Journal of Electrical and Computer Engineering Innovations
(JECEI)
Journal homepage: http://www.jecei.sru.ac.ir

Research paper

Fast and Power Efficient Signed/Unsigned RNS Comparator & Sign Detector

***Z. Torabi*[1,*], *A. Belghadr*[2]**

[1]*Faculty of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran.*

[2]*Department of Computer Science and Engineering, Shahid Beheshti University, Tehran, Iran.*

Article Info

Article History:
Received 15 January 2022
Reviewed 15 March 2022
Revised 18 April 2022
Accepted 25 may 2022

Keywords:
Computer arithmetic
Residue number system
Complicated operations
Signed number comparison
Dynamic range partitioning

*Corresponding Author's Email Address: z.torabi@sru.ac.ir

Abstract

Background and Objectives: Residue number system (RNS) is considered as a prominent candidate for high-speed arithmetic applications due to its limited carry propagation, fault tolerance and parallelism in "Addition", "Subtraction", and "Multiplication" operations. Whereas, "Comparison", "Division", "Scaling", "Overflow Detection" and "Sign Detection" are considered as complicated operations in residue number systems, which have also received a surge of attention in a multitude of publications.
Efficient realization of Comparators facilitates other hard-to-implement operations and extends the spectrum of RNS applications. Such comparators can substitute the straightforward method (i.e. converting the comparison operands to binary and comparing them with wide word binary comparators) to compare RNS numbers.
Methods: Dynamic Range Partitioning (DRP) method has shown advantages for comparing unsigned RNS numbers in the 3-moduli sets $\{2^n, 2^n \pm 1\}$ and $\{2^n, 2^n - 1, 2^{n+1} - 1\}$, in comparison with other methods. In this paper, we employed DRP components and designed a unified unit that detects the sign of operands and also compares numbers, for the 5-moduli set $\gamma = \{2^{2n}, 2^n \pm 1, 2^n \pm 3\}$. This unit can be used for comparison of signed and also unsigned RNS numbers in the moduli set γ.
Results: Synthesized comparison results reveal 47% (54%) speed-up, 35% (32%) less area consumption, 25% (24%) lower power dissipation, and 60% (65%) less energy for $n = 8$ (16) in comparison to the straightforward signed comparator.
Conclusion: According to the results of this study, DRP method for sign detection and comparison operations outperforms other methods in different moduli sets including 5-moduli set $\gamma = \{2^{2n}, 2^n \pm 1, 2^n \pm 3\}$.

Introduction

Nowadays, with the increased versatility of electronic products, high-performance computations with low-power consumption are of vital importance. Residue number system has offered the advantage of high-speed and low-power addition, subtraction, and multiplication operations, and thus it has received much attention for high-throughput computations, particularly in digital signal processing [1], data transmission [2], cryptography [3], steganography [4], and image processing [5].

Residue Number System (RNS) is a number system with k integer modulus $\{m_1, m_2, \dots, m_k\}$. A number X is represented as $(x_1, x_2, \dots, x_k)$, where $x_i = |X|_{m_i}$ (i.e., the remainder of integer division $\frac{X}{m_i}$). Cardinality of the residue number system is maximized (i.e., $M = m_1 \times \dots \times m_k$), where the moduli are pair-wise prime. In RNS,

which is an unweighted number system, some arithmetic operations such as division, scaling, comparison and sign/overflow detection are difficult to implement. Whereas, these complicated operations are fundamental to develop processors with practical interest. For example, comparison, sign and overflow detection are essential for some nonlinear procedures, such as median and rank-order filtering [6].

Sign detection is needed in applications dealing with positive and negative numbers. In such cases, dynamic range (i.e., M) is partitioned into two parts of $[0, \lfloor M/2 \rfloor)$ and $[\lfloor M/2 \rfloor, M)$ in order to represent positive and negative numbers, respectively. The straightforward sign detection method in RNS is based on converting the operand to binary format and then comparing it with $\frac{M}{2}$.

Comparison plays a crucial role in the development of division and overflow/sign detection units in RNS, therefore an efficient comparison method would be cost-effective to implement other complicated operations [7]-[9]. Contrary to the parallelism that residue number system offers to the addition and multiplication, no parallel RNS comparison scheme can be envisaged via independent modular comparator in concurrent residue channels. For example, in the moduli set {64,7,9,11,5}, 44352=(0,0,0,0,2) is greater than 6=(6,6,6,6,1), which is not clearly apprehended from their modular representations.

The RNS comparison schemes proposed so far [6], [10]-[16] can be categorized into a conversion-based method [6], [10], [11], [15], parity checking technique [12], [14], and mapping function [13], [16]-[23] that will be described in second Section. For RNS unsigned number comparison in 3-moduli sets, Dynamic Range Partitioning (DRP) method [17] yields the best performance [17], [18]. However, we have not encountered any DRP-based RNS comparator for moduli sets with more than three moduli.

In many RNS applications, domain of numbers is expanded. Utilizing wider moduli and increasing the number of moduli, are two different ways to fulfill the need for expanded range of numbers, while both of them make reverse conversion and complex operations more complicated. However, since the conversion process is not frequent, the burden of a lengthier reverse conversion for moduli sets with more than three moduli is bearable [18]. Several moduli sets with four to eight moduli have been reported in the literature. For example moduli set $\gamma = \{2^{2n}, 2^n \pm 1, 2^n \pm 3\}$ with $6n$-bit dynamic range whereas its signed/unsigned reverse converter have been introduced in [24], [25].

In this paper, we focus on the realization of a DRP-based sign detector and comparator for the moduli set γ. To this aim, we convert the 5-residue operands of γ to an equivalent 3-moduli set $\{2^{2n}, 2^{2n}-1, 2^{2n}-9\}$, where the DRP can be applied. For evaluation of the proposed comparator, we have not found any hardware realization of a comparator for γ, thus, we compare our method with the straightforward comparators [24], [25] and one of the recent previous general comparators [24].

We also compare the proposed sign detection method with the γ-sign-detection unit of [25]. The proposed work has considerable merits on the reference works [24], [25], in terms of latency, area, and power, presented through analytical and synthesized evaluations.

The rest of the paper is organized as follows. The second section reviews briefly different RNS comparison and sign detection methods. In the third section, the new sign detector and signed/unsigned comparator for γ are proposed, while its implementation scrutiny is discussed in the fourth section.

Evaluations are found in the fifth section and finally in the last section we draw our conclusions.

Background Materials and Related Works

In this section, we describe the representation of signed numbers in RNS, sign identification methods, and then review a number of comparison methods briefly.

In RNS, numbers are defined as positive integers in the range between [0, M−1], but in applications with signed numbers, as shown in Fig. 1, dynamic range is divided into two parts, positive and negative numbers. The sign of an RNS number X can be detected by (1).

$$\text{Sign}(X) = \begin{cases} 0 & if \quad 0 \le X < \lfloor M/2 \rfloor \\ 1 & if \quad \lfloor M/2 \rfloor \le X < M \end{cases} \tag{1}$$

Sign(X) usually indicates by the most significant bit (MSB) of X, therefore in fast and low power sign detection methods, before complete conversion of the operand to binary format via mixed radix representation (MRC) [26] or Chinese remainder theorem (CRT) [26], MSB of the operand is extracted.

In [27] and [28], with the usage of last MRC digit, MSB of the operand and consequently sign bit extracted. In [25] a sign detection unit and signed reverse converter is proposed for γ, based on CRT.

A wide variety of techniques have been proposed for RNS comparison in the literature [6], [9]-[23], some of which are summarized in Table 1. Most of the comparison methods compare two unsigned numbers and cannot be easily extended to compare signed RNS numbers due to the complexity of sign detection process.

In conversion-based methods [6], [9]-[11], [15], before full reverse conversion, comparison takes place. Comparing the corresponding MRC digits [26] or New CRT coefficients [29] fall into this category.

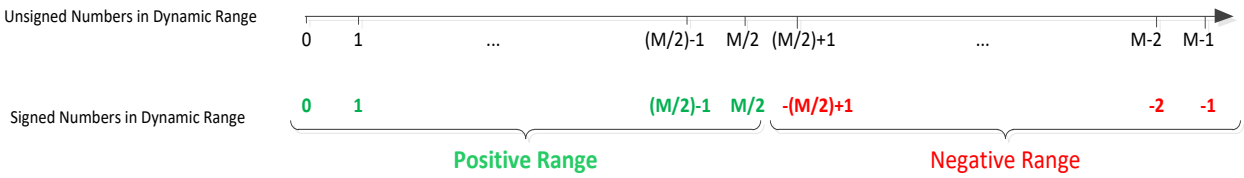

Fig. 1: Distribution of positive and negative numbers in dynamic range.

In parity checking technique [12], comparison is based on the parity of the operands and their difference. One of the major drawbacks of this method is that it is applicable only on moduli sets which do not have even moduli, while in practice numerous moduli sets comprise at least a power-of-two modulo, owing to an efficient arithmetic channel realizations.

In the mapping technique [13], a number is assigned to each RNS number in the dynamic range. For comparing two numbers X and Y, $D(X)$ and $D(Y)$ are compared, such that $D(X) > D(Y)$ leads to $X > Y$. This method, similar to the CRT, is based on a large modulo SQ operation, where $SQ = \sum_{i=1}^{n}(M/m_i)$. Since direct implementation of diagonal function is not efficient for comparing two RNS numbers, some modifications for diagonal function computation were proposed [23], [30]. In [23], $D(X)$ is computed in modulo 2^u, where $u = \log(m_n - 1)SQ$ and m_n is the largest modulo in the moduli set. Although 2^u is smaller than SQ, in comparison to other methods, [23] still needs computation in the large module 2^u.

Efficient computations of diagonal function results in introducing new moduli sets that allow for efficient hardware implementation of $D(X)$. Some algorithms were introduced in [30] to generate 3- and 4- moduli sets in such a way that $SQ = 2^v$ and $SQ = 2^v - 1$, respectively, for some v. In [31], similar to [30], several methods proposed to design moduli sets with SQ forms 2^n, $2^n - 1$, and 2^n+1.

In [16], [19], for implementing non-modular operations including comparison, sign detection, division, and scaling, the authors proposed a method to compute the interval evaluation of $X = (x_1, x_2, \dots, x_k)$. Such computations are performed in limited precision of fractional representation of X.

Ambiguity cases arise when X is very small or big, in such cases MRC digits were used for non-modular operations in this method which leads to sequential computations.

In [20], [21], dynamic range $[0, M)$ is divided into $M_k = m_1 \times m_2 .. \times m_{k-1}$ intervals. With a large amount of computations, the numerical intervals which contain X and Y are determined and after that, comparison can be done by comparing numerical intervals of X and Y.

Minimum-range monotonic core function is proposed in [22] which is a modification of core function [32].

In this solution, comparison of every two number is carried out through comparing their core functions. In [22], core function is monotonic and computed in module M_k. They also show that diagonal function is a special case of core function.

DRP [17], divides the dynamic range of any 3-moduli set into m_1 partitions of size $m_2 \times m_3$, where each partition is divided into m_2 sections of size m_3. For any moduli set $\{m_1, m_2, m_3\}$, DRP components (i.e. $p_1(X)$ and $p_2(X)$), are defined in (2), where $x_{23} = |X|_{m_2 m_3}$, $x_2 = |X|_{m_2}$, $x_3 = |X|_{m_3}$ and $M_1 = m_2 \times m_3$. $p_1(X)$ and $p_2(X)$ are the number of partition and section that are computed for an RNS number X, respectively.

$$\begin{cases} p_1(X) = \left|\left|{M_1}^{-1}\right|_{m_1}(x_1 - x_{23})\right|_{m_1} \\ p_2(X) = \left|\left|{m_3}^{-1}\right|_{m_2}(x_2 - x_3)\right|_{m_2} \end{cases} \quad (2)$$

Comparison of two numbers $X = (x_1, x_2, x_3)$ and $Y = (y_1, y_2, y_3)$ can be reduced to the comparison of $[p_1(X), p_1(Y)]$, $[p_2(X), p_2(Y)]$, $[x_3, y_3]$ in three different comparators.

Sign detection and signed number comparison of [6] for the moduli set $\{2^n - 1, 2^{n+x}, 2^n + 1\}$ are based on an optimized version of the MRC. It performs the comparison through utilizing the sign bits of comparison operands and their difference. In this method, the sign of RNS numbers can be identified by comparing the third MRC digit with 2^{n+k-1}.

Proposed Sign Detector and Comparator

In this section, a new DRP-based method is derived for sign detection and comparing two RNS numbers X and Y. As mentioned earlier, DRP has been utilized in unsigned numbers comparison methods [17], [18]. However, in this paper, DRP is applied to sign identification (Theorem 1) and comparison for the 5-moduli set γ.

The above DRP scheme (2) for 3-moduli RNS comparison can be extended to 5-moduli cases. In fact, the aforementioned 5-moduli set γ, can be reduced to the 3-moduli set $\tau = \{2^{2n}, 2^{2n} - 1, 2^{2n} - 9\}$, where the conjugate moduli $2^n \pm 1$ and $2^n \pm 3$, are combined to moduli $2^{2n} - 1$ and $2^{2n} - 9$ through two simple reverse conversion operations.

Table 1: Comparison of 10 previous RNS comparators

Ref.	Category	Moduli set	Signed / Unsigned numbers	Method
[9]	Reverse conversion	$\{2^n \pm 1, 2^n, m\}$, $m \in \{2^{n+1} \pm 1, 2^{n-1}-1\}$	Unsigned	New CRT
[17]	Mapping function	$\{2^n \pm 1, 2^n\}$	Unsigned	DRP
[18]	Mapping function	$\{2^n-1, 2^n, 2^{n+1}-1\}$	Unsigned	DRP
[10]	Reverse conversion	$\{2^n \pm 1, 2^n\}$	Unsigned	MRC-CRT
[11]	Reverse conversion	Arbitrary moduli set	Unsigned	New CRT
[12]	Parity checking	Odd moduli set	Unsigned	Parity checking
[13], [23]	Mapping function	Arbitrary moduli set	Unsigned	Diagonal mapping
[14]	Parity checking	$\{2^n \pm 1, 2^{n+1} \pm 1\}$	Unsigned	parity checking
[16], [19]	Mapping function	Arbitrary moduli set	Unsigned	floating-point interval evaluation, MRC
[20], [21]	Mapping function	Arbitrary moduli set	Unsigned	interval evaluation
[22]	Mapping function	Arbitrary moduli set	Unsigned	Core function
[6]	Reverse conversion	$\{2^n-1, 2^{n+x}, 2^n+1\}$	Signed	MRC
[15]	Reverse conversion	$\{2^{n+k}, 2^n \pm 1, 2^{n\pm1}-1\}$	Signed	MRC

Therefore the 3-moduli DRP method can be applied to the new 3-moduli set. Here we compute DRP components for the new 3-moduli set τ. Prior to that, the required multiplicative inverses are described as β_1, β_2 and β_3.

Property 1: $\beta_1 = |(2^n+3)^{-1}|_{2^n-3}$

$$= \begin{cases} \frac{2^{n-1}-1}{3} & n = 2k+1 \\ -\frac{2^{n-1}-2}{3} & n = 2k \end{cases}$$

Property 2: $\beta_2 = |(2^{2n}-9)^{-1}|_{2^{2n}-1} = -2^{2n-3}$

Property 3: $\beta_3 = |((2^{2n}-9)(2^{2n}-1))^{-1}|_{2^{2n}}$

$$= \begin{cases} \frac{2^{2n+3}+1}{9} & n = 3p \\ \frac{2^{2n+1}+1}{9} & n = 3p+1 \\ 2^{2n-1} + \frac{2^{2n-1}+1}{9} & n = 3p+2 \end{cases}$$

Let $m_1 = 2^{2n}, m_2 = 2^n-1, m_3 = 2^n+1, m_4 = 2^n-3, m_5 = 2^n+3$ and the corresponding residues of an operand X for the new moduli set τ based on CRT and New CRT be denoted as (x_1, x_{23}, x_{45}) where $x_1 = |X|_{2^{2n}}$, $x_{23} = |X|_{2^{2n}-1} = |x_3 + (2^n+1)2^{n-1}(x_2 - x_3)|_{2^{2n}-1}$ and $x_{45} = |X|_{2^{2n}-9} = x_5 + (2^n+3)\,|\beta_1(x_4 - x_5)|_{2^n-3}$.

In the following Eqns. 3 and 4, we derive $p_2(X)$ and $p_1(X)$ as DRP components in moduli set τ, based on Eqn. set 2, where $x_{2345} = |X|_{(2^{2n}-9)(2^{2n}-1)} = x_{45} + (2^{2n}-9)|(2^{2n}-9)^{-1}(x_{23} - x_{45})|_{2^{2n}-1}$.

$$p_2(X) = |\beta_2(x_{23} - x_{45})|_{2^{2n}-1}$$
$$= |2^{2n-3}(-x_{23} + x_{45})|_{2^{2n}-1} \quad (3)$$

$$p_1(X) = |((2^{2n}-9)(2^{2n}-1))^{-1}(x_1 - x_{2345})|_{2^{2n}}$$
$$= \left|\beta_3\left(x_1 - x_{45} + 9p_2(X)\right)\right|_{2^{2n}} \quad (4)$$

Theorem 1: X in the moduli set γ is negative if and only if $\mathrm{MSB}(p_1(X)) = 1$.

Proof: Based on the DRP method [8], in the moduli set τ we have $X = p_1(X)M_1 + x_{23} = p_1(X)(2^{2n}-1)(2^{2n}-9) + x_{23}$ and $p_1(X) < 2^{2n}$. With consideration of $\frac{M}{2} = 2^{2n-1}(2^{2n}-1)(2^{2n}-9)$, our proof consists of two parts as follows:

a. $(\mathrm{MSB}(p_1(X)) = 1) \Longrightarrow X \geq \frac{M}{2}$

If $MSB(p_1(X)) = 1 \Longrightarrow p_1(X) \geq 2^{2n-1} \Longrightarrow X \geq 2^{2n-1}(2^{2n}-1)(2^{2n}-9) \Longrightarrow X$ is negative.

b. $X \geq \frac{M}{2} \Longrightarrow (\mathrm{MSB}(p_1(X)) = 1)$

let $x_{23} = 2^{2n}-2$ to find the minimum value of $p_1(X)$, where X is negative. The following condition must hold:

$$p_1(X)(2^{2n}-1)(2^{2n}-9) + 2^{2n} - 2 \geq 2^{2n-1}(2^{2n}-1)(2^{2n}-9)$$

which leads to $p_1(X) \geq 2^{2n-1}$ and $MSB\big(p_1(X)\big) = 1$. ■

Therefore by implementing one of the DRP components (i.e., $p_1(X)$), the sign of an RNS number (i.e., $sign(X)$) in the moduli set γ is identified. For comparing two signed RNS numbers, which belong to the same range and both have the same sign (positive or negative), comparing them without considering their signs determines the result. Therefore, for comparing two RNS numbers X and Y, first the signs of operands are identified. If only one of them is positive, the result of comparison is clear, whereas both of them are positive or negative, comparison is undertaken via DRP components (i.e. $p_1(X), p_1(Y), p_2(X)$ and $p_2(Y)$). Comparison can be reduced to the comparison of $p_1(X)$ and $p_1(Y)$. In the case of $p_1(X) = p_1(Y), p_2(X)$ and $p_2(Y)$ are compared. If $p_1(X) = p_1(Y)$ and $p_2(X) = p_2(Y)$, comparison of x_{45} and y_{45} yields the final result. Flowchart of the proposed comparator is illustrated in Fig. 2.

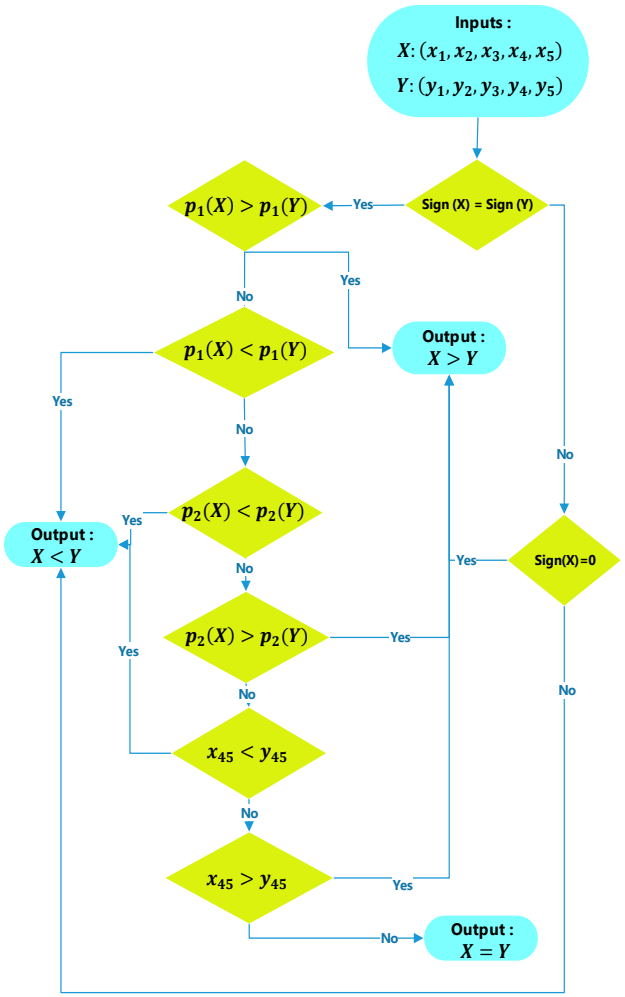

Fig. 2: Algorithm of the proposed comparator.

Since sign detection is performed with $p_1(X)$, and it is also required for comparison, with eliminating first step of Fig. 2 (comparing sign(X) and sign (Y)), it can be used for unsigned comparison. The overall architecture for signed/unsigned comparator is visualized by Fig. 3 where E and C show that $X = Y$ and $X > Y$ respectively.

Example 1. Consider $\gamma = \{256, 15, 17, 13, 19\}$ with $n = 4$. Let $X = 1 = (1,1,1,1)$ and $Y = 1000000 = (64,10,9,1,11)$ be two RNS numbers to be compared. The equivalents of X and Y in the corresponding moduli set $\tau = \{256, 255, 247\}$ are $(1,1,1)$ and $(64,145,144)$ respectively. Based on Eqns. 3 and 4, $p_1(X) = p_2(X) = 0$, $p_1(Y) = 15$ and $p_2(Y) = 223$. According to the Theorem 1 and Fig. 2, both X and Y are positive and $p_1(Y) > p_1(X)$ so $Y > X$.

Implementation

Sign detection and comparator units in the proposed work are based on DRP components, therefore, in this section, we provide the implementation details of $p_1(X)$ and $p_2(X)$ generators. Here with the assumption of $n = 3p + 1$ and usage of the properties 1-3, we investigate implementation-friendly equations for $p_1(X)$ and $p_2(X)$. Computation and implementation of DRP components with $n \neq 3p + 1$ are quite similar.

$$p_1(X) = \left| \frac{2^{2n+1}+1}{9} \left(\begin{matrix} -(2^n+3) \left| \frac{2^{n-1}-1}{3}(x_4 - x_5) \right|_{2^n-3} \\ +x_1 - x_5 + 9\, p_2(X) \end{matrix} \right) \right|_{2^{2n}} \quad (5)$$

$$p_2(X) = \left| 2^{2n-3} \left(\begin{matrix} (2^n+3) \left| \frac{2^{n-1}-1}{3}(x_4 - x_5) \right|_{2^n-3} \\ x_5 - x_3 - (2^n+1)2^{n-1}(x_2 - x_3) \end{matrix} \right) \right|_{2^{2n}-1} \quad (6)$$

Replacing $-x_3 = \overline{x_3} - 2^{n+1} + 1$, $-x_2 = \overline{x_2} - 2^n + 1$, $-x_5 = \overline{x_5} - 2^{n+1} + 1$, $U = \left| \frac{2^{n-1}-1}{3}(x_4 - x_5) \right|_{2^n-3} = \left| \sum_{i=0}^{i=\frac{n-3}{2}} 2^{2i}\,(x_4 + \overline{x_5}) - 5 \times \frac{2^{n-1}-1}{3} \right|_{2^n-3}$ and $-U = \overline{U} - 2^n + 1$ in (5) and (6) result (7) and (8), respectively.

$$p_1(X) = \left| \frac{2^{2n+1}+1}{9}(x_1 + \overline{x_5} + (2^n+3)\overline{U} \right. \left. \begin{matrix} \\ -2^{n+2} + 4) + p_2(X) \end{matrix} \right|_{2^{2n}} \quad (7)$$

$$p_2(\mathrm{X}) = \left| \begin{matrix} 2^{2n-3}x_5 + (2^{n-3} + 3 \times 2^{2n-3})\, U + 2^{2n-3}\overline{x_3} + \\ 2^{2n-3} - 2^{n-2} + (2^{2n-4} + 2^{n-4})(x_3 + \overline{x_2}) \end{matrix} \right|_{2^{2n}-1} \quad (8)$$

One $(n-1,\ 2^n - 3)$ multi operand modular adder (MOMA) [33] followed by an n-bit modular adder is required to generate U expression. Based on (8), after computation of U, $p_2(X)$ is obtained with a two-level CSA followed by a $2n$-bit modular adder. In parallel with $p_2(X)$, $\frac{2^{2n+1}+1}{9}(x_1 + \overline{x_5} + (2^n+3)\overline{U} - 3 \times 2^n + 4)$ is being obtained through a $(2n-4\ ,2^{2n})$ MOMA. The required architecture for generation of $p_1(X)$ and $p_2(X)$ is depicted in Fig. 4.

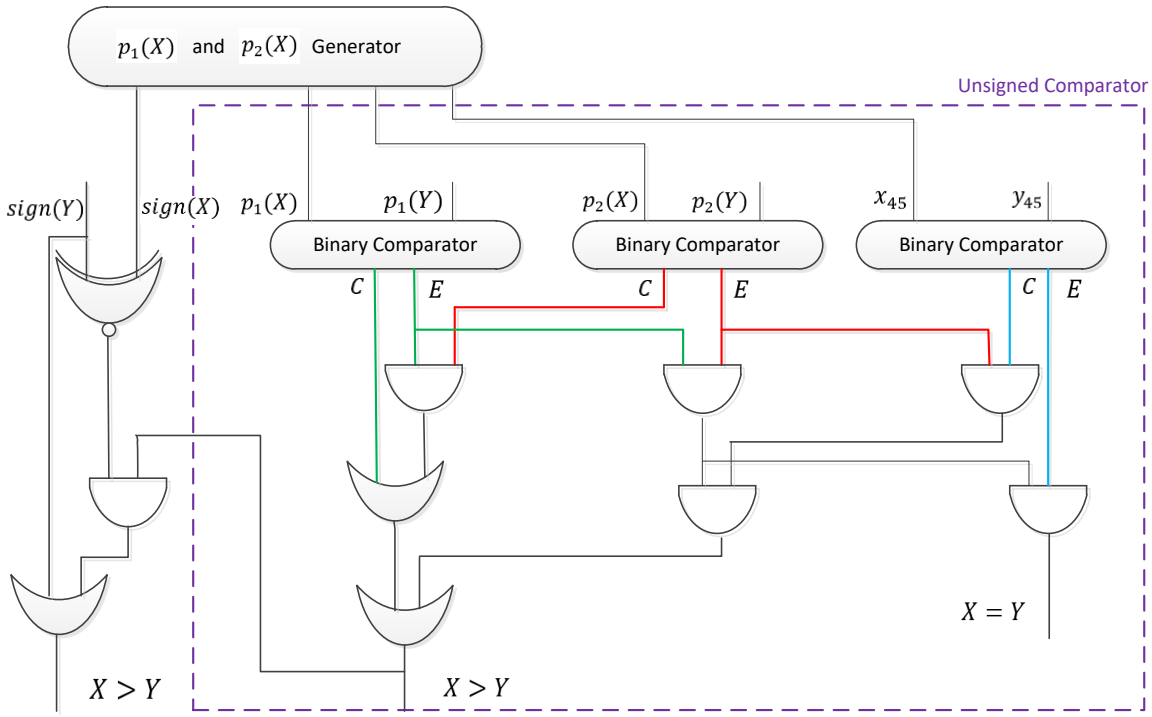

Fig. 3: The proposed signed/unsigned γ −comparator.

Evaluation

In this section, we present the performance evaluation of the proposed design and compare it with previous related works.

The proposed design consists of sign detection module and comparator. In the literature, two reverse converters [24], [25] and one sign identifier [25] designed for moduli set γ.

In [25], a $\gamma -$ signed reverse converter proposed wherein the sign of operand is extracted in the middle of conversion. In the case of negative sign, the output of reverse converter should be added to 2's complement of M.

In [24] a γ −reverse converter proposed which is based on New CRT [27] and the output is positive number in the range $[0\ M)$.

We evaluate the proposed comparator against a straightforward comparator which consists of two reverse converters for converting the operands to binary format and a binary comparator for comparing two operands. Moreover, we evaluate unsigned general comparators of [16], [19]-[23], which are based on mapping function that has recently received attentions in literature.

In addition, we evaluate the proposed sign detection method with sign detection module of [25] and straightforward sign detection method of [24] (i.e., Conversion of operand to binary format and comparing it with $\frac{M}{2}$).

The delay and cost measures of the proposed comparator and sign detector are compiled in Tables 2 and 3, based on the unit gate model [34].

In our analytical evaluations, the cost and delay of one simple 2-input logic gate (e.g., AND, OR, NAND, NOR) are considered as 1 unit of cost ($\#G$) and delay (ΔG). For example, delay and cost of an n-bit carry ripple adder is assumed to be $2n\Delta G$ and $7n\#G$ respectively. The comparators of [28], [29] have less delay in return of extra cost.

Between general comparators described in Tables 2 and 3 (i.e., [16], [19]-[23]), the comparators proposed in [22] and [27] have reasonable delay and cost.

So as to find better insight into merits of the proposed design, we have synthesized the proposed comparator and γ −comparators of [24], [25], and comparator of [22] in case of $n = 8$ and $n = 16$, with the TSMC 90nm CMOS standard logic cell library by Synopsys Design Compiler. Synthesized results are compiled in Table 4 which approve superiority of the proposed comparator in comparison with the reference designs, in terms of delay, area, power and energy.

Based on the results of Table 4, the ratios of delay and power ($n = 8$) of straightforward signed comparator are higher than other methods.

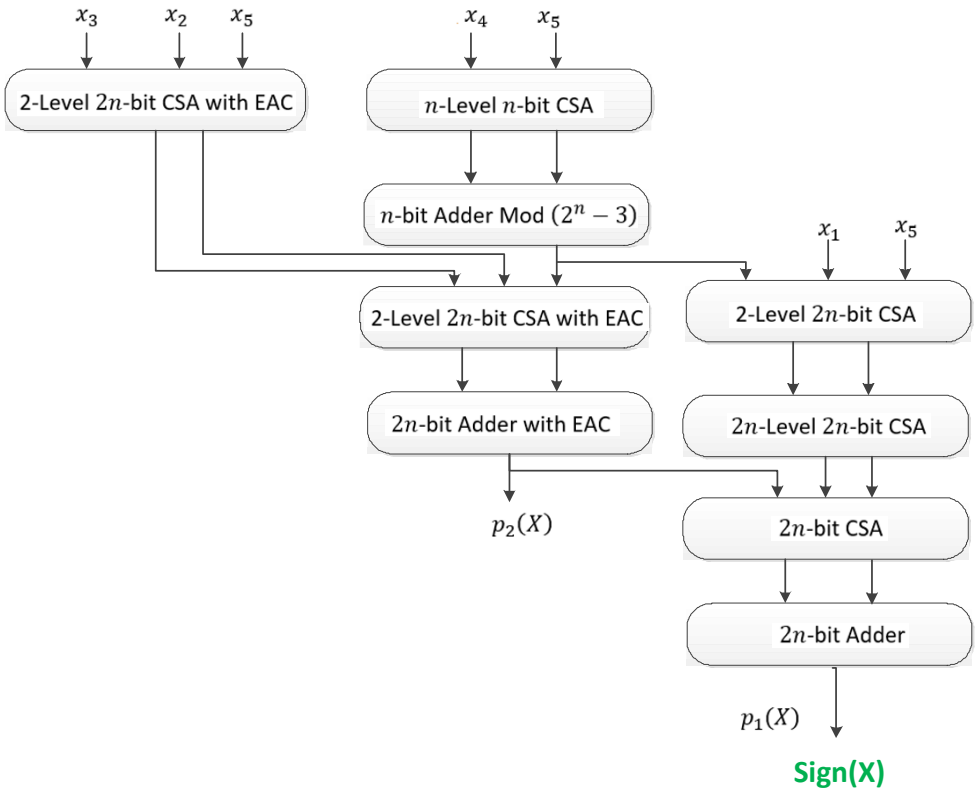

Fig. 4: $p_1(X)$ and $p_2(X)$ generator and sign detection circuit.

Table 2: Analytical delay comparison

Operation	Method	Adder					CSA	Comparator				Total Delay
		n-bit	$2n$-bit	$4n$-bit	$6n$-bit	$7n$-bit		n-bit	$2n$-bit	$6n$-bit	$7n$-bit	
Sign Detection	[24]		3	1			$3\log n + 1$			1		$(32n + 12\log n + 4)\Delta G$
	[25]	1	4	1	1		$\log n + 5$					$(38n + 4\log n + 20)\Delta G$
	proposed	1	2				$\log 2n + \log n + 3$					$(10n + 8\log n + 16)\Delta G$
Comparison	[24]		3	1			$3\log n + 1$			1		$(32n + 12\log n + 4)\Delta G$
	[25]	1	4	1	1		$\log n + 5$			1		$(50n + 4\log n + 20)\Delta G$
	proposed	1	2				$\log 2n + \log n + 3$		1			$(14n + 8\log n + 16)\Delta G$
	[23]					1	$\log 2n$				1	$(28n + 8\log n)\Delta G$
	[16], [19]	4	1				$12\log n$	1	1			$(18n + 48\log n)\Delta G$
	[22]			1			$\log n$		2			$(16n + 4\log n)\Delta G$
	[20], [21]		2				$\log n$		1			$(12n + 4\log n)\Delta G$

Table 3: Analytical cost comparison

Operation	Method	Adder					CSA	Comparator				Total Cost
		n -bit	$2n$- bit	$4n$- bit	$6n$- bit	$7n$ -bit	n-bit	n -bit	$2n$ - bit	$6n$- bit	$7n$ - bit	
Sign Detection	[24]	1	5	1			$8n+6$			1		$(56n^2+273n)\#G$
	[25]	1	4	1			$5n+42$					$(35n^2+141n)\#G$
	proposed	1	2				$5n+14$					$(35n^2+133n)\#G$
Comparison	[24]	1	5	1			$8n+6$			3		$(56n^2+357n)\#G$
	[25]	1	4	1	2		$5n+42$			1		$(35n^2+267n)\#G$
	proposed	1	2				$5n+14$		3			$(35n^2+175n)\#G$
	[23]					1	$10n$				1	$(70n^2+98n)\#G$
	[16], [19]	4	1	1			$10n$	4	3			$(70n^2+140n)\#G$
	[22]			1			$6n$		4			$(42n^2+84n)\#G$
	[20], [21]	$4(2^{2n}-1)(2^{2n}-9)+5$					$(2^{2n}-1)(2^{2n}-9)n$	$4(2^{2n}-1)(2^{2}$ $-9)$				$(2^{2n}-1)(2^{2n}-9)(14n)\#G$

Table 4: Synthesis based comparison results

Design	n	Delay (ns)	Ratio	Area (μm^2)	Ratio	Power (mW)	Ratio	Energy (pJ)	Ratio
[24]	8	10.80	1.56	84075.61	2.22	69.74	2.21	720.79	3.31
[25]	8	13.20	1.91	58972.18	1.56	42.15	1.33	556.38	2.55
[22]	8	12.70	1.84	212472.50	5.62	110.85	3.51	1407.79	6.46
proposed	8	6.90	1.00	37800.76	1.00	31.54	1.00	217.62	1.00
[24]	16	16.30	1.58	189451.71	1.32	191.22	1.25	3116.88	1.98
[25]	16	22.70	2.20	210462.79	1.47	200.03	1.31	4540.68	2.88
[22]	16	14.8	1.43	350311.09	2.45	178.43	1.16	2640.76	1.67
proposed	16	10.30	1.00	142929.73	1.00	152.81	1.00	1573.94	1.00

Conclusion

In residue number systems, one of the most complicated operations are sign detection and comparison which also play a prominent role in the development of division and overflow detection components in RNS. The 5-moduli set $\gamma = \{2^{2n}, 2^n \pm 1, 2^n \pm 3\}$, has been shown to have efficient RNS arithmetic circuits as well as efficient reverse converter. To extend applicability of this moduli set, we provided the first efficient signed/unsigned RNS comparator circuit in this work.

In the proposed comparator, with the advantage of dynamic range partitioning technique, sign of the operands are identified and then comparison performed effectively. Synthesis-based results confirmed analytical

evaluation and revealed 47% (54%), 35% (32%), 25% (24%) and 60% (65%) delay, area, power, and energy improvements, respectively, for the new signed RNS number comparator in comparison with the reference design.

As regards the relevant future work, we plan to apply DRP method to other 4- and 5-moduli sets, to improve comparison operation and so other complicated operations.

Author Contributions

Zeinab Torabi contributed to the idea, simulation, writing, review, and editing the paper. Armin Belghadr contributed for writing, review, and editing the paper.

Acknowledgment

The authors would like to thank the editor and anonymous reviewers.

Conflict of Interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Abbreviations

RNS	Residue Number System
MRC	Mixed Radix Representation
CRT	Chinese Remainder Theorem
DRP	Dynamic Range Partitioning
MSB	Most Significant Bit

References

[1] G. C. Cardarilli, L. D. Nunzio, R. Fazzolari, A. Nannarelli, M. Petricca, M. Re, "Design space exploration based methodology for residue number system digital filters implementation," IEEE Trans. Emerging Top. Comput., 10(1): 186-198, 2020.

[2] I. Z. Alhassan, E. D. Ansong, G. Abdul-Salaam, S. Alhassan, "Enhancing image security during transmission using residue number system and k-shuffle," Earthline J. Math. Sci., 4(2): 399-424, 2020.

[3] D. Schoinianakis, "Residue arithmetic systems in cryptography a survey on modern security applications," J. Cryptographic Eng., 10(3): 249-267, 2020.

[4] M. A. Belhamra, E. M. Souidi, "Steganography over Redundant Residue Number System Codes," J. Inf. Secur. Appl., 51: 102434, 2020.

[5] M. I. Youssef, A. E. Emam, M. Abd Elghany, "Image multiplexing using residue number system coding over MIMO-OFDM communication system," Int. J. Electr. Comput. Eng., 9(6): 4815-4825, 2019.

[6] L. Sousa, P. Martins, "Sign detection and number comparison on RNS 3-Moduli sets $\{2^n\text{-}1, 2^{n+x}, 2^n+1\}$," Circ. Syst. Signal Process., 36: 1224-1246, 2017.

[7] C. Y. Hung, B. Parhami, "An approximate sign detection method for residue numbers and its application to RNS division," Comput. Math. Appl., 27: 23–35, 1994.

[8] T. Tomczak, "Fast sign detection for RNS $\{2^n-1, 2^n, 2^n+1\}$," IEEE Trans. Circuits Syst. I Regul. Pap., 55(6): 1502–1511, 2008.

[9] Z. Torabi, G. Jaberipur, "Fast low energy RNS comparators for 4-moduli sets $\{2^n \pm 1, 2^n, m\}$ with $m \in \{2^{n+1} \pm 1, 2^{n-1}\text{-}1\}$", Integr. VLSI J., 55: 155-161, 2016.

[10] S. Bi, W. J. Gross, "The mixed-radix Chinese remainder theorem and its applications to residue comparison," IEEE Trans. Comput., 57(12): 1624-1632, 2008.

[11] Y. Wang, X. Song, M. Aboulhamid, "A new algorithm for RNS magnitude comparison based on new Chinese remainder theorem II," in Proc. Ninth Great Lakes Symposium on VLSI: 362-365, 1999.

[12] M. Lu, J. S. Chiang, "A novel division algorithm for the residue number system," IEEE Trans. Comput., 1: 1026–1032, 1992.

[13] G. Dimauro, S. Impedovo, G. Pirlo, A. Salzo, "RNS architectures for the implementation of the diagonal function," Inf. Process. Lett., 73: 189–198, 2000.

[14] L. Sousa, "Efficient method for magnitude comparison in RNS based on two pairs of conjugate moduli," in Proc. IEEE Symposium on Computer Arithmetic (ARITH): 240-250, 2007.

[15] S. Kumar, C. H. Chang, TF Tay, "New algorithm for signed integer comparison in $\{2^{n+k}, 2^n\text{-}1, 2^n+1, 2^{n\pm1}\text{-}1\}$ and its efficient hardware implementation," IEEE Trans. Circuits Syst. I: Reg. Pap., 64(6): 1481-1493, 2016.

[16] K. Isupov, "Using floating-point intervals for non-modular computations in residue number system," IEEE Access, 8: 58603-58619, 2020.

[17] Z. Torabi, G. Jaberipur, "Low-power/cost RNS comparison via partitioning the dynamic range," IEEE Trans. Very Large Scale Integr. VLSI Syst., 24(5): 1849-1857, 2016.

[18] Z. Torabi, A. Belghadr, "Efficient RNS comparator via dynamic range partitioning: The case of $\{2^n\text{-}1, 2^n, 2^{n+1}\text{-}1\}$," CSI J. Comput. Sci. Eng., 16(2): 38-43, 2019.

[19] K. Isupov, "High-performance computation in residue number system using floating-point arithmetic," Comput., 9(2): 9-24, 2021.

[20] V. A. Krasnobayev, A. S. Yanko, S. A. Koshman. "A method for arithmetic comparison of data represented in a residue number system," Cybern. Syst. Anal., 52(1): 145-150, 2016.

[21] V. Krasnobayev, S. Koshman, K. Myslyvtsev,, K. Kuznetsova, , T. Ivko, T. Katkova, "Method of arithmetic comparison of data in the residue numeral system," in Proc. IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T): 483-487, 2019.

[22] M. Babenko, S. J. Piestrak, N. Chervyakov, M. Deryabin, "The study of monotonic core functions and their use to build RNS number comparators," Electron., 10(9): 1041, 2021.

[23] M. Babenko, M. Deryabin, S. J. Piestrak, P. Patronik, N. Chervyakov, A. Tchernykh, A. Avetisyan, "RNS number comparator based on a modified diagonal function," Electron., 9(11): 1784, 2020.

[24] H. Ahmadifar, G. Jaberipur, "A new residue number system with 5-Moduli Set: $\{2^{2q}, 2^q \pm 3, 2^q \pm 1\}$," The Comput. J., 58: 1548-1565, 2014.

[25] M. Mojahed, A. S. Molahosseini, A. A. E. Zarandi, "A multifunctional unit for reverse conversion and sign detection based on the 5-moduli set," Comput. Sci., 22(1), 2021.

[26] N. S. Szabó, R. I. Tanaka, Residue Arithmetic and Its Applications to Computer Technology. New York, NY, SA: McGraw-Hill, 1967.

[27] L. Sousa, P. Martins, "Efficient sign identification engines for integers represented in RNS extended 3-moduli set {2n − 1, 2n + k , 2n + 1}," 50(16): 1138-1139, 2014.

[28] M. Xu, Z. Bian, R. Yao, "Fast sign detection algorithm for the RNS moduli set {2^{n+ 1}-1, 2^{n}-1, 2^{n}\}," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., 23(2): 379-383, 2014.

[29] Y. Wang, "New Chinese remainder theorems," in Proc. IEEE Asilomar Conference on Signals, Systems and Computers: 165-171, 1998.

[30] P. Boyvalenkov, N. I. Chervyakov, P. Lyakhov, N. Semyonova, A. Nazarov, M. Valueva, G. Boyvalenkov, D. Bogaevskiy, D. Kaplun, "Classification of moduli sets for residue number system with special diagonal function," IEEE Access, 8: 156104-156116, 2020.

[31] M. Valueva, G. Valuev, N. Semyonova, P. Lyakhov, N. Chervyakov, D. Kaplun, D. Bogaevskiy, "Construction of residue number system using hardware efficient diagonal function," Electron., 8(6): 694, 2019.

[32] G. Dimauro, S. Impedovo, G. Pirlo, "A new technique for fast number comparison in the residue number system," IEEE Trans. Comput., 42(5): 608-612, 1993.

[33] B. Cao, C. H. Chang, T. Srikanthan, "Adder based residue to binary converters for a new balanced 4-moduli set," in Proc. IEEE International Symposium on Image and Signal Processing and Analysis: 820-825, 2003.

[34] A. Tyagi, "A reduced-area scheme for carry-select adders," IEEE Trans. on Comput., 42: 63–70, 1993.

Biographies

Zeinab Torabi received her Ph.D. degree in Computer Architecture from Shahid Beheshti University, Tehran, Iran, in 2016. She is currently an Assistant Professor in Faculty of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran. Her research interests include computer arithmetic, residue number system, and algorithms.

- Email: z.torabi@sru.ac.ir
- ORCID: 0000-0002-2526-688X
- Web of Science Researcher ID: ABG-9144-2022
- Scopus Author ID : 56958405600
- Homepage: https://www.sru.ac.ir/en/school-of-computer/zeinab-torabi/

Armin Belghadr received the B.S. degree in computer hardware engineering and the M.S. degree in computer architecture from Shahid Beheshti University, Tehran, Iran, in 2011 and 2013, respectively. He has also received his Ph.D. degree in computer architecture with the Department of Computer Science and Engineering, Shahid Beheshti University in year 2019. His-research interests include computer arithmetic and particularly residue number systems.

- Email: a_belghadr@sbu.ac.ir
- ORCID: 0000-0003-4835-6607
- Web of Science Researcher ID: Q-7750-2019
- Scopus Author ID: 55865963000
- Homepage: http://facultymembers.sbu.ac.ir/a_belghadr/

How to cite this paper:
Z. Torabi, A. Belghadr, "Fast and power efficient signed/unsigned RNS comparator & sign detector," J. Electr. Comput. Eng. Innovations, 11(1): 41-50, 2023.

DOI: 10.22061/JECEI.2022.8321.505

URL: https://jecei.sru.ac.ir/article_1717.html