An Effective New CRT Based Reverse Converter for a Novel Moduli Set $\left\{2^{2n+1}-1, 2^{2n+1}, 2^{2n}-1\right\}$

Edem Kwedzo Bankas, Kazeem Alagbe Gbolagade
Department of Computer Science, Faculty of Mathematical Sciences,
University for Development Studies, Navrongo, Ghana
E-mails: eb433007@ohio.edu, gkazy1@yahoo.com

Sorin Dan Cotofana
Computer Engineering Lab.,
Delft University of Technology, Delft,
The Netherlands.
Email: sorin@ce.et.tudelft.nl

***Abstract*—In this paper, a novel 3-moduli set $\left\{2^{2n+1}-1, 2^{2n+1}, 2^{2n}-1\right\}$, which has larger dynamic range when compared to other existing 3-moduli sets is proposed. After providing a proof that this moduli set always results in legitimate RNS, we subsequently propose an associated reverse converter based on the New Chinese Remainder Theorem. The proposed reverse converter has a delay of $(4n+6)t_{FA}$ with an area cost of $(8n+2)FAs$ and $(4n-2)HAs$, where FA, HA, and t_{FA} represent Full Adder, Half Adder, and delay of a Full Adder, respectively. We compared the proposed reverse converter with state of the art converters for similar or equal dynamic range RNS and our analysis indicate that for the same dynamic range the best converter requires $(16n+1)FAs$ and exhibits a delay of $(8n+2)t_{FA}$. This indicates that, theoretically speaking, our proposal achieves about 37.5% area reduction and it is about 2 times faster than equivalent state of the art converters. Moreover, the product of the area with the square of the delay is improved up to about 84.4% over the state of the art.**

***Keywords*—Moduli Set, Dynamic Range, Reverse Converter, Chinese Remainder Theorem, New Chinese Remainder Theorem.**

I. Introduction

A Residue Number System (RNS) is an integer number representation system which, speeds up arithmetic computations by decomposing a number X into a set of elements, say $(x_1, x_2, ..., x_n)$, called the residues of the integer X with respect to a moduli set $\{m_1, m_2, ..., m_n\}$ [1].

RNS has the following inherent characteristics: carry free operations, parallelism, modularity, and fault tolerance. These characteristics make RNS an alternative candidate for high speed Digital Signal processing applications, such as, digital filtering, convolution, fast Fourier transform, image processing, digital communications and the like [1], [3], [6].

However, its effectiveness is limited by a number of issues, i.e., the capability to do fast modulo operations (which depends on the moduli form), and the capability to do fast conversion as magnitude comparison, sign detection, overflow detection, etc., rely heavily on conversions. The moduli set selection is an issue of major importance as the complexity and the speed of the RNS processor depend on the selected moduli set [6]. It has been well established that powers-of-two related moduli sets simplify the required arithmetic operations and generates efficient hardware implementations of the RNS architecture. Moreover, the utilization of powers of two moduli sets, result in the realization of ROM-less reverse converters.

Extensively, several interesting moduli sets, such as $\{2^n, 2^n-1, 2^n+1\}$ [7], [8], $\{2^n, 2^n-1, 2^{n-1}-1\}$ [9], [10], $\{2^{n+1}+1, 2^{n+1}-1, 2^n\}$ [11], $\{2^n, 2^{n+1}-1, 2^n-1\}$ [12] have been proposed in order to reduce RNS processor's hardware complexity. Based on those moduli sets, efficient reverse conversion algorithms, which give room for a widespread utilization of RNS in special purpose processors, have been proposed [17].

Due to the fact that arithmetic operations with respect to 2^n+1 modulus is not as simple as the end around carry based 2^n-1 modulus and this degrades the RNS architecture performance, the moduli set $\left\{2^{n+1}-1, 2^n, 2^n-1\right\}$ [12] was proposed by removing the modulus 2^n+1 from the moduli set $\left\{2^{n+1}-1, 2^n+1, 2^n, 2^n-1\right\}$. Subsequently, the moduli sets $\left\{2^{2n+1}-1, 2^n, 2^n-1\right\}$ and $\left\{2^{2n+1}-1, 2^{2n}, 2^n-1\right\}$, with their associated converters, were proposed in [13] and [19], respectively. Given that applications requiring larger Dynamic Range (DR) than the ones offered by the moduli set $\left\{2^{2n+1}-1, 2^{2n}, 2^n-1\right\}$ are of practical interest, we propose in this paper the moduli set $\left\{2^{2n+1}-1, 2^{2n+1}, 2^{2n}-1\right\}$ as an alternative candidate to the one in [19]. Apart from having a larger DR, the suggested moduli set is more balanced when compared with the moduli set $\left\{2^{2n+1}-1, 2^{2n}, 2^n-1\right\}$.

After demonstrating that this moduli set always results in legitimate RNS, we propose a novel reverse converter based on the New Chinese Remainder Theorem (CRT). The novel reverse converter has a delay of $(4n+6)t_{FA}$ with an area cost of $(8n+2)FAs$ and $(4n-2)HAs$. We compared the proposed reverse converter with state of the art converters for similar or equal dynamic range RNS and our analysis indicate that for the same dynamic range the best converter requires $(16n+1)FAs$ and exhibits a delay of $(8n+2)t_{FA}$. This therefore indicates that, potentially speaking, our proposal is about 2 times faster and achieves about 37.5% reduction in area resources. Generally, considering the $area \times delay^2$ $(\Delta\tau^2)$ metric, our proposal demonstrates about 84.4% improvement over the state of the art.

The rest of the paper is structured as follows. Section 2 provides a brief background on reverse conversion methods. In Section 3, the novel moduli set is introduced, and the corresponding algorithm is presented in Section 4. Section 5 describes the hardware implementation of the proposed converter and evaluates and compares its performance. The paper is concluded in Section 6.

II. Background

Given a moduli set $\{m_i\}_{i=1,k}$, the residues $(x_1, x_2, ..., x_k)$ can be converted into the corresponding decimal (base 10) number X in the following ways: First, by the use of the well known Chinese Remainder Theorem (CRT), which is given as [1]:

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

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

Second, the New CRT I proposed in [13] could also be used to convert RNS to its decimal equivalent. Given a 3-moduli set $\{m_1, m_2, m_3\}$, the number X can be converted from its residue representation (x_1, x_2, x_3) as follows:

$$X = x_1 + m_1 \left| k_1(x_2 - x_1) + k_2 m_2 (x_3 - x_2) \right|_{m_2 m_3} , \tag{2}$$

where

$$|k_1 m_1|_{m_2 m_3} = 1, \tag{3}$$
$$|k_2 m_1 m_2|_{m_3} = 1. \tag{4}$$

It has been demonstrated in [4] that given any integer B, m_1, and m_2,

$$|B|_{m_1 m_2} = m_1 \left| \left\lfloor \frac{B}{m_1} \right\rfloor \right|_{m_2} + |B|_{m_1} . \tag{5}$$

This property is used in the proof of one of our theorems.

III. $\{2^{2n+1} - 1, 2^{2n+1}, 2^{2n} - 1\}$ Moduli set

For a given RNS moduli set to be valid, it is required that all the elements in the moduli set are co-prime. Thus in order to prove that the proposed set can be utilized for the construction of valid RNS architecture, we have to demonstrate that the moduli $2^{2n+1} - 1, 2^{2n+1}$, and $2^{2n} - 1$ are pair-wise relatively prime.

Theorem 1: The moduli $2^{2n+1} - 1, 2^{2n+1}$, and $2^{2n} - 1$ are pair-wise relatively prime numbers.

Proof:

From the Euclidean theorem, we have $gcd(a, b) = gcd(b, |a|_b)$, therefore, $gcd(2^{2n+1} - 1, 2^{2n+1}) = gcd(2^{2n+1}, \left|2^{2n+1} - 1\right|_{2^{2n+1}}) = 1$. Similarly,

$gcd(2^{2n+1}, 2^{2n} - 1) = gcd(2^{2n} - 1, \left|2^{2n+1}\right|_{2^{2n}-1}) = 1$. Again, $gcd(2^{2n+1} - 1, 2^{2n} - 1) = gcd(2^{2n} - 1, \left|2^{2n+1} - 1\right|_{2^{2n}-1}) = 1$ Thus, from these results, it can be concluded that the moduli set $\{2^{2n+1} - 1, 2^{2n+1}, 2^{2n} - 1\}$ contains relatively prime moduli and it is a valid RNS moduli set. ■

IV. Reverse Conversion Algorithm

Given the RNS number representation (x_1, x_2, x_3) for the moduli set $\{2^{2n+1} - 1, 2^{2n+1}, 2^{2n} - 1\}$, we propose an algorithm that computes its decimal equivalent based on New CRT in [13].

Theorem 2: Given the $\{2^{2n+1} - 1, 2^{2n+1}, 2^{2n} - 1\}$ moduli set, the following hold true:

$$\left|(2^{2n+1} - 1)^{-1}\right|_{(2^{2n+1})(2^{2n}-1)} = 2^{2n+1} - 1, \tag{6}$$

$$\left|((2^{2n+1} - 1)(2^{2n+1}))^{-1}\right|_{(2^{2n}-1)} = 2^{2n-1}. \tag{7}$$

Proof: If it can be demonstrated that $\left|(2^{2n+1} - 1) \times (2^{2n+1} - 1)\right|_{(2^{2n+1})(2^{2n}-1)} = 1$, then $2^{2n+1} - 1$ is the multiplicative inverse of $2^{2n+1} - 1$ with respect to $(2^{2n+1})(2^{2n} - 1)$. $\left|(2^{2n+1} - 1) \times (2^{2n+1} - 1)\right|_{(2^{2n+1})(2^{2n}-1)} = \left|2^{4n+2} - 2^{2n+2} + 1\right|_{2^{4n+1}-2^{2n+1}} = \left|2^{2n+2} - 2^{2n+2} + 1\right|_{2^{4n+1}-2^{2n+1}} = 0 + 1 = 1$.
Similarly, $\left|(2^{2n+1} - 1) \times (2^{2n+1}) \times (2^{2n-1})\right|_{(2^{2n}-1)} = \left|(2^{2n+1} - 1) \times (2^{4n})\right|_{(2^{2n}-1)} = \left|(2^{2n+1} - 1)\right|_{(2^{2n}-1)} = 1$.
Thus (7) and (8) holds true. ■

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 $\{2^{2n+1} - 1, 2^{2n+1}, 2^{2n} - 1\}$, can be computed as follows:

$$X = x_1 + (2^{2n+1} - 1)(2^{2n+1})w + (2^{2n+1} - 1) \left| x_1 - x_2 \right|_{2^{2n+1}} , \tag{8}$$

where, $w = \left| \left\lfloor x_2 - x_1 + 2^{2n-1} x_3 - 2^{2n-1} x_2 \right\rfloor \right|_{2^{2n}-1}$.

Proof:

Substituting (6) and (7) into (2), we obtain

$$X = x_1 + (2^{2n+1} - 1) \left| (2^{2n+1} - 1)(x_2 - x_1) + (2^{2n-1})(2^{2n+1})(x_3 - x_2) \right|_{(2^{2n+1})(2^{2n}-1)}. \tag{9}$$

Simplifying further,

$$X = x_1 + (2^{2n+1} - 1) \left| (2^{2n+1} - 1)(x_2 - x_1) + (2^{4n})(x_3 - x_2) \right|_{(2^{2n+1})(2^{2n}-1)}. \tag{10}$$

Rewriting (10), we have:

$$X = x_1 + (2^{2n+1} - 1) \left| T \right|_{(2^{2n+1})(2^{2n}-1)} , \tag{11}$$

where

$$T = (2^{2n+1} - 1)(x_2 - x_1) + (2^{4n})(x_3 - x_2). \quad (12)$$

Applying (5) to (11), we obtain:

$$X = x_1 + (2^{2n+1} - 1)(2^{2n+1})w + (2^{2n+1} - 1)C, \quad (13)$$

where,

$$\begin{aligned} w &= \left|\left\lfloor \frac{T}{2^{2n+1}} \right\rfloor\right|_{2^{2n}-1} \\ &= \left|\left\lfloor x_2 - x_1 + 2^{2n-1}x_3 - 2^{2n-1}x_2 \right\rfloor\right|_{2^{2n}-1}, \end{aligned} \quad (14)$$

and

$$C = |x_1 - x_2|_{2^{2n+1}}. \quad (15)$$

Further simplification gives,

$$X = x_1 + 2^{4n+2}w - 2^{2n+1}w + 2^{2n+1}C - C, \quad (16)$$

where all the parameters remain as defined. ■

We can further reduce the hardware complexity by making use of the following properties to simplify (16) [7].

Property 1: The multiplication of a residue number by 2^k in modulo $(2^p - 1)$ is computed by a k bit circular left shift.

Property 2: A negative number in modulo $(2^p - 1)$ is calculated by subtracting the number in question from $(2^p - 1)$. In binary representation, the one's complement of the number gives the result.

Let the residues (x_1, x_2, x_3) have the binary representation as follows:

$$x_1 = (x_{1,2n}x_{1,2n-1}...x_{1,1}x_{1,0}), \quad (17)$$

$$x_2 = (x_{2,2n}x_{2,2n-1}...x_{2,1}x_{2,0}), \quad (18)$$

$$x_3 = (x_{3,2n-1}x_{3,2n-2}...x_{3,1}x_{3,0}). \quad (19)$$

In (14), the various parameters are simplified using Property 1 and 2 as follows:

$$\begin{aligned} v_1 &= |x_2|_{2^{2n}-1} \\ &= |(x_{2,2n}x_{2,2n-1}...x_{2,0})|_{2^{2n}-1} \\ &= \left(\underbrace{x_{2,2n-1}x_{2,2n-2}...x_{2,0} \wedge x_{2,2n}}_{2n}\right) \end{aligned} \quad (20)$$

$$|-x_1|_{2^{2n}-1} = \left|v_2^{'} + v_2^{''}\right|_{2^{2n}-1}$$

$$v_2^{'} = \left(\underbrace{11...11x_{1,2n}}_{2n}\right) \quad (21)$$

$$v_2^{''} = \left(\underbrace{\overline{x}_{1,2n-1}\overline{x}_{1,2n-2}...\overline{x}_{1,0}}_{2n}\right) \quad (22)$$

$$\begin{aligned} v_3 &= \left|2^{2n-1}x_3\right|_{2^{2n}-1} \\ &= \left|2^{2n-1}\left(x_{3,2n-1}x_{3,2n-2}...x_{3,0}\right)\right|_{2^{2n}-1} \\ &= \left(\underbrace{x_{3,0}x_{3,2n-1}...x_{3,1}}_{2n}\right) \end{aligned} \quad (23)$$

$$\left|-2^{2n-1}x_2\right|_{2^{2n}-1} = \left|v_4^{'} + v_4^{''}\right|_{2^{2n}-1}$$

$$v_4^{'} = \left(\underbrace{x_{2,2n}11...11}_{2n}\right) \quad (24)$$

$$v_4^{''} = \left(\underbrace{\overline{x}_{2,0}\overline{x}_{2,2n-1}...\overline{x}_{2,1}}_{2n}\right) \quad (25)$$

Now, let us rewrite (14) as :

$$\begin{aligned} w &= \left|\left\lfloor \frac{T}{2^{2n+1}} \right\rfloor\right|_{2^{2n}-1} \\ &= \left|\left\lfloor v_1 + v_2^{''} + v_3 + v_4^{''} + v_4^{'} + v_2^{'} \right\rfloor\right|_{2^{2n}-1}, \end{aligned} \quad (26)$$

where, $T, v_1, v_2^{''}, v_3, v_4^{''}, v_4^{'}$, and $v_2^{'}$ are representing (12), (20), (22), (23), (25), (24) and (21), respectively.

Similarly,

$C = x_{1,2n}x_{1,2n-1}...x_{1,1}x_{1,0} + \overline{x}_{2,2n}\overline{x}_{2,2n-1}...\overline{x}_{2,1}\overline{x}_{2,0}$.

V. Hardware Realization and Performance Comparison

The hardware structure of the proposed reverse converter for the Moduli set $\left\{2^{2n+1} - 1, 2^{2n+1}, 2^{2n} - 1\right\}$, is based on (13) and (26). The realization of (13) is as a result of the reduction of modulo $(2^{2n+1})(2^{2n} - 1)$ operation in (11) into two modulo operations in parallel. One is based on 2^{2n+1} and the other is based on $2^{2n} - 1$. Also, the operand T is reduced to $\left\lfloor \frac{T}{2^{2n+1}} \right\rfloor$ without any additional hardware required. It must be noted that, $|x_1 - x_2|_{2^{2n+1}}$ is a truncation and a $(2n + 1)$ Least Significant Bits (LSB) of T, while the floor of T, i.e., $\left|\left\lfloor \frac{T}{2^{2n+1}} \right\rfloor\right|_{2^{2n}-1}$ is the remaining part after the truncation. Also, since T is a $(4n + 1)$ bit number, $\left|\left\lfloor \frac{T}{2^{2n+1}} \right\rfloor\right|_{2^{2n}-1}$ is the $2n$ Most Significant Bit (MSB) of T.

The parameters $v_1, v_2^{''}, v_3, v_4^{''}, v_4^{'}$, and $v_2^{'}$ in (26) are added by 4 cascaded $2n$ bit Carry Save Adders (CSAs) with end-around carries (EACs) resulting in the values s_4 and c_4 which are further reduced to one number w by modulo $2^{2n} - 1$ carry propagate adder in $(4n)t_{FA}$ delay. The floor of the parameters in (26) must be added modulo $2^{2n} - 1$. Again, to speed up the

computation process in (14), we anticipate two cases. For case 1, if $x_2 - x_1 + 2^{2n-1}x_3 - 2^{2n-1}x_2 < 0$, then $2^{2n+1}\left\lfloor \frac{T}{2^{2n+1}} \right\rfloor = 0$, reducing (16) drastically in terms of computational load. Case 2 invovles all the parameters in the addition modulo $2^{2n}-1$. Similarly, in parallel, x_1 and x_2 are addded with CPA1 with EAC with a conversion time of $2(2n+1)t_{FA}$. Simultaneously, the other branch which involves the addition of 4 cascaded $2n$ bit CSAs results in $(4n+6)t_{FA}$ delay. Hence, the proposed converter has $(4n+6)t_{FA}$ delay.

It is interesting to note that, some of the operands in (26) result in the reduction of FAs to HAs. Since, (21) has $(2n-1)$ bits of 1's and (24) also has $(2n-1)$ bits of 1's, $(2n)$ of the Full Adders (FAs) in the CSA with EAC are reduced to $(2n-1)$ HAs in CSA2 operands. This means that the proposed converter uses $(8n+2)$FA and $(4n-2)$HA area resources. The final result is computed based on (16) just by a shift and concatenation operation involving w, C, and x_1. The overall structure of the proposed converter is presented in Figure 1. We note that the operand preparation units do not require any additional hardware and do not induce any extra delay as they just concatenate and place the bits in the right position by proper wire routing.

The performance of the proposed reverse converter is evaluated theoretically in terms of conversion time and area cost. The hardware utilization of our proposal is computed in terms of Full Adders (FAs) and Half Adders (HAs). We compare our proposal with equivalent best known state of the art reverse converters presented in [20] and [22]. In [22], two four-moduli sets $\{2^n+1, 2^n-1, 2^n, 2^{2n+1}-1\}$ and $\{2^n+1, 2^n-1, 2^{2n}, 2^{2n+1}-1\}$ were investigated. For easy reference, [22]-I denotes $\{2^n+1, 2^n-1, 2^n, 2^{2n+1}-1\}$ while [22]-II represents $\{2^n+1, 2^n-1, 2^{2n}, 2^{2n+1}-1\}$.

We note that for reverse converters with different moduli sets to be fairly compared, the moduli sets should provide the same dynamic range. That notwithstanding, we compare our proposal with similar dynamic range moduli set and other existing lesser dynamic range moduli sets. The performance of our converter and of equivalent state of the art is presented in Table 1.

The proposed reverse converter requires a delay of $(4n+6)t_{FA}$ while the best known $6n$ bit DR [22]-I has $(8n+2)t_{FA}$ delay. In terms of area, our proposal utilizes $8n+2$ FAs , $4n-2$ HAs, while the best known state of the art requires $(16n+1)$ FAs. To simplify the area comparison we assumed that one FA has an area about twice as large than the HA and expressed the area cost for all the considered designs in terms of HAs. One can observe in the Table that our converter outperforms all the counter candidates in terms of area and delay. In particular, for the same $6n$ DR, our proposal provides a $2\times$ speedup and 37.5% area reduction when compared with the converter corresponding to the moduli set [22]-II. Overall, considering the $\Delta\tau^2$ metric, our proposal demonstrates about 84.4% improvement over the state of the art.

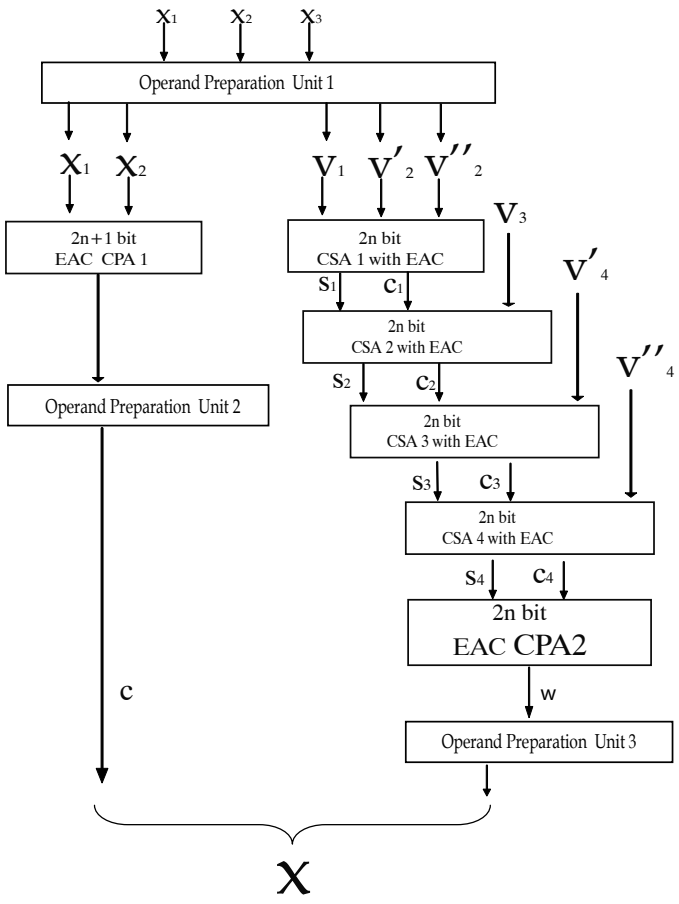

Fig. 1. Block diagram for the Proposed Converter

VI. Conclusions

In this paper, we introduced a new moduli set $\{2^{2n+1}-1, 2^{2n+1}, 2^{2n}-1\}$ which contains only low-cost moduli and has a large dynamic range. A novel and effective reverse converter is proposed based on the New CRT. Additionally, we further simplified the resulting architecture in order to obtain a reverse converter that utilizes 4 levels of CSAs namely, CSA1, CSA2, CSA3, and CSA4 together with two CPAs i.e., CPA1 and CPA2. The proposed converter is purely adder based and memoryless. Theoretically speaking, our proposal has a delay of $(4n+6)t_{FA}$ with an area cost of $(8n+2)FAs$ and $(4n-2)HAs$. We compared the proposed reverse converter with state of the art converters for similar or equal dynamic range RNS and our analysis indicate that for the same dynamic range the best state of the art converter requires $(16n+1)FAs$ and exhibits a delay of $(8n+2)t_{FA}$. This indicates that, theoretically speaking, our proposal achieves about 37.5% area reduction and its about 2 times faster. Moreover, the metric product of area and the square of the delay is improved up to about 84.4% over the state of the art.

Table 1. Area and Delay Comparison

Converter	$\{2^{2n+1}-1, 2^n, 2^n-1\}$	$\{2^n+1, 2^n-1, 2^n, 2^{2n+1}-1\}$	$\{2^n+1, 2^n-1, 2^{2n}, 2^{2n+1}-1\}$	Proposed
DR	$4n$	$5n$	$6n$	$6n$
FA	$9n+2$	$13n+2$	$16n+1$	$8n+2$
HA	$5n+4$	$-$	$-$	$4n-2$
Area Cost in HA (Δ)	$23n+8$	$26n+4$	$32n+2$	$20n+2$
Delay (τ)	$(7n+7)t_{FA}$	$(8n+1)t_{FA}$	$(8n+2)t_{FA}$	$(4n+4)t_{FA}$
$\Delta\tau^2$	$\approx 1127n^3$	$\approx 1664n^3$	$\approx 2048n^3$	$\approx 320n^3$

REFERENCES

[1] N.S. Szabo and R.I. Tanaka. *Residue Arithmetic and its Applications to Computer Technology*, McGraw Hill. New Tork, 1967.

[2] M. Shew, S. Lin, C. Chen and S. Yang. *An Efficient VLSI Design for a Residue to Binar Converter for General Balance moduli* $\{2^n-3, 2^n+1, 2^n-1, 2^n+3\}$. IEEE Transactions on Circuits and Systems -II Express Briefs, Vol. 51, No.3, pp. 152-155 March, 2004.

[3] B. Parhami. *Computer Arithmetic: Algorithms and Hardware Designs*. Oxford University press, 2000.

[4] S. Bi, W. Wang, and A. Al-Khalili. *Modulo Deflation in* $\{2^n+1, 2^n, 2^n-1\}$ *Converters*. IEEE International Symposium on Circuit and System (ISCAS), pp. 429–432. 2004.

[5] S. Lin, M. Sheu and C. Wang. *Efficient VLSI Design of Residue-to-Binary Converter for the moduli set*. IEICE Trans Inf and Syst., Vol. E91-D, No.7, pp. 2058-2060, , July, 2008.

[6] K.A. Gbolagade, G.R. Voicu, S.D. Cotofana. *Memoryless RNS-to-Binary Converters for the* $\left\{2^{n+1}-1, 2^n, 2^n-1\right\}$. IEEE International Conference on Application Specific System, Architectures and Processors (ASAP 2010) pp 301-304, Rennes, France. July, 2010.

[7] E.K. Bankas and K.A. Gbolagade. *A Speed Efficient RNS-to-Binary Converter for a the Moduli set* $\{2^n, 2^n+1, 2^n-1\}$. Journal of Computing. Volume 4, Issue 5, pp. 83-88. May, 2012.

[8] Y. Wang, X. Song, M. . Abouihamid, and H. Shen. *Adder based residue to binary number converters for* $\{2^n, 2^n, 2^n-1\}$. IEEE Trans. on Signal Processing, Vol. 50, pp. 1772-1779. July, 2002.

[9] M. Hosseinzadeh, A.S. Molahosseini and K. Navi. *A parallel Implementation of the Reverse Converter for the moduli set* $\left\{2^n, 2^n-1, 2^{n-1}-1\right\}$. World Academy of Science, Engineering and Technology, Vol. 55, pp. 494-498. 2009.

[10] A. A. Hiasat and H.S. Abdel-AtyZohdy. *Residue-to-Binary arithmetic Converters for the moduli set* $\left\{2^k, 2^k-1, , 2^{k-1}-1\right\}$. IEEE Transactions on Circuits and Systems -II Analog and Digital Signal Processing, Vol. 45, No.2, pp. 204-209 Feb., 1998.

[11] A. S. Molahosseini, K. Navi. *New Arithmetic residue to binary Converters* . International Journal of Computer Sciences and Engineering Systems, Vol. 1, No.4, pp. 295-299 Oct., 2007.

[12] P.V.A. Mohan. *RNS-to-Binary Converters for a new three moduli set* $\left\{2^{n+1}-1, 2^n, 2^n-1\right\}$ IEEE Transactions on Circuits and Systems -II. Express brief, Vol. 54, No.9, pp. 775-779 September, 2007.

[13] 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.

[14] B. Cao, C. Chang and T Srikanthan. *Adder Based Residue-to-Binary Converter for a New Balanced 4-moduli set*. Proceedings of the 3rd International Symposium on Image and Signal Processing and Analysis. pp. 820-825 2003.

[15] B. Cao, C. Chang and T Srikanthan. *An Efficient Reverse Converter for the 4-moduli set* $\left\{2^n-1, 2^n, 2^n+1, 2^{2n}+1\right\}$ *Based on the New Chinese Remainder Theorem*. IEEE Transactions on Circuits and Systems -I. Fundamental Theory and Applications. Vol. 50, No.10. Pp. 1296 - 1303, October, 2003.

[16] Y. Wang. *New Chinese Remaider Theorem*. In proc. Asilomar Conference, USA. pp. 165-171. Nov. 1998.

[17] A. S. Molahosseini, K. Navi and C. Dadkhah, O. Kavehei and S. Timarcli . *Efficient Reverse Converter Designs for the New 4-Moduli sets* $\left\{2^n-1, 2^n, 2^n+1, 2^{2n+1}-1\right\}$ *and* $\left\{2^n-1, 2^n, 2^{2n}, 2^{2n}+1\right\}$ *Based on New CRTs*. IEEE Transactions on Circuits and Systems -I. Vol. 57, No.4, 823 -835. April, 2010.

[18] A. S. Molahosseini, C. Dadkhah, and K. Navi. *A new five-moduli set for efficient hardware implementation of the reverse converter*. IEICE Electronic Express. Vol.6. pp. 1006-1012. July, 2009.

[19] K.A. Gbolagade, R. Chaves, L. Sousa, and S.D. Cotofana. *Residue-to-Binary Converters for the* $\left\{2^{2n+1}-1, 2^{2n}, 2^n-1\right\}$ *Moduli set*. 2nd IEEE International Conference on Adaptive Science and Technology. pp. 26 - 33, Accra, Ghana. December, 2009.

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

[21] B. Cao, T. Srikanthan, and C.H. Chang. *Efficient reverse converters for the four-moduli sets* $\left\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1, \right\}$ *and* $\left\{2^n-1, 2^n, 2^n+1, 2^{n-1}-1\right\}$. IEEE Proc. Computers and Digital Tech. vol. 152, no. 5, pp. 687-696. Sept. 2005.

[22] L. Sousa and S. Antao. *MRC based RNS Reverse Converters for the Four Moduli Sets* $\left\{2^n+1, 2^n-1, 2^n, 2^{2n+1}-1\right\}$ *and* $\left\{2^n+1, 2^n-1, 2^{2n}, 2^{2n+1}-1\right\}$. IEEE Transactions on Circuits and Systems II: Express Briefs. vol. 59, no. 4, pp. 244-248. April, 2012.

[23] P.V Ananda Mohan and A. B. Premkumar. *RNS-to-binary converters for two four-moduli sets* $\left\{2^n, 2^n+1, 2^n-1, 2^{n+1}-1\right\}$ *and* $\left\{2^n, 2^n+1, 2^n-1, 2^{n+1}+1\right\}$. IEEE Transactions on Circuits and Systems I: Regular papers, vol. 54, no. 6, pp. 1045-1054. June, 2007.

[24] A. Omondi and A. B. Premkumar. *Residue Number Systems. Theory and Implementations*. Imperial College Press. 2007.