n-1}+1\}$	0.9189	0.9596	0.9774	0.9848	0.9885
$R_{10}=\{2^n-1,2^n,2^n+1,2^{2n}+1\}$	0.7586	0.7636	0.7664	0.7673	0.7678
$R_{11}=\{2^n-1,2^n,2^n+1,2^{2n+1}-1\}$	0.7586	0.7636	0.7664	0.7673	0.7678
$R_{12}=\{2^n-1,2^{2n},2^n+1,2^{2n+1}-1\}$	0.7647	0.7576	0.7538	0.7526	0.7519
$R_{13}=\{2^n-1,2^n+1,2^{2n}-2,2^{2n+1}-3\}$	0.7647	0.7576	0.7538	0.7526	0.7519

表 6 常见五通道余数基平衡性

Table 6 The BQ performance of common used 5-channel moduli sets

Moduli sets	n=4	n=8	n=16	n=24	n=32
$R_{14}=\left\{\begin{array}{l}2^n-1,2^n,2^n+1,\\2^{n-1}-1,2^{n+1}+1\end{array}\right\}$	0.8333	0.9052	0.9491	0.9652	0.9736
$R_{15}=\left\{\begin{array}{l}2^n,2^{n/2}-1,2^{n/2}+1,\\2^n+1,2^{2n-1}-1\end{array}\right\}$	0.6835	0.6679	0.6600	0.6574	0.6561
$R_{16}=\left\{\begin{array}{l}2^n-1,2^n,2^n+1,\\2^n-2^{(n+1)/2}+1,\\2^n+2^{(n+1)/2}+1\end{array}\right\}$	0.9016	0.9459	0.9716	0.9807	0.9854

要提取权重信息的操作时, 通道数需要尽量减小, 反之则要增加通道数. 因此, 本文不考虑具体系统实现, 而直接从余数基的形式抽象出余数基的并行度.

当动态范围位宽 W 一定时, 要平均位宽 $\overline{W}$ 与通道数 L 同时到达最优值, 则只需在 $\overline{W}\cdot L=W$ 条件下, 求出让 $\overline{W}+L$ 有最小值的 $\overline{W}$ 和 L. 由于 $\overline{W}=W/L$, 令 $f(L)=\overline{W}+L=W/L+L$, 两边求导求其极值有 $f'(L)=-W/L^2+1=0$, 解之有, 当 $L=\overline{W}=\sqrt{W}$ 时, $f(L)$ 有最小值.

据此, 可以对余数系统并行度有如下定义: 余数系统并行度指余数系统余数基通道个数与位宽之和同其最优通道个数与位宽之和的比值:

$$PD=\frac{2\sqrt{W}}{L+\overline{W}}. \tag{7}$$

表 7　常见三通道余数基并行度

Table 7　The PD performance of common used 3-channel moduli sets

Moduli sets	n=4	n=8	n=16	n=24	n=32
$R_1=\{2^n-1,2^n,2^n+1\}$	0.9833	0.8824	0.7241	0.6252	0.5575
$R_2=\{2n-1,2n,2n+1\}$	0.9986	0.9833	0.9600	0.9428	0.9340
$R_3=\{2^n-1,2^n+1,2^{2n}+1\}$	0.9428	0.8136	0.6499	0.5551	0.4922
$R_4=\{2^{n-1}-1,2^n-1,2^n\}$	0.9950	0.8992	0.7345	0.6320	0.5623
$R_5=\{2^n-1,2^n,2^{2n+1}+1\}$	0.9428	0.8136	0.6499	0.5551	0.4922
$R_6=\{2^n,2^{2n}-1,2^{2n}+1\}$	0.9165	0.7684	0.6000	0.5077	0.4478

表 8　常见四通道余数基并行度

Table 8　The PD performance of common used 4-channel moduli sets

Moduli sets	n=4	n=8	n=16	n=24	n=32
$R_7=\{2^n-1,2^n,2^n+1,2^{n+1}-1\}$	0.9983	0.9330	0.7926	0.6947	0.6248
$R_8=\{2^n-1,2^n,2^n+1,2^{n-1}-1\}$	1.0000	0.9428	0.8000	0.6999	0.6285
$R_9=\{2^n-1,2^n,2^n+1,2^{n-1}+1\}$	0.9995	0.9379	0.7963	0.6973	0.6266
$R_{10}=\{2^n-1,2^n,2^n+1,2^{2n}+1\}$	0.9875	0.8939	0.7392	0.6403	0.5720
$R_{11}=\{2^n-1,2^n,2^n+1,2^{2n+1}-1\}$	0.9875	0.8939	0.7392	0.6403	0.5720
$R_{12}=\{2^n-1,2^{2n},2^n+1,2^{2n+1}-1\}$	0.9712	0.8571	0.6947	0.5967	0.5306
$R_{13}=\{2^n-1,2^n+1,2^{2n}-2,2^{2n+1}-3\}$	0.9712	0.8571	0.6947	0.5967	0.5306

表 9　常见五通道余数基并行度

Table 9　The PD performance of common used 5-channel moduli sets

Moduli sets	n=4	n=8	n=16	n=24	n=32
$R_{14}=\left\{\begin{array}{l}2^n-1,2^n,2^n+1,\\2^{n-1}-1,2^{n+1}+1\end{array}\right\}$	0.9980	0.9673	0.8463	0.7514	0.6806
$R_{15}=\left\{\begin{array}{l}2^n,2^{n/2}-1,2^{n/2}+1,\\2^n+1,2^{2n-1}-1\end{array}\right\}$	0.9907	0.9811	0.8718	0.7791	0.7083
$R_{16}=\left\{\begin{array}{l}2^n-1,2^n,2^n+1,\\2^n-2^{(n+1)/2}+1,\\2^n+2^{(n+1)/2}+1\end{array}\right\}$	0.9980	0.9673	0.8463	0.7514	0.6806

在该定义下, 并行度的最大值为 1, 且并行度越大, 则余数系统具有更好的并行性能. 利用余数系统并行度的定义可以对常用余数基进行分析, 由此可以估计出其并行性能, 也可利用已经进行 VLSI 实现的余数基的实际性能对并行度的定义进行验证.

6　一种多通道余数基构建方法

余数基构建中, 首先应该满足各余数基分量互质. 为了减少各运算通道基本计算单元 —— 模加法器的实现复杂度, 2^n 和 $2^n\pm1$ 形式的余数基在余数基构建中得到了广泛应用. 但这类形式的基分量在构建多通道余数系统时很难满足互质的基本要求, 目前基于这 3 个分量很难构成五通道以上的余数基, 这

表 10 本文方法所构建的余数基性能对比分析

Table 10 The DUR, PD and BQ performance of the proposed multi-channel moduli set

Channel number	Ref.	Moduli sets	DUR	PD	BQ
3	Proposed	$\{2^3, 2^3-1, 2^3-2^1-1\}$	0.9033	1.0000	1.0000
	R_2	$\{2\times3-1, 2\times3, 2\times3+1\}$	0.8571	1.0000	1.0000
	Ref. [10]	$\{2^2-1, 2^2+1, 2^4+1\}$	0.7994	0.9986	0.7500
4	Proposed	$\{2^4, 2^4-1, 2^4-2^1-1, 2^4-2^2-1\}$	0.9417	1.0000	1.0000
	R_7	$\{2^4-1, 2^4, 2^4+1, 2^5-1\}$	0.9416	0.9983	0.9000
	Ref. [10]	$\{2^2-1, 2^2+1, 2^4+1, 2^8+1\}$	0.8421	0.9963	0.6786
5	Proposed	$\{2^5, 2^5-1, 2^5-2^1-1, 2^5-2^2-1, 2^5-2^3-1\}$	0.9636	1.0000	1.0000
	R_{16}	$\{2^5-1, 2^5, 2^5+1, 2^5-2^3+1, 2^5+2^3+1\}$	0.9259	0.9993	0.9184
	Ref. [10]	$\{2^2-1, 2^2+1, 2^4+1, 2^8+1, 2^{16}+1\}$	0.8889	0.9836	0.6081
6	Proposed	$\left\{\begin{array}{l} 2^6, 2^6-1, 2^6-2^1-1, \\ 2^6-2^2-1, 2^6-2^3-1, 2^6-2^4-1 \end{array}\right\}$	0.9757	1.0000	1.0000
	Ref. [10]	$\{2^2-1, 2^2+1, 2^4+1, 2^8+1, 2^{16}+1, 2^{32}+1\}$	0.9275	0.9493	0.5610
8	Proposed	$\left\{\begin{array}{l} 2^8, 2^8-1, 2^8-2^1-1, 2^8-2^2-1, \\ 2^8-2^3-1, 2^8-2^4-1, 2^8-2^5-1, 2^8-2^6-1 \end{array}\right\}$	0.9871	1.0000	1.0000
	Ref. [10]	$\{2^2-1, 2^2+1, 2^4+1, 2^8+1, 2^{16}+1, 2^{32}+1, 2^{128}+1\}$	0.9624	0.8871	0.5299

在大动态范围应用场合将限制 RNS 的应用. 文献 [10] 给出的 $\{2^n-1, 2^{2^0 n}+1, 2^{2^1 n}+1, \ldots, 2^{2^k n}+1\}$ 形式的多通道余数基较好地利用了模 $2^n\pm1$ 加法器的优点. 然而, 每增加一个余数基的位宽均为其他余数基位宽之和, 从而使该余数基各通道间极不平衡. 因此, 有必要探索构建具有较好性能的多通道余数基构建方法.

针对余数基的并行度、平衡性、动态范围利用率等问题, 这里除使用具有高效基本运算单元性能的 2^n 和 2^n-1 分量外, 再引入一个具有通用表达形式的基分量, 其形式为 2^n-2^k-1 $(1\leqslant k\leqslant n-2)$, 通过 n 和 k 的不同组合来构建多通道余数基, 所构建的余数基基本形式为 $\{2^n, 2^n-1, 2^n-2^1-1, \ldots, 2^n-2^k-1, \ldots, 2^n-1-2^{n-2}\}$. 基于 MATLAB 的验证结果表明当 $n=2,3,4,5,6,8$ 时各种 k 值下该余数基均满足 RNS 的互质要求, 而当 $n=7,9$ 时去掉少量的基即可满足互质要求. 由于每个通道的位宽均为 n bit, 因此具有良好的通道间平衡特性. 令余数基通道个数为 L, 由于该余数基具有 $\{2^n, 2^n-1, 2^n-2^1-1, \ldots, 2^n-2^k-1, \ldots, 2^n-1-2^{n-2}\}$ 的形式, 必然有 $L\leqslant n$. 换言之, 它构建的余数基最大通道个数同各通道的位宽相同. 由并行度的定义可知, 当 L 与平均位宽相近时 RNS 具有较好的并行度.

另一方面, 若应用中所需要的通道数 $L<n$, 则可利用基本形式中任意 L 个分量来构建所需的余数基. 此外, 还可以将平均位宽较低的余数基加以选择构成平均位宽较低的多通道余数基, 例如可以由三通道和四通道余数基构成五通道余数基 $\{7,5,16,13,11\}$. 总之, 这种形式的余数基的构建非常灵活, 但它们只有 2^n, 2^n-1 或 2^n-2^k-1 三种形式的基分量, 其中模 2^n 和模 2^n-1 加法器是目前具有最高设计效率的模加法器, 而我们所提出的模 2^n-2^k-1 加法器, 也具有优化的统一实现结构和设计方法 [12].

根据表 1~9 中对常见不同通道数的余数基的动态范围利用率、通道间平衡度和并行度的分析结果, 本文从 $R_1\sim R_{16}$ 中选择出具有最大 DUR, PD 和 BQ 乘积的余数基, 然后同本文所提出的多通道

余数基基本形式进行对比分析, 结果如表 10 所示, 表 10 中还包含了文献 [10] 所提出的多通道余数基性能分析. 可见, 仅利用 2^n 和 $2^n \pm 1$ 分量很难构造五通道以上的余数基, 文献 [10] 所提出的多通道余数基构建方法虽然理论上可以构建多通道余数基, 但在六通道时最大运算位宽已经达到了 32 bit, 而且每增加一个通道, 新的余数基位宽将翻一倍, 在构建多通道余数基时不具有实用性. 而本文所提出的多通道余数基构建方法无论通道个数多少其动态范围利用率、并行度和平衡度都较其他余数基的性能更好.

7 结论

由于余数基的具体形式是决定其 VLSI 实现的关键因素, 而目前的余数基构建通常只考虑某方面的实现性能且种类繁多, 构建具有一定的随意性, 同时仅针对具体应用和电路实现进行性能评估, 未进一步揭示余数基本身所带来的性能内在影响. 本文避免了具体应用场合、实现手段等因素的影响, 从余数基的形式抽象出基本运算单元实现复杂度、动态范围利用率、平衡性和并行度这几个参数进一步对余数系统的性能进行评估分析, 连同通常使用的面向特定电路实现的评估方法为工程实践提供参考依据, 特别是为余数基的构建提供指导性意见. 基于此, 本文通过引入一个新的余数基分量并提出了一种新的多通道余数基构建方法, 所构建的多通道余数基具有优良的性能.

参考文献

1 Chang C H, Molahosseini A S, Zarandi A A E, et al. Residue number systems: a new paradigm to datapath optimization for low-power and high-performance digital signal processing applications. IEEE Circ Syst Mag, 2015, 15: 26–44

2 Wang W, Li X, Wang W, et al. Maximum likelihood estimation based robust Chinese remainder theorem for real numbers and its fast algorithm. IEEE Trans Signal Process, 2015, 63: 3317–3331

3 Wang W, Swamy M N S, Ahmad M O, et al. A comprehensive study of three moduli sets for residue arithmetic. In: Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering, Edmonton, 1999, 1: 513–518

4 Mohan P V A. RNS-to-binary converter for a new three-moduli set $\{2^{n+1}-1, 2^n, 2^n-1\}$. IEEE Trans Circ Syst II: Express Briefs, 2007, 54: 775–779

5 Wey C L, Lin S Y. VLSI implementation of residue-to-binary converters for digital signal processing. In: Proceedings of IEEE International Conference on Electro/Information Technology, Chicago, 2007. 536–541

6 Cao B, Chang C H, Srikanthan T. An efficient reverse converter for the 4-moduli set $\{2^n-1, 2^n, 2^n+1, 2^{2n}+1\}$ based on the new Chinese remainder theorem. IEEE Trans Circuits Syst I: Fundamental Theory Appl, 2003, 50: 1296–1303

7 Sheu M H, Lin S H, Chen C Y, et al. An efficient VLSI design for a residue to binary converter for general balance moduli $(2^n-3, 2^n-1, 2^n+1, 2^n+3)$. IEEE Trans Circ Syst II: Express Briefs, 2004, 51: 152–155

8 Cao B, Srikanthan T, Chang C H. Efficient reverse converters for four-moduli sets $\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1\}$ and $\{2^n-1, 2^n, 2^n+1, 2^{n-1}-1\}$. IEEE Proc Comput Digital Tech, 2005, 152: 687–696

9 Cao B, Chang C H, Srikanthan T. A residue-to-binary converter for a new five-moduli set. IEEE Trans Circ Syst I: Regular Papers, 2007, 54: 1041–1049

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

11 Wang W, Swamy M N S, Ahmad M O. Moduli selection in RNS for efficient VLSI implementation. In: Proceedings of the International Symposium on Circuits and Systems (ISCAS'03), Bangkok, 2003, 4: 512–515

12 Ma S, Hu J H, Wang C H. A novel modulo 2^n-2^k-1 adder for residue number system. IEEE Trans Circ Syst I: Regular Papers, 2013, 60: 2962–2972

13 Piestrak S J. Design of residue generators and multioperand modular adders using carry-save adders. IEEE Trans Comput, 1994, 423: 68–77

14 Dugdale M. VLSI implementation of residue adders based on binary adders. IEEE Trans Circ Syst II: Analog Digital Signal Process, 1992, 39: 325–329
15 Patel R A, Benaissa M, Powel N, et al. ELMMA: a new low power high-speed adder for RNS. In: Proceedings of IEEE Workshop on Signal Processing Systems (SIPS 2004), Austin, 2004. 95–100
16 Patel R A, Boussakta S. Fast parallel-prefix architectures for modulo addition with a single representation of zero. IEEE Trans Comput, 2007, 56: 1484–1492
17 Dimitrakopoulos G, Vergos H T, Nikolos D, et al. A systematic methodology for designing area-time efficient parallel-prefix modulo adders. In: Proceedings of the International Symposium on Circuits and System (ISCAS'03), Bangkok, 2003, 5: 225–228
18 Lin S H, Sheu M H. VLSI design of diminished-one modulo $2^n + 1$ adder using circular carry selection. IEEE Trans Circuits Syst II: Express Briefs, 2008, 55: 897–901
19 Vergos H T, Efstathiou C. A unifying approach for weighted and diminished-1 modulo $2^n + 1$ addition. IEEE Trans Circuits Syst II: Express Briefs, 2008, 55: 1041–1045
20 Efstathiou C, Vergos H T, Nikolos D. Fast parallel-prefix modulo $2^n + 1$ adders. IEEE Trans Comput, 2004, 53: 1211–1216
21 Patel R A, Benaissa M, Boussakta S, et al. Power-delay-area efficient modulo $2^n + 1$ adder architecture for RNS. Electron Lett, 2005, 41: 231–232
22 Patel R A, Benaissa M, Boussakta S. Fast modulo $2^n - \left(2^{n-2} + 1\right)$ addition: a new class of adder for RNS. IEEE Trans Comput, 2007, 56: 572–576

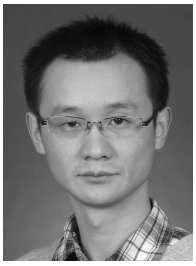
A systemic performance estimation and moduli set selection method for residue number systems

Shang MA*, Chenhao WANG, Jianhao HU & Yi YAO

National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731*, China*
*E-mail: mashang@uestc.edu.cn

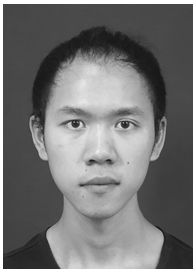
Abstract The residue number system (RNS) has been receiving considerable attention for many decades owing to its inherent carry-free and parallel properties in addition, subtraction, and multiplication operations. In RNS-based systems, the method by which the moduli set is selected and evaluation of its performance are important issues. A systemic performance evaluation method for RNS based on the properties of the moduli set is proposed in this paper. By abstracting the inherent properties of moduli sets, such as the complexity of arithmetic units, utilization ratio of dynamic range, parallelism, and balance between residue channels, information can be provided on moduli set selection and performance estimation before circuit implementation. Furthermore, we also propose a new multi-channel moduli set that utilizes a new radix component in this paper. Performance analysis and comparison results show that the proposed multi-channel moduli set has good systemic performance.

Keywords residue number system, performance estimation, utilization ratio of dynamic range, balance, parallelism



Shang MA was born in 1978. He received a Ph.D. degree from University of Electronic Science and Technology of China (UESTC), Chengdu, China in 2009. From July 2001 to May 2010, he was with Southwest University of Science and Technology, Mianyang, China. Since May 2010, he has been with UESTC. His current research interests include computer arithmetic and baseband processing for communications.

Jianhao HU was born in 1971. He received B.E. and Ph.D. degrees in communication systems from University of Electronic Science and Technology of China (UESTC) in 1993 and 1999, respectively. He was with City University of Hong Kong from 1999 to 2000 as a postdoctoral researcher. From 2000 to 2004, he served as a senior systems engineer at the 3G Research Center, University of Hong Kong. He has been a professor in the National Key Laboratory of Communication, UESTC since 2005. His areas of research include high-speed low-power DSP technology with VLSI, NoC, wireless communications, and software radios.



Chenhao WANG was born in 1989. He received an M.E. degree from University of Electronic Science and Technology of China (UESTC), Chengdu, in 2015. Currently, he is an engineer at Shanghai Fudan Microelectronics Group Company Limited.