ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Efficient Fast Sign Detection Algorithm for the RNS Moduli Set

N.Nagender Patel
M.Tech,
VLSI System Design,
GNIT JNT University, Hyd.
Nagender89@gmail.com

Dr.N.Srinivas
Professor,
GNIT JNT University, Hyd.
nsrinivas.gnit@gmail.com

Dr.M.Narendra Kumar
Vice Principal,
GNIT JNT University, Hyd.
Narendrskumar_maddargi@yahoo.com

Dr.S.Sreenatha Reddy
Principal,
GNIT JNT University, Hyd.
Sreenath_sakkamm@yahoo.com

Abstract:

This brief presents a fast sign detection algorithm for the residue number system moduli set $\{2^{n+1}-1, 2^n-1, 2^n\}$. 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 $\{2^{n+1}-1, 2^n-1, 2^n\}$ 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. The experimental results demonstrate that the proposed circuit unit 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 algorithms.

Keywords:

Residue Number System (RNS),Chinese Reminder Theorem (CRT),Moduli Set {2n+1 -1, 2n -1,2n }.

INTRODUCTION:

Residue Number System is an unconventional system. In this system, an integer X is represented by its reminder modulo a number of different bases. The Residue Number System (RNS) is a non-positional number system that has been invented in order to decompose certain operations on large integers into sets of operations on small numbers. The simplicity of such RNS operations as addition, subtraction and multiplication is offset by the difficult realization of scaling, division, sign detection, magnitude comparison and overflow detection. Hence the RNS can be advantageous for the realization of these algorithms where the operations of the first group dominate. To such algorithms belong those of the digital signal processing such as the Finite Impulse Response (FIR) and the Fast Fourier Transform (FFT). Here examining sign of the residue number system. This sign detection problem has been investigated by many researchers, and derived general theorem for sign detection of RNS[2]. Selected class of sign detection carried as a sum modulo 2of digits in associated mixed radix system(MRS) in [3] .The modulo operations of sign detection bounded by size √M. Here sign detection algorithm is presented for restricted moduli set {2n+1 -1,2n -1,2n}. First sign algorithm for only modulo 2n in the RNS. Our new sign detection consists of carry save adder, comparator and carry generation unit. The new Chinese reminder theorem used to sign detected here[5].This algorithm uses nth mixed radix conversion (MRC) for sign detection[6].This sign detection method only applicable for moduli set, {2n+1 - 1,2n -1,2n}. The proposed sign detection method is better than on area and delay by comparing existing methods.

I. RELATED WORK:

The standard RNS case positive integers in the range [0,M).Implicit signed number system split positive half of range and negative half of the range. A. RNS representation An RNS is defined by a set of relatively prime integers called the moduli. The moduli-set is denoted as {m1,m2,…mn} where mi is the ithmodulus. Each integer X can be represented as a set of smaller integers called theresidues. The residue-set is denoted as { r1,r2….rn}where ri is the ithresidue. The residue ri is defined as the least positive remainder when X is divided by the modulus mi. This relation can be notationally written based on the congruence:

$$X \bmod mi = ri \quad (1) \qquad (1)$$

The same congruence can be written in an alternative notation as:

$$|X|mi = ri \quad (2) \qquad (2)$$

The RNS is capable of uniquely representing all integers that lie in its dynamic range. The dynamic

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

range is determined by the moduli-set { m1,m2...mn} and denoted as M where:

$$M=\prod_{i=1}^{n} mi \qquad (3)$$

The RNS provides unique representation for all integers in the range between 0 and M-1 . If the integer X is greater than M-1 , the RNS representation repeats itself. Therefore, more thanone integer might have the same residue representation. It is important to emphasize that the moduli have to be relatively prime to be able to exploit the full dynamic range . Converting from residue to weighted number, X in the interval [0,M/2) carries implicit representation of the sign of the actual result Y,

$$Y=\begin{cases} X, if\ 0 \le X \frac{M}{2} \\ X-m, if \frac{M}{2} \le X < M \end{cases} \qquad (4)$$

Theorem I:

Given { m1, m2, ….., mn}, the magnitude of the residue number x = (x1,x2,…..,Xn) is calculated as follows:

$$X=\sum_{j=1}^{N-2}(\alpha_{j+1}\prod_{i=1}^{j+1} mi, +\alpha 1 m1+\alpha 0 \qquad (5)$$

II. EXISTING CONCEPT:

Sign detection plays an essential role in branching operations, magnitude comparisons, and overflow detection. Because the sign information is concealed in each residue digit in a residue number system (RNS), sign detection in an RNS is more difficult than that in the weighted number system, in which the sign is the most significant bit (MSB).Furthermore, sign detection in an RNS is not as efficient as modular operations, such as addition, subtraction, and multiplication, because of its complexity.

III. ALGORITHM DEFINITION:

A sign detection algorithm for the restricted moduli set is described. The new algorithm allows for parallel implementation and consists exclusively of modulo 2^nadditions**.**

IV. DRAWBACKS:

- Sign detection in an RNS is not as efficient
- More Complexity
- Area & Delay Increased

V. PROPOSED SIGN DETECTION METHOD:

A standard RNS is defined exclusively for positive integers, for negative integers, signed numbers are divided into positive half of the range and negative half of the range. To detect overflow in moduli set {2n+1 -1, 2n -1, 2n }, we distribute the numbers in dynamic representation range M into several groups. Proposed sign detection unit is based on following properties namely:

Property 1:

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

$$X=\sum_{j=0}^{N-1}(\propto j+1\prod_{i=1}^{j+1} mi)+\alpha_1 m_{1+}\ \alpha_0 \qquad (1)$$

Property 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 αj in property 1 is independent of the others, and thus, the mixed radix coefficients can be computed in a fully parallel manner. And also this property explains about multiplicative inverse. With property 1, we can deduce property 2 as follows.

Property 2:

For the moduli set {m1,m2, . . . ,mN−1,mN = 2 n }, the value of αN−1 is equal to 2 n-1 when the integer X is M/2. αN−1(M/2) is denoted as the value of αN−1 for X = M/2,

$$\alpha_{N-1}(M/2)= 2^n-1 \qquad (2)$$

Proof:

For the moduli set {m1,m2, . .,mN−1,mN = 2n }, we have

M/2= m1m2… mN−1mN/2= m1m2 ..mN−1. 2 n −1 **(3)**

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

By substituting the values, m/2 can be obtained by

M/2= m1m2 . . .mN−1 | yN xN/m2m3 · · · mN−1 | 2 n (4)

when comparing (3) and (4).

αN-1 (M/2)= | yNxN/m2m3.....mN-1 | 2 n =2n-1 (5)

Property 3:

In the moduli set {m1,m2, . . . ,mN−1,mN = 2 n }, for a residue representative number (x1, x2, . . . , xN), αN−1 is

$$\alpha_{N-1} = \left| y_1x_1 + y_2x_2 + \ldots\ldots + y_Nx_N / m_2m_3\ldots\ldots m_{N-1} \right|_{2^n} \quad (6)$$

Then the proposed sign detection function is

$$\text{sgn}(x_1, x_2, \ldots, x_N) = \begin{cases} 0, & \text{if } \alpha_{N-1} < 2^n - 1 \\ 1, & \text{if } \alpha_{N-1} \geq 2^n - 1 \end{cases}$$

This property 3 provides an efficient sign detection algorithm for moduli set {m1,m2, . ,mN−1,mN =2 n } because it consists exclusively of modulo 2n addition and the residue digits can be computed in a fully parallel manner. Based on property 3, the sign output is the MSB of αN−1

VI. SIGN DETECTION FOR THE MODULI SET {2 n+1 − 1, 2 n − 1, 2 n}:

In this section, a high-efficiency sign detection unit for the moduli set {2 n+1 − 1, 2 n − 1, 2 n } is presented. The sign detection unit is concurrent and suitable for VLSI implementation based on the proposed sign detection algorithm. Based on above three property a new property is derived for the moduli set {2 n+1 − 1, 2 n − 1, 2 n }.

Property 4:

For the moduli set {2n+1 − 1, 2n − 1, 2n}, the sign detection of X = (x1, x2, x3) is

Sgn(x1,x2,x3) =MSB (| -2x1+x2+x3+(x2-x1/2n -1) | 2 n) (7)

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

$$|N_1 \cdot N^{-1}_1|m_1 = |(2^n - 1) \cdot 2^n \cdot (-4)|_{2^{n+1}-1} = 1 \quad (8)$$

$$|N_2 \cdot N^{-1}_2|m_2 = |(2^{n+1} - 1) \cdot 2^n \cdot 1|_{2^n-1} = 1 \quad (9)$$

$$|N_3 \cdot N^{-1}_3|m_3 = |(2^{n+1} - 1) \cdot (2^n - 1) \cdot 1|_{2^n} = 1 \quad (10)$$

Thus, we have |N −1 1|2 n+1 −1= |−4| 2 n+1 −1, |N −1 2|2 n −1 = 1 and |N −1 3|2 n = 1, by substituting these values we get α2 =(| -2x1+x2+x3+(x2-x1/2n -1) | 2 n

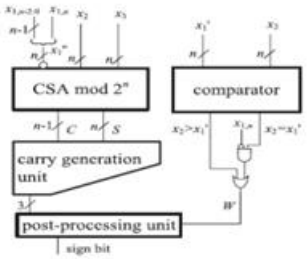

Fig.1. sign detection unit for the moduli set {2^{n+1} − 1, 2^n − 1, 2}

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.

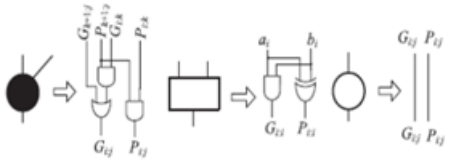

Fig.2. Block of the carry generation unit and comparator unit

The hardware implementation of for the MSB sign detection is shown in Fig. 1. The circuit comprises four main blocks: The CSA, carry generation unit, comparator, and final post processing unit. In Fig. 1, the CSA mod 2 n is used to implement the sum of n bit inputs and will get two n-bit vectors sum S and carry C. The goal of the carry generation unit and post processing unit is to achieve the nth bit which is 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 . The blocks of the carry generation unit and comparator unit are shown in Fig. 2.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

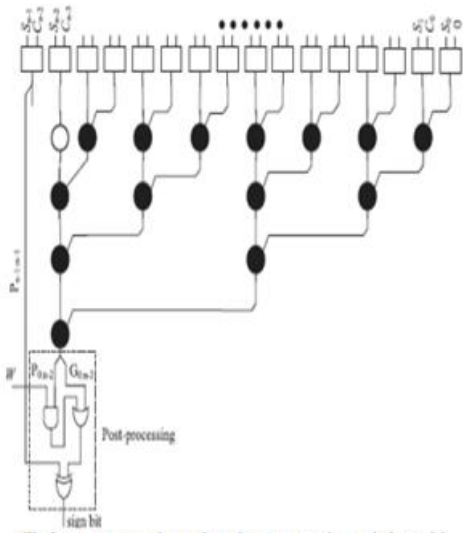

Fig.3. carry generation unit and post processing unit for n=16

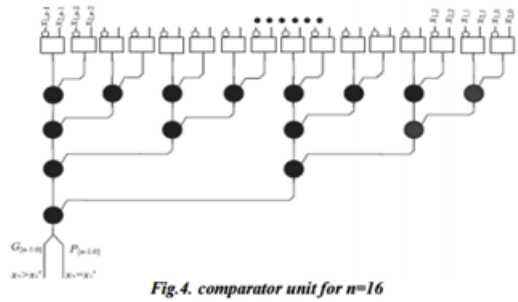

Fig.4. comparator unit for n=16

The comparator unit is used to set up the comparison of x2 > x1‖ and x2 = x1‖. Parallel implementation of the least-significant-bit first approach comparison algorithm is 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.

VII. PERFORMANCE EVALUATION:

In this section, the performance of the proposed sign detection unit of the moduli set {2 n+1 − 1, 2 n − 1, 2 n} is evaluated. The sign detection unit is compared with two units extended by two best sign detection algorithms to demonstrate the high efficiency of the new sign detection algorithm.

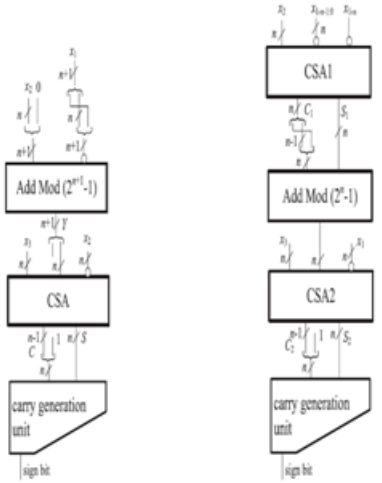

Fig. 5. (a) Sign detection unit for RNS {2n+1 −1, 2n −1, 2n} (b) Sign detection unit for RNS {2n+1 − 1, 2n − 1, 2n }

The proposed unit is the first dedicated to the moduli set {2 n+1 − 1, 2 n − 1, 2 n } sign detection circuit. We chose the sign detection algorithms presented in [5] and [6] to develop two efficient sign detection units for the moduli set {2 n+1 − 1, 2 n − 1, 2 n } and compare them with our circuit. From [5], we optimize the sign detection circuit for the moduli set {2 n+1 − 1, 2 n − 1, 2 n } as follows. With the sign detection algorithm from [5], we can obtain the sign detection by using two-level calculations of the residue representation X = (x1, x2, x3) of the moduli set {2 n+1 −1, 2 n −1, 2 n } as X12 = (x1, x2) for {2 n+1 −1, 2 n −1, 2 n } and X = (X12, x3) for {2 n+1 −1, 2 n −1, 2 n }.

According to the algorithm in [6], L(x) < 2n−1 is established if and only if X < M/2, X is positive. L(x) > 2n−1 is established if and only if X > M/2, X is negative. Thus, the nth bit of the L(x) can serve as the sign bit. Fig. 5(a) shows the architecture of the sign detection unit for the moduli set {2 n+1 − 1, 2 n − 1, 2 n } based on [5]. In Fig. 5(a), the sign detection unit for the moduli set {2 n+1 - 1, 2 n − 1, 2 n } based on [5] consists mainly of three blocks: the mod (2 n+1 −1) adder, CSA unit, and carry generation unit. The area and delay of the sign detection unit based on [5] are

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

$A_E = A_{mod} + A_{CSA} + A_{CG} = 1.5(n+1)\log_2(n+1) + 20n + 2$ $T_E = T_{mod} + T_{CSA} + T_{CG} = 4\log_2(n) + 13$.

For a more realistic comparison, the three sign detection units for the moduli set {2 n+1 −1, 2 n −1, 2 n } were implemented using static CMOS VLSI technology. At first, we used the VHDL language to generate hardware models for the proposed unit and the sign detection units based on [5] and [6] for the moduli set {2 n+1 −1, 2 n −1, 2 n }. The delay in our proposed unit is equal to the sum of the delays of the one-level CSA, n-bit prefix adder and two additional logic levels. In contrast, the delay of the sign detection unit based on [5] is equal to the sum of the delays of one modulo 2 n+1−1 adder, one-level CSA, n-bit prefix adder and two additional logic levels. The delay of the sign detection unit based on [6] is equal to the sum of the delays of one modulo 2n − 1 adder, two levels CSA, n-bit prefix adder and two additional logic levels. The total area of our proposed unit is n full adders and two n-bit wide prefix carry propagation circuits. In contrast, the area of the sign detection unit based on [4] is n full adders, one modulo 2 n+1 − 1 adder and one n-bit wide prefix carry propagation circuit. The area of the sign detection unit based on [6] is n + 1 full adders, n − 1 half adders, one modulo 2n −1 adder and one n bit wide prefix carry propagation circuit.

VIII. RESULTS:

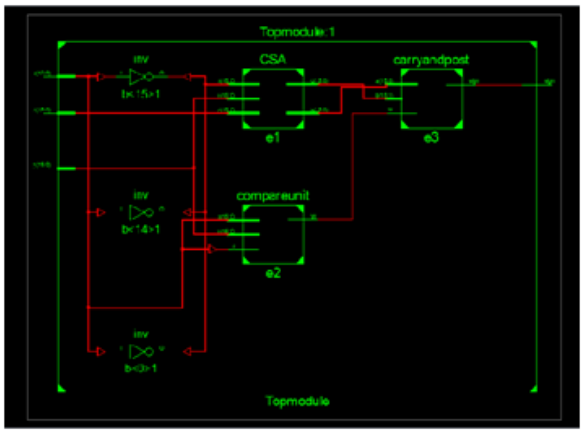

Fig 6. RTL Schametic

Fig 7. Timing analysis

IX. ADVANTAGES:

- Sign detection in an RNS is as efficient
- Less Complexity
- Area & Delay Decreased

X. APPLICATIONS:

- Pseudorandom number
- Generation and cryptography
- Digital Computer & Arithmetic High-Speed Systems.

XI. FUTURE ENHANCEMENT:

We will design existing and proposed system 16 bit. This two system compare proposed system is better because proposed system is takes less area and delay. So, our modification proposed system same concept but increase the bit size.

XII. CONCLUSION

In this brief an efficient fast sign detection algorithm for the residue number system moduli set {2 n+1 -1, 2n -1,2n } is presented. The proposed algorithm allows parallel implementation and include modulo 2n additions. Based on existing sign detection algorithm, an efficient sign detection algorithm is proposed. The sign detection unit can be implemented using one carry save adder, one comparator and one prefix adder. Here efficiency achieved is better than other algorithm for sign detection.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

REFERENCES:

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

[2] A. Baraniecka and G. A. Jullien, ―On decoding techniques for residue number system realizations of digital signal processing hardware,‖ IEEE Trans. Circuits Syst., vol. CAS-25, no. 11, pp. 935–936, Nov. 1978.

[3] T. V. Vu, ―Efficient implementations of the Chinese Remainder Theorem for sign detection and residue decoding,‖ IEEE Trans. Comput., vol. C-34, no. 7, pp. 646–651, Jul. 1985.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] P. Mohan, ―RNS-to-binary converter for a new three-moduli set {2n+1 − 1, 2n, 2n − 1},‖ IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 54, no. 9, pp. 775–779, Sep. 2007.