Residue-to-Decimal Converters for Moduli Sets with Common Factors

Kazeem Alagbe Gbolagade[1,2], Member, IEEE and Sorin Dan Cotofana[1], Senior Member IEEE,
1. Computer Engineering Laboratory, Delft University of Technology,
The Netherlands. E-mail: {gbolagade,sorin}@ce.et.tudelft.nl
2. University for Development Studies, Navrongo, Ghana.

***Abstract*—In this paper, we investigate Residue Number System (RNS) to decimal conversion for moduli sets with common factors. First, we propose a new RNS to decimal converter for the moduli set $\{2n{+}2, 2n{+}1, 2n\}$ for any integer $n > 0$, which is a generalization of a recently proposed reverse converter for this moduli set. Second, we provide a general 4-moduli RNS conversion scheme and then present a compact form of multiplicative inverses, valid for odd-n, for the moduli set $\{2n{+}3, 2n{+}2, 2n{+}1, 2n\}$. This extended moduli set increases the dynamic range and the processing parallelism enabling efficient conversion.**

***Index Terms*—Residue Number System, RNS-Decimal Conversion, Moduli Set With Common Factors, Multiplicative Inverses, Chinese Remainder Theorem.**

I. Introduction

The Residue Number System (RNS) is an integer system which speeds up arithmetic computations by spliting them into smaller parts in such a way that each part is independent of the other. RNS has the following interesting inherent features: parallelism, modularity, fault tolerance, and carry free operations [4]. These features make RNS to be widely used in Digital Signal Processing (DSP) applications such as digital filtering, convolution, fast Fourier transform, and image processing [1]. For successful application of RNS, data conversion must be very fast so that the conversion overhead doesn't nullify the RNS advantages. In view of this, data Conversion, which is usually based on either the Chinese Remainder Theorem (CRT) [3], [6], [8] or the Mixed Radix Conversion (MRC) [2] has been actively investigated. The RNS for a three moduli set has been studied for a long time with $\{2^n + 1, 2^n, 2^n - 1\}$ being the most popular one [6]. However, the moduli set $\{2n + 2, 2n + 1, 2n\}$ is a strong alternative candidate for decimal numbers which fall beyond the range specified by the $\{2^n + 1, 2^n, 2^n - 1\}$ moduli set resulting in the use of next higher index for n [6], [7], and [8]. The moduli set $\{2n + 2, 2n + 1, 2n\}$ is desirable because the numbers are consecutive, enabling nearly equal width adders and multipliers in the hardware implementation. Based on the weight concept, the decoding of RNS numbers for the moduli set $\{2n{+}2, 2n{+}1, 2n\}$ has been presented in [8]. The dynamic range provided by the three moduli sets is in some cases insufficient for high performance DSP applications requiring a large dynamic range. In view of that, in [5], the moduli set $\{2n + 2, 2n + 1, 2n\}$ was extended by adding $(2n{+}3)$ in order to obtain the 4-moduli superset $\{2n + 3, 2n + 2, 2n + 1, 2n\}$.

In this paper, we first propose a new RNS to decimal converter for the moduli set $\{2n + 2, 2n + 1, 2n\}$ for any integer $n > 0$. This eliminates the restriction in the reverse converter proposed in [4]. Second, we provide a general 4-moduli RNS conversion scheme and then present a compact form of multiplicative inverses (valid for n-odd) for the moduli set $\{2n + 3, 2n + 2, 2n + 1, 2n\}$. This again also removes the restriction in the converter presented in [5].

The rest of the article is organised as follows: Section II presents the necessary background. In Section III, for both n-even and odd, we present a reverse converter for the moduli set $\{2n + 2, 2n + 1, 2n\}$. We describe a reverse conversion algorithm, valid for n-odd, for the $\{2n + 3, 2n + 2, 2n + 1, 2n\}$ moduli set in Section IV, while the paper is concluded in Section V.

II. Background

RNS is defined in terms of a set of relatively prime moduli set $\{m_i\}_{i=1,t}$ such that $\gcd(m_i, m_j) = 1$ for $i \neq j$, where gcd means the greatest common divisor of m_i and m_j, while $M = \prod_{i=1}^{t} m_i$, is the dynamic range. The residues of a decimal number X can be obtained as $x_i = |X|_{m_i}$ thus X can be represented in RNS as $X = (x_1, x_2, x_3, ..., x_t)$, $0 \leq x_i < m_i$. This representation is unique for any integer $X \in [0, M - 1]$. We note here that in this paper we use $|X|_{m_i}$ to denote the X mod m_i operation.

For a moduli set $\{m_i\}_{i=1,t}$ with the dynamic range $M = \prod_{i=1}^{t} m_i$, the residue number $(x_1, x_2, x_3, ..., x_t)$ can be converted into the decimal number X, according to the Chinese Reminder Theorem, as follows [9]:

$$X = \left| \sum_{i=1}^{t} M_i \left| M_i^{-1} x_i \right|_{m_i} \right|_M , \quad (1)$$

where $M = \prod_{i=1}^{t} m_i$, $M_i = \frac{M}{m_i}$, and M_i^{-1} is the multiplicative inverse of M_i with respect to m_i. We note here that the moduli set $\{m_i\}_{i=1,t}$ must be pairwise relatively prime for Equation (1) to be directly used. The moduli set $\{2n + 2, 2n + 1, 2n\}$ has a common factor of 2. This implies that to utilize Equation (1) in the conversion this moduli set must be first mapped to a set of relatively prime moduli. If a moduli set is not pairwise relatively prime, then not every residue set $(x_1, x_2, x_3, ..., x_t)$ corresponds to a number and this results into inconsistency. As discussed in [9], a set of residues is consistent if and only if $|x_i|_k = |x_j|_k$ where

978-1-4244-4480-9/09/$25.00 ©2009 IEEE

$k = gcd(m_i, m_j)$ for all i and j. If this holds true the decimal equivalent of $(x_1, x_2, x_3, ..., x_t)$ for moduli set which are not pairwise relatively prime can be computed as follows:

$$|X|_{M_L} = \left|\sum_{i=1}^{t} \alpha_i x_i\right|_{M_L}, \qquad (2)$$

where M_L is the Lowest Common Multiple (LCM) of $\{m_i\}_{i=1,t}$, the set of moduli sharing a common factor, X is the decimal equivalent of $\{x_i\}_{i=1,t}$, α_i is an integer such that $|\alpha_i|_{\frac{M_L}{\mu_i}} = 0$ and $|\alpha_i|_{\mu_i} = 1$, and $\{\mu_i\}_{i=1,t}$ is a set of integers such that $M_L = \prod_{i=1}^{t} \mu_i$ and μ_i divides m_i. It should be noted that α_i may not exist for some i. In [3], Equation (2) has been represented as:

$$|X|_{M_L} = \left|\sum_{i=1}^{t} \beta_i \left|\beta_i^{-1}\right|_{\mu_i} x_i\right|_{M_L}, \qquad (3)$$

where $M_L = LCM\,\{m_i\}_{i=1}^{t} = \prod_{i=1}^{t} \mu_i$, $\beta_i = \frac{M_L}{\mu_i}$, $\left|\beta_i^{-1}\right|_{\mu_i}$ is the multiplicative inverse of β_i with respect to μ_i.

III. A Conversion Algorithm for the $\{2n+2, 2n+1, 2n\}$ Moduli Set

Given the RNS number (x_1, x_2, x_3) with respect to the moduli set $\{m_1 = 2n+2, m_2 = 2n+1, m_3 = 2n\}$, the proposed algorithm computes the decimal equivalent of the RNS number based on a further simplification of the well-known traditional CRT. We show that the computation of the multiplicative inverses can be eliminated for this moduli set. It should be noted that Equation (1) cannot be directly used for the conversion since in the moduli set $\{2n+2, 2n+1, 2n\}$, the moduli $2n+2$ and $2n$ share a common factor of 2. The moduli set must be first mapped into a set of relatively prime integers. In [8], it has been demonstrated that such a mapping can easily be done and that the set of relatively prime moduli for $\{2n+2, 2n+1, 2n\}$ moduli set, for any even and odd integer $n > 0$, respectively, are given by $\{n+1, 2n+1, 2n\}$ and $\{2n+2, 2n+1, n\}$, meaning that the new moduli set, respectively, are $\left\{\frac{m_1}{2}, m_2, m_3\right\}$ and $\left\{m_1, m_2, \frac{m_3}{2}\right\}$.

Theorem 1: Given the moduli set $\{m_1, m_2, m_3\}$ with $m_1 = 2n+2, m_2 = 2n+1, m_3 = 2n$ for any even integer n, the following hold true:

$$\left|(\frac{m_1}{2} m_2)^{-1}\right|_{m_3} = n+1, \qquad (4)$$

$$\left|(m_2 m_3)^{-1}\right|_{\frac{m_1}{2}} = \frac{n}{2}+1, \qquad (5)$$

$$\left|(\frac{m_1}{2} m_3)^{-1}\right|_{m_2} = 2n-1. \qquad (6)$$

Proof:

This has been proved in [4]. ■

Theorem 2: Given the moduli set $\{m_1, m_2, m_3\}$ with $m_1 = 2n+2, m_2 = 2n+1, m_3 = 2n$ for any odd integer n, the following hold true:

$$\left|(m_1 m_2)^{-1}\right|_{\frac{m_3}{2}} = \frac{n+1}{2}, \qquad (7)$$

$$\left|\left(m_2 \frac{m_3}{2}\right)^{-1}\right|_{m_1} = n+2, \qquad (8)$$

$$\left|\left(m_1 \frac{m_3}{2}\right)^{-1}\right|_{m_2} = 2n-1. \qquad (9)$$

Proof: If it can be shown that $\left|\frac{(n+1)}{2} \times (m_1 m_2)\right|_{\frac{m_3}{2}} = 1$, then $\frac{(n+1)}{2}$ is the multiplicative inverse of $(m_1 m_2)$ with respect to $\frac{m_3}{2}$. $\left|\frac{(n+1)}{2} \times (m_1 m_2)\right|_{\frac{m_3}{2}}$ is given by: $|(n+1)(n+1)(2n+1)|_n = |(n^2+2n+1)(2n+1)|_n = |2n^3+5n^2+4n+1|_n = ||2n^3|_n+|5n^2|_n+|4n|_n+|1|_n|_n = |0+0+0+1|_n = 1$, thus Equation (7) holds true.

In the same way, if $\left|(n+2) \times \left(m_2 \frac{m_3}{2}\right)\right|_{m_1} = 1$, then $(n+2)$ is the multiplicative inverse of $\left(m_2 \frac{m_3}{2}\right)$ with respect to m_1. $\left|(n+2)\left(m_2 \frac{m_3}{2}\right)\right|_{m_1}$ is given by: $|(n+2)(2n+1)(n)|_{2n+2} = |(n+2)(2n^2+n)|_{2n+2} = |2n^3+n^2+4n^2+2n|_{2n+2} = |2n^3+2n^2+n^2+n(2n+2)|_{2n+2} = |(n^2+n)(2n+2)+n^2|_{2n+2} = ||(n^2+n)(2n+2)|_{2n+2}+|n^2|_{2n+2}|_{2n+2} = |0+1|_{2n+2} = 1$, thus Equation (8) holds true.

Again, if $|\left((2n-1) \times m_1 \frac{m_3}{2}\right)|_{2n+1} = 1$, then $2n-1$ is the multiplicative inverse of $m_1 \frac{m_3}{2}$ with respect to m_2. $|\left((2n-1) \times m_1 \frac{m_3}{2}\right)|_{2n+1}$ is given by $|(2n-1)(2n+2)(n)|_{2n+1} = |(2n-1)(2n^2+2n)|_{2n+1} = |4n^3+4n^2-2n^2-2n|_{2n+1} = |4n^3+2n^2-2n|_{2n+1} = |2n^2(2n+1)-2n|_{2n+1} = ||2n^2(2n+1)|_{2n+1}+|-2n|_{2n+1}|_{2n+1} = |0+1|_{2n+1} = 1$, thus Equation (9) holds true. ■

As stated in Section II, for moduli sets with a common factor, not all remainder sets are valid numbers. The following proposition states the condition for a 3-residue set to represent a valid number.

Proposition 1: For RNS with the moduli set $\{m_1, m_2, m_3\}$ sharing a common factor, (x_1, x_2, x_3) represents a valid number if and only if $(x_1 + x_3)$ is even.

Proof: This proposition has been proved in [6]. ■

The following theorem introduces a simplified way to compute 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 $\{2n+2, 2n+1, 2n\}$ for both even and odd integer $n > 0$.

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 $\{2n+2, 2n+1, 2n\}$ for any integer $n > 0$ is given by:

$$X = \left|\frac{m_2 m_3}{2} x_1 - m_1 m_3 x_2 + \frac{m_1 m_2}{2} x_3\right|_{M_L}, \qquad (10)$$

where $M_L = \frac{m_1 m_2 m_3}{2}$.

Proof: Given that Equation (10) was proved to be true for n-even in [4], we only need to prove it for n-odd.
For $t = 3$, Equation (1) becomes:

$$X = \left|\sum_{i=1}^{3} M_i \left|M_i^{-1} x_i\right|_{m_i}\right|_{M_L}. \qquad (11)$$

By substituting Equations (7), (8), and (9) into Equation (11) we obtain the following:

$$\begin{aligned} X &= \Big|\left(m_2\frac{m_3}{2}\right)(m_1+2)x_1 + \left(m_1\frac{m_3}{2}\right)(m_2-2)x_2 \\ &\quad +(m_1m_2)\frac{(m_3+2)}{4}\Big|_{M_L} \\ &= \Big|\frac{m_1m_2m_3}{4}x_1 + \frac{m_2m_3}{2}x_1 + \frac{m_1m_2m_3}{2}x_2 \\ &\quad -m_1m_3x_2 + \frac{m_1m_2m_3}{4}x_3 + \frac{m_1m_2}{2}x_3\Big|_{M_L} \\ &= \Big|\left(\frac{m_2m_3}{4}\right)x_1(m_1-2) + m_2m_3x_1 + M_Lx_2 \\ &\quad -m_1m_3x_2 + \frac{m_1m_2}{4}x_3(m_3+2)\Big|_{M_L} \end{aligned}$$

Further simplifications give:

$$\begin{aligned} X &= \Big|\Big|\frac{M_L}{2}(x_1+x_3)\Big|_{M_L} + \Big|(\frac{m_2m_3}{2})x_1\Big|_{M_L} \\ &\quad -|m_1m_3x_2|_{M_L} + \Big|(\frac{m_1m_2}{2})x_3\Big|_{M_L}\Big|_{M_L} \end{aligned} \qquad (12)$$

Since each of the terms $\frac{m_2m_3}{2}x_1$, $m_1m_3x_2$, and $\frac{m_1m_2}{2}x_3$ in Equation (12) is positive and less than M_L and also from Proposition I, (x_1+x_3) must always be even, which implies that, $\left|(x_1+x_3)\frac{M_L}{2}\right|_{M_L} = 0$. Equation (12) therefore reduces to:

$$X = \Big|\frac{m_2m_3}{2}x_1 - m_1m_3x_2 + \frac{m_1m_2}{2}x_3\Big|_{M_L} \qquad (13)$$

Thus, Equation (10) holds true for both n-even and odd. ■

Therefore, the following simplification for Equation (10) proposed in [4] for any even integer n also holds true for any odd integer n.

Theorem 4: 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 $\{2n+2, 2n+1, 2n\}$ for both even and odd integer $n > 0$ is computed as follows:

$$\begin{aligned} X &= (x_2-x_1)m_1 + x_1 \\ &\quad +m_1m_2\Big|\frac{(x_1+x_3)}{2} - x_2\Big|_{\frac{m_3}{2}} \end{aligned} \qquad (14)$$

Proof: Equation (14) has been proved in [4] for n-even starting from the expression in Equation (10). Given that, as proved in Theorem 3, Equation (10) holds true for n-even, Equation (14) holds true for that case too. ■

Given that larger dynamic range is of practical interest, we present an efficient reverse converter for the moduli set $\{2n+3, 2n+2, 2n+1, 2n\}$, which is an extension of the $\{2n+2, 2n+1, 2n\}$ moduli set in the next section.

IV. A Conversion Algorithm for the $\{2n+3, 2n+2, 2n+1, 2n\}$ Moduli Set

Given the RNS number (x_1, x_2, x_3, x_4) with respect to the moduli set $\{m_1 = 2n+3, m_2 = 2n+2, m_3 = 2n+1, m_4 = 2n\}$, the decimal equivalent of the RNS number is computed based on a further simplification of the well-known traditional CRT. However, it should be noted that Equation (1) cannot be directly used for the conversion since the moduli $2n+2$ and $2n$ share a common factor of 2. In [5], it has been shown that the set of relatively prime moduli for $\{2n+3, 2n+2, 2n+1, 2n\}$ moduli set are $\{2n+3, n+1, 2n+1, 2n\}$ and $\{2n+3, 2n+2, 2n+1, n\}$ respectively, for n even and odd.

Theorem 5: For a moduli set $\{m_i\}_{i=1,4}$, $m_1 > m_2 > m_3 > m_4$, the decimal equivalent X of the residues (x_1, x_2, x_3, x_4) can be computed by using mod-m_4 (the smallest modulus) instead of the large mod-M operations as:

$$\begin{aligned} X = (x_1+x_2+x_3) + m_1m_2m_3|k_1x_1 + k_2x_2 \\ +k_3x_3 + \left|M_4^{-1}\right|_{m_4} x_4|_{m_4}, \end{aligned} \qquad (15)$$

where M_4^{-1} is the multiplicative inverse of M_4,
$k_1 = \frac{\left(M_1\left|M_1^{-1}\right|_{m_1}-1\right)}{m_1m_2m_3}$,
$k_2 = \frac{\left(M_2\left|M_2^{-1}\right|_{m_2}-1\right)}{m_1m_2m_3}$ and $k_3 = \frac{\left(M_3\left|M_3^{-1}\right|_{m_3}-1\right)}{m_1m_2m_3}$.

Proof: It has been proved in [5]. ■

Next, we show that the compact forms of multiplicative inverses do exist for the moduli set $\{2n+3, 2n+2, 2n+1, 2n\}$ using the following theorems:

Theorem 6: Given the moduli set $\{m_1, m_2, m_3, m_4\}$ with $m_1 = 2n+3, m_2 = 2n+2, m_3 = 2n+1, m_4 = 2n$, the following hold true:

$$\left|M_2^{-1}\right|_{m_2} = \frac{n}{2} + 1, \qquad (16)$$

$$\left|M_3^{-1}\right|_{m_3} = 2n. \qquad (17)$$

Proof: This has been proved in [5] ■

The multiplicative inverses of M_1 and M_4 can be computed as demonstrated by the following theorems:

Theorem 7: For odd numbers of the form $\{5, 11, 17, 23, 29, 35, ...\}$, represented by $n = \{6k-1\}_{k=1,2,3,...}$

$$\left|M_1^{-1}\right|_{m_1} = 4k, \qquad (18)$$

$$\left|M_4^{-1}\right|_{m_4} = k, \qquad (19)$$

Proof: From the Theorem, $|M_1^{-1}|_{m_1} = 4k = 4(k)$. Thus, $|M_1^{-1}|_{m_1} = 4|M_4^{-1}|_{m_4}$, then we shall show the proof of $|M_1^{-1}|_{m_1}$ only. $M_1 = m_2m_3\frac{m_4}{2}$, meaning that $M_1 = (2n+2)(2n+1)(n)$, for different values of n, $|M_1M_1^{-1}|_{m_1}$ will be given by: $n = 5$, when $|M_1^{-1}|_{m_1} = 4$, and also $|4(2n+2)(2n+1)(n)|_{2n+3} = |16n^3 + 24n^2 + 8n|_{2n+3} = ||8n^2(2n+3)|_{2n+3} + |8n|_{2n+3}|_{2n+3} = |0+1|_{2n+3} = 1$.

Similarly, when $n = 11$, $|M_1^{-1}|_{m_1} = 8$, and $|8(2n+2)(2n+1)(n)|_{2n+3} = |32n^3+48n^2+16n|_{2n+3} = ||16n^2(2n+3)|_{2n+3} + |16n|_{2n+3}|_{2n+3} = |0+1|_{2n+3} = 1$.

Again, when $n = 17$, $|M_1^{-1}|_{m_1} = 12$, and $|12(2n+2)(2n+1)(n)|_{2n+3} = |48n^3+72n^2+24n|_{2n+3} = ||24n^2(2n+3)|_{2n+3} + |24n|_{2n+3}|_{2n+3} = |0+1|_{2n+3} = 1$. Hence, if it is true for $n = 5, 11, 17$, then it will be true for any odd integer n in this category. ■

Theorem 8: For odd numbers of the form $\{7, 13, 19, 25, 31, ...\}$, represented by $n = \{6k + 1\}_{k=1,2,3,...}$

$$\left|M_1^{-1}\right|_{m_1} = 8k + 3, \tag{20}$$

$$\left|M_4^{-1}\right|_{m_4} = 5k + 1, \tag{21}$$

Proof: We first show that $|M_1^{-1}|_{m_1}$ is valid as follows: $M_1 = m_2 m_3 \frac{m_4}{2} = (2n + 2)(2n + 1)(n)$, for different values of n, $|M_1 M_1^{-1}|_{m_1}$ will be given by: $n = 7$, when $|M_1^{-1}|_{m_1} = 11$, and also $|11(2n + 2)(2n + 1)(n)|_{2n+3} = |44n^3 + 66n^2 + 22n|_{2n+3} = ||22n^2(2n + 3)|_{2n+3} + |22n|_{2n+3}|_{2n+3} = |0 + 1|_{2n+3} = 1$.

Similarly, when $n = 13$, $|M_1^{-1}|_{m_1} = 19$, and $|19(2n + 2)(2n + 1)(n)|_{2n+3} = |76n^3 + 114n^2 + 38n|_{2n+3} = ||38n^2(2n + 3)|_{2n+3} + |38n|_{2n+3}|_{2n+3} = |0 + 1|_{2n+3} = 1$.

Again, when $n = 19$, $|M_1^{-1}|_{m_1} = 27$, and $|27(2n+2)(2n+1)(n)|_{2n+3} = |108n^3 + 162n^2 + 54n|_{2n+3} = ||54n^2(2n + 3)|_{2n+3} + |54n|_{2n+3}|_{2n+3} = |0 + 1|_{2n+3} = 1$. Hence, if it is true for $n = 7, 13, 19$, then it will be true for any odd integer n in this category.

We then show the validity of $|M_4^{-1}|_{m_4}$ as follows: $M_4 = m_1 m_2 m_3 = (2n + 3)(2n + 2)(2n + 1)$, for different values of n, $|M_4 M_4^{-1}|_{m_4}$ will be given by: $n = 7$, when $|M_4^{-1}|_{m_4} = 6$, and also $|6(2n+3)(2n+2)(2n+1)|_n = |6(8n^3+24n^2+22n+6)|_n = ||6(8n^2 + 24n + 22)(n)|_n + |36|_n|_n = |0 + 1|_n = 1$.

Similarly, when $n = 13$, $|M_4^{-1}|_{m_4} = 11$, and $|11(2n + 3)(2n + 2)(2n + 1)|_n = |11(8n^3 + 24n^2 + 22n + 6)|_n = ||11(8n^2 + 24n + 22)(n)|_n + |66|_n|_n = |0 + 1|_n = 1$.

Again, when $n = 19$, $|M_4^{-1}|_{m_4} = 16$, and $|16(2n+3)(2n+2)(2n + 1)|_n = |16(8n^3 + 24n^2 + 22n + 6)|_n = ||16(8n^2 + 24n + 22)(n)|_n + |96|_n|_n = |0 + 1|_n = 1$. Hence, if it is true for $n = 7, 13, 19$, then it will be true for any odd integer n in this category.

■

Putting $m_2 = 2n + 2$ and $m_4 = 2n$ in Equations (16) and (17), respectively, we obtain:

$$\left|M_2^{-1}\right|_{m_2} = \frac{m_2 + 2}{4}, \left|M_3^{-1}\right|_{m_3} = m_4. \tag{22}$$

Using Equation (22) and by proper substitutions in Theorem 5, we can particularize it for 4-moduli RNS sharing a common factor as follows:

Corollary 1: For the moduli set $\{2n + 3, 2n + 2, 2n + 1, 2n\}$, the decimal equivalent X of the residues $(x_{1,} x_2, x_3, x_4)$ can be computed as follows:

1) (**Using Theorem 7**):

$$X = (x_1 + x_2 + x_3) + m_1 m_2 m_3 |k_1 x_1 + k_2 x_2 + k_3 x_3 + k x_4|_{m_4}, \tag{23}$$

where $k_1 = \frac{(4k m_2 m_3 m_4 - 1)}{m_1 m_2 m_3}$,
$k_2 = \frac{\left(m_1 m_3 m_4 \left(\frac{m_2+2}{4}\right) - 1\right)}{m_1 m_2 m_3}$, and

$k_3 = \frac{(m_1 m_2 m_4 (m_4) - 1)}{m_1 m_2 m_3}$

2) (**Using Theorem 8**):

$$X = (x_1 + x_2 + x_3) + m_1 m_2 m_3 |k_1 x_1 + k_2 x_2 + k_3 x_3 + (5k + 1) x_4|_{m_4}, \tag{24}$$

where $k_1 = \frac{(m_2 m_3 m_4 (8k+3) - 1)}{m_1 m_2 m_3}$,

$k_2 = \frac{\left(m_1 m_3 m_4 \left(\frac{m_2+2}{4}\right) - 1\right)}{m_1 m_2 m_3}$ and

$k_3 = \frac{(m_1 m_2 m_4 (m_4) - 1)}{m_1 m_2 m_3}$

Proof: Trivial with proper substitutions for the values of $\left|M_2^{-1}\right|_{m_2}$ and $\left|M_3^{-1}\right|_{m_3}$ together with $\left|M_1^{-1}\right|_{m_1}$ and $\left|M_4^{-1}\right|_{m_4}$, which are obtained from Theorems 7 and 8. ■

In terms of both area and delay, the reverse converter proposed in here for the moduli set $\{2n+3, 2n+2, 2n+1, 2n\}$ and the one in [5] are the same. However, we show here that for n-odd, this moduli set can still be utilized whereas the applicability of this moduli set was only demonstrated in [5] for n-even.

V. Conclusions

In this paper, we first demonstrated that for the $\{2n+2, 2n+1, 2n\}$ moduli set, the computation of multiplicative inverses can be eliminated and proved that for n even or odd, the hardware realization is the same eliminating the restriction in the reverse converter proposed in [4]. Second, we provided a general 4-moduli RNS conversion scheme and then presented a compact form of multiplicative inverses for the moduli set $\{2n+3, 2n+2, 2n+1, 2n\}$. This increases the dynamic range and the processing parallelism enabling efficient conversion. Moreover, the proposed schemes operate on smaller magnitude operands, requiring less complex adders and multipliers, which potentially result in faster and smaller implementations.

References

[1] R. Conway and J. Nelson. Improved rns fir filter architectures. *IEEE Trans. on Circuits and Systems-II: Express briefs, Vol. 51, No.1, pp. 26-28, January*, 2004.

[2] W.S. McCormick D.F. Miller. An arithmetic free parallel mixed radix conversion algorithm. *IEEE Trans. on Circuits and Systems-II: Analog and Digital Signal Processing, Vol. 45, No.1, pp. 158-162, January*, 1998.

[3] K.A. Gbolagade and S.D. Cotofana. Residue number system operands to decimal conversion for 3-moduli sets. *Proceedings of 51st IEEE Midwest Symposium on Circuits and Systems, pp.791-794, Knoxville, USA, August*, 2008.

[4] K.A. Gbolagade and S.D. Cotofana. A residue to binary converter for the $\{2n + 2, 2n + 1, 2n\}$ moduli set. *To appear in proceedings of 42nd Asilomar Conference on Signals, Systems, and Computers, California, USA, October*, 2008.

[5] K.A. Gbolagade and S.D. Cotofana. A reverse converter for the new 4-moduli set $\{2n + 3, 2n + 2, 2n + 1, 2n\}$. *Submitted to IEEE NEWCAS-TAISA, Toulouse, France, July*, 2009.

[6] M.N.S. Swamy M.O. Ahmad, Y. Wang. Residue to binary number converters for three moduli set. *IEEE Trans. on Circuits and Systems-II, Vol. 46, No.7, pp. 180-183, Feb.*, 1999.

[7] A.B. Premkumar. An rns to binary converter in 2n+1,2n,2n-1 moduli set. *IEEE Trans. on Circuits and Systems-II: Analog and Digital Signal Processing, Vol. 39, No.7, pp. 480-482, July*, 1992.

[8] A.B. Premkumar. Residue to binary converter in three moduli set with common factors. *IEEE Trans. on Circuits and Systems-II: Analog and Digital Signal Processing, Vol. 42, No.4, pp. 298-301, April*, 1995.

[9] N. Szabo and R Tanaka. *Residue Arithmetic and its Application to Computer Technology*. MC-Graw-Hill, New York, 1967.