MRC Technique for RNS to Decimal Conversion Using the Moduli Set $\{2n + 2, 2n + 1, 2n\}$

Kazeem Alagbe Gbolagade[1,2], Member, IEEE and Sorin Dan Cotofana[1], Senior Member IEEE,
1. Computer Engineering Laboratory, Delft University of Technology,
Mekelweg 4, 2628 CD Delft, the Netherlands.
Tel: +31-15-278-6267, Fax: +31-15-278-4898.
E-mail: {gbolagade,sorin}@ce.et.tudelft.nl
2. University for Development Studies, Navrongo, Ghana.

***Abstract*—This paper investigates the conversion of Residue Number System (RNS) operands to decimal, which is an important issue concerning the utilization of RNS numbers in digital signal processing applications. We present a Mixed Radix Conversion (MRC) technique for efficient RNS to decimal conversion using the moduli set $\{2n + 2, 2n + 1, 2n\}$, which has a common factor of 2. First, we provide two important theorems which show that, using such a moduli set, the computation of multiplicative inverses can be eliminated. The usage of these theorems with the traditional MRC results into two reverse converters. In terms of area, the proposed converters require 3 adders, 4 mutipliers and mod-m_2 and m_3 operations. The proposed converters also require 2 additions, 2 multiplications with mod-m_3 operation in terms of critical path delay. Our proposals outperform state of the art equivalent Chinese Remainder Theorem (CRT) based reverse converter in terms of delay and due to the fact that the numbers involved in the calculations are smaller it results in less complex adders and multipliers.**

***Index Terms*—Residue Number System, Mixed Radix Conversion, Data Conversion, Mixed Radix Digits, arithmetic operations**

I. Introduction

The usage of Residue Number System (RNS) in Digital Signal Processing (DSP) applications has received considerable attention due to its attractive carry-free property which yields arithmetic processors that are inherently parallel, modular and fault isolating [1],[2],[7]. For successful application of RNS, data conversion must be very fast so that the conversion overhead doesn't nullify the RNS advantages [7].

The work on residue to binary conversion is based on Chinese Remainder Theorem (CRT) [6],[8]-[12] or on Mixed Radix Conversion (MRC) [3]-[5],[13]. CRT is desirable because the computation can be parallelized while MRC is by its very nature a sequential process. However many up to date RNS to binary/decimal converters are based on MRC due to the complex and slow modulo-M operation (M being the system dynamic range thus a rather large constant) required by CRT. The main problem with the MRC is that the computations of the MR digits is done in a serial manner and requires a large number of arithmetic operations.

In this paper, we present an MRC technique for efficient RNS to decimal conversion using the moduli set $\{2n + 2, 2n + 1, 2n\}$, which has a common factor of 2. First, we provide two important theorems which show that, using such a moduli set, the computation of multiplicative inverses can be eliminated. The usage of these theorems with the traditional MRC results into two reverse converters. In terms of area, the proposed converters require 3 adders, 4 mutipliers and mod-m_2 or m_3 operations. The proposed converters also require 2 additions, 2 multiplications with mod-m_3 operation in terms of critical path delay. Our proposals outperform state of the art equivalent Chinese Remainder Theorem (CRT) based reverse converter in terms of required operations and due to the fact that the numbers involved in the calculations are smaller it results in less complex adders and multipliers.

The rest of the article is organised as follows: Section II presents the necessary background. In Section III we describe the proposed algorithm. In Section IV, we evaluate the performance of our proposal while the paper is concluded in Section V.

II. Background

RNS is defined in terms of a set of relatively prime moduli set $\{m_i\}_{i=1,n}$ 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 $M = \prod_{i=1}^{n} m_i$, 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 $X = (x_1, x_2, x_3..., x_n)$, $0 \leq x_i < m_i$. 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 and the operator Θ to represent the operation of addition, subtraction, or multiplication. Given any two integer numbers K and L in RNS represented by $K = (k_1, k_2, k_3, ..., k_n)$ and $L = (l_1, l_2, l_3, ..., l_n)$, respectively, $W = K\Theta L$, can be calculated as $W = (w_1, w_2, w_3, ..., w_n)$, where $w_i = |k_i \Theta l_i|_{m_i}$, for $i = 1, n$. This means that the complexity of the calculation of the Θ operation is determined by the number of bits required to represent the residues and not by the one required to represent the input operands.

The conversion from RNS to decimal using MRC can be formulated as follows [2]:

Given an n-digit number $X = (x_1, x_2, x_3, ..., x_n)$ in an RNS with the set of relatively prime integer moduli $\{m_i\}_{i=1,n}$ find a set of digits $\{a_1, a_2, a_3, ..., a_n\}$, which are the mixed radix digits (MRD), such that Equation (1) holds true.

$$\begin{aligned} X &= a_1 + a_2 m_1 + a_3 m_1 m_2 + ... \\ &+ a_n m_1 m_2 m_3 ... m_{n-1} \end{aligned} \tag{1}$$

The mixed radix digits can be computed as follows [13]:

$$\begin{aligned} a_1 &= x_1 \\ a_2 &= \left| (x_2 - a_1) \left| m_1^{-1} \right|_{m_2} \right|_{m_2} \\ a_3 &= \left| \left((x_3 - a_1) \left| m_1^{-1} \right|_{m_3} - a_2 \right) \left| m_2^{-1} \right|_{m_3} \right|_{m_3} \\ & ... \\ a_n &= |((...(x_n - a_1)|m_1^{-1}|_{m_n} - a_2)|m_2^{-1}|_{m_n} - ... \\ & -a_{n-1})|m_{n-1}^{-1}|_{m_n}|_{m_n} \end{aligned} \tag{2}$$

Given the MRD $a_i, 0 \leq a_i < m_i$, any positive number in the interval [0, $\Pi_{i=1}^{N} m_i - 1$] can be uniquely represented.

For a moduli set $\{m_i\}_{i=1,n}$ with the dynamic range $M = \prod_{i=1}^{n} m_i$, the residue number $(x_1, x_2, x_3, ..., x_n)$ can be converted into the decimal number X, according to the Chinese Reminder Theorem, as follows [2]:

$$X = \left| \sum_{i=1}^{n} M_i \left| M_i^{-1} x_i \right|_{m_i} \right|_{M}, \tag{3}$$

where $M = \prod_{i=1}^{n} m_i$, $M_i = \frac{M}{m_i}$, and M_i^{-1} is the multiplicative inverse of M_i with respect to m_i.

The proposed MRC presented in the last section can be further simplified if certain moduli such as $\{2n+2, 2n+1, 2n\}$ are utilized. For this moduli set, different converters have been presented based on the simplification of the well known traditional CRT. The best of such converters is given in [6] and represented as :

$$\begin{aligned} X &= x_2 + m_2 \left| \left\lfloor \frac{(x_1 - x_3) + 2z_0 n}{2} \right\rfloor \right. \\ &+ \left. 2n \left\lfloor \frac{(x_1 - 2x_2 + x_3) + 2z_0 n}{2} \right\rfloor \right|_{m_1 m_3}, \end{aligned} \tag{4}$$

where z_0 is the XOR over the least significant bits of x_1 and x_3.

We assume the same moduli sets $\{2n+2, 2n+1, 2n\}$ and we introduce an RNS to decimal converter based on the traditional MRC. We first show that the computation of the required multiplicative inverses can be eliminated using this moduli set. By doing that we obtain relations that use lesser number of arithmetic operations when compared to Equation (4).

In the following section we present two reverse converters using the moduli set $\{2n+2, 2n+1, 2n\}$. The two converters use smaller moduli operation compared to Equation (4).

III. Proposed Algorithm

Given the RNS number (x_1, x_2, x_3) with respect to the moduli set $\{m_1, m_2, m_3\}$ in the form $\{2n+2, 2n+1, 2n\}$, the proposed algorithm computes the decimal equivalent of this RNS number based on the well-known traditional MRC. First, we demonstrate that the computation of the multiplicative inverses can be eliminated using this moduli set. Next, based on the compact forms of the multiplicative inverses, we obtain two reverse converters that use modulo m_2 and modulo m_3 instead of modulo $m_1 m_3$ used by the state of the art CRT based equivalent converter.

Theorem 1: Given the moduli set $\{2n+2, 2n+1, 2n\}$ with $m_1 = 2n+2, m_2 = 2n+1, m_3 = 2n$, for any even integer $n > 0$, the following hold true:

$$|(\frac{m_1}{2})^{-1}|_{m_2} = 2, \tag{5}$$

$$|(m_2)^{-1}|_{m_3} = 1, \tag{6}$$

$$|(\frac{m_1}{2})^{-1}|_{m_3} = \frac{m_1}{2}. \tag{7}$$

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

In the same way if $|1 \times m_2|_{m_3} = 1$, then 1 is the multiplicative inverse of m_2 with respect to m_3. $|1 \times$

$m_2|_{m_3}$ is given by: $|1 \times (2n+1)|_{2n} = ||2n|_{2n} + |1|_{2n}|_{2n} = |0+1|_{2n} = 1$, thus Equation(6) holds true.

Again, if $|(\frac{m_1}{2})(\frac{m_1}{2})|_{m_3} = 1$, then $\frac{m_1}{2}$ is the multiplicative inverse of $\frac{m_1}{2}$ with respect to m_3. $|(\frac{m_1}{2})(\frac{m_1}{2})|_{m_3}$ is therefore given by $|(n+1)(n+1)|_{2n} = |n^2+2n+1|_{2n} = ||n^2|_{2n} + |2n|_{2n} + |1|_{2n}|_{2n} = |0+0+1|_{2n} = 1$, thus Equation(7) holds true. ■

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

$$|(m_1)^{-1}|_{m_2} = 1, \quad (8)$$

$$|(m_2)^{-1}|_{\frac{m_3}{2}} = 1, \quad (9)$$

$$|(m_1)^{-1}|_{\frac{m_3}{2}} = \frac{m_1}{4}. \quad (10)$$

Proof: If it can be demonstrated that $|1 \times (m_1)^{-1}|_{m_2} = 1$, then 1 is the multiplicative inverse of m_1 with respect to m_2. $|1 \times (m_1)^{-1}|_{m_2}$ is given by: $|1 \times (2n+2)|_{2n+1} = |2n+2|_{2n+1} = 1$, thus Equation (8) holds true.

In the same way if $|1 \times m_2|_{\frac{m_3}{2}} = 1$, then 1 is the multiplicative inverse of m_2 with respect to $\frac{m_3}{2}$. $|1 \times m_2|_{\frac{m_3}{2}}$ is given by: $|1 \times (2n+1)|_n = ||2n|_n + |1|_n|_{2n} = |0+1|_n = 1$, thus Equation(9) holds true.

Again, if $|(\frac{m_1}{4})m_1|_{\frac{m_3}{2}} = 1$, then $(\frac{m_1}{4})$ is the multiplicative inverse of m_1 with respect to $\frac{m_3}{2}$. $|(\frac{m_1}{4})m_1|_{\frac{m_3}{2}}$ is therefore given by: $|(\frac{(2n+2)}{4})(2n+2)|_n$= $|(n+1)(n+1)|_n = |n^2+2n+1|_n = ||n^2|_n + |2n|_n + |1|_n|_n = |0+0+1|_n = 1$, thus Equation(10) holds true. ■

Proposition 1: For RNS with 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]. ■

Making the appropriate substitution in Equation (1), we can particularize it for 3-moduli RNS sharing a common factor as follows:

Corollary 1: For the moduli set $\{2n+2, 2n+1, 2n\}$ the decimal equivalent X of the residue set $\{x_1, x_2, x_3\}$, $(x_1 + x_3)$ being even, can be computed as follows:

1) If n is **even**, $n > 0$:

$$\begin{aligned} a_1 &= x_1 \\ a_2 &= |2(x_2 - a_1)|_{m_2} \\ a_3 &= |(\frac{m_1}{2}(x_3 - a_1) - a_2)|_{m_3} \end{aligned}$$

2) If n is **odd**, $n > 1$:

$$\begin{aligned} a_1 &= x_1 \\ a_2 &= |2(x_2 - a_1)|_{m_2} \\ a_3 &= |(\frac{m_1}{2}(x_3 - a_1) - a_2)|_{m_3} \end{aligned}$$

Operations	[6]	CI for n-even	CII for n-odd
Additions	7	5	5
Multiplications	2	4	3
Reduced M	$m_1 m_3$	m_2 and m_3	m_2 and m_3

Table I
PERFORMANCE COMPARISON

Proof: Trivial with proper substitutions from Theorem 1 and Theorem 2 and also due to Proposition 1. ■

IV. PERFORMANCE EVALUATION

Clearly, it can be seen that the numbers involved in the multiplication are very small when compared to the numbers involved in the direct CRT or MRC implementations. Additionally, the large modulo M calculations in the traditional CRT are replaced by modulo calculations with the m_2 and m_3 moduli in the moduli set under consideration.

Previous work on 3-moduli RNS in [6,8] has demonstrated improvement over traditional CRT in terms of operands magnitude as this determines the complexity and delay of the associated RNS hardware. Additionally, [6] outperformed [8] in terms of the operands magnitude thus we compare our proposal with this approach. Table I presents performance comparison in terms of the number of arithmetic calculation and magnitude of the modulo operation. We note here in Table I that the following notations are utilized: CI for n-even stands for the proposed converter for n-even while CII for n-odd stands for the proposed converter n-odd. As indicated in Table I converter for n-even requires more arithmetic operations but smaller modulo calculations than [6] whereas converter for n-odd requires the same arithmetic operations as [4] but also smaller modulo calculations than [6]. Consequently, the operands magnitude is significantly reduced which is more important for the hardware complexity.

V. CONCLUSIONS

In this paper, we investigated the conversion of RNS operands to decimal, which is an important issue concerning the utilization of RNS numbers in DSP applications. We present an MRC technique for efficient RNS to decimal conversion using the moduli set $\{2n+2, 2n+1, 2n\}$, which has a common factor of 2. First, we provided two important theorems which show that, using such a moduli set, the computation of multiplicative inverses can be eliminated. The usage of these theorems with the traditional MRC results into two reverse converters. In terms of area, the proposed converters require 3 adders, 4 mutipliers and mod-m_2 or m_3 operations. The proposed converters also require 2 additions, 2 multiplications with mod-m_3 operation in terms of critical path delay. Our proposals outperform state of the art CRT based reverse converter in terms of delay and due to the fact that the numbers involved in the calculations are smaller it results in less complex adders and multipliers.

References

[1] H.L. Garner, The residue Number System, IRE Trans. on Electronic Computers, pp. 140-147, 1959.

[2] Szabo, N., and Tanaka, R. : Residue arithmetic and its application to computer technology, McGraw-Hill, New York, 1967.

[3] N.B. Chakraborti, J.S. Soundararajan and A.L.N. Reddy, An implementation of mixed-radix conversion for residue number applications, IEEE Trans. computer, Vol. C-35, Aug., 1986.

[4] C.H. Huang, A fully parallel mixed-radix conversion algorithm for residue number applications, IEEE Trans. computer, Vol. C-32, pp. 398-402, April, 1983.

[5] D.F. Miller and W.S. McCormick, An arithmetic free parallel mixed-radix conversion algorithm, IEEE Trans. Circuits Syst. II Analog and Digital Signal Processing, Vol. 45, pp. 158-162, Jan., 1998.

[6] M.O. Ahmad, Y. Wang, M.N.S Swamy, Residue to Binary Converters for three moduli set, IEEE Trans. Circuits Syst. II,, Vol. 46, pp. 180-183, Feb., 1999.

[7] M. A. Soderstrand, W. K. Jenkins, G. A. Jullien, and F. J. Taylor, Residue Number System Arithmetic: Modern Applications in Digital Signal Processing. New York, IEEE press, 1986.

[8] A. B. Premkuma, An RNS to Binary Converter in a Three Moduli Set with Common Factors, IEEE Trans. on Circuits and Systems-II: Analog and Digital Processing, Vol. 42, No. 4, pp 298-301, April, 1995.

[9] A. B. Premkuma, Corrections to An RNS to Binary Converter in a Three Moduli Set with Common Factors, IEEE Trans. on Circuits and Systems-II: Analog and Digital Processing, Vol. 51, No.1, pp 43, January, 2004.

[10] W. Wang, M.N.S. Swamy, M.O. Ahmad and W. Wang, A study of Residue to Binary Converters for the Three-Moduli Sets, IEEE Trans. on Circuits and Syst-Fundamental Theory and Applications, Vol. 50, No. 2, pp 235-245, 2003.

[11] Y. Wang, New Chinese Remainder Theorems, in Proc. Asilomar Conference, USA, pp. 165-171, Nov., 1998.

[12] 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.

[13] H.M. Yassine and W.R. Moore, Improved mixed-radix conversion for residue number architectures, IEEE proceedings, Vol. 138, No.1 pp120-124, Feb. 1991.