A Novel Power Saving Approach for Residue Number System Moduli Set Based On Fast Sign Detection Algorithm

S.Kiranmayi (Pg Scholar)¹ B. Sanjai Prasada Rao Associate Professor² Department of ECE, Lords Institute of Engineering and Technology, Hyderabad, INDIA

Abstract

Although lot of research done o residue number system to save power but still it is considered as concerned area in the field of VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS the proposed method presents an sign detection unit offers significant savings in delay, area and power compared with the sign detection units and recorded good performance over traditional approaches. The processing's of the proposed work is performed in two steps namely, first, a sign detection algorithm for the restricted moduli set is described. The new algorithm allows for parallel implementation and consists exclusively of modulo 2n additions. Then, a sign detection unit for the moduli set $\{2n+1 - 1, 2n - 1, 2n\}$ is proposed based on the new sign detection algorithm for the restricted moduli set is described. The new algorithe adder, one comparator and one prefix adder First, a sign detection algorithm for the restricted moduli set is described. The new algorithe new algorithm allows for parallel implementation and consists exclusively of modulo 2n algorithm. The unit can be implemented using one carry save adder, one comparator and one prefix adder First, a sign detection algorithm for the restricted moduli set is described. The new algorithm allows for parallel implementation and consists exclusively of modulo 2n additions. Then, a sign detection unit for the moduli set $\{2n+1 - 1, 2n - 1, 2n - 1, 2n\}$ is proposed based on the new sign detection algorithm. The unit can be implemented using one carry save adder, one comparator and one prefix adder. Finally the experimental results shows that the proposed work offers 63.8%, 44.9%, and 67.6% savings on average in area, delay and power, respectively, compared with a unit based on one of the best sign detection algorithm.

KEYWORDS: Residue number system, Moduli set, Carry save adder, Computer arithmetic, Sign detection

1. INTRODUCTION

Residue number systems (RNS) have been for a long time a topic of intensive research. Their usefulness has been demonstrated, especially for computations where additions, subtractions and multiplications dominate, because such operations can be done independently for each residue digit without carry propagation. Other operations such as overflow detection, sign detection, magnitude comparison and division in RNS are very difficult and time consuming. However, above mentioned operations are essential in certain applications, e.g. in exact arithmetic or computational geometry, where residue arithmetic is applied.

Moduli selection is one of the greatest RNS challenges. This is because, the speed and complexity of the

resulting RNS architecture is dependent on the form and the number of moduli set. It has been well established that powers-of-two moduli sets simplify the required arithmetic operations and generate efficient hardware implementations of the RNS architecture.

The sign detection problem has been investigated by many researchers. A general theorem is derived by establishing the necessary conditions for sign detection. The sign detection for a selected class of RNS is carried out as a sum modulo 2 of digits in the associated mixed radix system (MRS). A sign detection technique based on fractional representation is proposed to reduce the sum modulo M in the conversion formula to a sum modulo 2.A sign detection algorithm based on the new Chinese remainder theorem (CRT) II is presented. The modulo operations in the sign detection algorithm are bounded by size \sqrt{M} . In [5], a sign detection algorithm uses the nth mixed radix digit in mixedradix conversion (MRC) to detect the sign function. To date, the only brief to use the combinational logic to implement a sign detection algorithm based on $\{2n -1, 2n, 2n +1\}$. However, the method cannot be extended to other moduli sets.

The proposed sign detection algorithm requires only the addition of the modulo 2n. Then, a new sign detection unit is developed for the moduli set $\{2n+1-1, 2n-1, 2n\}$ based on the proposed sign detection algorithm. This unit only consists of a carry save adder (CSA), a comparator, and a carry generation unit. The proposed algorithm is the first proposed for the moduli set $\{2n+1-1, 2n-1, 2n\}$. The achieved efficiency is better than that of other methods, such as algorithms based on ROM technology.

2. BACKGROUND

2.1 RESIDUE NUMBER SYSTEM (RNS)

The RNS implementations can provide speedup for addition, subtraction and multiplication. In RNS, a decimal number is represented by an n-tuple of its remainders with respect to each modulus in the moduli set. A remainder called r, of a number X with respect to a modulus m is denoted by r = Xmod m and is calculated by r = X - m q, where q is the largest integer which yields a non-negative r. To illustrate an RNS number (SODERSTRAND.M.A and AL MARAYATI.K (1995)), let us consider X to be a decimal number and set $\{m0, m1, m2, \dots, m(n-1)\}$ to be the moduli set for a residue number system. This RNS can be the moduli set for a residue number system. This RNS can represent any number from 0 to (M-1), where M is the product of all the moduli in the set. Number X in this system will be represented by n-tuple (r0, r1, r2, $\dots, r(n-1)$), where $ri = X \mod mi 0 \le i \le n-1$.

As for the number of modulus in a set, no limitation has been set. On one hand, the choice of moduli set affects the performance of the algorithms. Most of RNS applications today use 3 or 4 numbers of modules. One of the major attractive features of RNS is that each of the residue digits is independent of each other and hence, there is no carry propagation from one residue digit to another. This characteristic is very important in some of cyclic operations such as addition, subtraction and multiplication. This makes it possible for those operations to be performed on all residue digits in parallel

2.2 CHOICE OF MODULI SET

There are no fixed rules regarding moduli set used in RNS. The only requirement for a modulus to be in a set is that it has to be a pair-wise relatively prime to any other moduli in the set. However, that guideline is not always necessary. A moduli set can have moduli that have common factor; hence they are not relatively prime to one another.

1. The dynamic range for the set is the closest to the dynamic range of its 3n binary counterpart.

2. As all the moduli are almost equal, number of operations in the set is spread out almost evenly throughout the moduli set.

3. Implementation of RNS can be accomplished using conventional hardware.

3. LITERATURE REVIEW

(1) M. BHARDWAJ and A. BALARAM (1998) proposed low power architecture using residue numbers and also discussed the related issues.

(2) G. C. CARDARILLI, A. NANNARELLI and MARCO RE (2002) dealt with the power dissipation in FIR filters and also discussed to reduce power in FIR filter using Residue Number System (RNS).

(3) R. CONWAY and J. NELSON (1999) proposed Fast Converter for 3 Moduli RNS Using New Property of CRT and also discussed about the direct method of implementation of RNS. (4) M.A. SODERSTRAND and K.AL MARAYATI (1995) discussed about the design of higher order FIR filters and related issues.

(5) W.L. FREKING and K.K. PARHI (1998) proposed the design of low power digital filters using residue arithmetic and comparison made with existing methods.

(6) SANGYAN HWANG and SUNGHO KANG (2004) proposed the implementation of low power FIR filter using distributed arithmetic algorithm.

4. PROPOSED METHOD

A standard RNS is defined exclusively for positive integers in the range [0, M). To accommodate negative integers, an implicit signed number system may be considered to be split into a positive half of the range and a negative half of the range. The dynamic range M of the moduli set {m1, m2... m N-1, m N = 2n} is even. After conversion from the residue number to the weighted number, the resulting non integer X in the interval [0, M/2) carries an implicit representation of the sign of the actual result Y, which can be obtained in its range [-M/2, M/2 - 1) as follows

$$Y = \begin{cases} X, & if \quad 0 \le X < M/2 \\ X - m, & if \quad M/2 \le X < M \end{cases}$$
(1)

Theorem 1: Given $\{m1, m2. ..., mN\}$, the magnitude of a residue number X = (x1, x2, ..., xN) is calculated as follows:

$$X = \sum_{j=1}^{N-2} (\alpha_{j+1} \prod_{i=1}^{j+1} m_i) + \alpha_1 m_1 + \alpha_0 \quad (2)$$

Where

 $\begin{aligned} \alpha_{j+1} &= \left[\left[\sum_{i=1}^{j+2} \gamma_i \, x_i / \prod_{i=2}^{j+1} m_i \right] \right]_{m_{j+2}}, & \alpha_{j+1} &= |\gamma_1 x_1 + \\ \gamma_2 x_2|_{m_2}, \, \alpha_0 &= x_1, \, N > 1, \, \gamma_1 &= (N_1 | N_1^{-1} |_{m_1} - 1) / m_1, \, \gamma_i &= \\ M \, |N_1^{-1}|_{m_1} / m_1 \, m_i, \text{ for } i &= 1, \, 2, \, 3, \, \dots, \, N. \text{ The floor} \\ \text{function} & \text{is} & \text{denoted} & \text{by} \end{aligned}$

Theorem 1 provides the mixed radix form of the CRT that converts residue numbers to weighted numbers; it requires modulo mi operations only. The calculation process for each mixed radix α j in Theorem 1 is independent of the others, and thus, the mixed radix coefficients can be computed in a fully parallel manner. With Theorem 1, we can deduce Theorem 2 as follows

Theorem 1, we can deduce Theorem 2 as follows. Theorem 2: For the moduli set {m1, m2, ..., m N-1, m N = 2n}, the value of α N-1 is equal to 2n-1 when the integer X is M/2. α N-1(M/2) is denoted as the value of α N-1 for X = M/2, and it has

$$\alpha_{N-1} \ (\frac{M}{2}) = 2^{n-1} \ (3)$$

Proof: For the moduli set $\{m1, m2. ..m N-1, m N = 2n\}$, we have

$$\frac{M}{2} = m_1 m_2, \dots, m_{N-1}, m_{N-1}, 2^{n-1}$$
 (4)

For i = 1, 2, ..., N - 1, the following function is established:

$$\left|\frac{M}{2}\right|_{m_i} = |2^{n-1} \prod_{i=1}^{N-1} m_i|_{m_i} = 0. \quad (5)$$

With (5), the RNS representation of M/2 is

$$\frac{M}{2} = (0,0,...,0,|m_1m_2,...,m_{N-1},m_{N-1},2^{n-1}|_{2^n}$$

Thus, unfold (2), and we have

$$X = x_{1} + m_{1} |\gamma_{1}x_{1} + \gamma_{2}x_{2}|_{m_{2}} + m_{1}m_{2} \left[\frac{\gamma_{1}x_{1} + \gamma_{2}x_{2} + \gamma_{3}x_{3}}{m_{2}} \right]_{m_{3}} + m_{1}m_{2}m_{3} \left[\frac{\gamma_{1}x_{1} + \gamma_{2}x_{2} + \gamma_{3}x_{3} + \gamma_{4}x_{4}}{m_{2}} \right]_{m_{3}} + \dots + m_{1}m_{2}\dots m_{N-1} \left[\frac{\gamma_{1}x_{1} + \gamma_{2}x_{2} + \dots + \gamma_{N}x_{N}}{m_{2}m_{3}\dots m_{N-1}} \right]_{m_{N}}$$
(7)

Then, (6) can be substituted in (7), and we have

$$\frac{M}{2} = m_1 m_2 \dots m_{N-1} \left[\frac{\gamma_N x_N}{m_2 m_3 \dots m_{N-1}} \right]_{2^n} (8)$$

By comparison of (4) and (8), we can obtain

$$\alpha_{N-1}(\frac{M}{2}) = \left[\left[\frac{\gamma_N x_N}{m_2 m_3 \dots m_{N-1}} \right] \right]_{2^n} = 2^{n-1}$$
(9)

Theorem 3: In the moduli set $\{m1, m2, ..., mN-1, mN = 2n\}$, for a residue representative number (x1, x2, ..., xN), $\alpha N-1$ is

 $\alpha_{N-1} = \left[\left[\frac{\gamma_1 x_1 + \gamma_2 x_2 + \dots + \gamma_N x_N}{m_2 m_3 \dots m_{N-1}} \right] \right]_{2^n} (10)$

Then the proposed sign detection function is

$$gn(x_1, x_2, \dots, x_N) = \begin{cases} 0, & \text{if } \alpha_{N-1} < 2^{n-1} \\ 1, & \text{if } \alpha_{N-1} \ge 2^{n-1} \end{cases}$$
(11)

Proof: From (2), (8), and (9), in residue representation X < M/2 can be rewritten as

$$x_1 + \sum_{j=1}^{N-1} (\alpha_j \prod_{i=1}^j m_i) < 2^{n-1} \prod_{i=1}^{N-1} m_i$$
(12)

Then, rewrite (12), and we have

$$(\alpha_{N-1} - 2^{n-1}) < -\frac{x_1 + \sum_{j=1}^{N-2} (\alpha_j \prod_{i=1}^{j} m_i)}{\prod_{i=1}^{N-1} m_i} < 0 \quad (13)$$

Thus, the sufficiency of Theorem 3 is established. The necessity of the Theorem 3 proof is presented as follows. With Theorem 1 and because $\alpha j < m j+1$ for j < N - 1, it is easy to verify that

$$x_{1} + \sum_{j=1}^{N-1} (\alpha_{j} \prod_{i=1}^{j} m_{i}) \leq (m_{1} - 1) + \sum_{j=1}^{N-2} ((m_{j+1} - 1) \prod_{i=1}^{j} m_{i}) < \prod_{i=1}^{N-1} m_{i} .$$
(14)

Because the condition $\alpha N-1 < 2n-1$ is established, we can deduce X in residue representation as

- 11 1

- 11 1

$$x_{1} + \sum_{j=1}^{N-1} (\alpha_{j} \prod_{i=1}^{j} m_{i}) < \prod_{i=1}^{N-1} m_{i} + \alpha_{N-1} \prod_{i=1}^{N-1} m_{i}$$

$$\leq \prod_{i=1}^{N-1} m_{i} + (2^{n-1} - 1) \prod_{i=1}^{N-1} m_{i}$$

$$= 2^{n-1} \prod_{i=1}^{N-1} m_{i}$$

$$= \frac{M}{2}$$
(15)

Hence, when $\alpha N-1 < 2n-1$, X < M/2 becomes true.

In summary, with (13) and (15), X < M/2 is true if and only if $\alpha_{N-1} < 2^{n-1}$. Similarly, X < M/2 is true if and only if $\alpha_{N-1} \ge 2^{n-1}$, therefore, Theorem 3 is established.

Theorem 3 provides an efficient sign detection algorithm for moduli set {m1, m2. . . m N-1, m N = 2n} because it consists exclusively of modulo 2n addition and the residue digits can be computed in a fully parallel manner. Analyzing further, from the definitions of γ i in Theorem 1, we can simplify (10) as follows:

$$\begin{split} \mathbf{X} &= \left[\left[\frac{\sum_{i=1}^{N} \gamma_{i} x_{i}}{\prod_{i=1}^{N-1} m_{i}} \right] \right]_{m_{N}} \\ &= \left[\left[\frac{N_{1} \left| N_{i}^{-1} \right|_{m_{1}} - 1}{m_{i} \prod_{i=2}^{N-1} m_{i}} x_{1} + \sum_{i=2}^{N} \frac{M \left| N_{i}^{-1} \right|_{m_{1}}}{m_{1} m_{i} \prod_{j=2}^{N-1} m_{j}} x_{i} \right] \right]_{m_{N}} \end{split}$$

$$= \left[\frac{\left(\prod_{i=1}^{N} m_{i}\right) |N_{1}^{-1}|_{m_{1}} - 1}{\prod_{i=2}^{N-1} m_{i}} x_{1} + \sum_{i=2}^{N} \frac{m_{N} |N_{i}^{-1}|_{m_{i}}}{m_{i}} x_{i} \right]_{m_{N}}$$
$$= \left[\sum_{i=1}^{N} \frac{m_{N} |N_{i}^{-1}|_{m_{i}}}{m_{i}} x_{i} - \frac{1}{\prod_{i=1}^{N-1} m_{i}} x_{1} \right]_{2^{n}}$$
(16)

Based on Theorem 3, the sign output is the MSB of $\alpha N-1$. Therefore, the summation of the last level of (16) needs only one carry generation circuit to obtain the n-th bit of $\alpha N-1$.

SIGN DETECTION FOR THE MODULI SET

In this section, a high-efficiency sign detection unit for the moduli set $\{2n+1 - 1, 2n - 1, 2n\}$ is presented. The sign detection unit is concurrent and suitable for VLSI implementation based on the proposed sign detection algorithm.

Theorem 4: For the moduli set $\{2n+1 - 1, 2n - 1, 2n\}$, the sign detection of X = (x1, x2, x3) is

$$sgn(x_1, x_2, x_3) = MSB\left(\left|\left|-2x_1 + x_2 + x_3 + \frac{x_2 - x_1}{2^{n} - 1}\right|\right|_{2^n}\right)$$
(17)

Proof: For the moduli set $\{2n+1-1, 2n-1, 2n\}$, let m1 =2n+1-1, m2 = 2n - 1, and m3 = 2n. With Theorem 1, the multiplicative inverses of the moduli set can be obtained from

$$|N_1 \cdot N_1^{-1}|_{m_1} = |(2^n - 1) \cdot 2^n \cdot (-4)|_{2^{n+1} - 1} = 1 \quad (18)$$

$$|N_2 \cdot N_2^{-1}|_{m_2} = |(2^{n+1} - 1) \cdot 2^n \cdot 1|_{2^{n-1} - 1} = 1 \quad (19)$$

$$|N_3 \cdot N_3^{-1}|_{m_3} = |(2^{n+1} - 1) \cdot (2^n - 1) \cdot 1|_{2^n} = 1 \quad (20)$$

Then, we substitute these expressions into (16) to achieve

$$\alpha_{2} = \left\| \frac{2^{n}(2^{n+1}-1-4)}{2^{n+1}-1} x_{1} + \frac{2^{n} \cdot 1}{2^{n}-1} x_{2} + \frac{2^{n} \cdot 1}{2^{n}} x_{3} - \frac{1}{(2^{n+1}-1)(2^{n}-1)} x_{1} \right\|_{2^{n}}$$

$$= \left\| (2^{n}-2)x_{1} - \frac{2}{2^{n+1}-1} x_{1} + x_{2} + -\frac{1}{(2^{n}-1)} x_{2} + x_{3} - \frac{1}{(2^{n+1}-1)(2^{n}-1)} \right\|_{2^{n}}$$

$$= \left\| \left| -2x_{1} + x_{2} + x_{3} + \frac{1}{2^{n}-1} x_{2} - \frac{2(2^{n}-1)+1}{(2^{n+1}-1)(2^{n}-1)} x_{1} \right\|_{2^{n}}$$



Figure 1: Sign detection unit for the moduli set $\{2n+1 - 1, 2n - 1, 2n\}$



Figure 2: Blocks of the carry generation unit and comparator unit.

According to (9), the MSB of $\alpha 2$ can be viewed as the sign output, and thus, (17) is established. ______ In binary representation, the words x1, x2, and x3 are n + 1, n and n bits, respectively. We denote x1,n as the n + 1th bit of x1, and denote x1 as the least n bits of x1. Because the word x1

is with one more bit than x2, the floor of the fractional part

$$\left| \left| \frac{x_2 - x_1}{2^n - 1} \right| \right|_{2^n} = \left| \left| \frac{x_2 - x_1 - x_n n}{2^n - 1} \right| \right|_{2^n} \quad (22)$$

of (21) can be transformed as

We rewrite (22) in a new form that is more easily implemented in circuit design

$$\left\| \left| \frac{x_2 - x_1}{2^n - 1} \right| \right\|_{2^n} = -x_{1,n} - \overline{W} \quad (23)$$

W in (23) is ones complement of W, which is defined as

$$W = 1 - \overline{W} = 1 + \left\lfloor \frac{x_2 - x_1^{'} - x_n, n}{2^n - 1} \right\rfloor$$

$$= \begin{cases} 0, & if x_1, n = 0 \text{ and } x_2 < x'_{1,n} = 1 \text{ and } x_2 \le x'_1 \\ 1, & if x_1, n = 0 \text{ and } x_2 < x'_{1,n} = 1 \text{ and } x_2 \le x'_1 \end{cases}$$
(24)

Then, we denote x1 as a n-bit digit that equals 2x1,n-2:0 + x1,n, which is concatenated by the least n-1 bits of x1 and x1,n. Therefore, (21) can be rewritten as

The goal of the carry generation unit and post processing unit is to achieve the nth bit of $\alpha 2 = C + S + W$. The carry generation unit and post processing unit, as shown in Fig. 3, are identical to the CG1 (carry generation unit) and post processing units







Figure 4: Comparator unit for n = 16

The comparator unit is used to set up the comparison of $x_2 > x_1$ and $x_2 = x_1$. Parallel implementation of the least-significant-bit first approach comparison algorithm is

DOI: 10.18535/ijecs/v4i10.21

adopted to implement the comparator unit as shown in Fig. 4. This comparator unit is a carry generation circuit for addition with one input vector being set in ones complement.

the Life Concession			(energie (energie)	A	114
			-		
	-				
The second secon					-11
		-			

5. SIMULATION RESULTS



Figure 5: CARRY GENERATION UNIT

the late interaction of	-			_			and the second second
			- 11973 		1		
		A. (2010)					
all land on the second		n an	.00				
					-		
0.5	0		16.14	-		18	

Figure 6: CARRY SAVE BLOCK



Figure 7: COMPARATOR UNIT

Figure 8: TOP SIGN DETECTION 16



Figure 9: TOP SIGN DETECTION 32

Real Property lies	100				
1	-			-	
	_				
		Concession of the local distance of the loca			
		119	11 C		
	ange få ster derer, og	a second for the second second			
and the second				-	
	-				

Figure 10: TOP SIGN DETECTION 8

6. CONCLUSION

In this brief, a fast sign detection algorithm is presented for restricted moduli set including the modulo 2n. The proposed algorithm allows for parallel implementation and consists exclusively of modulo 2n additions. A sign detection unit for the moduli set $\{2n+1 - 1, 2n - 1, 2n\}$ is proposed based on the proposed sign detection algorithm. The experimental results demonstrate that the proposed circuit achieves significant improvements in terms of area, delay, and power.

REFERENCES

[1] N. Szabo, "Sign detection in nonredundant residue systems," IRE Trans. Electron. Comput., vol. EC-11, no. 4, pp. 494–500, Aug. 1962.

[2] Z. Ulman, "Sign detection and implicit-explicit conversion of numbers in residue arithmetic," IEEE Trans. Comput., vol. 32, no. 6, pp. 590–594, Jun. 1983.

[3] T. V. Vu, "Efficient implementations of the Chinese remainder theorem for sign detection and residue decoding," IEEE Trans. Comput., vol. 34, no. 7, pp. 646–651, Jul. 1985.

[4] E. Al-Radadi and P. Siy, "RNS sign detector based on Chinese remainder theorem II (CRT II)," Comput. Math. Appl., vol. 46, nos. 10–11, pp. 1559–1570, 2003.

[5] M. Akkal and P. Siy, "Optimum RNS sign detection algorithm using MRC-II with special moduli set," J. Syst. Arch., vol. 54, no. 10, pp. 911–918, Oct. 2008.

[6] T. Tomczak, "Fast sign detection for RNS $\{2n - 1, 2n, 2n + 1\}$," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 55, no. 6, pp. 1502–1511, Jul. 2008.

[7] P. Mohan, "RNS-to-binary converter for a new threemoduli set $\{2n+1 - 1, 2n, 2n - 1\}$," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 54, no. 9, pp. 775–779, Sep. 2007.

[8] S. Bi and W. Gross, "The mixed-radix Chinese remainder theorem and its applications to residue comparison," IEEE Trans. Comput., vol. 57, no. 12, pp. 1624–1632, Dec. 2008.

[9] S. Piestrak, "Design of residue generators and multioperand modular adders using carry-save adders," IEEE Trans. Comput., vol. 43, no. 1, pp. 68–77, Jan. 1994.

[10] R. Zimmermann, "Efficient VLSI implementation of modulo $(2n \pm 1)$ addition and multiplication," in Proc. 14th IEEE Symp. Comput. Arithmetic, 1999, pp. 158–167.

[11] K. Furuya, "Design methodologies of comparators based on parallel hardware algorithms," in Proc. 10th ISCIT, Oct. 2010, pp. 591–596.