Design of an Efficient Reverse Converter for Moduli Sets $2^{4p}+1, 2^{p}+1, 2^{p}-1, 2^{2p}+1, 2^{2p}$

DOI : 10.36909/jer.ICMET.17193

Patel Beerendra*, Jitendra Kanungo

Department of Electronics & Communication Engineering, Jaypee University of Engineering & Technology, Guna-473226, India.

*Email: beerendrapatel23@gmail.com; Corresponding Author

ABSTRACT

In this paper, the reverse converter design for moduli sets $2^p-1, 2^p, 2^p+1$ is proposed. This design for five moduli sets $2^{4p}+1, 2^{2p}, 2^{2p}+1, 2^p+1, 2^p-1$ by using the new Chinese Remainder Theorem (CRT-1) formulates the wide modular devaluation. The appropriate selection of moduli has a significant impact on the reverse converter's speed and complexity. The modified converter depends upon the arithmetic designs that are implemented without the read - only memories and lookup tables. The Carry Save Adder and Carry Propagate Adder are used in the reverse converter and modulo adder gives higher speed and less hardware complexity. The proposed converter has been implemented to get the conversion time and area as supported by the reverse converter of 12-bits and maximum up to 100-bits.

Key words:R/B converter, Chinese remainder theorem (CRT), End around carry (EAC), CSA.

INTRODUCTION

Few numbers formularized and exist to promote the design of the reverse converters [Hwang (1979)]. The key advantages of the RNS are shorter circuits and propagation paths, notably for converters. A reverse converter and a set of data path channels that achieve useful estimations comprise the general structure of a data path with an RNS. Therefore, the conversion becomes simpler at the cost of the complete data path. So, converter cost should be reduced. To increase the hardware use of the available dynamic range and the performance of the logic circuits the data path gain over positional is required and may be implemented with the channel modular arithmetic operators in the RNS data path [L. Sousa *et al.* (2017)]. The implementation of the arithmetic circuits primarily depends on efficiency and performance [B. Patel et al. (2021)]. The performance of the rest of the data path may be obtained, if special moduli set severely confined. So, main motive is to give useful converter for a given arbitrary moduli set. Conversion between of weighted and residual representation there are four main forms [N.S. Szabo et al.(1967)]. In the literature, two modifications in the Chinese Remainder Theorem (CRT) have been found [A. Hiasat (2021)]. These are Mixed Radix Conversion (MRC) and the selection of moduli set [Teghipour et al. (2015)]. In the design of a devoted hardware structure the mathematical calculations are used for a specific modulus set [Patel *et al.* (2018)]. In the Mixed Radix Conversion, the main difficulty has been the sequential form of arithmetic digits [Teghipour et al. (2015)]. Chinese remainder theorem even though gives implicit parallelism. The development of a large modular expansion tree is required. Apart from the architecture that was presented in [Phalguna et al. (2018)], the CRT approach can be used to design the converters for special moduli sets. After all, the inner products of the Chinese Remainder Theorem (CRT) are large moduli. A big problem of calculation with a binary number the segment eradication of the modulus in the addition and multiplication. In [A.S.Molahossaini (2017)], a design called New CRT-II, a tree has been proposed with tree disintegration along with the modular contraction on each level. This work has been proposed the reverse converter design based on fully parallel preferred five moduli sets, the moduli $2^a - 1$. These sets achieve speed, and area performance.

Main aim is to provide the converter for the special moduli sets with type 2^k. The channels cost performance metric can easily be updated by modifying this option, if necessary. The converter is required for an Even number of channels on one form, but both forms (direct and multiplied) are desired. There is no need to use Read Only Memory (ROM) in a path that is strictly arithmetic, where the path is in series [A. S. Molahossaini (2017)].

A reverse converter with a five modulo set $2^{4p}+1, 2^{2p}, 2^{2p}+1, 2^{p}+1, 2^{p}-1$ is proposed. In this converter design, the modified Chinese remainder theorem has been applied. The proposed converter has displayed superior to other converters in respect of the conversion time. This conversion algorithm is analyzed and it achieves less area and higher speed; an efficient implementation.

To this end, study the theoretical background of reverse converter is presented in this section, the proposed architecture of reverse converter using multiplicative inverse modulo, Extended Euclidean theorem is discussed. The proposed converter using new Chinese remainder theorem-I and discuss mixed radix technique (MRC). The goal is to reduce conversion process time and save area in reverse converter. Finally, the simulation results have been evaluated, last section is conclusion.

THEORETICAL BACKGROUND

The CRT gives an algorithmic technique for decoding the residue encoded number back into its traditional form. This theorem is regarded as the foundation for realizing RNS system. When a huge number is encoded into a set of small numbers, the overall data processing becomes faster [Srikanthan, T. (2007)]. This fact favors the use of RNS in situations where extensive processing is unavoidable.

The RNS is characterized as a sequence of relatively prime numbers that are positive pair wise $\{m_i\}$ =1, k termed the moduli set, so that greatest common divisor $(m_i, m_j)=1$ for $i \neq j$ While $M=\prod_{i=1}^{k} m_i$, is the Dynamic Range (DR). In residue form, the decimal number X can be written as x_i = |X|, This means that in RNS, X can be represented as $X=(x_1, x_2, x_3, x_4)$, $0 \leq x_i < m_i$.

Mixed Radix Conversion (MRC) and new CRTs have been employed [P.S. Phalguna et al. (2018)].

Assume the set of five moduli $S=\left\{2^{4p}+1,2^{2p},2^{2p}+1,2^{p}+1,2^{p}-1\right\}=\{m_1,m_2,m_3,m_4,m_5\}$

where p shows a natural number (which is greater than 1) and integer X which makes the analogous residues and represent bit level residue as follows:

$$x_1=(x_{1,2p-1}x_{1,2p-2}x_{1,2p-3}\ldots\ldots\ldots\ldots x_{1,1}x_{1,0})_2 \quad (1)$$

$$x_2=(x_{2,4p}x_{2,4p-1}x_{2,4p-2}\ldots\ldots\ldots\ldots x_{2,1}x_{2,0})_2 \quad (2)$$

$$x_3=(x_{3,2p}x_{3,2p-1}x_{3,2p-2}\ldots\ldots\ldots\ldots x_{3,1}x_{3,0})_2 \quad (3)$$

$$x_4=(x_{4,p}x_{4,p-1}x_{4,p-2}\ldots\ldots\ldots\ldots x_{4,1}x_{4,0})_2 \quad (4)$$

$$x_5=(x_{5,p-1}x_{5,p-2}x_{5,p-3}\ldots\ldots\ldots\ldots x_{5,1}x_{5,0})_2 \quad (5)$$

PROPOSED ARCHITECTURE

MULTIPLICATIVE INVERSE MODULO

The multiplicative inverse modulo perform number *'x' mod' y'* as $\left|x^{-1}\right|_y$. The amount $\left|x^{-1}\right|_y$ occurs, in the case that x and y are co-prime with one another, i.e, gcd $(x,y)=1$.

$$\left|x^{-1}\right|_m=y;y\in\{1,2,3,\ldots\ldots.m-1\} \quad (6)$$

Where y is such that $|x.y|_m=1$

Ex: $\left|5^{-1}\right|_{11}=9$

In literature, it is found that many algorithms have been used to find the multiplicative inverse modulus. Few of them are based on Fermat's theorem, Euclidean algorithm and Euler Function [Hwang (1967)]. The Extended Euclidean algorithm is also used to calculate the multiplicative inverse modulus.

EXTENDED EUCLIDEAN THEOREM

An expanded version of Euclidean method [Y. Wang (2000)], the modified Euclidean algorithm is used to find two numbers (f and g) which are co-prime to each other. In the document, that is stated as:

$$f_x + g_y = \text{gcd}(f, g) \tag{7}$$

where f, g represent integers.

With translation of inverse modulus, f_x is identical to $|1|_g$ Thus, 'g' is the divisor of $f_x - 1$, they provide the subsequent,

$$f_x - g_y = 1 \tag{8}$$

An integer 'y' is substituted in for the modulus value of the values 'f' and 'g' in the Equation (8).

An example is given as: Suppose the amount of $|12^{-1}|_5$. Use Equation (7), and error method and imminent route, it is construct that x =7 and y = 10. The amount of $|12^{-1}|_5$ is 7.

Theorem-1 The moduli $2^{4p}+1, 2^{2p}, 2^{2p}+1, 2^p+1, 2^p-1$ where $p = 3,4,5.......$ is comparatively prime in terms of pairs.

Proof:- It has been thoroughly described, for the moduli $2^{2p}+1, 2^p-1, 2^p, 2^p+1$ to be pair-wise. Hence, it is shown that the moduli $2^{4p}+1$ is pair wise approximately prime to moduli $2^p-1, 2^p, 2^{2p}+1, 2^p+1$. From Euclid's method, gcd $\left(2^{4p}+1, 2^{2p}+1\right)=1$ is determined as follows:

$$\left|2^{4p}+1\right|_{2^{2p}+1} = 2$$
$$\left|2^{2p}+1\right|_2 = 1$$
$$|2|_1 = 0$$

Therefore, gcd $\left(2^{4p}+1, 2^{2p}+1\right)=1$

Determining gcd $\left(2^{4p}+1, 2^p-1\right)$ using Euclidean algorithm:

$$\left|2^{4p}+1\right|_{2^p-1} = 2$$
$$\left|2^p-1\right|_2 = 1$$
$$|2|_1 = 0$$

Therefore, gcd $\left(2^{4p}+1,2^{p}-1\right)=1$

Determining gcd $\left(2^{4p}+1,2^{p}+1\right)$ using Euclidean algorithm:

$\left|2^{4p}+1\right|_{2^{p}+1}=2$

$\left|2^{p}+1\right|_{2}=1$

$\left|2\right|_{1}=0$

Therefore, gcd $\left(2^{4p}+1,2^{p}+1\right)=1$

Determining gcd $\left(2^{4p}+1,2^{2p}\right)$ using Euclidean algorithm:

$\left|2^{4p}+1\right|_{2^{2p}}=\left|0+1\right|_{2^{2p}}=1$

$\left|2^{p}\right|_{1}=0$

Therefore, gcd $\left(2^{4p}+1,2^{2p}\right)=1$ hence, the GCD stands for Greatest Common Divisor is equal one. The moduli set with $2^{4p}+1,2^{2p}+1,2^{p}-1,2^{2p},2^{p}+1$ is pair-wise co-prime applicable to all values 'n' which is greater than 1.

Property-1:- Here, multiplicative inverse of $\left|2^{2p}\right|_{2^{8p}-1}$ is given as:

$$\left|m^{-1}\right|_{m_2m_3m_4m_5}=\left|(2^{2p})^{-1}\right|_{2^{8p}-1}=2^{6p} \qquad (9)$$

Here 'p' represents natural number which is greater than 1

Proof:- Using property, whenever $\left|a^{-1}\right|_{m}=b$ then $\left|a.b\right|_{m}=1$

Since, $\left|(2^{2p})^{-1}\right|_{2^{8p}-1}=2^{6p}$

We have $\left|2^{2p}.2^{6p}\right|_{2^{8p}-1}=\left|2^{8p}\right|_{2^{8p}-1}=1$

Property-2:- Here, multiplicative inverse of $\left|2^{2p}(2^{4p}+1)\right|_{2^{4p}-1}$ is given as:

$$\left|(m_1m_2)^{-1}\right|_{m_3m_4m_5}=\left|(2^{2p}(2^{4p}+1))^{-1}\right|_{2^{4p}-1}=2^{2p}-1 \qquad (10)$$

Here 'p' represent natural number, where p >1

Proof:-Applying equation (1) whenever $\left|a^{-1}\right|_{m}=b$ when $\left|a.b\right|_{m}=1$

Since $\left|(2^{2p}(2^{4p}+1))^{-1}\right|_{2^{4p}-1} = 2^{2p}-1$, we have

$$\left|2^{2p}(2^{4p}+1).2^{2p-1}\right|_{2^{4p}-1} = \left|2^{2p}(2).2^{2p-1}\right|_{2^{4p}-1} = \left|2^{4p}\right|_{2^{4p}-1} = 1$$

Property-3:- The multiplicative inverse of $2^{2p}(2^{4p}+1)(2^{2p}+1)$ modulo $2^{2p}-1$ is given as:

$$\left|(m_1m_2m_3)^{-1}\right|_{m_4m_5} = \left|(2^{2p}(2^{4p}+1)(2^{2p}+1))^{-1}\right|_{2^{4p}-1} = 2^{2p-2}$$

(11)

Here p' represent natural number, where p >1

Proof:-Applying equation (1) whenever $\left|a^{-1}\right|_m = b$ when $\left|a.b\right|_m = 1$

Since $\left|(2^{2p}(2^{4p}+1)(2^{2p}+1))^{-1}\right|_{2^{4p}-1} = 2^{2p-2}$,we have

$$\left|2^{2p}(2^{4p}+1)(2^{2p}+1).2^{2p-2}\right|_{2^{2p}-1}$$
$$= \left|2^{2p}(2)(2).2^{2p-2}\right|_{2^{2p}-1} = \left|2^{4p}\right|_{2^{2p}-1} = 1$$

Property-4:- The multiplicative inverse of $2^{2p}(2^{4p}+1)(2^{2p}+1)(2^{p}+1)$ modulo $2^{p}-1$ is given as:

$$\left|(m_1m_2m_3m_4)^{-1}\right|_{m_5} = \left|(2^{2p}(2^{4p}+1)(2^{2p}+1)(2^{p}+1))^{-1}\right|_{2^{p}-1} = 2^{2p-3}$$

(12)

Here 'p' represents natural number which is greater than 1

Proof:-Applying equation (1) whenever $\left|a^{-1}\right|_m = b$ when $\left|a.b\right|_m = 1$

Since $\left|(2^{2p}(2^{4p}+1)(2^{2p}+1)(2^{p}+1))^{-1}\right|_{2^{p}-1} = 2^{2p-3}$, We have

$$\left|(2^{2p}(2^{4p}+1)(2^{2p}+1)(2^{p}+1))^{-1}\right|_{2^{p}-1} = 2^{2p-3}$$

$$\left|2^{2p}(2^{4p}+1)(2^{2p}+1)(2^{p}+1).2^{2p-3}\right|_{2^{p}-1}$$
$$\left|2^{2p}(2)(2)(2).2^{2p-3}\right|_{2^{p}-1} = \left|2^{3p}\right|_{2^{p}-1} = 1$$

MIXED RADIX CONVERSION (MRC)

RNS of integer X can be depicted in the following way $(x_1, x_2 ...., x_L)$ employing the moduli set $S = (m_1, m_2 ...., m_L)$, gcd $(m_i, m_j) = 1$ for $i \neq j$. The number X could be performed against its residue reproduction X_i by MRC [N.S.Szabo (1967)] and shown below:

$$X = x_1^{'} + m_1 x_2^{'} + m_1 m_2 x_3^{'} + m_1 m_2 m_3 x_4^{'} + ... + m_1 m_2 m_3 m_4 .... m_{L-1} . x_L^{'}$$

(13)

The mixed radix digits are $x_1^{'}, x_2^{'}, x_3^{'}, x_4^{'} .... x_L^{'}$ and $x_i^{'}$ apply to $Z_{m_i} = [0, m_i - 1]$. The mixed radix digits $x_1^{'}, x_2^{'}, x_3^{'}, x_4^{'} .... x_L^{'}$ may be expressed as a function of the number of residues $(x_1, x_2 ...., x_L)$ and the moduli of $\{m_1, m_2 ...., m_L\}$.

In a two moduli set $\{m_1, m_2\}$, $GCD(m_1, m_2) = 1$, The residue representation (x_1, x_2) of the number X can be used to formulate the number by using the Mixed Radix Technique as [2]-

$$X = x_1 + m_1 \left| \left| m_1^{-1} \right|_{m_2} .(x_2 - x_1) \right|_{m_2}$$

(14)

NEW CHINESE REMAINDER THEOREM (CRT-I)

The exhibition of RNS of an integer X could be in the form $(x_1, x_2 ...., x_L)$ employing the moduli set $S = (m_1, m_2 ...., m_L)$, gcd $(m_i, m_j) = 1$ for $i \neq j$. New CRT-1 can create the following number X from its residue representation:

$$X = x_1 + m_1 \left| k_1 (x_2 - x_1) + k_2 m_2 (x_3 - x_2) + ... k_{L-1} m_1 .... m_{L-1} (x_L - x_{L-1}) \right|_{m_2 .... m_{L-1} m_L}$$

(15)

$$k_1 = \left|m_1^{-1}\right|_{m_2....m_L}, k_2 = \left|(m_1m_2)^{-1}\right|_{m_3...m_L}, ...k_{L-1} = \left|(m_1m_2.....m_{L-1})^{-1}\right|_{m_L}$$

(16)

Considering three moduli set $\{m_1, m_2, m_3\}$ and the representation of binary number X determined with the new CRT-1:

$$X = m_1 \left|k_1(x_2 - x_1) + k_2m_2(x_3 - x_2)\right|_{m_2m_3} + x_1$$

(17)

$$k_1 = \left|m_1^{-1}\right|_{m_2m_3}, k_2 = \left|(m_1m_2)^{-1}\right|_{m_3}$$

(18)

Considering four moduli set $\{m_1, m_2, m_3, m_4\}$ and the representation of binary number X determined with the new CRT-1:

$$X = m_1 \left|k_1(x_2 - x_1) + k_2m_2(x_3 - x_2) + k_3m_2m_3(x_4 - x_3)\right|_{m_2m_3m_4} + x_1$$

(19)

$$k_1 = \left|m_1^{-1}\right|_{m_2m_3m_4}, k_2 = \left|(m_1m_2)^{-1}\right|_{m_3m_4}, k_3 = \left|(m_1m_2m_3)^{-1}\right|_{m_4}$$

(20)

For a five moduli set $\{m_1, m_2, m_3, m_4, m_5\}$ the representation of binary number X determined with new CRT-1:

$$\begin{aligned} X = m_1 \mid & k_1(x_2 - x_1) + k_2m_2(x_3 - x_2) + \\ & k_3m_2m_3(x_4 - x_3) + k_4m_2m_3m_4(x_5 - x_4) \mid_{m_2m_3m_4m_5} + x_1 \end{aligned} \quad (21)$$

Where as

$$k_1 = \left|m_1^{-1}\right|_{m_2m_3m_4m_5}, k_2 = \left|(m_1m_2)^{-1}\right|_{m_3m_4m_5}$$

$$k_3 = \left|(m_1m_2m_3)^{-1}\right|_{m_4m_5}, k_4 = \left|(m_1m_2m_3m_4)^{-1}\right|_{m_5} \quad (22)$$

Substituting the values of (9), (10), (11), and (12) in (14), the value of can be simplified as:

$$X = x_1 + 2^{2p}.M \quad (23)$$

$$M = \left|H_1 + H_2 + H_3 + H_4 + H_5 + H_6 + H_7\right|_{2^{8p}-1} \quad (24)$$

CONVERTER IMPLEMENTATION

The architecture of the proposed reverse converter for the moduli sets $\left\{2^{4p}+1, 2^{2p}, 2^{2p}+1, 2^{p}+1, 2^{p}-1\right\}$ is given in Figure-1. The addition of modulo $H_1, \mathrm{H}_2, \mathrm{H}_3, \mathrm{H}_4, \mathrm{H}_5, \mathrm{H}_6$ and H_7 is five 8p-bit wide Carry Save Adders with End-Around Carry execute the task (EAC-CSA). The hardware complexity of the 8p-bit CPA1 with EAC is the same as that of a conventional CPA, with the exception of the delay, which is twice that of a regular CPA. The CSA1 adds vectors $H_1 H_2, \mathrm{H}_3$ produces output sum1 and carry1. Similarity, CSA2 adds vectors $H_5, \mathrm{H}_6, \mathrm{H}_7$ produces output sum_2 and carry_2. This sum_1 and carry_1 and vectors H are later added with a 8p-bit large carry save adder with EAC adder. With a modulo $2^{8p}+1$ adder, one 8p-bit wide Carry propagate adder with End-Around Carry (EAC-CPA) outputs 8p-bits. At last, ‘X’ is simply calculated of $'x_1'$ and 8p-bit wide output input without needing any additional Logic. In this reverse converter, the cost of hardware and delay are explored and analyzed. Approximate Dynamic Range (DR) is presented in Table-1 for the

five moduli sets $2^{4p}+1, 2^{2p}, 2^{2p}+1, 2^{p}+1, 2^{p}-1$.It shows the advantage of reverse converter for moduli set $2^{4p}+1, 2^{2p}, 2^{2p}+1, 2^{p}+1, 2^{p}-1$ designed by using new CRT-1 [P.S. Phalghuni et al. (2018)]. The proposed design is efficient as compared to the reported reverse converter designs. The reverse converter has shown less hardware complexity compared to others for available a dynamic range. The proposed reverse converter is found to be suitable for moduli set $2^{4p}+1, 2^{2p}, 2^{2p}+1, 2^{p}+1, 2^{p}-1$ in a dynamic range from 20-bits to 110-bits.

Table-1 Description of Proposed reverse converter for the moduli set $\mathbf{2^{4p}+1, 2^{2p}+1, 2^{p}-1, 2^{2p}, 2^{p}+1}$ in terms of basic gate

Parts	NOT Gate	Full Adder	AND/XOR gate pairs	OR/XNOR gate pairs	Delay
Operand Preparation Unit1	30	-	-	-	t_{NOT}
Carry Save Adder1	-	8	11	5	t_{FA}
Carry Save Adder2	-	4	4	16	t_{FA}
Carry Save Adder3	-	14	10	-	t_{FA}
Carry Save Adder4	-	24	-	-	t_{FA}
Carry Save Adder5	-	24	-	-	t_{FA}
Carry Propagation Adder1	-	24	-	-	48 t_{FA}

If a dynamic range below of 16 bits is considered then the converter is recommended for three moduli set $\{2^p+1, 2^p, 2^p-1\}$ designed by using the modified CRT. Another significant approach to MVL-RNS systems has developed a system that uses ROM table look-up techniques [A.S. Molahossaini et al. (2020)]. Because of their large sizes and lengthier accessing times, these are evidently less appropriate and uncomfortable for systems with wide dynamic ranges. With a certain speed requirement, the resultant RNS sets are extremely balanced and accomplish large dynamic ranges.

SIMULATION RESULT

The Circuits are designed by the using the VHDL language and functional verification executed through test benches.

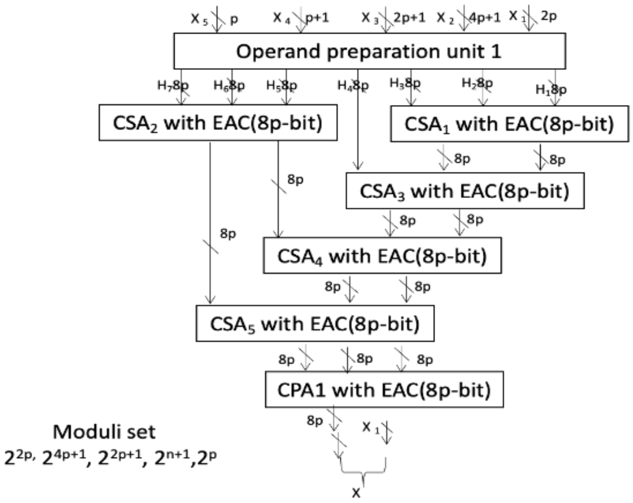

Figure 1: The proposed design of Reverse Converter for moduli set

The designs are synthesized and analyzed with the Electronic Design Automation (EDA) tool ‘Synopsys design’ at TSMC 65 nm CMOS technology. The circuit area and power consumption have been determined with help of EDA tool and gate count.

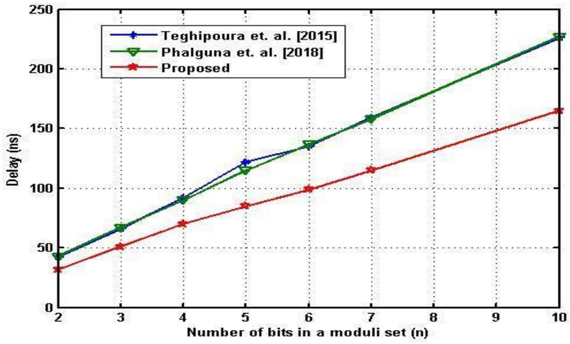

Figure 2: Delay comparison for the reported and proposed design for the various moduli set $\{S_1, S_2, S_3\}$

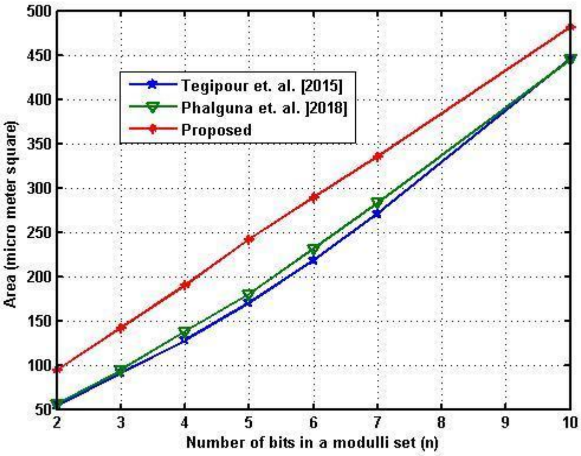

Figure 3: Area comparison for the reported and proposed design for the different moduli set $\{S_1, S_2, S_3\}$

Area and Delay comparison for the proposed design and the reported design for the moduli set $S_1 = \left\{2^{2p-1} - 1, 2^p - 1, 2^p, 2^p + 1, 2^{2p} + 1\right\}$ and $S_2 = \left\{2^{2p-1} - 1, 2^{2p} + 1, 2^p - 1, 2^p + 1, 2^{2p}\right\}$ respectively [Teghipour et al. (2015); Phalguna et al. (2018)] have shown in Fig-2 and Fig-3.

The proposed design using moduli set $S_3 = \left\{2^{4p} + 1, 2^{2p} + 1, 2^{2p}, 2^p - 1, 2^p + 1\right\}$ has also been camed out. The proposed converter has shown less delay than the reported design [Phalguna et al. (2018)] and consumes less area Teghipour et al. (2015).

Table-2 Reverse Converter of Different Dynamic ranges for the moduli set $\{S_1, S_2, S_3\}$

Moduli Sets		S_1	S_2	S_3
Conversion Algorithm		CRT + MRC [Shiva Taghi et al. (2015)]	CRT + MRC [P. S. Phalguna et al. (2018)]	Modified CRT **(Proposed)**
p=2	DynamicRange	13	15	20
p=3	Dynamic Range	20	23	30
p=4	Dynamic Range	27	32	40
p=5	Dynamic Range	33	39	50
p=6	Dynamic Range	40	47	60
p=7	Dynamic Range	47	56	71
p=10	Dynamic Range	68	78	100

Delay and area for the new moduli sets $2^{4p} + 1, 2^{2p} + 1, 2^p - 1, 2^{2p}, 2^p + 1$ have been calculated by using 'Design Compiler'. The calculated area and delay are obtained with the number of full adder, NOT gate, XOR/AND and XNOR/OR gates. Fig-2 and Fig-3 represent the reported design results and comparison of these with the proposed design results. Results show the advantages in terms of design area and delay. With a certain speed requirement, the resultant RNS sets are extremely balanced and accomplish large dynamic range. Table-2 represents the moduli sets made up of pair-wise moderately prime moduli. As a result, for these sets, the RNS-to-binary converter is also straightforward. The calculated total area and delay are*:*

$$\begin{aligned}Total\,area &= (10p-5)A_{XOR}+(30p+8)A_{FA}+(9p+3)A_{NOT}\\ &+(10p-5)A_{AND}+(8p-3)A_{XNOR}+(8p-3)A_{OR}\end{aligned}$$

$$Total\,delay = t_{NOT}+(16p+4)t_{FA}$$

Where, A_{XOR} = area of XOR gate, A_{FA} = area of Full Adder, A_{NOT} = area of NOT gate, A_{AND} = area of NOT gate, A_{XNOR} = area of XNOR gate, A_{OR} = area of OR gate.

t_{NOT} = Time consumption of NOT gate, t_{FA} = Time Consumption of Full Adder.

A reverse converter has been proposed for the new moduli set $\left\{2^{4p}+1, 2^{2p}, 2^{2p}+1, 2^{p}+1, 2^{p}-1\right\}$, especially for arithmetic unit having four dynamic ranges $(20, 30, 40, 50, 60, 71, 100)$ to best fit it for the DSP word size. With two premises, the moduli selection is based on finer-grained channel which is faster. Following two requirements must be met when selecting a moduli set: first, it should be operated on the dynamic range, and second, it should allow the efficient implementation of data path or arithmetic unit. In the survey, it is found that non-relatively prime moduli pose problems in the selection of sets, which our study has overcome by utilizing the mentioned scale factor's operation. The synthesis results are shown in Table-2 represent the reported design results and comparison of these with the proposed design results. Table-2 shown for the five moduli sets, in comparison to reverse converters' dynamic range (DR). The new CRT-1 based moduli set conversion is faster as compared to the reported design of reverse converters and also it consumes less logic resources. The moduli set converter is the best option when a dynamic range of 20 to 100 bits is required. For dynamic ranges less than 16 bits, the converter for moduli sets built with new CRT-1 and MRC is suggested. Other converters from Table-2 can also be selected for a specific dynamic range, taking into account the area and delay considerations as given in Fig 2 and Fig. 3. The outcome of the comparison is based on the flatten configuration, which allows for an approximation of the area and delay complexity in terms of a single bit full adder.With a 5-moduli set, the converters with the newly presented methods are best in terms of area conversion time. These parameters are decreased by about 15% and 21%, respectively.

CONCLUSION

A reverse converter with five modulo sets $2^{4p}+1, 2^{2p}, 2^{2p}+1, 2^{p}+1, 2^{p}-1$ has been proposed in this paper. The modified Chinese remainder theorem has been applied. The proposed converter has displayed superior to other converters in respect of conversion time. This conversion algorithm is analyzed for achieving the small area and higher speed. This converter design provides the dynamic range without affecting the hardware requirements substantially. Straightforward implementation of VLSI architecture of the reverse converter is designed by applying the possible ideas and expedite with the use of modulo 2^k and modulo 2^k+1 adders (where k represent natural number). The inclusive dynamic range backed by the reverse converter is reconfigured from 12-bits to 100-bits. The future scope of this research work may be the design of reverse converter (residue to binary converters) for a modular system with a wide range of options.

REFERENCES

Hwang, K., 1979. Computer arithmetic principle, architecture and design. Wiley Press: New York pp 223–248.

N.S. Szabo, R.I. Tanaka, 1967. Residue Arithmetic and its Applications to Computer Technology. McGraw Hill: USA pp 173–185.

Y. Wang, 2000. Residue-to-binary converters based on new Chinese Remainder Theorem IEEE Trans. Circuits Syst. II 47 (3) pp 197–205

Wang, Y., Aboulhamid M., Shen, H., 2002. Adder based residue to binary number converters for (2n -1, 2n, 2n +1) IEEE Transactions on Signal Processing vol. 50 no 7 pp 1772-1779.

Hiasat, A. 2021. A Modulo $\left\{2^n-2,\ 2^{n-2}-1\right\}$ Adder Design In Communication and Intelligent Systems, Springer, Singapore pp. 789-802.

A. S. Molahosseini, A. A. E. Zarandi, P. Martins and L. Sousa 2017.A multifunctional unit for designing efficient RNS-based datapaths IEEE Access vol. 5 pp 25972-25986.

TaghipourEivazi, S., Hosseinzadeh, M., & HabibizadNovin, A. 2015. Efficient RNS converter via two-part RNS Journal of Circuits, Systems and Computers, 24(01), 1550016.

P. S. Phalguna and D. V. Kamat 2018.RNS-to-binary converters for new three-moduli sets {2k -3, 2k -2, 2k -1} and {2k +1, 2k +2, 2k +3} J. Circuits, Systems and Computers vol. 27 pp 1850224-1-20.

P. Patronik, S.J. Piestrak 2017. Design of residue generators with CLA/compressor trees and multi-bit EAC, in: Proc. Latin America Symp. Circ. & Syst pp 1-4.

A. S. Molahosseini, Mohammad Reza Taheri 2020. Efficient Incorporation of the RNS Data Path in Reverse Converter IEEE Access vol. 5 pp 25972-25986.

P. Patronik, S. J. Piestrak, 2017.Hardware/software approach to designing low-power RNS-enhanced arithmetic units, IEEE Trans. Circ. Syst. I, Reg. Pap. 64 (5) 1031–1039.

B. K. Patel, J. Kanungo 2021.Diminished-1 multiplier using modulo 2^n+1 adder International journal of engineering and Technology, vol. 4, no. 20 pp 31-35.

T. Van Vu 1985.Efficient implementations of the Chinese Remainder Theorem for sign detection and residue decoding, IEEE Trans. Comput. C-34 (7) pp 646–651.

T. Srikanthan, M. Bhardwaj, C.T. Clarke 1998.Area-time-efficient VLSI residue-to-binary converters, IEEE Proc. Comput. Digital Tech. 145 (3) pp. 229–235.

M. Re, A. Nannarelli, G.C. Cardarilli, R. Lojacono 2001. FPGA realization of RNS to binary signed conversion architecture, in: Proc. Int. Symp. Circ. & Syst., vol. 4, 2001, pp. 350–353.

Beerendra K. Patel, J.K. 2021. Efficient Tree Multiplier Design by using Modulo 2^n+1 Adder IEEE Xplore on Emerging Trends in Industry 4.0 (ETI 4.0) DOI:10.1109/ETI4.051663.2021.9619220.

Cao, B., Chang, C.-H., Srikanthan, T. 2007.A Residue-to-Binary Converter for a New FiveModuli Set," Circuits and Systems I: IEEE Transactions on Regular Paper, vol.54, no.5, pp.1041-1049.

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