An Effective New CRT Based Reverse Converter for a Novel Moduli Set \( \{2^{2n+1} - 1, 2^{2n+1}, 2^{2n} - 1\} \)

Edem K. Bankas ¹, Kazeem A. Gbolagade ¹, and Sorin D. Cotofana ²

¹Department of Computer Science, Faculty of Mathematical Sciences, University for Development Studies, Ghana

²Computer Engineering Lab., Delft University of Technology, Delft, The Netherlands

June 5, 2013
Introduction
Advantages, Challenges of RNS, and Background Information
Problem Statement and Proposed Moduli set
Proposed Reverse Conversion Algorithm
Hardware Realization and Performance Analysis
Conclusions
Introduction

Carry Propagation Problem in Binary Number System Processors

The main issue of concern nowadays in the design of processors is performance, low cost hardware and low power consumption. These issues are best solved from the computational point of view.

Simple operation in RNS - Addition

\[ 11_{10} \rightarrow (3, 1, 2)_{RNS(4|5|3)} \]
\[ 38_{10} \rightarrow (2, 3, 2)_{RNS(4|5|3)} \]

By adding:
\[ 49_{10} \rightarrow (1, 4, 1)_{RNS(4|5|3)} \]
The basis for an RNS is a set of relatively prime integers 
\{m_1, m_2, m_3, ..., m_n\} such that \(gcd(m_i, m_j) = 1\), where \(i \neq j\).

The Dynamic range (DR) \(M = \prod_{i=1}^{n} m_i = m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_n\).

The DR defines the range of representable residue classes

\[ X \rightarrow (x_1, x_2, x_3, ..., x_n) \]

\[ x_i = |X|_{m_i} = X \mod m_i \]
Advantages of RNS

- The design of High speed processors (Premkumar, 1992)
- The design of Low Power consumption processors (Jenkins, 1978)
- Reduced Hardware Complexity (Premkumar, 1992)
- Fault tolerance (Premkumar, 1992)

Example (Applications of RNS)

- Cryptography
- Digital Signal Processing
- Convolution
- Digital Communication etc.
Challenges of RNS

Difficult Arithmetic Operations

- Sign detection
- Magnitude Comparison
- Overflow detection
- Division
- Other complex arithmetic operations e.g., square root, exponentiation, etc.

Moduli selection and Data conversion
Background Information

Reverse Conversion Methods

- Chinese Remainder Theorem (CRT)
- New Chinese Remainder Theorem
- Mixed Radix Conversion (MRC)
Chinese Remainder Theorem

\[ X = \left\lfloor \sum_{i=1}^{k} M_i \left\lfloor M_i^{-1} \right\rfloor_{M_i} x_i \right\rfloor_M, \]

where \( M = \prod_{i=1}^{k} m_i \), \( M_i = \frac{M}{m_i} \), and \( M_i^{-1} \) is the multiplicative inverse of \( M_i \) with respect to \( m_i \).
New Chinese Remainder Theorem

\[ X = x_1 + m_1 \, |k_1(x_2 - x_1) + k_2 m_2 (x_3 - x_2)|_{m_2 m_3}, \]  

(2)

where

\[ |k_1 m_1|_{m_2 m_3} = 1, \]  

(3)

\[ |k_2 m_1 m_2|_{m_3} = 1. \]  

(4)
Applications requiring Larger Dynamic Range (DR) is of necessity. To achieve larger DR, there are two main approaches:

- Increasing the number of channels from length 3 above, to maximize the parallelism advantage of RNS to achieve an efficient reverse converter
- Using length 3 moduli, but achieve larger DR and an efficient corresponding reverse converter

Given that, a larger DR moduli set is required, we seek to obtain a novel length 3, $6n$ bit moduli set and then design an efficient reverse converter that outperforms the current state of the art?
Proposed Moduli Set \( \{2^{2n+1} - 1, 2^{2n+1}, 2^{2n} - 1\} \)

**Theorem 1**
The moduli \(2^{2n+1} - 1\), \(2^{2n+1}\), and \(2^{2n} - 1\) are pair-wise relatively prime numbers.
Theorem 2
Given the \( \{2^{2n+1} - 1, 2^{2n+1}, 2^2n - 1\} \) moduli set, the following holds true:

\[ |(2^{2n}+1 - 1)^{-1}|_{(2^{2n+1})(2^{2n} - 1)} = 2^{2n+1} - 1, \]

(5)

\[ |((2^{2n}+1 - 1)(2^{2n}+1))^{-1}|_{(2^{2n} - 1)} = 2^{2n-1}. \]

(6)
Theorem 3

The decimal equivalent of the RNS number \((x_1, x_2, x_3)\) with respect to the moduli set \(\{m_1, m_2, m_3\}\) in the form \(\{2^{2n+1} - 1, 2^{2n+1}, 2^{2n} - 1\}\), can be computed as follows:

\[
X = x_1 + (2^{2n+1} - 1)(2^{2n+1})w + (2^{2n+1} - 1)C,
\]

where

\[
w = \left\| \frac{T}{2^{2n+1}} \right\|_{2^{2n-1}} \nonumber
= \left\| x_2 - x_1 + 2^{2n-1}x_3 - 2^{2n-1}x_2 \right\|_{2^{2n-1}},
\]

and

\[
C = \left| x_1 - x_2 \right|_{2^{2n+1}}.
\]
Further reduction in the hardware complexity yielded:

\[ v_1 = \left( \overbrace{x_{2,2n-1}x_{2,2n-2} \cdots x_{2,0} \wedge x_{2,2n}}^{2n} \right) \]  

\[ v_2' = \left( \overbrace{11 \cdots 11x_{1,2n}}^{2n} \right) \]  

\[ v_2'' = \left( \overbrace{x_{1,2n-1}x_{1,2n-2} \cdots x_{1,0}}^{2n} \right) \]
Further reduction in the hardware complexity (cont.)

\[ v_3 = \begin{pmatrix} x_{3,0}x_{3,2n-1} \ldots x_{3,1} \\ 2n \end{pmatrix} \]  (13)

\[ v_4' = \begin{pmatrix} x_{2,2n1111} \ldots 11 \\ 2n \end{pmatrix} \]  (14)

\[ v_4'' = \begin{pmatrix} \bar{x}_{2,0}\bar{x}_{2,2n-1} \ldots \bar{x}_{2,1} \\ 2n \end{pmatrix} \]  (15)
Further reduction in the hardware complexity (cont.):

Therefore,

\[
\begin{align*}
w &= \left\lfloor v_1 + v''_2 + v_3 + v''_4 + v'_4 + v'_2 \right\rfloor_{2^{2n-1}}, \text{ and} \\
C &= x_{1,2n}x_{1,2n-1} \ldots x_{1,1}x_{1,0} + \overline{x}_{2,2n}\overline{x}_{2,2n-1} \ldots \overline{x}_{2,1}\overline{x}_{2,0}.
\end{align*}
\]

(17)
Performance Comparison

We compared our proposal with equivalent best known state of the art reverse converters.

**Table: Area and Delay Comparison**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DR</td>
<td>$4n$</td>
<td>$5n$</td>
<td>$6n$</td>
<td>$6n$</td>
</tr>
<tr>
<td>FA</td>
<td>$9n + 2$</td>
<td>$13n + 2$</td>
<td>$16n + 1$</td>
<td>$8n + 2$</td>
</tr>
<tr>
<td>HA</td>
<td>$5n + 4$</td>
<td>$-$</td>
<td>$-$</td>
<td>$4n - 2$</td>
</tr>
<tr>
<td>Area in HA ($\Delta$)</td>
<td>$23n + 8$</td>
<td>$26n + 4$</td>
<td>$32n + 2$</td>
<td>$20n + 2$</td>
</tr>
<tr>
<td>Delay ($\tau$)</td>
<td>$(7n + 7)t_{FA}$</td>
<td>$(8n + 1)t_{FA}$</td>
<td>$(8n + 2)t_{FA}$</td>
<td>$(4n + 6)t_{FA}$</td>
</tr>
<tr>
<td>$\Delta\tau^2$</td>
<td>$\approx 1127n^3$</td>
<td>$\approx 1664n^3$</td>
<td>$\approx 2048n^3$</td>
<td>$\approx 320n^3$</td>
</tr>
</tbody>
</table>
Conclusions

We propose a novel Moduli set \( \{2^{2n+1} - 1, 2^{2n+1}, 2^{2n} - 1\} \)

- Subsequently, we presented an efficient reverse converter based on MRC which is adder based and memoryless.
- Theoretical analysis, reveals that our proposal has a delay of \((4n + 6)t_{FA}\) with an area cost of \((8n + 2)FAs\) and \((4n - 2)HAs\).
- The best state of the art converter requires \((16n + 1)FAs\) and exhibits a delay of \((8n + 2)t_{FA}\).
- This indicates that, theoretically speaking, our proposal achieves about 37.5% area reduction and its about twice faster than the state of the art.
Thank you for your attention.