Modulo Operation Free Reverse Conversion in the $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$ Moduli Set

H. Siewobr and K.A.Gbolagade
Department of Computer Science,
University for Development Studies,
Navrongo, Ghana

ABSTRACT

This paper proposes a fast Mixed Radix Conversion based reverse converter for the recently proposed moduli set $\{\mathbf{2^{2n+1}-1, 2^n, 2^{2n}-1}\}$. It shows that the computation of multiplicative inverses could be eliminated from the conversion process and presents a low complexity and modulo operation free implementation. Theoretical analysis shows that the proposed scheme outperforms all state of the art equivalent converters in terms of both area cost and delay.

General Terms

Residue Number System, Circuits and Systems, Computer Arithmetic, Computer Architecture, Digital Signal Processing.

Keywords

Reverse Conversion, Mixed Radix Conversion, Moduli Set, Multiplicative Inverses.

1. INTRODUCTION

Residue Number System (RNS) is an integer number system with the capabilities to support parallel, carry-free addition, borrow-free subtraction and single step multiplication without partial product. These features enable RNS utilization in Digital Signal Processing (DSP) applications such as digital filtering, convolution, fast Fourier transform and image processing [9], [8]. For successful application of RNS, data conversion must be very fast so that the conversion overhead doesn't nullify the RNS advantages [9].

Data Conversion, which is usually based on either the Chinese Remainder Theorem (CRT) [7], [8] or the Mixed Radix Conversion (MRC) [9] can be categorized into forward and reverse conversions. The forward conversion involves converting a binary ordecimal number into its RNS equivalent while the reverse conversion is the inverse operation, i.e., it involves converting RNS number into binary or decimal. Relatively, reverse conversion is more complex. Many algorithms have been designed for performing the reverse conversion with different choices of moduli sets, e.g., $\{2^n-1, 2^n, 2^n+1\}$ [3], $\{2^n, 2^{n+1}-1, 2^n-1\}$ [1], [5] [6]. Recently, the moduli set $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$ was proposed in [8] from the moduli set $\{2^n-1, 2^n, 2^n+1, 2^{2n+1}-1\}$, in [5]. The major advantage of the moduli set $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$ is that it eliminates the long delay modulus (2^n+1) which increases the computation time of all the operations of the processor [8]. The proposed reverse converter in [8] has a slow conversion time.

In this paper, a new MRC based reverse converter for the $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$ moduli set proposed. It shows that the computation of the multiplicative inverses could be eliminated and presents a fast conversion process. Theoretically speaking, the proposed converter is cheaper and faster than the ones in [5], [6] and [8].

The rest of this article is organized as follows. In Section 2, the necessary background information is presented. Section 3 presents the proposed algorithm. The hardware implementation of the proposed scheme is presented in Section 4. Section 5 evaluates the performance of the proposed scheme while the paper is concluded in Section 6 and references provided in Section 7.

2. BACKGROUND

The MRC can be represented as [3]:

$$X = a_1 + a_2m_1 + a_3m_1m_2 + \cdots + a_nm_1m_2m_3 \ldots m_{n-1} \quad (1)$$

where the Mixed Radix Digits (MRDs), $a_i, i = 1, n$ can be computed as follows [1,4]:

$$a_1 = x_1$$

$$a_2 = |(x_2 - a_1)|m_1^{-1}|_{m_2}|_{m_2}$$

$$a_3 = \left|((x_3 - a_1)|m_1^{-1}|_{m_3} - a_2)|m_2^{-1}|_{m_3}\right|_{m_3}$$

$$a_n = \left|((\ldots(x_n - a_1)|m_1^{-1}|_{m_n} - a_2)|m_2^{-1}|_{m_3} - \cdots - a_{n-1})|m_{n-1}^{-1}|_{m_n}\right|_{m_n}$$

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

3. PROPOSED ALGORITHM

This section presents a fast reverse converter for the moduli set $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$.

Theorem 1: Given the moduli set $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$, where $m_1 = 2^{2n+1}-1$, $m_2 = 2^n$, and $m_3 = 2^{2n}-1$ for every integer $n > 1$, the followings hold true:

$$|m_1^{-1}|_{m_2} = 2^n - 1 \quad (3)$$

$$|m_2^{-1}|_{m_3} = 2^n \quad (4)$$

$$|m_1^{-1}|_{m_3} = 1 \quad (5)$$

Proof*:* If it can be demonstrated that $|(2^n-1)*(2^{2n+1}-1)|_{2^n} = 1$, then $2^n - 1$ is the multiplicative inverse of m_1 with respect to m_2.

$$\begin{aligned} |(2^n-1)*(2^{2n+1}-1)|_{2^n} &= |2^{3n+1} - 2^n - 2^{2n+1} + 1|_{2^n} \\ &= || 2^{2n+1}|_{2^n} - |2^n|_{2^n} - |2^{2n+1}|_{2^n} \\ &\quad + |1|_{2^n}|_{2^n} = |1|_{2^n} = 1 \end{aligned}$$

Thus (3) holds true.

Similarly, if it can be demonstrated that $|\,(2^n * 2^n)|_{2^{2n}-1} = 1$, then 2^n is the multiplicative inverse of m_2 with respect to m_3.

$$|\,(2^n * 2^n)|_{2^{2n}-1} = |2^{2n}|_{2^{2n}-1} = 1$$

Thus (4) holds true.

Again, if it can be demonstrated that $|\,(2^{2n+1}-1) * 1|_{2^{2n}-1} = 1$, then 1 is the multiplicative inverse of m_1 with respect to m_3.

$$\begin{aligned}|\,(2^{2n+1}-1) * 1|_{2^{2n}-1} = 1, &= |2(2^{2n}-1)+1|_{2^{2n}-1} \\ &= ||2(2^{2n}-1)|_{2^{2n}-1} + |1|_{2^{2n}-1}|_{2^{2n}-1} \\ &= |1|_{2^{2n}-1} = 1\end{aligned}$$

Thus (5) holds true.

The following properties are important to the computation of MRDs a_1, a_2 and a_3;

Property 1: Modulo 2^s of a number is equivalent to s least significant bits of the number.

Property 2: Modulo $(2^s - 1)$ of a negative number is equivalent to the one's complement of the number, which is obtained by subtracting the number from $(2^s - 1)$ [7].

Property 3: Modulo $(2^s - 1)$ multiplication of a residue number by 2^t , where s and t are positive integers, is equivalent to t bit circular left shifting [7].

Using Equations (2), (3), (4) and (5), the MRDs a_1, a_2 and a_3 can be represented as:

$$a_1 = x_1 = \underbrace{x_{1,2n}x_{1,2n-1} \dots x_{1,1}x_{1,0}}_{2n+1} \tag{6}$$

$$\begin{aligned}a_2 &= \left|(x_2 - a_1)|m_1^{-1}|_{m_2}\right|_{m_2} \\ &= |(x_2 - x_1)\, 2^n - 1\,|_{2^n} \\ &= |\, 2^n(x_2 - x_1) - (x_2 - x_1)|_{2^n} \\ &= |(x_1 - x_2)|_{2^n} = z_1 + z_2 + 1\end{aligned} \tag{7}$$

where,

$$z_1 = |x_1|_{2^n} = \underbrace{x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0}}_{n} \tag{8}$$

$$z_2 = -x_2 = \underbrace{\bar{x}_{2,n-1}\bar{x}_{2,n-2} \dots \bar{x}_{2,1}\bar{x}_{2,0}}_{n} \tag{9}$$

$$\begin{aligned}a_3 &= \left|((x_3 - a_1)|m_1^{-1}|_{m_3} - a_2)|m_2^{-1}|_{m_3}\right|_{m_3} \\ &= |(x_3 - x_1) - a_2)\, 2^n|_{2^{2n}-1} \\ &= |(x_3 + z_3 + z_4)\, 2^n|_{2^{2n}-1} \\ &= |\, 2^n A|_{2^{2n}-1}\end{aligned} \tag{10}$$

where,

$$\begin{aligned}z_3 &= |-x_1|_{2^{2n}-1} \\ &= x_{1,2n-1}x_{1,2n-2} \dots x_{1,1}x_{1,0} \vee x_{1,2n}\end{aligned} \tag{11}$$

$$\begin{aligned}z_4 &= |-a_2|_{2^{2n}-1} \\ &= \underbrace{11 \dots 1\bar{a}_{2,n-1}\bar{a}_{2,n-2} \dots \bar{a}_{2,1}\bar{a}_{2,0}}_{2n}\end{aligned} \tag{12}$$

$$A = x_3 + z_3 + z_4 + 1 \tag{13}$$

Or $$A = x_3 + z_3 + z_4 + 0 \tag{14}$$

$$a_3 = \underbrace{A_{n-1}A_{n-2} \dots A_1A_0A_{2n-1} \dots A_n}_{2n} \tag{15}$$

From Equation (1);

$$\begin{aligned}X &= a_1 + a_2\,(2^{2n+1}-1) + a_3\,(2^{2n+1}-1)(\,2^n) \\ &= a_1 + 2^{2n+1}a_2 - a_2 + 2^{3n+1}a_3 - 2^n a_3\end{aligned} \tag{16}$$

Let,

$$X = \gamma_4 + \gamma_3 \tag{17}$$

where,

$$\gamma_4 = 2^{3n+1}a_3 \tag{18}$$

and,

$$\gamma_3 = \gamma_1 + \gamma_2 + 1 \tag{19}$$

with,

$$\begin{aligned}\gamma_1 &= a_1 + 2^{2n+1}a_2 \\ &= \underbrace{a_{2,n-1}a_{2,n-2} \dots a_{2,1}a_{2,0}}_{n}\,\underbrace{00 \dots 0}_{2n+1} + \underbrace{x_{1,2n} \dots x_{1,1}x_{1,0}}_{2n+1} \\ &= \underbrace{a_{2,n-1}a_{2,n-2} \dots a_{2,1}a_{2,0}x_{1,2n} \dots x_{1,1}x_{1,0}}_{3n+1}\end{aligned} \tag{20}$$

$$\begin{aligned}\gamma_2 &= -a_2 - 2^n a_3 \\ &= \underbrace{\bar{a}_{3,2n-1} \dots \bar{a}_{3,1}\bar{a}_{3,0}}_{2n}\,\underbrace{00 \dots 0}_{n} + \underbrace{\bar{a}_{2,n-1} \dots \bar{a}_{2,1}\bar{a}_{2,0}}_{n} \\ &= \underbrace{1\bar{a}_{3,2n-1} \dots \bar{a}_{3,1}\bar{a}_{3,0}\bar{a}_{2,n-1} \dots \bar{a}_{2,1}\bar{a}_{2,0}}_{3n+1}\end{aligned} \tag{21}$$

Thus, from (16):

$$X = \underbrace{a_{3,2n-1} \dots a_{3,0}}_{2n}\,\underbrace{00 \dots 0}_{3n+1} + \underbrace{\gamma_{3,3n} \dots \gamma_{3,0}}_{3n+1} \tag{22}$$

$$= \underbrace{a_{3,n-1}a_{3,n-2}\cdots a_{3,1}a_{3,0}}_{2n}\underbrace{\gamma_{5,3n}\cdots\gamma_{5,1}\gamma_{5,0}}_{3n+1}$$

4. HARDWARE REALIZATION

The hardware structure of the proposed reverse converter is based on Equations (7), (10), (13) or (14). In Figure 1, z_1 and z_2 are added using a regular Carry Propagate Adder (CPA), notably CPA 1. Also, to compute a_3, a Carry Save Adder (CSA) notably CSA 1 with EAC and either of the regular CPAs 2 and 3 are used to compute (13) or (14) respectively depending on whether or not the carry out of CSA 1 would be a 1 or 0. γ_1 is easily obtained by concatenating the x_1 with a_2 whilst γ_2 is obtained by concatenating the inverse of a_3 with the inverse of a_2 . These concatenations do not require any additional hardware. γ_1, γ_2 are added using regular CPA 4 to obtain γ_3. It should be noted that in order to make γ_2 a $(3n+1)$ −bit number, 1 is appended to the result of concatenation, as given in (21). The final result, computed from Equation (22) is obtained simply by a concatenation operation not requiring any additional hardware resources.

5. PERFORMANCE EVALUATION

The performance of the proposed residue to binary converter is evaluated by comparing it with the best known similar state of the art equivalent converters in [5], [6] and [8] in terms of hardware cost and conversion delay. The results of this comparison are presented in Table 1.

In Table 1 [6] and [8] are the best converters in literature for the moduli sets $\{2^n-1, 2^n, 2^n+1\ , 2^{2n+1}-1\}$ and $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$ respectively.

The complexity of a FA is considered as twice that of a HA and a two-input AND gate. Hence, the total hardware complexity of the proposed reverse converter can be calculated as;

2(9n)HA+(9n+2)AND+(n+1)HA=(19n+1)HA+(n+1)AND

Theoretical analysis (presented in Table 1) shows that the proposed converter performs faster than all the other existing converters with Area-Time complexity analysis also clearly showing that the proposed scheme outperforms all similar state of the art schemes in literature. In addition, the proposed scheme does not require the explicit use of any modulo operation, thereby further enhancing both area and speed.

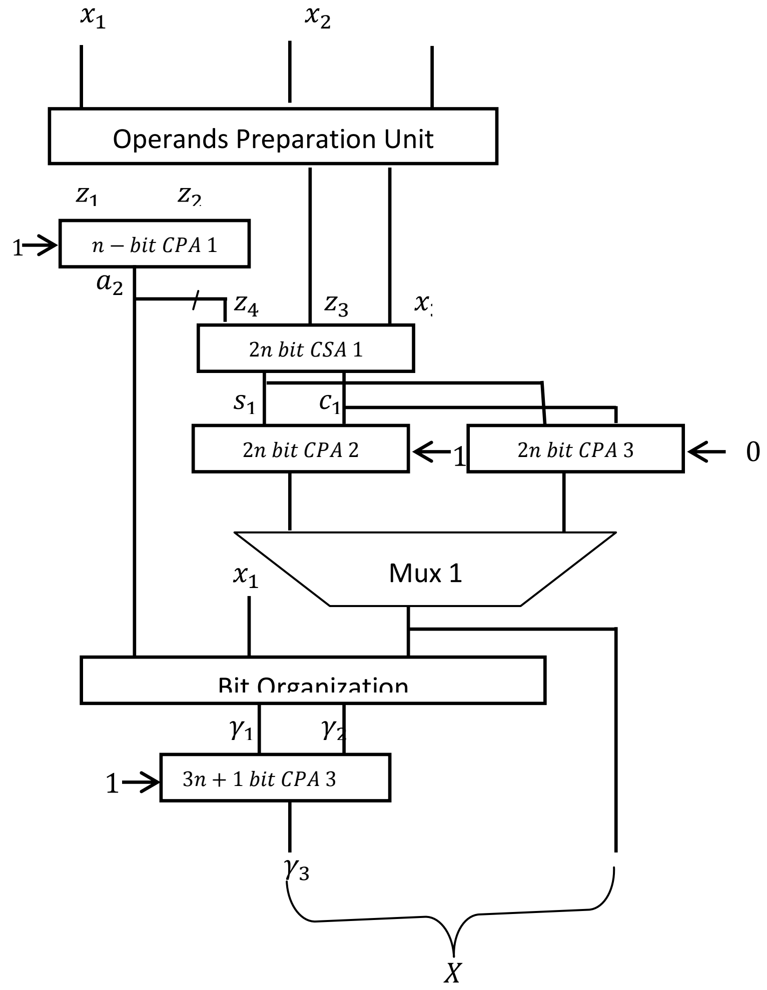

Fig. 1: Block Diagram of Proposed Reverse Converter

Table 1. Hardware Complexity Comparison

Converters	**Complexity**	**Delay**	**Time-complexity**
[5]	(23n+6)HA+(10n + 4)AND	$(12n + 5)t_{FA}$	276n^2
[6]	(26n+4)HA+(13n+2)AND	$(8n+1)t_{FA}$	208n^2
[8]	$(17n+5)HA + (6n+2)AND$	(11n+4)t$_{FA}$	187n^2
Proposed	(19n+5)HA+(9n+2)AND	$(6n+3)t_{FA}$	114n^2

6. CONCLUSION

In this paper, a fast MRC based converter for the recently proposed $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$ moduli set is presented. The proposed converter uses basic logic units, is modulo operation free and outperforms the best known similar state of the art equivalent converters.

7. REFERENCES

[1] A.S. Molahosseini, K. Navi, and M.K. Rafsanjani. A New residue to binary converter based on mixed-radix conversion, 3rd International Conference On Information and Communication Technologies: From Theory to Applications (ICTTA 2008), pp. 1-6, April, 2008.

[2] A.P. Vinod and A.B. Premkumar, A memoryless residue to binary converter for the 4-superset $\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1\}$, Journal of Circuits, Syst. and Computers, Vol. 10, pp. 85-99,2000.

[3] K.A. Gbolagade and S.D. Cotofana, MRC Technique for RNS to Decimal Conversion for the Moduli Set $\{2n+2, 2n+1, 2n\}$, 16th Annual Workshop on Circuits, Systems, and Signal Processing, pp. 318-321, Veldhoven, The Netherlands, November, 2008.

[4] K.A. Gbolagade, G.R. Voicu, and S.D. Cotofana, An Efficient FPGA Design of Reverse Converter for the Moduli Set$\{2n+2, 2n+1, 2n\}$, 5th International Summer School on Advanced Computer Architecture and Compilation for Embedded Systems(ACACES 2010), pp. 117-120, Terrassa, Spain, July 11-17, 2010.

[5] A.S. Molahosseini, K. Navi, C. Dadkhah, O. Kavehei, S. Timarchi, Efficient Reverse Converter Designs for the New 4-Moduli Sets $\{2^n-1, 2^n, 2^n+1, 2^{2n+1}-1\}$ and $\{2^n-1, 2^n+1, 2^{2n}, 2^{2n+1}-1\}$ Based on New CRTs, IEEE Trans. Circuits and Systems-I, vol. 57, pp. 823, Apr2010.

[6] Leonel Sousa, Samuel Antao, MRC-Based RNS reverse converters for the Four-Moduli sets $\{2^n+1, 2^n-1, 2^n, 2^{2n+1}-1\}$ and $\{2^n+1, 2^n-1, 2^{2n}, 2^{2n+1}-1\}$, IEEE Transactions on Circuits and Systems 59-II (4), pp. 244-248, 2012.

[7] K.A. Gbolagade, R. Chaves, L. Sousa, and S.D. Cotofana, An Improved RNS Reverse Converter for the $\{2^{2n+1}-1, 2^n, 2^n-1\}$ Moduli Set, IEEE International Symposium on Circuits and Systems (ISCAS2010), pp. 2103-2106, Paris, France, June, 2010.

[8] K. A. Gbolagade, An Efficient MRC based RNS-to-Binary Converter for the $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$ moduli set, AIMS SA, 2011.

[9] K.A. Gbolagade and S.D. Cotofana, An O(n) Residue Number System to Mixed Radix Technique, IEEE International Symposium on Circuits and Systems (ISCAS 2009), pp. 521-524, Taipei, Taiwan, China, May, 2009.