

基于余数基 $\{2^n-1, 2^n, 2^n+1\}$ 的高效 RNS 缩放结构

赵英旭, 李 磊

(电子科技大学 电子科学技术研究院, 四川 成都 610054)

摘 要: 针对三模余数基 $\{2^n-1, 2^n, 2^n+1\}$ 提出了一种高效的余数系统(RNS)缩放算法和缩放结构, 本设计运用中国剩余定理(CRT)选择 $2^n(2^n+1)$ 作为缩放因子实现了基于全加器(FA)的缩放结构, 从而使三个余数通道的余数和缩放后的二进制整数相同, 因此可以节约一个面积和延迟都很大的余数到二进制(R/B)转换模块. 在特定条件下本设计会出现缩放误差, 但是这个误差值统一都为 1. 本设计实现了简单高速的特性, 且在很大的动态范围内面积时延(AT)积比目前最简单最快的基于全加器的缩放结构小一倍.

关键词: 余数系统(RNS); 中国剩余定理(CRT); 余数到二进制转换(R/B); 缩放(Scaling)

中图分类号: TN403

文献标识码: A

文章编号: 1000-7180(2014)05-0071-03

An Efficient RNS Saler for $\{2^n-1, 2^n, 2^n+1\}$

ZHAO Ying-xu, LI Lei

(Research Institute of Electronic Science and Technology, UESTC, Chengdu 610054, China)

Abstract: This paper presents an efficient Residue Number System (RNS) scaling algorithm and architecture for the balanced special moduli set $\{2^n-1, 2^n, 2^n+1\}$. Based on Chinese Remainder Theorem (CRT), the scaling constant has been chosen as $2^n(2^n+1)$ such that all residues of the scaled integer are identical and equal to the scaled integer output. This is particularly useful as no expensive and slow residue-to-binary converter is required for interfacing with conventional number system after the digital signal processing and scaling in RNS domain. The scaling error occurs only conditionally and is proven to be at most unity. The proposed architecture can be implemented entirely based on full adders with complexity commensurate with a multi-operand modulo adder. Its area-time complexity is about 2 times smaller than one of the fastest based on full adders scaler architecture for the same moduli set over a wide dynamic range.

Key words: Residue Number System; Chinese Remainder Theorem; R/B; Scaling

1 引言

在超大规模集成电路设计中, 由于余数系统(RNS)的并行和无权重特性, 所以在加法、减法和乘法运算中具有十分良好的面积、功耗和延迟性能. 在余数系统中, 一个整数 X 在特定余数基下被分解成几个较小的数, 从而运算能同时独立地运行且关键路径的延时大大减小, 所以余数系统在乘加运算繁多的数字信号处理(DSP)系统中得到广泛的运用^[1].

在数字信号处理(DSP)系统中, 余数系统(RNS)的动态范围会随着乘加运算的进行而变得

越来越大, 为了避免运算的溢出, 在乘加运算之后必须进行一定的缩放运算. 由于余数系统的无权重特性, 缩放运算不是那么容易实现, 所以在数字信号处理(DSP)系统中缩放运算成为了余数系统中运算的瓶颈^[1].

2 提出的缩放算法

余数系统(RNS)由一组两两互质的余数基 $\{m_1, m_2, \dots, m_n\}$ 定义, 一个二进制数 X 在该余数系统中表示为: $X = \{x_1, x_2, \dots, x_n\}$, 其中 $x_i = X \bmod m_i$, 记为 $x_i = |X|_{m_i}$, $i = 1, 2, \dots, n$. $M = \prod_{i=1}^n m_i$ 称

为该余数系统的动态范围^[2].

基于中国剩余定理(CRT)^[3], X 可以表示为

$$X = \left| \sum_{i=1}^n M_i \mid M_i^{-1} \mid_{m_i} x_i \mid_M \right. \quad (1)$$

式中, $M_i = (M/m_i)$.

由于本文的缩放算法是基于三模余数基 $\{2^n - 1, 2^n, 2^n + 1\}$ 的, 故 $n = 3$ 且式(1) 可变形为

$$X = \left| m_2 m_3 \mid M_1^{-1} \mid_{m_1} x_1 + m_1 m_3 \mid M_2^{-1} \mid_{m_2} x_2 + m_1 m_2 \mid M_3^{-1} \mid_{m_3} x_3 \mid_M \right. \quad (2)$$

运用下面的原理和定理可以得到本文的缩放算法^[4]:

原理 1: $A \mid B \mid_B = \mid AB \mid_{AB}$

$$\begin{aligned} Y &= \left[\frac{X}{k} \right] = \left[\frac{X}{m_2 m_3} \right] \\ &= \left[\frac{\left| m_2 m_3 \mid M_1^{-1} \mid_{m_1} x_1 + m_1 m_3 \mid M_2^{-1} \mid_{m_2} x_2 + m_1 m_2 \mid M_3^{-1} \mid_{m_3} x_3 \mid_M \right.}{m_2 m_3} \right] \\ &= \left[\left| M_1^{-1} \mid_{m_1} x_1 + \frac{m_1}{m_2} \mid M_2^{-1} \mid_{m_2} x_2 + \frac{m_1}{m_3} \mid M_3^{-1} \mid_{m_3} x_3 \mid_{m_1} \right. \right] \\ &= \left[\left| 2^{n-1} x_1 + \frac{(2^n - 1)(2^n - 1)}{2^n} x_2 + \frac{(2^n - 1)(2^{n-1} + 1)}{2^n + 1} x_3 \right|_{2^{n-1}} \right] \\ &= \left[\left| 2^{n-1} x_1 + \frac{2^{2n} - 2^{n+1} - 1}{2^n} x_2 + \frac{\frac{1}{2}(2^n - 1)(2^n + 1) + \frac{1}{2}(2^n + 1) - 1}{2^n + 1} x_3 \right|_{2^{n-1}} \right] \\ &= \left[\left| 2^{n-1} x_1 + (2^n - 2) x_2 + 2^{n-1} x_3 + \frac{1}{2^n} x_2 - \frac{1}{2^n + 1} x_3 \right|_{2^{n-1}} \right] \\ &= \left[\left| 2^{n-1} x_1 - x_2 + 2^{n-1} x_3 + \frac{2^n(x_2 - x_3) + x_2}{2^n(2^n + 1)} \right|_{2^{n-1}} \right] \\ &\cong \left| 2^{n-1} x_1 - x_2 + 2^{n-1} x_3 \right|_{2^{n-1}} \quad (6) \end{aligned}$$

因为 $2^n - 1$ 是此余数基中最小的模, 所以没有必要再对缩放后的二进制整数 Y 做模 2^n 和模 $2^n + 1$ 运算, 缩放后的三个余数通道的余数与式(7) 计算出的二进制整数相同, 即 $y_i = \mid Y \mid_{m_i}, i = 1, 2, 3$.

等式(6) 计算出的结果为真实的缩放后的二进制整数 Y_{exact} , 令 $c = \frac{2^n(x_2 - x_3) + x_2}{2^n(2^n + 1)}$, 有下式:

$$Y_{\text{exact}} = \left[\left| 2^{n-1} x_1 - x_2 + 2^{n-1} x_3 + c \right|_{2^{n-1}} \right] \quad (8)$$

定义 $\mid x \mid_m = x - um$, 其中 u 是非负整数, 故下列两式成立:

$$Y_{\text{exact}} = \left[\left| 2^{n-1} x_1 - x_2 + 2^{n-1} x_3 + c - u(2^n - 1) \right| \right] \quad (9)$$

$$Y = 2^{n-1} x_1 - x_2 + 2^{n-1} x_3 - u(2^n - 1) \quad (10)$$

因为 $0 \leq x_2 \leq 2^n - 1, 0 \leq x_3 \leq 2^n$, 所以 $-2^n \leq x_2 - x_3 \leq 2^n - 1$, 故 $-1 < c = \frac{2^n(x_2 - x_3) + x_2}{2^n(2^n + 1)} < 1$, 当 $-1 < c < 0$ 时,

$$Y_{\text{exact}} = 2^{n-1} x_1 - x_2 + 2^{n-1} x_3 - u(2^n - 1) - 1 \quad (11)$$

原理 2: $\mid X \pm Y \mid_m = \mid \mid X \mid_m \pm \mid Y \mid_m \mid_m$

原理 3: $\mid X \cdot Y \mid_m = \mid \mid X \mid_m \cdot \mid Y \mid_m \mid_m$

定理 1 令 $p = kq$, 其中 k 为整数, 有 $\mid \mid X \mid_p \mid_q = \mid X \mid_q$.

定理 2 令余数基为 $\{m_1, m_2, m_3\}$, 其中 $m_1 = 2^n - 1, m_2 = 2^n, m_3 = 2^n + 1$, 则下列等式成立.

$$\mid M_1^{-1} \mid_{m_1} = 2^{n-1} \quad (3)$$

$$\mid M_2^{-1} \mid_{m_2} = 2^n - 1 \quad (4)$$

$$\mid M_3^{-1} \mid_{m_3} = 2^{n-1} + 1 \quad (5)$$

令 $k = m_2 m_3 = 2^n(2^n + 1)$, 其中 k 为缩放因子, 对式(2) 两边同时除以 k , 并向下取整, 运算过程如下:

当 $0 \leq c < 1$ 时,

$$Y_{\text{exact}} = 2^{n-1} x_1 - x_2 + 2^{n-1} x_3 - u(2^n - 1) \quad (12)$$

综上所述, 当 $-1 < c < 0$ 时, Y_{exact} 和 Y 有统一的 1 的误差且 $Y_{\text{exact}} = Y - 1$, 当 $0 \leq c < 1$ 时, Y_{exact} 和 Y 相等.

3 设计实现

性质 1: 2^r 乘以一个 n 位二进制数 x 然后再做模 $2^n - 1$ 运算相当于对 x 做循环左移 r 位的运算, 即下式^[4]:

$$\mid 2^r x \mid_{2^n - 1} = \text{CLS}_n(x, r) \quad (13)$$

其中 $\text{CLS}_n(x, r)$ 表示一个 n 位二进制数 x 循环左移 r 位.

性质 2:

$$\mid -2^r x \mid_{2^n - 1} = \mid 2^r(2^n - 1 - x) \mid_{2^n - 1} = \mid 2^r \bar{x} \mid_{2^n - 1} \quad (14)$$

式中, $\bar{x}$ 表示二进制数 x 的反码^[4].

应用性质1和性质2,式(7)可变形为

$$\begin{aligned} Y &= |2^{n-1}x_1 - x_2 + 2^{n-1}x_3|_{2^n-1} \\ &= |2^{n-1}x_1 + \overline{x_2} + 2^{n-1}x_3|_{2^n-1} \end{aligned} \quad (15)$$

根据上式,复杂的RNS缩放运算可以简化成3个运算数的模加运算,因为 2^n-1 是此三模余数基中最小的模,所以不需要对缩放后的二进制整数Y做额外的模运算,运算流程如图1所示。

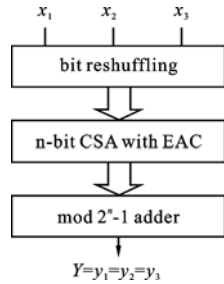


图1 本设计的运算流程

4 性能评估与性能比较

接下来我们将利用单位门延迟模型来评估本设计的面积和延迟,如与门(AND)和与非门(NAND)这样的两输入门被认为具有一个单位的面积和一个单位的延迟,一个异或门(XOR)被认为具有两个单位的面积和两个单位的延迟,反相器(inverter)的面积和延迟可以忽略,所以被认为不具有面积和延迟,基于单位门延迟模型,一个全加器(FA)具有7个单位的面积和4个单位的延迟^[4]。

一个 n 位的进位保存加法器(CSA)由 n 个全加器(FA)组成,故它的面积和延迟分别为 $7n$ 个单位和4个单位,基于文献[4],模 2^n-1 加法器的面积和延迟分别为 $3n[\log_2 n-1]+12n$ 个单位和 $2[\log_2 n-1]+3$ 个单位。根据图1,本设计只需要一个 n 位的进位保存加法器(CSA)和一个模 2^n-1 加法器,由于在单位门延迟模型中,一个单位的面积相当于6个晶体管,因此一个 n 位的进位保存加法器(CSA)的数量为 $42n$,一个模加法器的晶体管数量为 $18n[\log_2 n-1]+72n$,所以本设计的基于单位门延迟模型的晶体管数量和延迟分别为 $18n[\log_2 n-1]+114n$ 和 $2[\log_2 n-1]+7$ 。

根据文献[5],缩放结构由2级 n 位的进位保存加法器(CSA)和1个模加法器构成,所以文献[5]中的晶体管数目和延迟分别为 $18n[\log_2 n-1]+156n$ 和 $2[\log_2 n-1]+11$ 。文献[5]在特定条件下也会产生1的统一的误差。

当 $n=5,6,7,8$,即动态范围大约在15到24位的范围内时,本设计与文献[5]中晶体管的数目

(A)、延迟(T)以及面积时延积(AT)的比较如表1所示。

表1 本设计与文献[5]的晶体管数目与延迟的比较

	Proposed	文献[5]
n	(A, T, AT)	(A, T, AT)
5	(750, 11, 8 250)	(960, 15, 14 400)
6	(900, 11, 9 900)	(1 152, 15, 17 280)
7	(1 050, 11, 11 550)	(1 344, 15, 20 160)
8	(1 200, 11, 13 200)	(1 536, 15, 23 040)

从表1可以看出,本设计使用的晶体管数量与延迟都比文献[5]中的晶体管数量与延迟要小,且面积延迟积大约只有文献[5]的二分之一,这是因为文献[5]中用了两级进位保存加法器(CSA),而本设计只使用了一级进位保存加法器(CSA),综上所述,本设计性能远远高于文献[5]的性能。

5 结束语

本文针对最常用的三模余数基 $\{2^n-1, 2^n, 2^n+1\}$ 提出了一种更简单和更快的RNS缩放结构。本文运用中国剩余定理(CRT)选择 $2^n(2^n+1)$ 作为缩放因子实现了基于全加器的缩放结构,该缩放结构使得缩放后的三个余数通道的余数与缩放后的二进制整数相同,所以在缩放运算后可以省略一个面积和延迟都很大的余数到二进制(R/B)转换模块。本文提出的RNS缩放结构的面积时延积(AT)比目前最简单最快的RNS缩放结构小一半,大大提高了缩放结构的性能。

参考文献:

- [1] Shang Ma, Jianhao Hu, Lin Zhang, et al. An efficient RNS scaler and its VLSI implementation[J]. Communications, Circuits and Systems, 2008(5):1370-1373.
- [2] Yanlong Ye, Shang Ma, Jianhao Hu. An efficient RNS scaler for moduli set[J]. Information Science and Engineering, 2008(2):511-515.
- [3] Jeremy Yung, Shern Low, Chiphong Chang. A VLSI efficient programmable power-of-two scaler for[J]. IEEE Transactions on Circuits and Systems—I, 2012(59):2911-2919.
- [4] Chiphong Chang, Jeremy Yung, Shern Low. Simple, fast, exact RNS scaler for the three-moduli set[J]. IEEE Transactions on Circuits and Systems—I, 2011(58):2686-2697.

(下转第78页)

通过客观和主观评价,验证了去雾效果图质量的改善.但是对于调整信息图,本文参数 L 需要手动调

整,并且对于去雾效果图没有统一的评价函数,因此,这两点将成为我们接下来的工作.

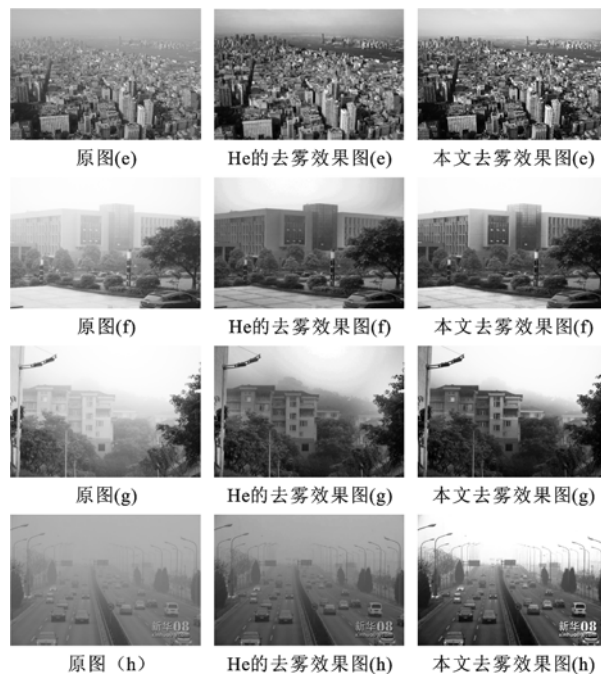


图4 实验结果图与 He 的结果对比

参考文献:

- [1] He Kaiming, Sun jian, TangXiaoou. Single image haze removal using dark channel prior[J]. Pattern Analysis and Machine Intelligence, 2011, 33(12): 2341-2353.
- [2] 孙红光, 房超, 张慧杰. 一种自适应基于暗通道先验的去雾方法[J]. 吉林大学学报, 2012, 50(5): 987-992.
- [3] Fattal R. Single image dehazing[J]. ACM Transactions on Graphics, 2008, 27(3): 721-729.
- [4] Levin A, Lischinski D, Weiss Y. A closed form solution to natural image matting[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE Computer Society, 2008, 30(2): 228-242.
- [5] 陈勇, 李愿, 谢正祥. 标准化变化在视频隐形图像重现中应用[J]. 半导体光电, 2013, 34(2): 307-310.
- [6] 徐晶, 刘鹏, 唐降龙. 大气光估计对单幅图像去雾复原的影响[J]. 智能计算机与应用, 2012, 2(3): 68-71.

- [7] 郭璠. 图像去雾方法和评价及其应用研究[D]. 长沙: 中南大学, 2011.
- [8] He K M, Sun J, Tang X O. guided image filter[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2013, 35(6): 1307-1409.
- [9] 陈勇, 李愿, 吕霞付, 等. 视觉感知的彩色图像质量积极评价[J]. 光学精密工程, 2013, 21(3): 742-750.

作者简介:

方紫娟 女, (1988—), 硕士研究生. 研究方向为视频图像处理及应用.

谢正祥 男, (1938—), 教授, 博士生导师. 研究方向为生物学信号和图像处理.

吕霞付 男, (1966—), 教授, 研究生导师. 研究方向为视频图像处理及应用.

冯 鹏 男, (1987—), 硕士研究生. 研究方向为视频图像处理及应用.

(上接第 73 页)

- [5] Jeremy Yung, Shern Low, Chiphong Chang. A new RNS scaler for[J]. IEEE Symposium on Circuits and Systems, 2011(59): 1431-1434.

作者简介:

赵英旭 男, (1989—), 硕士研究生. 研究方向为 SoC 的设计.

李 磊 男, (1982—), 博士. 研究方向为 ASIC 和 SoC 的设计.