

一种基于余数系统的奇偶检测算法及 VLSI 实现

张译匀, 周婉婷, 李 磊

(电子科技大学 电子科学技术研究院, 四川 成都 611731)

摘 要: 提出了一种基于常用三模基 $\{2^n+1, 2^n-1, 2^{2n}+1\}$ 改进的奇偶检测算法, 此方法仅使用一个 n 位的模加器, 一个 $n+1$ 位的进位选择加法器(CSA), 一个 $2n$ 位的比较器及一些简单的组合单元即可实现, 有效节省了资源, 并简化了设计的复杂度. 当 $n=30$ 时, 面积仅为 $6\,130.958\,\mu\text{m}^2$, 延迟仅为 $0.67\,\text{ns}$.

关键词: 余数系统; 奇偶检测; VLSI

中图分类号: TN403

文献标识码: A

文章编号: 1000-7180(2014)03-0032-04

Parity Detection Algorithm and VLSI Implementation Based on the RNS

ZHANG Yi-yun, ZHOU Wan-ting, LI Lei

(Research Institute of Electronic Science and Technology, UESTC, Chengdu 611731, China)

Abstract: A parity checker based on triple-mode $\{2^n+1, 2^n-1, 2^{2n}+1\}$ is proposed in this paper, this checker only need a n bit adder, a $n+1$ bit CSA adder, a $2n$ bit comparator and some simple combination unit, it lowers the resource consumption and simplifies the design effectively. When $n=30$, an area of only $6130.958\mu\text{m}^2$, the delay is only 0.67ns .

Key words: RNS; Parity detection; VLSI

1 引言

余数系统作为一种非权重系统, 其多通道并行处理的特点, 使其在加法、减法、乘法等操作^[1-4]可以达到很高的速度, 因此余数系统广泛的应用于高速数字信号处理(DSP)以及密码学中. 而在这个系统中进行数值大小比较、符号检测以及奇偶检测却比较困难, 且会消耗大量的时间. 为了解决以上问题, 文献[5-6]各自提出了一种奇偶检测方法, 但这些方法均是基于查找表(LUT)以及除法运算实现奇偶检测, 浪费了大量的资源和增加了延迟; 本文提出一种更加有效的基于三模基 $\{2^n+1, 2^n-1, 2^{2n}+1\}$ 改进的奇偶检测方法, 此方法的实现避免了查找表(LUT)与除法操作的使用, 节省了资源和减小了延迟.

2 余数系统介绍

余数系统(RNS)是由一组互质的余数基 $\{l_1,$

$l_2, \dots, l_n\}$ 来确定的, 若 X, Y 为整数, 且 X, Y 在 $[0, M)$ 范围内, 则在余数系统中 X, Y 都可以唯一地表示为

$$\begin{cases} X \xrightarrow{\text{RNS}} \{x_1, x_2, \dots, x_n\} \\ Y \xrightarrow{\text{RNS}} \{y_1, y_2, \dots, y_n\} \end{cases}$$

式中, M 是该余数系统的动态范围, 满足 $M = \prod_{i=1}^n l_i$.

x_i 是 X 对 l_i 取模的值, 同样 y_i 是 Y 对 l_i 取模的值. 本文对求模操作符记为 $x_i = \langle X \rangle_{l_i}$.

若令整数 $Z = X \Delta Y$, 则 Z 在余数系统(RNS)中的运算可以表征为

$$\begin{aligned} Z &\xrightarrow{\text{RNS}} \{z_1, z_2, \dots, z_n\}; \\ \langle \{z_1, z_2, \dots, z_n\} &= \{\langle x_1 \Delta y_1 \rangle, \langle x_2 \Delta y_2 \rangle, \\ &\dots, \langle x_n \Delta y_n \rangle\} \end{aligned}$$

表达式中符号 Δ 可代表余数系统中的加法、乘法或者减法操作符.

在余数系统动态范围之内的整数可用其余数分

量唯一地表示.反之,若已知余数分量,也可以根据中国剩余定理(CRT)^[7]、混合基转换定理(MRC)^[8]进行R/B的后向转换得到二进制整数,本文就是选择基于CRT的理论实现奇偶检测单元的设计.

余数系统相关定理证明如下所示.

定理 1^[3]:

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

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

对定理 1 的证明如下:

$$\begin{aligned} & \langle 2^{n-1}(2^n - 1) \rangle_{2^{n+1}} \\ &= \langle 2^{n-1}(2^n + 1 - 2) \rangle_{2^{n+1}} \\ &= \langle 2^{n-1}(2^n + 1) - (2^n + 1) + 1 \rangle_{2^{n+1}} \\ &= 1 \\ & \langle 2^{n-1}(2^n + 1) \rangle_{2^{n-1}} \\ &= \langle 2^{n-1}(2^n - 1 + 2) \rangle_{2^{n-1}} \\ &= \langle 2^{n-1}(2^n - 1) + (2^n - 1) + 1 \rangle_{2^{n-1}} \\ &= 1 \end{aligned}$$

3 奇偶检测算法介绍

取三模余数基为 $\{l_1, l_2, l_3\} = \{2^n + 1, 2^n - 1, 2^{2n} + 1\}$, 则动态范围 $M = 2^{4n} - 1$. 若整数 Y 在余数系统(RNS)中的表示为 $\{y_1, y_2, y_3\}$. 利用中国剩余定理 II (CRT-II) 的理论可知, 由模 $\{l_1, l_2\}$ 可确定一个在 $[0, l_1 l_2 - 1]$ 范围内的中间数 y_{12} , 而在 $[0, M)$ 范围内的整数 Y 最终是由两模基 $\{l_1 l_2, l_3\}$ 以及 $\{y_{12}, y_3\}$ 确定. 此过程也就是一个三模转换为两模的过程.

结合中国剩余定理(CRT)以及定理 1 可知:

$$Y = (M/l_3) \cdot y_3 \langle (l_1 l_2)^{-1} \rangle_{l_3} + (M/l_1 l_2) \cdot y_{12} \langle (l_3)^{-1} \rangle_{l_1 l_2} - \delta M$$

$$\delta = \lfloor (y_{12}/l_1 l_2) \cdot \langle (l_3)^{-1} \rangle_{l_1 l_2} + (y_3/l_3) \cdot \langle (l_1 l_2)^{-1} \rangle_{l_3} \rfloor \quad (1)$$

式中, 式(1)中 $\lfloor \cdot \rfloor$ 代表向下取整操作; 式(1)中 Y 在本文中可具体化为

$$Y = (2^{2n} + 1)y_{12} \langle (2^{n+1})^{-1} \rangle_{2^{n-1}} + (2^{2n} - 1)y_3 \langle (2^n - 1)^{-1} \rangle_{2^{n+1}} - \delta M = (2^{2n} + 1)2^{n-1}y_{12} + (2^{2n} - 1)2^{n-1}y_3 - \delta M$$

由于 $(2^{2n} + 1)2^{n-1}y_{12} + (2^{2n} - 1)2^{n-1}y_3$ 一定为偶数, 且 M 为奇数, 因此 Y 的奇偶性仅由 δ 决定, 且二者奇偶性相同. 所以本文接下来就针对 δ 来展开讨论 Y 的奇偶性. 对于(1)中 δ 的表达式可根据定理 1 简化为式(2).

$$\delta = \lfloor (y_{12}/(2^{2n} - 1)) \cdot 2^{2n-1} + (y_3/(2^{2n} + 1)) \cdot$$

$$\begin{aligned} & 2^{2n-1} \rfloor \\ &= \lfloor ((y_{12}(2^{2n} + 1)) + y_3(2^{2n} - 1)) / \\ & (2^{4n} - 1) \rfloor 2^{2n-1} \rfloor \\ &= \lfloor (y_{12} + y_3) / 2 + \tau \rfloor \end{aligned} \quad (2)$$

其中:

$$\begin{aligned} \tau &= \lfloor y_{12}(2^{2n} + 1) - y_3(2^{2n} - 1) \rfloor / 2M \\ &= 2^{2n-1}(y_{12} - y_3) / M + (y_{12} + y_3) / 2M \end{aligned} \quad (3)$$

由于 y_{12}, y_3 满足 $y_{12} \in [0, 2^{2n} - 1), y_3 \in [0, 2^{2n} + 1)$, 因此结合式(3)就可以推出 $|\tau| < 0.5$.

下面对 y_{12}, y_3 分情况讨论 Y 的奇偶性:

(1) 当 $y_{12} > y_3$ 时, 则 τ 满足: $\tau \in [0, 0.5)$. 此时 $\delta = \lfloor (y_{12} + y_3) / 2 \rfloor$, 因此 Y 的奇偶性就由 $\lfloor (y_{12} + y_3) / 2 \rfloor$ 决定. 由于向下取整操作及 y_{12}, y_3 均为整数的特点, 所以 Y 的奇偶性与 $(y_{12} + y_3) / 2$ 相同. 若令 $K = y_{12} + y_3$, 并且设 K 的二进制表示为 $K_{2n} \cdots K_1 K_0$, 则 Y 的奇偶性就由 K_0 决定, 所以就不需要求解 K 的值, 只需求解 $(y_{12}[1:0] + y_3[1:0])$ 即可.

(2) 当 $y_{12} = y_3$ 时, 则 $\tau \in [0, 0.5)$, 此情况可归并到(1)中.

(3) 当 $y_{12} < y_3$, 并且满足: $\lfloor 2^{2n-1}(y_{12} - y_3) / M \rfloor \geq (y_{12} + y_3) / 2M$ 时, 则 $\tau \in (-0.5, 0]$. 由于 y_{12}, y_3 不可能同时为 0, 因此 $\tau \neq 0$, 即 $\tau \in (-0.5, 0)$. 由于 $\delta = \lfloor (y_{12} + y_3 - 1) / 2 + 0.5 + \tau \rfloor$, 并且有 $(0.5 + \tau) \in (0, 0.5)$, 所以 δ 可以重写为 $\delta = \lfloor (y_{12} + y_3 - 1) / 2 \rfloor$.

由数值的奇偶性知: $(y_{12} + y_3 - 1) / 2$ 与 $(y_{12}[1:0] + y_3[1:0] - 1) / 2$ 具有相同的奇偶性, 所以 δ 与 $\lfloor (y_{12}[1:0] + y_3[1:0] - 1) / 2 \rfloor$ 也具有相同的奇偶性, 此时 Y 的奇偶性可依据 $\lfloor (y_{12}[1:0] + y_3[1:0] - 1) / 2 \rfloor$ 来判断, 考虑到 $y_{12}[1:0] + y_3[1:0]$ 可能为 0 的情况, 下面分两种情况讨论:

① 当 $y_{12}[1:0] + y_3[1:0] = 0$ 时, 由于表达式 $\lfloor (y_{12}[1:0] + y_3[1:0] - 1) / 2 \rfloor = -1$, 一定为奇数, 因此 Y 就为奇数.

② 当 $y_{12}[1:0] + y_3[1:0] \neq 0$ 时, 满足 $y_{12}[1:0] + y_3[1:0] - 1 \geq 0$. 此时表达式 $\lfloor (y_{12}[1:0] + y_3[1:0] - 1) / 2 \rfloor$ 的奇偶性可由 $y_{12}[1:0] + y_3[1:0] - 1$ 右移一位的结果决定; 令 $s[1:0] = y_{12}[1:0] + y_3[1:0]$, 则 $s[1:0]$ 与 Y 奇偶性的关系如表 1 所示.

表 1 $s[1:0]$ 与奇偶性的关系

$s[1]$	$s[0]$	奇偶性
0	1	0
1	0	0
1	1	1

即 Y 的奇偶性为: $s[1]$ 与 $s[0]$ 同或的值.

(4) 当 $y_{12} < y_3$, 并且满足 $|2^{2^{n-1}}(y_{12} - y_3)/M| < |(y_{12} + y_3)/2M|$ 时, 则有

$$\tau \in (0, 0.5);$$

$$\langle 2^{2^{n-1}}(y_3 - y_{12})/M < (y_{12} + y_3)/2M \rangle, \text{ 即有}$$

下式:

$$\frac{2^{2^n} - 1}{2^{2^n} + 1} y_3 < y_{12} < y_3 \quad (4)$$

结合表达式(4)与 $y_3 \in [0, 2^{2^n} + 1)$ 可知 $(y_3 - y_{12}) \in (0, 2)$, 由此推出 $y_3 = y_{12} + 1, \delta = \lfloor (y_{12} + y_3)/2 + \tau \rfloor = \lfloor (y_{12} + y_3)/2 \rfloor$. 由于在此情况下 $y_{12} + y_3$ 为奇数, 所以可推出 $\delta = \lfloor (y_{12} + y_3)/2 \rfloor = \lfloor (y_{12} + y_3 - 1)/2 \rfloor$. 此时 Y 的奇偶性可以使用(3)中讨论的结论, 即可将(3)、(4)归结为同一种情况.

对于本文表达式中涉及到的 y_{12} 可以根据中国剩余定理 II (CRT-II) 的理论^[3] 按下述方式具体求解:

$$y_{12} = y_1 + \langle k_0(y_2 - y_1) \rangle_{l_2} l_1 \quad (5)$$

其中 k_0 满足: $\langle k_0 l_1 \rangle_{l_2} = 1$

即: $\langle k_0(2^n + 1) \rangle_{2^{n-1}} = 1$

由定理 1 可知 $k_0 = 2^{n-1}$, 因此式(5)可以重写为

$$y_{12} = y_1 + \langle 2^{n-1}(y_2 - y_1) \rangle_{2^{n-1}(2^n + 1)}$$

依据文献[7]中的内容可知: 若令 $A = \langle 2^{n-1}(y_2 - y_1) \rangle_{2^{n-1}(2^n + 1)}$, 并且 $A1 = \langle (y_2 - y_1) \rangle_{2^{n-1}}$, $A1$ 的二进制表示为 $A1_{n-1} \cdots A1_1 A1_0$ 时, $y_{12} = y_1 + A$, 其中, $A = A1_0 A1_{n-1} \cdots A1_1 A1_0 A1_{n-1} \cdots A1_1$;

综上所述可知: $y_{12} \geq y_3$ 时, Y 的奇偶性($y_{12}[1:0] + y_3[1:0]$)/2 确定. $y_{12} < y_3$ 时, 若 $y_{12}[1:0] + y_3[1:0] = 0$, Y 就为奇数; 否则, 令 $s[1:0] = y_{12}[1:0] + y_3[1:0]$, Y 的奇偶性就由 $s[1]$ 与 $s[0]$ 同或的值确定.

4 奇偶检测的 VLSI 实现

将本文提出的奇偶检测算法采用 Verilog 代码进行硬件电路实现, 并且使用 VCS 进行功能仿真, 验证结果表明本文算法是完全正确的, 最后利用 Synopsys 公司的 Design Compiler 综合得到门级网表及信息报告. 其奇偶检测电路的整体结构图如图 1 所示.

由于图 1 中 y_1 是 $n+1$ 位的, 而 B 是 $2n$ 位的. 为节省资源和提高性能, 可以对图 1 中求解 y_{12} 的 $2n$ 位加法器进行优化, 优化后的加法器结构如图 2 所示.

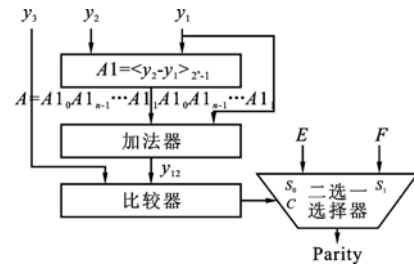


图 1 整体的奇偶检测电路结构图

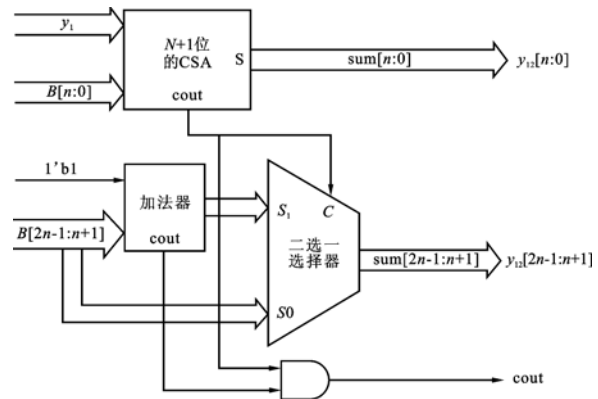


图 2 y_{12} 加法器优化结构图

由于图 1 中 E 代表的是当 $y_{12} \geq y_3$ 时, Y 的奇偶性, F 代表的是 $y_{12} < y_3$ 时, Y 的奇偶性. 对于 E, F 取值的具体推导过程在第 3 部分的算法介绍中有详细的说明, 在此只是给出求解 E, F 的结构图, 如图 3 所示.

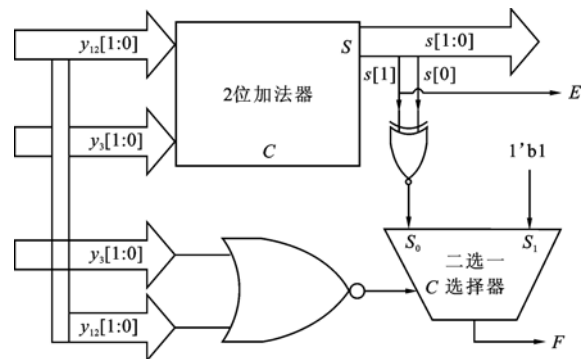


图 3 E, F 求解结构图

5 结果分析及结论

针对奇偶检测算法研究都利用查找表或除法运算来实现, 对资源和时间的消耗比较大的特点, 现就文献[5]中的方法与本文方法的资源利用情况进行对比分析. 文献[1]中实现奇偶检测是使用查找表代替了除法, 当用文献[5]的方法实现本文中三模基 $\{2^n + 1, 2^n - 1, 2^{2^n} + 1\}$ 的奇偶检测时, 则需要 $(4n + 2)(\log_2 nM + 2)$ 比特的存储器和两个宽度为 $\log_2 nM$ 的加法器; 而用本文方法实现则仅使用加法

器、比较器及一些其他比较小的组合逻辑单元即可,因此有效的避免了使用除法操作和查找表.具体资源利用对比结果如表2所示.

表2 资源利用对比结果

名称	文献[5]	本文
加法器	2个 $\log_2 nM$ 比特的加法器	1个 n bit 模加法器 1个 $n+1$ 位的CSA加法器
超前进位链	0	0
$2n$ 位的比较器	0	1
LUT	$(4n+2)(\log_2 nM+2)$	0

对本文算法实现的电路,使用Synopsys公司的Design Compiler工具,在TSMC 90 nm工艺库下进行综合,所得到的面积和延迟数据如表3所示.

表3 本文设计数据

n (模参数)	面积/ μm^2	延迟/ns
8	2 442.787	0.45
16	4 366.253	0.57
24	5 601.758	0.61
30	6 130.958	0.67

6 结束语

从上述数据可以看出,使用本文提出的方法来实现奇偶检测,即使当 $n=30$ 时,延迟也仅有0.67 ns,可提升设计性能,实现高速高性能的要求.所以可将本文提出的算法用于高速数字信号处理及密码学等领域.

参考文献:

[1] 敖思远,李磊.一种改进的模 2^n-1 乘法器[J].微电子学与计算机,2011,28(4):107-110.

- [2] Dimitrakopoulos G. A systematic methodology for designing area-time efficient parallel-prefix modulo 2^n-1 Adders[C]//Proc. Int'l Symp. Circuits and Systems, ISCAS03, Bangkok Thailand, 2003(5):225-228.
- [3] Riyaz A Patel, Mohammed Benaissa. Fast parallel-prefix architectures for modulo 2^n-1 addition with a single representation of zero[J]. IEEE Transactions on Computers, 2007, 56(11):1484-1492.
- [4] Haridimos T Vergos. On modulo 2^n+1 adder design[J]. IEEE Transactions on computers, 2012, 61(2):173-186.
- [5] Lu M, Chiang T S. A novel division algorithm for the residue number system[J]. IEEE Transactions on Computers, 1992, 41(8):1026-1032.
- [6] Yang J H, Chang C C, Chen C Y. A high-speed division algorithm in residuenumbersystem using parity-checking technique[J]. International Journal of Computer Mathematics, 2004, 81(6):775-780.
- [7] Ma S, Hu JH, Zhang L, et al. An efficient RNS parity checker for moduli set $\{2^n+1, 2^n-1, 2^{2n}+1\}$ and its applications. Science in China series F-Information [J]. SCIENCES, 2008, 5(10):1-10.
- [8] 马上,叶燕龙,胡剑浩.模 2^n-2^k-1 加法器高效VLSI设计与实现[J].微电子学与计算机,2010,27(10):1-7.

作者简介:

张译匀 女,(1988-),硕士.研究方向为余数系统算法研究和ASIC设计.

周婉婷 女,(1981-),博士.研究方向为专用集成电路(ASIC)和余数系统研究.

李磊 男,(1982-),副研究员.研究方向为专用集成电路(ASIC)和余数系统.