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. 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\} 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 show 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 √M. In [5], a sign
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 $r = X \mod m$ 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 $\{m_0, m_1, m_2, \ldots, m(n-1)\}$ 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 $(r_0, r_1, r_2, \ldots, r(n-1))$, where $ri = X \mod mi 0<=i<=n-1$.

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.
2.\[ \alpha_{2} = m \]  
\( m \)\[ \text{mod} \] \( m \) operations only. The calculation process for each mixed radix \( \alpha \) 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 \{m_1, m_2, . . . , m_{N-1}, m_N = 2n\}, the value of \( \alpha_{N-1} \) is equal to \( 2n-1 \) when the integer \( X \) is \( M/2 \). \( \alpha_{N-1}(M/2) \) is denoted as the value of \( \alpha_{N-1} \) for \( X = M/2 \), and it has

\[ \alpha_{N-1} \left( \frac{M}{2} \right) = 2^{n-1} \quad (3) \]

Proof: For the moduli set \{m_1, m_2 . . . m_{N-1}, m_N = 2n\}, we have

\[ M \equiv m_1 m_2 \cdots m_{N-1} \equiv 2n \quad (4) \]

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

\[ \left\lfloor \frac{M}{m_i} \right\rfloor = \left\lfloor 2^{n-1} \prod_{i=1}^{N-1} m_i \right\rfloor m_i = 0. \quad (5) \]

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

\[ \frac{M}{2} = (0,0,...,0, |m_1 m_2, ..., m_{N-1}, m_N | m_N = 2^{n-1} |_{\mathbb{Z}^n} \]

Thus, unfold (2), and we have

\[ X = x_1 + m_1 \gamma_1 x_1 + \gamma_2 x_2 + m_1 m_2 \left[ \frac{y_{x_1 x_2 x_3}}{m_2} \right] m_3 \]

+ \ldots + m_1 m_2 \ldots m_N \left[ \frac{y_{x_1 x_2 x_3} \ldots y_N x_N}{m_2 m_3 \ldots m_N} \right] m_N \quad (7) \]

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

\[ \frac{M}{2} = m_1 m_2 \ldots m_{N-1} \left[ \frac{y_{x_1 x_2 x_3} \ldots y_N x_N}{m_2 m_3 \ldots m_N} \right] m_N \quad (8) \]

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

\[ \alpha_{N-1} \left( \frac{M}{2} \right) = 2^{n-1} \quad (9) \]

Theorem 3: In the moduli set \{m_1, m_2, . . . , m_{N-1}, m_N = 2n\}, for a residue representative number \( (x_1, x_2, \ldots, x_N) \), \( \alpha_{N-1} \) is

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 \{m_1, m_2, . . . , 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

\[ Y = \begin{cases} X, & \text{if } 0 \leq X < M/2 \\ X - m, & \text{if } M/2 \leq X < M \end{cases} \quad (1) \]

Theorem 1: Given \( \{m_1, m_2, \ldots, m_N\} \), the magnitude of a residue number \( X = (x_1, x_2, \ldots, x_N) \) 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

\[ \alpha_{j+1} = [\sum_{i=1}^{j+2} y_{j+1} x_i / \prod_{i=1}^{j+1} m_i] m_{j+2}, \quad \alpha_j = [y_{j+1} x_j + r_j x_j] m_{j+2} \]

Theorem 1 provides the mixed radix form of the CRT that converts residue numbers to weighted numbers; it requires

DOI: 10.18535/ijecs/v4i10.21

S.Kiranmayi, IJECS Volume 04 Issue 10 October, 2015 Page No.14663-14669
\[ \alpha_{N-1} = \left[ \frac{\gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_N x_N}{m_2 m_3 - m_{N-1}} \right]_2 \quad (10) \]

Then the proposed sign detection function is

\[ g(n(x_1, x_2, \ldots, x_N)) = \begin{cases} 0, & \text{if } \alpha_{N-1} < 2^{n-1} \\ 1, & \text{if } \alpha_{N-1} \geq 2^{n-1} \end{cases} \quad (11) \]

Proof: From (2), (8), and (9), in residue representation \( X < M/2 \) can be rewritten as
\[
x_1 + \sum_{j=1}^{N-1} (a_j \prod_{i=1}^{j} m_i) < 2^{n-1} \prod_{i=1}^{N-1} m_i \quad (12) \]

Then, rewrite (12), and we have
\[
(a_{N-1} - 2^{n-1}) < \frac{x_1 + \sum_{j=1}^{N-1} (a_j \prod_{i=1}^{j} m_i)}{\prod_{i=1}^{N-1} m_i} < 0 \quad (13) \]

Thus, the sufficiency of Theorem 3 is established. The necessity of the Theorem 3 proof is presented as follows.

With Theorem 1 and because \( a_j < m_{j+1} \) for \( j < N - 1 \), it is easy to verify that
\[
x_1 + \sum_{j=1}^{N-1} (a_j \prod_{i=1}^{j} m_i) \leq (m_1 - 1) + \sum_{j=1}^{N-2} ((m_{j+1} - 1) \prod_{i=1}^{j} m_i) < \prod_{i=1}^{N-1} m_i \quad (14) \]

Because the condition \( \alpha_{N-1} < 2^{n-1} \) is established, we can deduce \( X \) in residue representation as
\[
x_1 + \sum_{j=1}^{N-1} (a_j \prod_{i=1}^{j} m_i) \leq \prod_{i=1}^{N-1} m_i + \alpha_{N-1} \prod_{i=1}^{N-1} m_i \]
\[
\leq \prod_{i=1}^{N-1} m_i + (2^{n-1} - 1) \prod_{i=1}^{N-1} m_i \]
\[
= 2^{n-1} \prod_{i=1}^{N-1} m_i \]
\[
= \frac{M}{2} \quad (15) \]

Hence, when \( \alpha_{N-1} < 2^{n-1} \), \( X < M/2 \) 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 \( \alpha_{N-1} \geq 2^{n-1} \), therefore, Theorem 3 is established.

Theorem 3 provides an efficient sign detection algorithm for the moduli set \( \{m_1, m_2, \ldots, m_{N-1}, m_N = 2n\} \) 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 \( \gamma_i \) in Theorem 1, we can simplify (10) as follows:
\[
X = \left[ \frac{\gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_N x_N}{\prod_{i=1}^{N-1} m_i} \right]_{M\gamma} \]
\[
= \left[ \frac{N \prod_{i=1}^{N-1} m_i}{\prod_{i=1}^{N-2} m_i} x_1 + \sum_{j=2}^{N} \frac{m_j \prod_{i=1}^{j-1} m_i}{\prod_{i=1}^{j} m_i} x_j \right]_{M\gamma} \]

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 \( \{2n+1 - 1, 2n - 1, 2n\} \), let \( m_1 = 2n+1 - 1, m_2 = 2n - 1, \) and \( m_3 = 2n \). With Theorem 1, the multiplicative inverses of the moduli set can be obtained from
\[
|N_1 N_1^{-1}|_{m_1} = [((2n - 1) - (2^{n-1} - 1)]_{2n+1-1} = 1 \quad (18) \]
\[
|N_2 N_2^{-1}|_{m_2} = [((2n+1 - 1) - (2^{n-1} - 1)]_{2n-1-1} = 1 \quad (19) \]
\[
|N_3 N_3^{-1}|_{m_3} = [((2^{n-1} - 1) - (2^{n-1} - 1)]_{2n} = 1 \quad (20) \]

Then, we substitute these expressions into (16) to achieve
\[
\alpha_2 = \left[ \frac{2^n (2^{n+1} - 1 - 4)}{2^{n+1} - 1} x_1 + \frac{2^n 1}{2^n - 1} x_2 + \frac{2^n 1}{2^n - 1} x_3 \right. \]
\[
- \frac{1}{(2^{n+1} - 1)(2^n - 1)} x_1 \right]_{2^n} \]
\[
= \left[ (2^n - 2) x_1 - \frac{2}{2^{n+1} - 1} x_1 + x_2 + \frac{1}{(2^n - 1)} x_2 + x_3 \right. \]
\[
- \frac{1}{(2^{n+1} - 1)(2^n - 1)} x_1 \right]_{2^n} \]
\[
= \left[ -2 x_1 + x_2 + x_3 + \frac{1}{2^n - 1} x_2 \right. \]
\[
- \frac{2(2^n - 1) + 1}{(2^{n+1} - 1)(2^n - 1)} x_1 \right]_{2^n} \]
\[ W = 1 - \bar{W} = 1 + \left| \frac{x_2 - x_1 - x_n \cdot n}{2^n - 1} \right| \]

Then, we denote \( x_1 \) as a \( n \)-bit digit that equals \( 2x_{1,n} - 2:0 + x_{1,n} \), which is concatenated by the least \( n-1 \) bits of \( x_1 \) and \( x_{1,n} \). Therefore, (21) can be rewritten as

The goal of the carry generation unit and post processing unit is to achieve the \( n \)-th 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.

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
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.

5. SIMULATION RESULTS

Figure 5: CARRY GENERATION UNIT

Figure 6: CARRY SAVE BLOCK

Figure 7: COMPARATOR UNIT

Figure 8: TOP SIGN DETECTION 16

Figure 9: TOP SIGN DETECTION 32

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


