A New Efficient Residue to Binary Converter for (5n+2)-bit Dynamic Range Moduli Set

Salifu Abdul-Mumin
Department of Computer Scienc
University for Development Studies
Navrongo, Ghana

Mohammed Ibrahim Daabo
Department of Computer Scienc
University for Development Studies
Navrongo, Ghana

Akobre Stephen
Department of Computer Scienc
University for Development Studies
Navrongo, Ghana

ABSTRACT

This paper proposes an efficient residue to binary converter on a new three-moduli set $(2^{2n+1}, 2^{2n+1}-1, 2^n-1)$ using the Mixed Radix Conversion. The proposed reverse converters are adder based and memoryless. In comparison with other moduli sets with similar dynamic range, the new schemes out-perform the existing schemes in terms of both hardware cost and propagation delay.

General Terms

RNS, High Speed Reverse Conversion method

Keywords

Reverse Converter, Mixed Radix Conversion, Dynamic Range, Moduli Set, Residue Number System

1. INTRODUCTION

RNS is a non-weighted number system which support parallelism and can perform carry-free arithmetic [1]. These inherent properties make RNS very suitable to achieve a fast digital signal processing (DSP) systems including intensive computations like digital filtering, convolutions, correlations, Discrete Fourier Transform (DFT) computations, Fast Fourier Transform (FFT) computations and Direct Digital Frequency (DDF) synthesis [2]. However, RNS has not found a widespread usage in general purpose computing due to some difficult operations including overflow detection, magnitude comparison, sign detection, moduli selection, and conversion from decimal/binary to RNS and most especially the vice visa, [3], [4], [5]. Of many of these numerous RNS difficult operations, Data conversion is very critical. For a milestone chalked in the application of RNS, The conversion overhead must not nullify the advantages of RNS, and hence the need for efficient conversion algorithm for data conversion either from binary/decimal to residue or from residue to binary/decimal. Data Conversion, which is usually based on either the Chinese Remainder Theorem (CRT) [6]],[7] [8] or the Mixed Radix Conversion (MRC) [9] can be categorized into forward and reverse conversions. The forward conversion is conversion of binary/decimal to a residue form while the reverse conversion involves converting the RNS number into binary or decimal [10], [5]. Relatively, reverse conversion is more complex.

In the early days, many famous moduli sets, such as $(2^n-1, 2^n, 2^n+1)$ and $(2^n-1,\ 2^n, 2^n+1, 2^{2n}+1)$ etc have been proposed to reduce the design overhead of their residue to binary converters [11], [12], [13], [14], [15]. But these could not maintain a high-speed internal RNS processing under a given dynamic range (DR) since the hardware requirement of performing the modulo $(2^n+1)-type$ arithmetic is so complex that it degrades the entire RNS system performance in terms of hardware cost and operation speed. To overcome the above constraint, the latest co-prime moduli set $(2^n, 2^{n+1}, 2^n-1)$ which is free of $(2^n+1)-type$ modulus is proposed in [16]. The internal RNS processing for the above mentioned moduli set only relies on efficient modulo 2^n and $(2^n+1)-type$ operations for leading to a simple and fast RNS system. However the Dynamic range of these moduli set are not relatively large and cannot be used by applications that require a large Dynamic Range.

In this paper, a moduli set with a large dynamic range is proposed. A residue to binary/decimal converter is designed and implemented using this moduli set. The conversion overhead is computed and compared with similar converters.

The rest of the paper is organized as follows; section 2 gave a brief background of RNS. The proposed reverse converter is presented in section 3and in section 4, the hardware realization is illustrated. Section 5 presented the evaluation comparison and the paper is concluded in section 6.

2. BACKGROUND

Residue Number System (RNS) is defined by the set S which includes N integers that are pair-wise relatively prime. That is S = {m_1, m_2, . . . ,m_N }, where gcd (m_i ,m_j) = 1 for i , j = 1, . . . , N and i = j and gcd means the greatest common divisor

Any integer X in [0, M − 1] can be uniquely represented with an N-tuple where $M = \prod_{i=1}^{N} m_i$, $X = (x_1, x_2, \ldots\ldots x_n)$ and $x_i = |X|_{m_i}$ [4].

3. PROPOSED REVERSE CONVERTER

3.1 Conversion Algorithm

Given the moduli set, $(2^{2n+1}, 2^{2n+1}-1, 2^n-1)$, let $m_1 = 2^{2n+1}$, $m_2 = 2^{2n+1}-1$, $m_3 = 2^n-1$. The information moduli are $(5n+2)-bit$ number. The Mixed Radix Conversion (MRC) is employed to convert the number in RNS representation to its (binary/decimal) equivalent. The general form of the MRC is given as follows;

$$X = d_1 + d_2m_1 + d_3m_1m_2 + \cdots + d_nm_1m_2m_3 \ldots m_{n-1} \quad (1)$$

Where $d_i, i = 1,2,\ldots,n$ are the Mixed Radix Digits (MRDs) and computed as follows:

$$d_1 = x_1$$

$$d_2 = \left|(x_2 - d_1)|m_1^{-1}|_{m_2}\right|_{m_2}$$

$$d_3 = \left|\left((x_3 - d_1)|m_1^{-1}|_{m_3} - d_2\right)|m_2^{-1}|_{m_3}\right|_{m_3}$$

$$\vdots$$

$$d_n = \left|\left(\ldots\left((x_3 - d_1)|m_1^{-1}|_{m_n} - d_2\right)|m_2^{-1}|_{m_n} - \cdots - d_{n-1}\right)|m_{n-1}^{-1}|_{m_n}\right|_{m_n} \quad (2)$$

That is, X in the interval $[0, M]$ can be uniquely represented

Theorem1: Given the moduli set $(2^{2n+1}, 2^{2n+1} - 1, 2^n - 1)$, where $m_1 = 2^{2n+1}$, $m_2 = 2^{2n+1} - 1$, $m_3 = 2^n - 1$, for every integer $n > 1$, the following hold true:

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

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

$$|m_2^{-1}|_{m_3} = 1 \quad (5)$$

Proof: If it can be demonstrated that $\left|\mathrm{m}_i^{-1} \times \mathrm{m}_i\right|_{\mathrm{m}_i} = 1$, then m_i^{-1} is the multiplicative inverse of m_i with respect to m_i. Thus;

For (3)

$$|(2^{2n+1})(1)|_{2^{2n+1}-1}$$

$$|(2^{2n+1} - 1 + 1)|_{2^{2n+1}-1} = 1$$

Also for (4),

$$|(2^{2n+1})(2^{n-1})|_{2^n-1}$$

$$|(2^{3n})|_{2^n-1} = 1$$

And finally for (5),

$$|(2^{2n+1} - 1)(1)|_{2^n-1}$$

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

$$|2 - 1|_{2^n-1} = 1$$

Therefore we can re-write (2) as

$$d_1 = x_1$$

$$d_2 = |(x_2 - d_1)(1)|_{2^{2n+1}-1}$$

$$= |x_2 - x_1|_{2^{2n+1}-1}$$

$$d_3 = |((x_3 - d_1)(2^{n-1}) - d_2)(1)|_{2^n-1}$$

$$= |2^{n-1}x_3 - 2^{n-1}x_1 - d_2|_{2^n-1} \quad (6)$$

And (1) then becomes;

$$X = x_1 + d_2(2^{2n+1)} + d_3(2^{4n+2} - 2^{2n+1})$$

$$= x_1 + 2^{2n+1}d_2 + 2^{4n+2}d_3 - 2^{2n+1}d_3 \quad (7)$$

3.2 Hardware Realization

Equation (6) and equation (7) are simplified as follows;

$$d_1 = \underbrace{x_{1,2n}x_{1,2n-1} \ldots\ldots\ldots . x_{1,1}x_{1,0}}_{2n+1}$$

$$d_2 = |\underbrace{x_{2,2n}x_{2,2n-1} \ldots\ldots\ldots . x_{2,1}x_{2,0}}_{2n+1} - \underbrace{x_{1,2n}x_{1,2n-1} \ldots\ldots\ldots . x_{1,1}x_{1,0}}_{2n+1}|_{2^{2n+1}-1}$$

$$= |\underbrace{x_{2,2n}x_{2,2n-1} \ldots\ldots\ldots . x_{2,1}x_{2,0}}_{2n+1} + \underbrace{\bar{x}_{1,2n}\bar{x}_{1,2n-1} \ldots\ldots\ldots . \bar{x}_{1,1}\bar{x}_{1,0}}_{2n+1}|_{2^{2n+1}-1}$$

$$= \underbrace{d_{2,2n}d_{2,2n-1} \ldots\ldots\ldots . d_{2,1}d_{2,1}}_{2n+1}$$

$$d_3 = |2^{n-1}\left(\underbrace{x_{3,n-1}x_{3,n-2} \ldots\ldots . x_{3,1}x_{3,0}}_{n}\right) - 2^{n-1}(\underbrace{x_{1,2n}x_{1,2n-1} \ldots\ldots\ldots . x_{1,1}x_{1,0}}_{2n+1}) - (\underbrace{d_{2,2n}d_{2,2n-1} \ldots\ldots\ldots . d_{2,1}d_{2,1}}_{2n+1})|_{2^n-1}$$

$$= |2^{n-1}\left(\underbrace{x_{3,n-1}x_{3,n-2} \ldots\ldots . x_{3,1}x_{3,0}}_{n}\right) + 2^{n-1}(\underbrace{\bar{x}_{1,2n}\bar{x}_{1,2n-1} \ldots\ldots\ldots . \bar{x}_{1,1}\bar{x}_{1,0}}_{2n+1}) + (\underbrace{\bar{d}_{2,2n}\bar{d}_{2,2n-1} \ldots\ldots\ldots . \bar{d}_{2,1}\bar{d}_{2,1}}_{2n+1})|_{2^n-1}$$

$$= |\underbrace{x_{3,0}}_{1-bit} + \underbrace{\bar{x}_{1,n+1}\bar{x}_{1,n} \ldots\ldots \bar{x}_{1,1}\bar{x}_{1,0}}_{n+2} + \overbrace{\bar{d}_{2,2n}\bar{d}_{2,2n-1} \ldots\ldots \bar{d}_{2,1}\bar{d}_{2,0}}^{2n+1}|_{2^n-1}$$

$$= \underbrace{d_{3,n-1}d_{3,n-2} \ldots\ldots . d_{3,1}d_{3,0}}_{n-bit}$$

From equation (7), let

$$C = x_1 + 2^{2n+1}d_2$$

$$= \overbrace{00 \ldots 00}^{2n+1} x_{1,2n}x_{1,2n-1} \ldots x_{1,0} + d_{2,2n}d_{2,2n-1} \ldots d_{2,0}\overbrace{00 \ldots 00}^{2n+1}$$

$$= x_{1,2n}x_{1,2n-1} \ldots x_{1,0} \bowtie d_{2,2n}d_{2,2n-1} \ldots d_{2,0}$$

$$= C_{4n+1}C_{4n} \ldots C_1C_0$$

And

$$A = C + 2^{4n+2}d_3$$

$$= \overbrace{00 \ldots 00}^{n} C_{4n+1}C_{4n} \ldots C_1C_0 + d_{3,n-1}d_{3,n-2} \ldots d_{3,0}\overbrace{00 \ldots 00}^{4n+2}$$

$$= C_{4n+1}C_{4n} \ldots C_1C_0 \bowtie d_{3,n-1}d_{3,n-2} \ldots d_{3,0}$$

$$= A_{5n+1}A_{5n} \ldots A_1A_0$$

Thus equation (7) becomes

$$X = \underbrace{A_{5n+1}A_{5n} \ldots A_1A_0}_{5n+2} - \underbrace{d_{3,n-1}d_{3,n-2} \ldots\ldots . d_{3,1}d_{3,0}}_{n-bit}\overbrace{00 \ldots 00}^{2n+1}$$

$$\underbrace{A_{5n+1}A_{5n}\dots A_1A_0}_{5n+2}$$

$$+\underbrace{\bar{d}_{3,n-1}\bar{d}_{3,n-2}\dots\dots.\bar{d}_{3,1}\bar{d}_{3,0}}_{n-bit}\overbrace{11\dots 11}^{2n+1}$$

The proposed schematic diagram will be as follows;

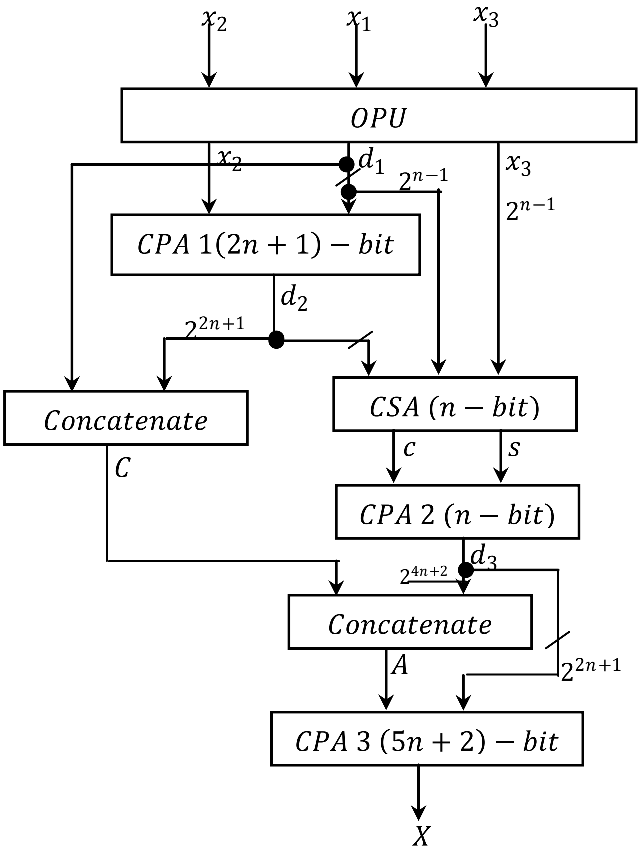

Fig 1: Schematic Diagram of the Reverse Converter

The hardware requirements of this architecture and the delay imposed in computing the binary number is as follows;

Area = Area (CPA1) + Area (CSA) + Area (CPA 2) + Area (CPA 3)

$$(2n+1)+n+n+(5n+2)=9n+3$$

$$Delay=(4n+2)+1+2n+10n+4=16n+7$$

4. PERFORMANCE EVALUATION

In this section, the performance of the proposed moduli set is evaluated with the state of the art as shown in the table below.

Table 1: Area and Delay Comparison

Reverse Converter	Area	Delay
[17]	$n^2+12n+12$	$16n+22$
[18a]	$2.5n^2+25.5n+12$	$18n+23$
[18b]	$23n+11$	$16n+14$
[19]	$(5n^2+43n)/6+16n-1$	$18n+7$
Proposed System	$9n+3$	$16n+7$

The area of the [17], [18a] and [19] all have an asymptotic complexity of O(n^2) whiles the proposed system has a corresponding value of O(n). In the system proposed in [18b], the area has an asymptotic complexity of O(n) but has superior values than the one in the proposed system for values of n. As the values of n increases, the time and space complexity for the proposed system is better than those proposed in [17], [18a], [18a] and [19].

Table 2 Area Analysis

Converters	Area	n-Values				
		2	3	4	5	6
[17]	$n^2+12n+12$	40	57	76	97	120
[18a]	$2.5n^2+25.5n+12$	73	111	154	202	255
[18b]	$23n+11$	57	80	103	126	149
[19]	$(5n^2+43n)/6+16$	2.86	3.28	3.65	4	4.34
Proposed System	$9n+3$	21	30	39	48	57

In table 2, converters [17], [18a] and [18b] have values of their area more than the proposed system. Therefore, the proposed system performs better than them in terms of area. From table 2, the converter in [19] will perform better than the proposed system in terms of area.

Table 3: Delay Analysis

Converters	Delay	n-Values				
		2	3	4	5	6
[17]	$16n+22$	54	70	86	102	118
[18a]	$18n+23$	59	77	95	113	131
[18b]	$16n+14$	46	62	78	94	110
[19]	$18n+7$	43	61	79	97	115
Proposed System	$16n+7$	39	55	71	87	103

In table 3, all the existing systems have values more than the proposed system. Therefore the proposed system performs better the existing systems in terms of delay.

5. CONCLUSION

A new reverse converter with a high dynamic range is proposed and implemented. This reverse converter is suitable for applications requiring high dynamic range like Digital Signal processing, Cryptography etc. The Area and the Propagation Delay of the proposed system are computed and compared to converters with similar Dynamic Range. The proposed system outperformed the state of the art in terms of Delay. The proposed system performs better than those proposed in [17], [18a] and [18b] in terms of Area. However, the converter proposed in [19], shows a gain in terms of Area over the proposed system even though it has an asymptotic complexity of $O(n^2)$.

6. REFERENCES

[1] N.S. Szabo and R.I. Tanaka, Residue arithmetic and its applications to computer technology, McGraw Hill, New York, 1967.

[2] M.A. Sonderstrand, W.K. Jenkins, G.A. Jullien, and F.J. Taylor, Residue number system arithmetic: Modern applications in digital signal processing, IEEE Press, New York, 1986.

[3] M. Bhardwaj, T. Srikanthan, and C. T. Clarke, "A reverse converter for the 4 moduli super set {2^n-1, 2^n, 2^n+1, 2^(n+1)+1}," *IEEE Conf. Comput. Arith.*, 1999.

[4] A. Hariri, R. Rastegar, and K. Navi, "High Dyanamic Range 3-Moduli Set with Efficient Reverse Converter," *Int. J. Comput. Math. Appl.*

[5] S. Abdul-Mumin, P. A. Agbedemnab and M. I. Daabo: New Efficient Reverse Converters for 8n-bit Dynamic Range Moduli Set, *International Journal of Computer Applications Volume 161 – No 9, pp: 23-27March 2017*

[6] E. K. Bankas and K. A. Gbolagade, "A New Efficient FPGA Design of Residue-To-Binary Converter," *Int. J. VLSI Des. Commun. Syst. VLSICS*, vol. 4, no. 6, Dec. 2013.

[7] H. Pettenghi, R. Chaves, and L. Sousa, "RNS Reverse Converters for Moduli Sets With Dynamic Ranges up to -bit," *IEEE Trans. Circuits Syst. Regul. Pap.*, vol. 60, no. 6, pp. 1487–1500, Jun. 2013.

[8] M. I. Daabo and K. A. Gbolagade, "RNS Overflow Detection Scheme for the Moduli set {M − 1, M}," *J. Comput.*, vol. 4, no. 8, pp. 39–44, 2012.

[9] K. A. Gbolagade, "New Adder-Based RNS-Binary Converters for the {2^(n+1)+1,2^(n+1)-1,2^n } Moduli Set.," *Int. Sch. Res. Netw*

[10] G. Jaberipur and H. Ahmadifar, "A ROM-less reverse RNS converter for moduli set 2q ?? 1, 2q ?? 3," *IET Comput. Digit. Tech.*, vol. 8, no. 1, pp. 11–22, Jan. 2014.

[11]Y. Wang, X. Song, M. Aboulhamid, and H. Shen, "Adder-based residue to binary number converters for (2*n* − 1, 2*n*, 2*n* + 1)," IEEE Trans. Signal Process., vol.50, no.7, pp.1772–1779, July 2002.

[12] W.Wang, M.N.S. Swamy, M.O. Ahmad, and Y.Wang, "A study of the residue-to-binary converters for the three-moduli sets," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol.50, no.2, pp.235–245, Feb. 2003.

[13] B. Cao, C.H. Chang, and T. Srikanthan, "An efficient reverse converter for the 4-moduli set (2*n* − 1, 2*n*, 2*n* + 1, 22*n* + 1) based on the new Chinese remainder theorem," IEEE Trans. Circuits Syst. I, vol.50, no.10, pp.1296–1303, Oct. 2003.

[14] B. Cao, T. Srikanthan, and C.H. Chang, "Efficient reverse converters for the four-moduli sets (2*n* − 1, 2*n*, 2*n* + 1, 2*n*+1 − 1) and (2*n* −1, 2*n*, 2*n* +1, 2*n*−1 −1)," Proc. IEE Comput. Digit. Tech., vol.152, no.5, pp.687–696, Sept. 2005.

[15] A.A. Hiasat, "VLSI implementation of new arithmetic residue to binary decoders," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol.13, no.1, pp.153–158, Jan. 2005.

[16] P.V.A. Mohan, "RNS-to-binary converter for a new three-moduli set (2*n*+1 − 1, 2*n*, 2*n* − 1)," IEEE Trans. Circuits Syst. II, vol.54, no.9, pp.775–779, Sept. 2007.

[17] P. V. Ananda Mohan and A. B. Premkumar, "RNS-to-binary converters for two four-moduli sets {2*n* − 1,2*n*, 2*n* + 1,2*n*+1 − 1} and {2*n* − 1,2*n*, 2*n* + 1,2*n*+1 + 1}," *IEEE Transactions on Circuits and Systems I*, vol. 54, no. 6, pp. 1245–1254, 2007.

[18] P.V. AnandaMohan, "Newreverse converters for themoduli set {2*n* −3, 2*n* −1, 2*n* +1, 2*n* +3}," *International Journal of Electronics and Communications (AEU)*, vol. 62, no. 9, pp. 643–658, 2008.

[19] B. Cao, C.-H. Chang, and T. Srikanthan, "A residue-to-binary converter for a new five-moduli set," *IEEE Transactions on Circuits and Systems I*, vol. 54, no. 5, pp. 1041–1049, 2007