Design of RNS Based Addition Subtraction and Multiplication Units

N Vivek\(^1\), K Anusudha\(^2\)

\(^1\) Department of Electronic Engineering, Pondicherry University, Pondicherry, India
\(^2\) Department of Electronic Engineering, Pondicherry University, Pondicherry, India

Abstract—Residue number systems have gained significant importance in the field of high-speed digital signal processing due to their carry-free nature and speed-up provided by parallelism. The cynical aspect in the application of RNS is the selection of the moduli set and the design of the conversion units. In the residue number system, a set of moduli which are independent of each other is given. An integer is represented by the residue of each modulus and the arithmetic operations are based on the residues individually. The arithmetic operations based on residue number system can be performed on various moduli independently to avoid the carry obtained in addition, subtraction and multiplication, which is usually time consuming. Thus, the comparison and division are more complicated and the fraction number computation is immured. In this paper, work is done by the residues of the number and performed Addition, Subtraction and Multiplication are performed which shows more advantages of Carry Free nature. Performance of RNS based Addition, subtraction and Multiplication Units has been implemented for modulo set \(\{2^n-1, 2^i, 2^j+1\}\) for \(n=2,3\) with the targeted device of Spartan 3E using hardware description language called Verilog and synthesized in Xilinx ISE 13.2.

Keywords—Residue Number System (RNS), New Chinese Remainder Theorem (NCRT), Multioperand Modular Adder (MOMA), Mixed Radix Theorem (MRT), Chinese Remainder Theorem(CRT), Carry Save Adder(CSA).

I INTRODUCTION

Residue Number System is a mathematical idea from Sun Tsu Suan-Ching (Master Sun’s Arithmetic Manual) in the 4th century AD from Chinese remainder theorem of modular arithmetic for its operation.

There has been interest in Residue Number System (RNS) arithmetic as a basis for computational hardware since the 1950’s. Due to its special features, the Residue Number System has many applications in arithmetic functions such as Digital Signal Processing, Digital Filtering, Coding, RSA ciphering system, Digital communications, Ad-hoc network, storing and retrieving information, Error detection and Correction, and fault tolerant systems [11].

The main reasons for the interests are the inherent properties of RNS such as the parallelism, modularity, fault tolerance and carry free operations. The advantages offered by this VLSI technology have added a new dimension in the implementation of RNS-based architectures. Several high-speed VLSI special purpose digital signal processors have been successfully implemented.

A residue number system (RNS) represents a large integer using a set of smaller integers, so that computation may be performed more efficiently. The main objective of the project is to reduce complexity in addition, subtraction and multiplication for large integers using the RNS technique, and this RNS is mainly used in cryptography as the moduli used as cipher (key) for both encryption and decryption.

This paper is organized as follows; Section II explains the existing model of the RNS for Filter application and section III explains the proposed model for Addition, Subtraction and Multiplication Unit with Forward and Reverse Conversion with MOMA circuit. Simulation & Results are analyzed in the section IV, Section V with the conclusion.

II. EXISTING RNS MODEL FOR FILTER DESIGN

Figure 1, depicts a basic N-Tap filter, where

\[
\begin{align*}
y(n) &= a(0)x(n) + a(1)x(n-1) + a(2)x(n-2) + \ldots + a(N-1)x(n-N+1) \\
&= \sum_{i=0}^{N-1} a(i)x(n-i)
\end{align*}
\]

(1)

Where,

- \(x[n]\) is the input signal,
- \(y[n]\) is the output signal,
- \(a(i)\)s the filter coefficients.

For FIR Filter of N order filter has
- Coefficients N+1
- Multipliers N+1
- Adders N

The 3 main blocks of RNS model are:

- Forward Conversion
- Channels (moduli)
- Reverse Conversion

Basic block diagram of RNS Model, is shown in Figure 2
A. FORWARD CONVERSION
The forward conversion stage is of paramount importance as it is considered as an overhead in the overall RNS. Forward converters are usually classified into two categories based on the moduli used. The first category includes forward converters based on arbitrary moduli-sets. These converters are regularly built using Look Up Tables (LUTS) which consists of ROM’s. The second category includes forward converters based on special moduli-sets. The use of these special moduli-sets simplifies the forward conversion algorithms and architectures.

Usually, the special moduli-sets are referred to as low-cost moduli-sets. A typical architecture for the implementation of a forward converter from binary to RNS representation using the special moduli-set is shown in Figure 3. One way of implementing a residue adder for modulo ‘m’ structure is composed of one n-bit adder among various ways [6].

C. REVERSE CONVERSION
Converting residue number to binary number is called reverse conversion. Reverse conversion algorithms are classified into 3 types:
- Chinese Remainder Theorem (CRT)
- New Chinese Remainder Theorem (NCRT)
- Mixed Radix Theorem (MRT)

The new Chinese Remainder Theorems (NCRT) makes the computation faster and efficient without any extra overheads. A new high-speed ROM-less residue-to-binary converter for the three moduli residue number system of the form \( \{2^{n-1}, 2^n, 2^n+1\} \) is used. Unlike any other converter, its delay includes the time of only one 1’s complement addition of two \( 2^n \)-bit numbers which is only 2/3 of the binary range of the RNS equal to \( 3^n \). Thus, it is potentially the fastest known residue-to-binary converter [12].

B. CHANNELS
The Standard channels in RNS are three moduli i.e., \( \{2^n-1, 2^n, 2^n+1\} \) in which n describes the way of splitting the decimal value of ‘X’ we consider in Figure 2.

One of the most important considerations while designing RNS system is choice of selecting moduli set. The choice of moduli affects the complexity of Forward and Reverse converters as well as RNS arithmetic Circuits [11]. Unbalanced and moduli-sets lead to uneven architectures, in which the role of largest moduli, with respect to both cost and performances, is excessively dominant. An example of a moduli-set with good balanced is \( 2^n-1, 2^n, 2^n+1 \) [7].
III. PROPOSED MODEL

The proposed structure is implementation of Addition, Subtraction and Multiplication Units in Residue Number System for order n=2 & 3 is shown as Figure 8

![Figure 8: Block Diagram of Proposed Model](image)

The basic formula for calculating Forward Conversion in RNS is

\[ r_1 = |B_1 + B_2 + B_3| 2^{n-1} \]  
\[ r_2 = B_3 \]  
\[ r_3 = |B_1 - B_2 + B_3| 2^{n+1} \]

Algorithms for New Chinese Reminder Theorem:

Let the three residues be denoted as X1, X2, and X3. MSB are given first the decimal value of X and it can be computed as

- **Property 1:**
  \[ x_i = |x| m_i \] and \[ y_i = |y| m_i \], then addition may be defined as
  \[ X + Y = Z \]
  \[ Z = (z_1, z_2, z_3, z_4) \]

- **Property 2:**
  \[ x_i = |x| m_i \] and \[ y_i = |y| m_i \], then Subtraction may be defined as
  \[ X - Y = Z \]
  \[ Z = (z_1, z_2, z_3, z_4) \]

- **Property 3:**
  \[ x_i = |x| m_i \] and \[ y_i = |y| m_i \], then Multiplication may be defined as
  \[ X \times Y = Z \]
  \[ Z = (z_1, z_2, z_3, z_4) \]

Here the New Chinese Reminder Theorem is considered due to the less complexity compared with Mixed Radix Theorem.

Consider the Example: RNS Number \( x = (1, 2, 3) \) given moduli set as \( (3, 5, 7) \) using MRT

\[ X = (a_1 + a_2 P_1 + a_3 P_2 + a_4 P_3) \]

Using equation (11) as follows

\[ X = (a_1 + a_2 P_1 + a_3 P_2 + a_4 P_3) \]
\[ |1/P_1| P_1 = 2 \]
\[ |1/P_2| P_2 = 5 \]
\[ |1/P_3| P_3 = 3 \]
\[ |1/P_4| P_4 = 8 \]
\[ a_1 = x_1 = 1 \]
\[ a_2 = (2-1) * |1/P_2| P_2 = 2 \]
\[ a_3 = ([x_3 - a_1] |1/P_3| P_3 - a_2) |1/P_2| P_3 \] \mod P_3
\[ a_4 = ([x_4 - a_1] |1/P_4| P_4 - a_2) |1/P_3| P_3 \] \mod P_4

\[ X = (1 + 2 * 3 + 3 * 5 + 3 * 5 * 7) = 367 \]

IV. SIMULATION RESULTS & RESULT ANALYSIS

The Top block of RNS based Adder, subtractor and Multiplication Units Consists of two operand as inputs of which are in bit size of 6 and 9 bit and corresponding input order ‘n’ i.e, n=2 and n=3.
The Simulation of RNS based Addition, Subtraction and Multiplication Units are synthesized with the Device XC3S100E, package of CP132 and Family SPARTAN 3E and Corresponding Timing Waveforms are taken from the Test Bench as shown in Figure 10, 11 and 12.

Table I: RNS Based Adder, Subtractor and Multiplication Units for n=2

<table>
<thead>
<tr>
<th>Topology</th>
<th>No of slices</th>
<th>No of LUT's</th>
<th>Delay(ns)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addition</td>
<td>55</td>
<td>96</td>
<td>32.750</td>
</tr>
<tr>
<td>Subtraction</td>
<td>53</td>
<td>94</td>
<td>30.164</td>
</tr>
<tr>
<td>Multiplication</td>
<td>73</td>
<td>129</td>
<td>38.061</td>
</tr>
</tbody>
</table>

Table II: RNS Based Adder, Subtractor and Multiplication Units for n=3

<table>
<thead>
<tr>
<th>Topology</th>
<th>No of slices</th>
<th>No of LUT's</th>
<th>Delay(ns)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addition</td>
<td>107</td>
<td>188</td>
<td>37.355</td>
</tr>
<tr>
<td>Subtraction</td>
<td>108</td>
<td>190</td>
<td>37.148</td>
</tr>
<tr>
<td>Multiplication</td>
<td>113</td>
<td>201</td>
<td>40.388</td>
</tr>
</tbody>
</table>

From the above Table 1 & 2 it shows that the RNS based Addition, Subtraction and Multiplication Unit for n=2 & 3.

V. CONCLUSION

An Efficient RNS based Addition, Subtraction and Multiplication Units for moduli set \( \{2^n-1, 2^n, 2^n+1\} \) for n=2 & 3 has been implemented and simulated in Environment of xilinx ISE 13.2. From the result analysis it is observed that the proposed model is efficient when compared conventional adder, multiplier and Subtraction Units.

VI. REFERENCES


