Scientific Journal Impact Factor (SJIF): 1.711

IJMTER International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

RNS Moduli Set $\{2^{n+1}-1, 2^n-1, 2^n\}$ Implementation Based on Fast Sign Detection Algorithm

Prabu Venkateswaran S[1] Divyarajalakshmi M[2]

[1]Assistant Professor, [2]PG Scholar (VLSI Design)

Department of Electronics and Communication Engineering, SNS College of Technology, Coimbatore, Tamil Nadu, INDIA

Abstract— An efficient fast sign detection algorithm for the residue number system moduli set $\{2^{n+1}-1, 2^n-1, 2^n\}$ is presented. Initially the restricted moduli set including modulo 2^n in the RNS are presented. The proposed algorithm which allows parallel implementation and include modulo 2^n additions. Based on existing sign detection algorithm, an efficient sign detection algorithm for the moduli set $\{2^{n+1}-1, 2^n-1, 2^n\}$ is proposed. The sign detection unit can be implemented using a carry save adder, a comparator, carry generation unit with a post processing unit.

Index Terms— Residue number system, sign detection, moduli set $\{2^{n+1}-1, 2^n-1, 2^n\}$

I. INTRODUCTION

The residue representation of numbers can perform arithmetic operations such as addition, subtraction, and multiplication in parallel manner, without depending a carry from one residue "digit" to another. The "carry-free" property of residue number system makes the learning of residue number systems (RNS) attractive from the point of view of high speed arithmetic unit design. The disadvantage of RNS is that the operation of sign detection and the related operations of division and magnitude comparison. Because the sign information is concealed in each residue digit in a residue number system (RNS), detection of sign in an RNS is more complicate than that in the weighted number system, where the sign is the most significant bit (MSB).

The sign detection problem has been investigated by many authors. In a generic approach, it can be realized as a conversion to a weighted number system and comparison with a suitable number, usually equal to 1/2 of RNS range. However, less expensive algorithms are known. In [1], the sign detection function for a selected class of RNS is implemented as a sum modulo 2 of digits in the associated mixed radix system (MRS). Another method is described in [2], where the sign of a number is defined as the most significant bit of a multi operand sum of fractional binary numbers obtained from individual residues. The algorithm devised by authors of [3] uses a base extension to a redundant modulus and requires two multi operand modulo adders and two modulo multipliers. A general theorem is derived by establishing the necessary conditions for sign detection [4]. In [5], a sign detection algorithm based on the new Chinese remainder theorem (CRT) II is presented. The modulo operations in the sign detection algorithm which are bounded by size $\sqrt{M}$. In [6], a sign detection algorithm uses the nth mixed radix digit in mixed-radix conversion (MRC) to detect the sign function. To date, [7] is the only brief to use the combinational logic to implement a sign detection algorithm based on $\{2^n-1, 2^n-1, 2^n\}$. However, the method cannot be extended to other moduli sets.

The moduli set $\{2^{n+1}-1, 2^n-1, 2^n\}$, only including the types of 2^n and 2^n-1, has been researched extensively in recent years because of its efficiency for modulo operations and reverse conversion [5]. In this brief, a sign detection algorithm is presented for the moduli set $\{2^{n+1}-1, 2^n-1, 2^n\}$. First, a sign detection algorithm is presented for the restricted moduli set including modulo 2^n in the RNS. The proposed sign detection algorithm requires only the addition of modulo 2^n. Then, a new sign detection unit is developed for the moduli set $\{2^{n+1}-1, 2^n-1, 2^n\}$ based on the proposed sign detection This unit only consists of a carry save adder (CSA), a comparator, and a carry generation unit with post processing unit.

This brief organised as follow, Section II describes the proposed sign detection algorithm. Section III presents the sign detection unit for the moduli set $\{2^{n+1}-1, 2^n-1, 2^n\}$. The achieved efficiency is better than that of other methods and based on [5] and [6]

II. 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 $\{2^{n+1}-1, 2^n-1, 2^n\}$, 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 m_i operations only. The calculation process for each mixed radix α_j 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 $\{m_1,m_2, . . . ,m_{N-1},m_N = 2^n\}$, the value of α_{N-1} is equal to 2^{n-1} when the integer X is M/2. $\alpha_{N-1}(M/2)$ is denoted as the value of α_{N-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

$$M/2= m_1m_2\ldots m_{N-1}m_{N/2}= m_1m_2 ..m_{N-1}.\ 2^n-1 \qquad (3)$$

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

$$M/2= m_1m_2 . . .m_{N-1}\left| y_N\ x_N/m_2m_3 \cdot \quad \cdot \quad \cdot\ m_{N-1}\right|_{2^n} (4)$$

when comparing (3) and (4).

$$\alpha_{N-1}\ (M/2)=\left|\ y_Nx_N/m_2m_3 ......m_{N-1}\right|_{2^n} =2^{n-1} \qquad (5)$$

Property 3:

In the moduli set $\{m_1,m_2, . . . ,m_{N-1},m_N = 2^n\}$, for a residue representative number $(x_1, x_2, . . . , x_N)$, α_{N-1} is

$\alpha_{N-1} = \left| \; y_1x_{1+}\, y_2x_2 + \ldots\ldots + y_Nx_N\, / m_2m_{3\ldots\ldots}m_{N-1} \right|_{2^n}$ (6)

Then the proposed sign detection function is

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

This property 3 provides an efficient sign detection algorithm for moduli set $\{m_1, m_2, \ldots, m_{N-1}, m_N = 2^n\}$ because it consists exclusively of modulo 2^n addition and the residue digits can be computed in a fully parallel manner. Based on property 3, the sign output is the MSB of α_{N-1}

III. 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

$\mathrm{Sgn}(x_1,x_2,x_3) = \mathrm{MSB}\left(\left| -2x_1+x_2+x_3+(x_2-x_1/2^n-1) \right|_{2^n} \right)$ (7)

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

$$|N_1 \cdot N^{-1}{}_1|m_1 = |(2^n - 1)\cdot 2^n \cdot (-4)|_{2^{n+1}-1} = 1 \qquad (8)$$
$$|N_2 \cdot N^{-1}{}_2|m_2 = |(2^{n+1} - 1)\cdot 2^n \cdot 1|_{2^n-1} = 1 \qquad (9)$$
$$|N_3 \cdot N^{-1}{}_3|m_3 = |(2^{n+1} - 1)\cdot (2^n - 1).\, 1|_{2^n} = 1 \qquad (10)$$

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

$\alpha_2 = (\left| -2x_1+x_2+x_3+(x_2-x_1/2^n-1) \right|_{2^n}$

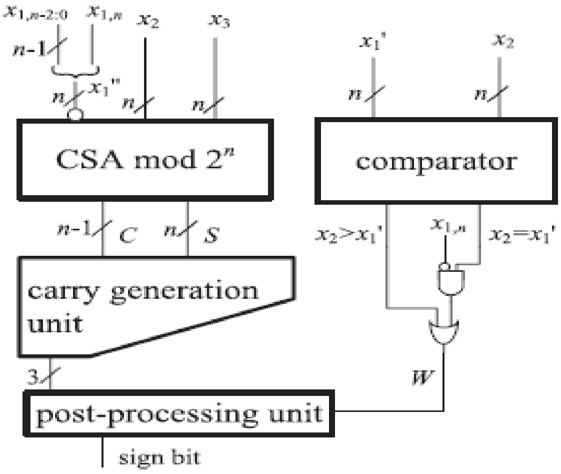

Fig.1. sign detection unit for the moduli set {2^{n+1} – 1, 2^n – 1, 2}

In binary representation, the words x_1, x_2, and x_3 are n + 1, n and n bits, respectively. We denote $x_{1,n}$ as the n + 1th bit of x_1, and denote x_1 as the least n bits of $x_{1.}$

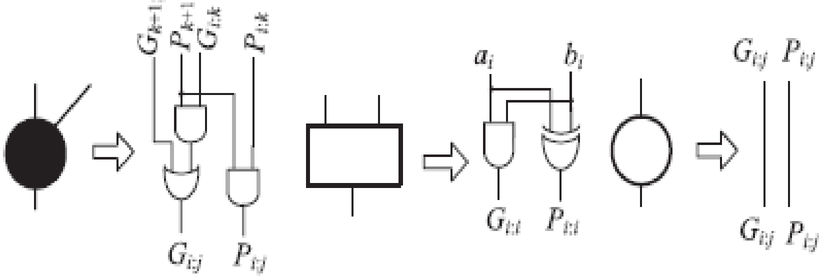

Fig.2. Block of the carry generation unit and comparator unit

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.

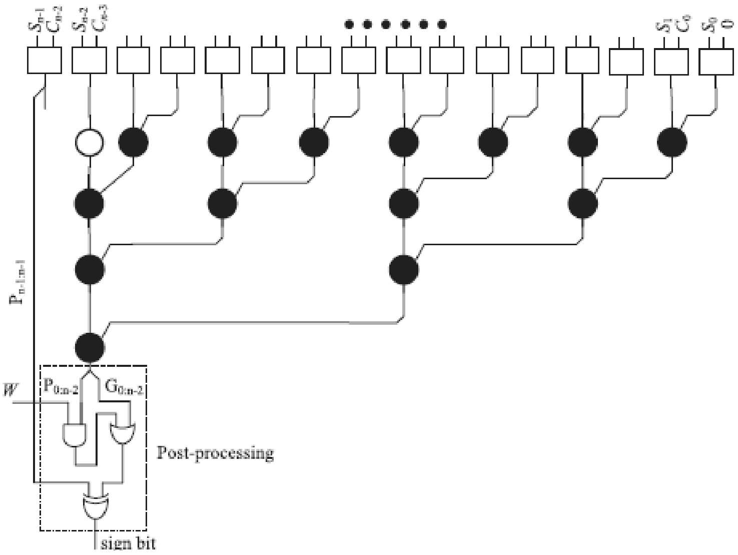

Fig.3. carry generation unit and post processing unit for n=16

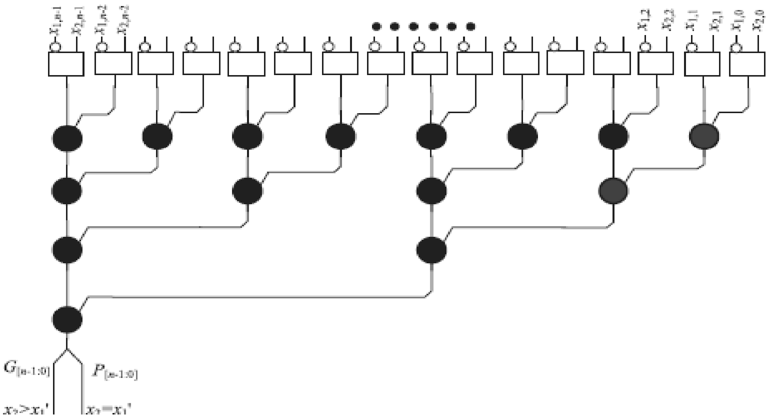

Fig.4. comparator unit for n=16

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.

IV. 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.

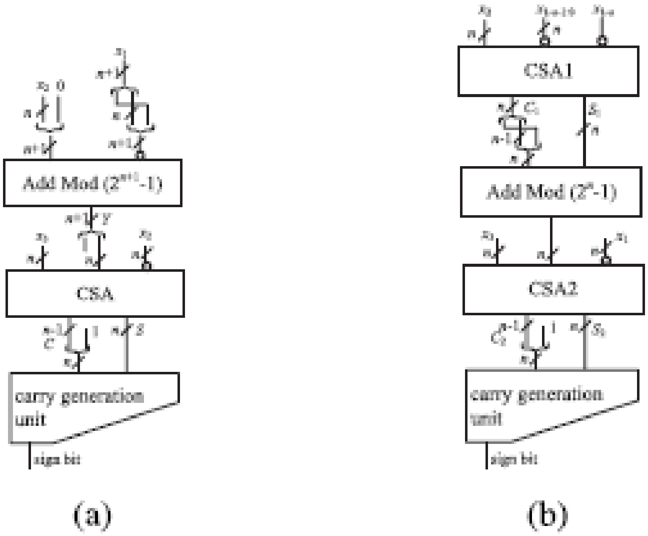

Fig.5. (a) Sign detection unit for RNS $\{2^{n+1} -1, 2^n -1, 2^n\}$ based on [4], (b) Sign detection unit for RNS $\{2^{n+1} - 1, 2^n - 1, 2^n\}$ based on [5].

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 $X = (x_1, x_2, x_3)$ of the moduli set $\{2^{n+1} -1, 2^n -1, 2^n\}$ as $X_{12} = (x_1, x_2)$ for $\{2^{n+1} -1, 2^n -1, 2^n\}$ and $X = (X_{12}, x_3)$ 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. $L(x) \geq 2n-1$ is established if and only if $X \geq M/2$, 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

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

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 $\{2^{n+1} -1, 2^n -1, 2^n\}$.

Table I shows that the area and delay of the proposed sign detection unit are better than those proposed in [5] and [6] for the moduli set $\{2^{n+1}- 1, 2^{n} − 1, 2^{n} \}$.

TABLE 1. COMPARISON OF THE EXPERIMENTAL RESULTS

EXISTING UNITS	n values	AREA (μm^2)	DELAY (ns)	POWER (mW)
[4]	8	421	17.395	47
[5]	8	475	16.007	48
OUR	8	245	6.514	44

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 $2^{n} − 1$ 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 $2^{n}−1$ adder and one n-bit wide prefix carry propagation circuit.

V. CONCLUSION

In this brief an efficient fast sign detection algorithm for the residue number system moduli set $\{2^{n+1}-1, 2^{n}-1,2^{n}\}$ is presented. The proposed algorithm which allows parallel implementation and include modulo 2^{n} 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.

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 {2*n* − 1, 2*n*, 2*n* + 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 {2*n*+1 − 1, 2*n*, 2*n* − 1},” *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 54, no. 9, pp. 775–779, Sep. 2007.

[11] 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.

[12] 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.

[13] R. Zimmermann, “Efficient VLSI implementation of modulo *(*2*n* •} 1*)* addition and multiplication,” in *Proc. 14th IEEE Symp. Comput. Arithmetic*, 1999, pp. 158–167.

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