IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 4, Issue 1, Ver. I (Jan. 2014), PP 44-49
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

Residue-to-Binary Converter for the New Moduli Set $\{2^{(3n+2)/2}-1, 2^{2n}, 2^{(3n+2)/2}+1\}$

H. Siewobr and K. A. Gbolagade
(Department of Computer Science, Faculty of Mathematical Sciences, University for Development, Ghana)

Abstract : *In this paper, we propose the new moduli set* $\{2^{(3n+2)/2}-1, 2^{2n}, 2^{(3n+2)/2}+1\}$ *with an efficient reverse converter. Experiments were performed on our converter and the state of the art using Xilinx ISE 14.3 software to target a Spartan 3 FPGA board. The results from these experiments suggest that on the average, the proposed converter outperforms the state of the art converters for the moduli sets* $\{2^n-1, 2^n, 2^n+1\}$ *and* $\{2^{2n}-1, 2^n, 2^{2n}+1\}$.

Keywords: *Residue Number System, Reverse Converter, Moduli Set, Mixed Radix Conversion, Chinese Remainder Theorem.*

I. INTRODUCTION

Arithmetic computations based on Residue Number System (RNS) has found wide spread usage in Digital Signal Processing (DSP) applications such as filtering, computation of the discrete Fourier transform , communication, and cryptography [1]. The main reasons for the interests are the inherent properties of RNS such as modularity, fault tolerance and also the fact that RNS converts weighted numbers into a set of small residues which can result in high speed addition, subtraction and multiplication as arithmetic operations on residues can be performed in parallel without carry propagation between channels [10]. The most RNS critical issues lie in moduli set selection and conversion from residue representation to weighted representation (Reverse Conversion (RC)). RC can be achieved either by the traditional Chinese Remainder Theorem (CRT) [4], [5] , the Mixed Radix Conversion (MRC) [1], [11] or the recently introduced new CRTs(CRT I and II) [3].
Several moduli sets have been proposed with algorithms designed for performing RC. Among them is the well-known three-moduli set $\{2^n-1, 2^n, 2^n+1\}$ [3], also known as the traditional moduli set. Due to its lower Dynamic Range (DR), the traditional moduli set was extended to the moduli set $\{2^{2n}-1, 2^n, 2^{2n}+1\}$ in [4]. However, the reverse conversion architecture in both [3] and [4] still appear complex for three-moduli sets. Another disadvantage of [4] is that it requires channel arithmetic modulo $2^{2n}+1$. This type of arithmetic have been well documented to be disadvantageous to the RNS processor [11].
In this paper, we propose the moduli set $\{2^{(3n+2)/2}-1, 2^{2n}, 2^{(3n+2)/2}+1\}$ for even n which eliminates the major disadvantages of [3] and [4] at similar DR.
The CRT which is used to derive reverse converters for the proposed moduli set is presented for three moduli sets as [5]:

$$X = \left|\sum_{i=1}^{3} \ell_i |k_i x_i|_{m_i}\right|_M \quad (1)$$

with,

$$M = \prod_{i=1}^{3} m_i \quad (2)$$

$$\ell_i = \frac{M}{m_i} \quad (3)$$

$$|k_i \ell_i|_{m_i} = 1, \forall\, i = [1,3] \quad (4)$$

The rest of this article is organized as follows. In Section II, we present the proposed algorithm for reverse conversion. Section III presents the performance evaluation of the proposed scheme whilst in Section IV we conclude the paper.

II. PROPOSED CONVERTERS

In this section, we present efficient reverse converters for the moduli set $\{2^{(3n+2)/2}-1, 2^{2n}, 2^{(3n+2)/2}+1\}$.
The following notations below are adopted from [1] for presenting the proposed method and the corresponding reverse converter:

1. For an n-bit value γ, bits are referred from the Most Significant Bit (MSB) to the Least Significant Bit (LSB) as $\gamma[n-1], \ldots, \gamma[0]$.

2. $\gamma^l[k]$ refers to an l-bit number such that: $\gamma^l[k] = \gamma[k+l-1]2^{l-1} + \ldots + \gamma[k+1]2 + \gamma[k]$;
3. $\mathcal{O}$ and $\mathcal{Z}$ each refer to a number whose binary representation is an all-one and all-zero string respectively;
4. The symbol $\bowtie$ operates the concatenation of the binary representation of two numbers.

The following Lemmas are important in the design of the proposed converters:

Lemma 1: 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].

Lemma 2: 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].

A. Proposed Method for Reverse Conversion

First, we show that the moduli are prime relative and suitable for RNS. Next, we show that the computation of multiplicative inverses could be avoided and present a low complexity design which requires only carry save adders (CSAs) and binary carry propagate adders (CPAs).

Theorem 1: The moduli set $\{2^{(3n+2)/2}-1, 2^{2n}, 2^{(3n+2)/2}+1\}$ includes pair wise relatively prime moduli.

Proof:

From Euclidean theorem, we have:

$gcd(a,b) = gcd(b, |a|_b)$,

therefore,

$\gcd(2^{2n}, 2^{(3n+2)/2}-1) = 1$

$\gcd(2^{(3n+2)/2}+1, 2^{(3n+2)/2}-1) = \gcd(2^{(3n+2)/2}-1, 2) = 1$

$\gcd(2^{2n}, 2^{(3n+2)/2}+1) = 1$

Thus the elements of the moduli set $\{2^{(3n+2)/2}-1, 2^{2n}, 2^{(3n+2)/2}+1\}$ are pairwise relatively prime.

Substituting $m_1 = 2^{2n}$, $m_2 = 2^{(3n+2)/2}-1$ and $m_3 = 2^{(3n+2)/2}+1$ into (2) and (3), we obtain:

$\ell_1 = 2^{3n+2} - 1$ (5)

$\ell_2 = 2^{2n}(2^{(3n+2)/2}+1)$ (6)

$\ell_3 = 2^{2n}(2^{(3n+2)/2}-1)$ (7)

Theorem 2: Given the moduli set $\{2^{(3n+2)/2}-1, 2^{2n}, 2^{(3n+2)/2}+1\}$ and holding all conditions as specified above, the followings hold true:

$k_1 = -1$ (8)

$k_2 = 2^{n+1}$ (9)

$k_3 = -2^{n+1}$ (10)

Proof:

Since:

$|(-1) * (2^{3n+2}-1)|_{2^{2n}} = 1, (|2^{3n+2}|_{2^{2n}} = 0)$

Then (7) holds true.

Similarly, since:

$\left|2^{n+1} * 2^{2n}(2^{(3n+2)/2}+1)\right|_{2^{(3n+2)/2}-1} = |2^{3n+2}|_{2^{3n+2}-1} = 1$

Then (8) holds true.

Finally, since:

$\left|-2^{n+1} * 2^{2n}(2^{(3n+2)/2}-1)\right|_{2^{(3n+2)/2}+1} = |2^{3n+2}|_{2^{3n+2}+1} = 1$

Then (9) holds true.

Theorem 3: The binary equivalent X, of an RNS number (x_1, x_2, x_3) can be computed as follows:

$X = \rho^{3n+2}[0] \bowtie x_1^{2n}[0]$ (11)

with,

$\rho = \left|-2^{n+2}x_1 + (2^{(3n+2)/2}x_2 + x_2)2^{n+1} + (1 - 2^{(3n+2)/2})2^{n+1}x_3\right|_{2^{(3n+2)}-1}$ (12)

Proof: By substituting (5) through to (10) into (1) and factorizing 2^{2n} from the right hand side we obtain (11).

We can further simplify (12) as:

$\rho = |\lambda_1 + \lambda_2 + \lambda_3|_{2^{(3n+2)}-1}$ (13)

with,

$\lambda_1 = |-2^{n+2}x_1|_{2^{(3n+2)}-1} = \overline{x_1^{2n}[0]} \bowtie \mathcal{O}^{n+2}[0]$ (14)

$\lambda_2 = \left|(2^{(3n+2)/2}x_2 + x_2)2^{n+1}\right|_{2^{3n+2}-1}$ (15)

$= |2^{n+1}(x_2 \bowtie x_2)|_{2^{(3n+2)}-1}$

$$= x_2^{n/2}[0] \bowtie x_2 \bowtie x_2^{n+1}[n/2]$$

$$\lambda_3 = \left|\left(1-2^{(3n+2)/2}\right)2^{n+1}x_3\right|_{2^{3n+2}-1} \quad (16)$$
$$= \left|2^{n+1}x_3 - 2^{\frac{5n}{2}+2}x_3\right|_{2^{3n+2}-1}$$
$$= |\lambda_{31}+\lambda_{32}|_{2^{3n+2}-1}$$

with,

$$\lambda_{31} = \left|-2^{\frac{5n}{2}+2}x_3\right|_{2^{3n+2}-1} \quad (17)$$
$$= \left|2^{n+2}\left(\overline{x_3} \bowtie \mathcal{O}^{3n/2}[0]\right)\right|_{2^{3n+2}-1}$$
$$= \overline{x_3^{n/2}[0]} \bowtie \mathcal{O}^{3n/2}[0] \bowtie \overline{x_3^{n+2}[n/2]}$$

$$\lambda_{32} = |2^{n+1}x_3|_{2^{3n+2}-1} \quad (18)$$
$$= \mathcal{Z}^{n/2-1}[0] \bowtie x_3 \bowtie \mathcal{Z}^{n+1}[0]$$

Substituting (16) into (13) we obtain :

$$\rho = |\lambda_1+\lambda_2+\lambda_{31}+\lambda_{32}|_{2^\tau-1} \quad (19)$$

A. Proposed Architecture

The schematic diagram for the proposed converter is showed in Fig. 1.

We use the method of [12] to compute ρ according to (13). By this method, two $3n+2$-bit CSAs and two $3n+2$-bit binary CPA's are required. The CPAs work in parallel (CPAs 2 and 3 in Fig. 1). Whilst one of the CPAs has a constant carry-in of zero, the other has a constant carry-in of one. The correct result is selected by a multiplexer (MUX 1) based on the carry-out of CPA with constant carry-in of zero. This result is concatenated with x_1 at no hardware cost to realize the final binary equivalent of any RNS number.

TABLE I: CHARACTERIZATION OF EACH PART OF THE PROPOSED REVERSE CONVERTER

Component	Area(Δ_{FA})	Delay(D_{FA})
CSA 1	0.5n	1
CSA 2	1.5n	1
CPA 1	3n + 2	3n + 2
CPA 2	3n + 2	3n + 2
Total	8n + 4	3n + 4

In order to better understand the delay and area performance of the proposed reverse converter, a simple theoretical model using Full Adders (FAs) as the finest grain component is adopted. In this model the estimation only considers 1-bit FA, with delay and area, since the applied bitwise logic operations do not impose a significant delay or area cost [8].

The values of area and delay are presented in Table 1. It is worth noting the following:

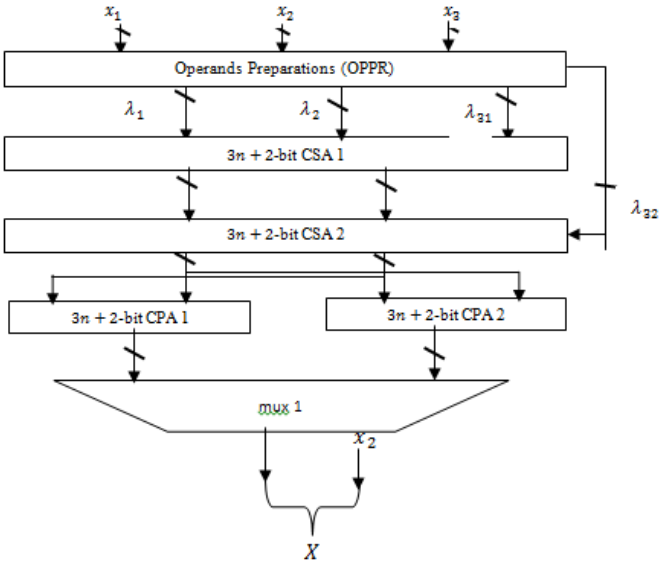
1. CSA 1 is made up of $(2.5n+2)$-bit pairs of XNOR/OR gates since λ_1 and λ_{31} contain $(n+2)$-bit and $(1.5n)$-bit 1s all in different bit positions. Thus, this CSA demands an area of $(0.5)\Delta_{FA}$ and imposes a delay of D_{FA}.
2. CSA 2 is made up of $(1.5n)$-bit AND/OR pairs since λ_{32} contains $(1.5n)$-bit 0s. Thus this CSA demands an area of $(1.5n+2)\Delta_{FA}$ and imposes a delay of D_{FA}.
3. The CPAs each demand $(3n+2)\Delta_{FA}$ and $(3n+2)D_{FA}$.
4. The proposed converter demand an area of $(8n+4)\Delta_{FA}$ and impose a delay of $(3n+4)D_{FA}$ since CPAs 1 and 2 are implemented in parallel.

III. PERFORMANCE EVALUATION

The major limiting factors of the moduli sets in [3] and [4] compared to the one proposed in this work is that, at equal DR our proposal presents faster RNS arithmetic unit speed as depicted in Table II.

TABLE II
COMPARISON OF THE SPEED OF THE DIFFERENT MODULI SETS

Moduli Set	Critical Path	Delay
[3]	2^n+1	$2\log_2(n)+6$
[4]	$2^{2n}+1$	$2\log_2(n)+8$
Proposed Converter	$2^{(3n+2)/2}+1$	$2\log_2(1.5n+1)+6$



Additionally, from theoretical analyses of the converter for the proposed moduli set and the state of the art converters in [3] and [4] presented in Table III we can expect a significant reduction of the delay regarding both [3] and [4] compared with the proposed reverse converter at the cost of some extra circuit area only in the case of [4].

Although fast parallel prefix modulo 2^n-1 adders with a delay proportional to $\log_2(n)$ but area proportional to $n\log_2(n)$ have been proposed in [9], we consider for this analysis, as in [3] and [4], that a n-bit CPA with End-Around Carry (EAC) has twice the delay of a normal n-bit CPA, but the same area. The EAC approach is an efficient method to compute modulo 2^n-1 addition, which consists in redirecting the resulting carry-out of an addition into the carry-in [1]. These results suggest the superiority of our schemes.

TABLE III: AREA, DELAY COMPARISON
$(\{2^{(3n+2)/2}-1, 2^{2n}, 2^{(3n+2)/2}+1\})$

Converter	DR	Area (Δ_{FA})	Delay (D_{FA})
[3]	$3n$	$4n$	$4n+2$
[4]	$5n$	$5n$	$8n+1$
Proposed Converter	$5n+2$	$8n+4$	$3n+4$

To fairly evaluate the performance of our schemes compared to the state of the art, a well known library of arithmetic units [9], which contains a structural specification of optimized prefix adders written in synthesizable VHDL code was employed to obtain the HDL specification of both the proposed and related state of the art converters. These HDL specification of the converters were used to perform experimental assessment using Xilinx ISE 14.3 software to target a Spartan 3 FPGA. The results obtained after design place and route presented in terms of the number of FPGA slices and input-to-output propagation delays (in nano seconds) for various DR requirements (different values of n) are presented in Table IV. It is worth noting that for every n in Table IV, the

corresponding area and delay for [3] is derived using the lower or upper bond of $(5n+2)/3$. These results suggest that at equal DR:

1. The proposed converter reduces the area demanded by the related state of the art converter in [3] by about 18.29% and delay by about 60.1%.
2. The proposed converter reduces the delay imposed by the related state of the art converter in [4] by about 55.34% at an area cost of about 15.07% (see Table V).
3. Following number 2 above, there is a need to further compare the proposed converter with [4] using the area delay square metric (ΔD^2)**.** Results from this metric (shown in Table V) suggest that this proposed converter is 78.64% better than [4] in terms of overall performance. Figures 2 through to 4 show graphical representations of the experimental findings.

TABLE IV
CONVERTERS' DELAY τ $[ns]$ AND AREA [NUMBER OF SLICES]

Converter	$n=2$		$n=4$		$n=8$		$n=16$	
	Δ	τ	Δ	τ	Δ	τ	Δ	τ
[3]	46	23.1	100	29.8	156	36.6	212	37
[4]	36	21.6	77	29.5	147	30	105	31.9
Proposed Converter	43	12	89	12.5	164	13.2	124	12.8

TABLE V
CONVERTERS' $\Delta D^2 [10^3\ slices\ ns^2]$

Converter	$n=2$	$n=4$	$n=8$	$n=16$
[4]	16	67	132	106
Proposed Converter	6	13	28	20

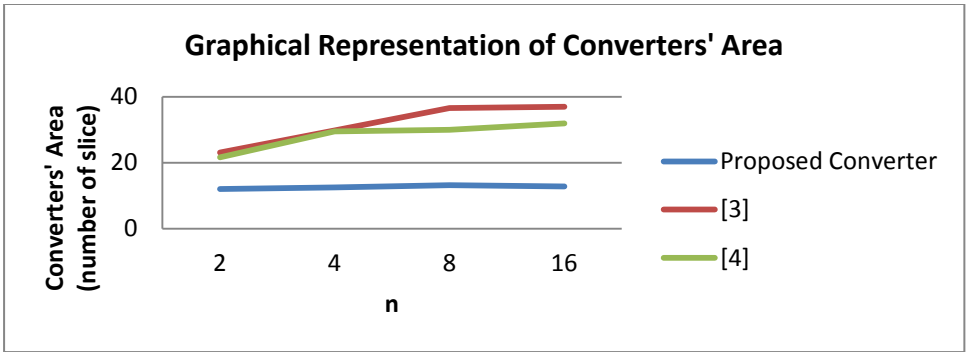


Figure 2: Graphical Representation of Converters' Area

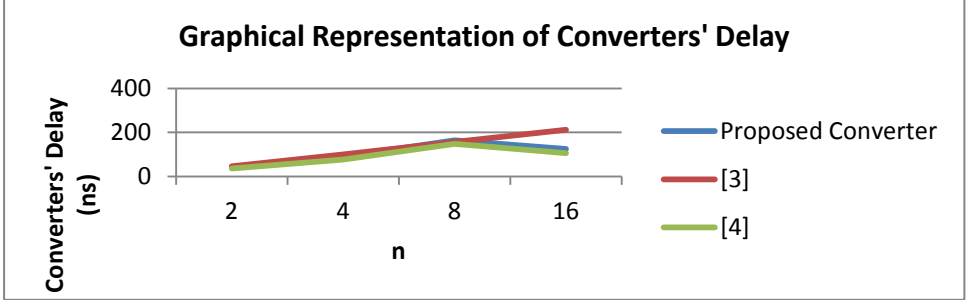


Figure 3: **Graphical Representation of Converters' Delay**

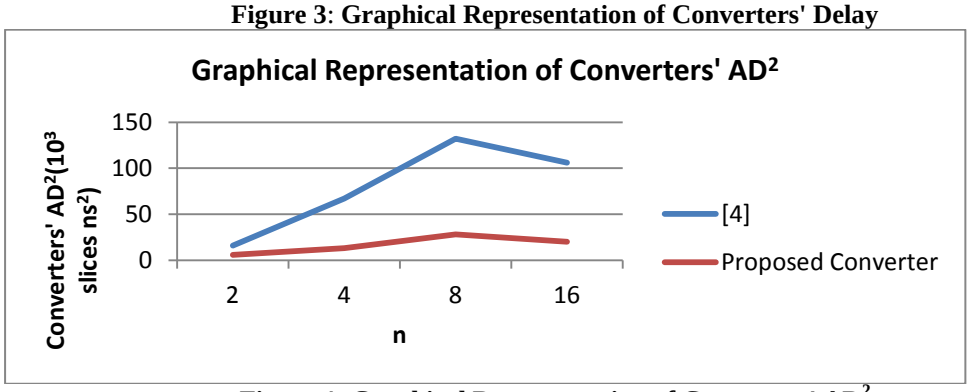


Figure 4: Graphical Representation of Converters' AD^2

IV. CONCLUSION

In this paper, we proposed an efficient residue-to-binary converter for the new moduli set $\{2^{(3n+2)/2}-1, 2^{2n}, 2^{(3n+2)/2}+1\}$. We presented an efficient architecture for reverse conversion in the new moduli set. Experiments performed on the proposed converter and the related state of the art using Xilinx ISE 14.3 software to target a Spartan 3 FPGA suggest that the proposed converters outperform the related state of the art schemes.

References

[1] L. Sousa, S. Antão, R. Chaves, On the Design of RNS Reverse Converters for the Four-Moduli Set $\{2^n+1, 2^n-1, 2^n, 2^{n+1}+1\}$ *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 21, no. 10, pp. 1945 - 1949, Oct. 2013.

[2] 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.

[3] 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 Transactions on Signal Processing*, Vol. 50, pp.1772–1779. 2002.

[4] A. Hariri, K. Navi, R. Rastegar, A new high dynamic range moduli set with efficient reverse converter, *International Elsevier Journal of Computers and Mathematics with Applications*, doi:10.1016/j.camwa.2007.04.028, 2007.

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

[6] P. V. A. Mohan and A. B. Premkumar, RNS-to-binary converters for two four-moduli $\{2^n+1, 2^n-1, 2^n, 2^{n+1}-1\}$ and $\{2^n+1, 2^n-1, 2^n, 2^{n+1}+1\}$, *IEEE Transactions on Circuits Systems I*, Reg. Papers, vol. 54, no. 6,pp. 1245–1254, Jun. 2007.

[7] S. Lin, M. Sheu, and C. Wang, Efficient VLSI design of residue to binary converter for the moduli set $\{2^n, 2^{n+1}-1, 2^n-1\}$, IEICE Trans.INF. and SYST., Vol. E91-D, No.7, pp. 2058-2060, July, 2008.

[8] W. Zhang and P. Siy, An efficient design of residue to binary converter for four moduli set {2n − 1, 2n + 1, 22n − 2, 22n+1 − 3} based on new CRT II, *Information Sciences*, vol. 178, no. 1, pp. 264–279, 2008.

[9] B. Cao, C. H. Chang, and T. Srikanthan, An efficient reverse converter for the 4-moduli set $\{2^n-1, 2^n, 2^n+1, 2^{2n}+1\}$ based on the new Chinese remainder theorem, *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 50, no. 10, pp. 1296–1303, 2003.

[10] R. Zimmermann, VHDL Library of Arithmetic Units, in *International Forum on Design Languages - FDL*. Lausanne: FDL Report, Sep. 1998, pp. 1–6. [Online]. Available: http://www.iis.ee.ethz.ch/_zimmi/arith_lib.html

[11] 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.

[12] A. S. Molahosseini, K. Navi, C. Dadkhah, O. Kavehei, and S. Timarchi, Efficient Reverse Converter Designs for the New 4-Moduli Sets $\{2^n+1, 2^n-1, 2^{2n}, 2^{2n+1}-1\}$ and $\{2^n+1, 2^n-1, 2^{2n}, 2^{2n}+1\}$Based on New CRTs, *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 4, pp. 823–835, 2010.

[13] 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 9-II (4), pp. 244-248, 2012.

[14] J. Mathew, D. Radhakrishnan, T. Srikanthan, Fast Residue-to-Binary Converter Architecture, *IEEE*, Las Cruces, NM, 2000, USA.