Available online at www.sciencedirect.com

ScienceDirect

Computers and Mathematics with Applications 55 (2008) 660–668

An International Journal
computers & mathematics with applications

www.elsevier.com/locate/camwa

# A new high dynamic range moduli set with efficient reverse converter

Arash Hariri[a,*], Keivan Navi[b], Reza Rastegar[c]

[a] Department of Electrical and Computer Engineering, The University of Western Ontario, Canada
[b] Department of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran
[c] Department of Mathematics, Southern Illinois University, IL, USA

Received 4 January 2006; received in revised form 10 April 2007; accepted 17 April 2007

**Abstract**

The Residue Number System (RNS) is a representation system which provides fast and parallel arithmetic. It has a wide application in digital signal processing and provides enhanced fault tolerance capabilities. In this work, we consider the 3-moduli set $\{2^n, 2^{2n} - 1, 2^{2n} + 1\}$ and propose its residue to binary converter using the Chinese Remainder Theorem. We present its simple hardware implementation that is mainly composed of one Carry Save Adder (CSA), a $4n$ bit modulo $2^{4n} - 1$ adder, and a few gates. We compare the performance and area utilization of our reverse converter to the reverse converters of the moduli sets $\{2^n - 1, 2^n, 2^n + 1, 2^{2n} + 1\}$ and $\{2^n - 1, 2^n, 2^n + 1, 2^n - 2^{(n+1)/2} + 1, 2^n + 2^{(n+1)/2} + 1\}$ that have the same dynamic range and we demonstrate that our reverse converter is better in terms of performance and area utilization.


*Keywords:* Residue number system (RNS); Computer arithmetic; Residue to binary converter; Chinese remainder theorem (CRT)

## 1. Introduction

The Residue Number System (RNS) with its carry-free operations, parallelism and enhanced fault tolerance properties has been used in computer arithmetic since the 1950s [1]. These properties have made it very useful in some applications including digital signal processing, fault tolerant systems, etc. [2–5]. Different moduli sets have been presented for the RNS that have different properties with regards to the reverse conversion (Residue to Binary or R/B), Dynamic Range (DR) and arithmetic operations. The moduli of the forms $2^n$, $2^n - 1$, and $2^n + 1$ are very popular according to their easy arithmetic operations. The most famous moduli set is $\{2^n - 1, 2^n, 2^n + 1\}$. Several methods have been proposed for its reverse conversion, e.g., [6,7], whereas the best method is outlined in [8]. On the other hand, there are some other moduli sets that have more moduli in comparison with this moduli set. They include the moduli sets $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1\}$ [9] and $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} + 1\}$ [10] that have the dynamic ranges of $4n$ and $4n + 1$ bits, respectively. In [11], the moduli set $\{2^n - 1, 2^n, 2^n + 1, 2^{2n} + 1\}$ is proposed with the dynamic range of $2^n \times (2^{4n} - 1)$. It is shown that the reverse converter of this moduli set has superior area/time complexity

* Corresponding author.
*E-mail addresses:* hariri@ieee.org (A. Hariri), navi@sbu.ac.ir (K. Navi), rrastegar@ieee.org (R. Rastegar).

0898-1221/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2007.04.028

in comparison with the reverse converters of [9,10]. In [12], the moduli set $\{2^n, 2^n-1, 2^n+1, 2^n-2^{(n+1)/2}+1, 2^n+2^{(n+1)/2}+1\}$ is studied. It has the same dynamic range of $2^n \times (2^{4n}-1)$ and a new reverse converter is proposed that is more efficient than the previous converters including [13,14]. In this paper, we introduce the moduli set $\{2^n, 2^{2n}-1, 2^{2n}+1\}$ that has the same dynamic range as [11,12], but the reverse conversion can be carried out faster and it requires lower hardware area in comparison with [11,12].

The rest of the paper is organized as follows. In Section 2, we provide a short background for the RNS and also introduce the moduli set $\{2^n, 2^{2n}-1, 2^{2n}+1\}$. In Section 3, we present two lemmas and consider the reverse conversion scheme for the proposed moduli set using the presented lemmas and the Chinese Remainder Theorem (CRT). In Section 4, we present the hardware implementation of the reverse converter and in Section 5, we evaluate this converter and compare the results to similar works. Finally, we present our conclusions in Section 6.

## 2. Background

The RNS is defined by the set $S$ which includes $N$ integers that are pair-wise relatively prime. That is

$$S = \{m_1, m_2, \ldots, m_N\},$$

where $\gcd(m_i, m_j) = 1$ for $i, j = 1, \ldots, N$ and $i \neq j$ and gcd means the greatest common divisor.

Every integer $X$ in $[0, M-1]$ can be uniquely represented with an $N$-tuple where,

$$M = \prod_{i=1}^{N} m_i, \qquad X \to (R_1, R_2, \ldots, R_N),$$

and

$$R_i = |X|_{m_i} = (X \bmod m_i); \quad \text{for } i = 1 \text{ to } N.$$

The set $S$ and the number $R_i$ are called the moduli set and the residue of $X$ modulo $m_i$, respectively. Some arithmetic operations can be carried out independently in each modulo, that is

$$(x_1, x_2, \ldots, x_N) \bullet (y_1, y_2, \ldots, y_N) = (|x_1 \bullet y_1|_{m_1}, |x_2 \bullet y_2|_{m_2}, \ldots, |x_N \bullet y_N|_{m_N}),$$

where $\bullet$ denotes one of the arithmetic operations of addition, subtraction, and multiplication.

Now, we propose the new moduli set $\{2^n, 2^{2n}-1, 2^{2n}+1\}$. First, we show that this set meets the requirements of an RNS moduli set.

**Theorem 1.** *The set* $\{2^n, 2^{2n}-1, 2^{2n}+1\}$ *is a moduli set for the RNS.*

**Proof.** We need to show that the moduli are pair-wise relatively prime for any natural number $n$. It is clear that the first modulo is relatively prime to the other moduli, therefore we only need to show that the second and the third moduli are relatively prime. We assume that $\gcd(2^{2n}-1, 2^{2n}+1) = d$. So, $d$ counts $(2^{2n}-1)$ and $(2^{2n}+1)$, or in the mathematical notation we have

$$d|(2^{2n}-1) \quad \text{and} \quad d|(2^{2n}+1),$$

therefore, $d|(2^{2n}+1-(2^{2n}-1))$ or $d|2$. So, $d = 1$ or $d = 2$. But, we know that $d \neq 2$ because $2^{2n}-1$ and $2^{2n}+1$ are odd numbers, so $\gcd(2^{2n}-1, 2^{2n}+1) = d = 1$. ■

Therefore, our proposed moduli set can be used in the RNS, and we can now consider its reverse converter.

## 3. Reverse converter

In this section, we present the reverse converter of the moduli set $\{2^n, 2^{2n}-1, 2^{2n}+1\}$ but first, we provide two lemmas which are based on the properties that have been used in obtaining the reverse converters in [2,11,8].

**Lemma 1.** *The residue of a negative residue number* $(-v)$ *in modulo* $(2^n-1)$ *is the one's complement of* $v$*, where* $0 \le v < 2^n - 1$.