An MRC Based Efficient RNS Backward Converter for Novel Moduli Set $\{2^{2n}+1, 2^{2n}-1, 2^{2n+1}\}$

Divya Chitla

Assistant Professor
ECE Department
TKR College of Engineering and Technology, Hyderabad, India.

***Abstract*—In this paper a new adders based backward converter for a 3-moduli set $\{2^{2n}+1, 2^{2n}-1, 2^{2n+1}\}$ is proposed. It is based on Mixed Radix Conversion technique with 6n bit dynamic range. The architecture is realized with CSAs (Carry Save Adders) and CPAs (Carry Propagate Adders) only. This backward converter has demonstrated to be faster when compared with other state of art backward converters of same dynamic range.**

***Index Terms*—Mixed Radix Conversion, backward converter, carry save adder, carry propagate adder.**

I. INTRODUCTION

In recent years RNS (Residue Number System) is an unconventional number system which has attracted many in the research field. RNS is a non-weighted number system which usually uses bases that are relatively prime to each other [10]. Its high speed performance in digital signal processing [8], computing architectures, cryptography and other high speed systems has made it a popular alternative to weighted number system [1]. But RNS applications are limited by its data conversion overhead. The data conversion involves both forward and backward. But backward conversion is more complex than the forward conversion. That is why many algorithms have been designed and implemented for backward conversion with different choices of moduli sets for example $\{2^n-1,2^n,2^n+1\}$[1], $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$[4], $\{2^n-1, 2^n+1, 2^n, 2^{2n+1}-1\}$, $\{2^n-1, 2^n+1, 2^{2n}, 2^{2n}+1\}$[2]etc. The novel moduli set $\{2^{2n}+1, 2^{2n}-1, 2^{2n+1}\}$ based on New CRT (Chinese Remainder Theorem) has been proposed in [6] where there was efficient power reduction when compared with other state of art backward converters.

In this paper a MRC based new efficient backward converter for $\{2^{2n}+1, 2^{2n}-1, 2^{2n+1}\}$ moduli set is proposed. Theoretically the proposed converter is faster than ones in [2], [4], and [6].

The rest of the paper is organized as follows. Section II presents background and whereas later the proposed technique is provided in section III with its hardware realization. In section IV the performance of proposed system is evaluated. The paper is concluded in section V along with references.

II. BACKGROUND

RNS can be defined in terms of co-prime or relatively prime moduli set $\{P_1, P_2 \ldots P_N\}$ where GCD $(P_i, P_j) = 1$ for $i \neq j$ and GCD (α, β) denotes the greatest common divisor of α and β. A weighted based number X can be represented as $X = (x_1, x_2, x_{3,\ldots,}x_n)$ where

$$Xi = X \bmod P_i = |X|_{Pi} \quad 0<xi< Pi \qquad (1)$$

Such a representation is unique for any integer X in range (0, P-1).Where $P=P_1, P_{2,}\ldots P_N$ is the dynamic range of moduli set $\{P_1, P_{2,}\ldots P_N\}$.

Mixed Radix Conversion (MRC): For a three moduli set $\{P_1, P_2, P_3\}$ the number X can be derived from its residue representation(x_1, x_2, x_3) i.e. backward converted by MRC as follows [7].

$$X = a_1+a_2P_1+a_3P_1P_2+\ldots\ldots \qquad (2)$$

Where

$$a_1 = x_1 \qquad (3)$$

$$a_2 = |(x_2 - a_1) \mid P_1^{-1}| P_2 |_{P_3} \qquad (4)$$

$$a_3 = |((x_3 - a_1) \mid P_1^{-1}| P_3 - a_2) \mid P_1^{-1}| P_3|_{P_3} \qquad (5)$$

III. PROPOSED BACKWARD CONVERTER DESIGN

In this section the Mixed Radix Conversion (MRC) is applied to derive backward conversion algorithm for proposed moduli set $\{2^{2n+1}, 2^{2n}-1, 2^{2n}+1\}$ and adder-based hardware implementation of the conversion technique is presented.

Conversion Algorithm: For the proposed moduli set MRC theorem is employed to design efficient backward conversion algorithm. The following theorems and properties are needed for the derivation of conversion algorithm.

First we prove that the moduli set consists if pair-wise relatively prime moduli.

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

Proof: from the Euclidean theorem, we have gcd(α, β) = gcd(β,$|\alpha|_\beta$),therefore gcd$(2^{2n+1}, 2^{2n}-1)$ = gcd $(2^{2n+1}, |2^{2n}-1|_{2^{2n}+1})$ = 1.Similarly gcd$(2^{2n}-1, 2^{2n}+1)$ = gcd $(2^{2n}+1, |2^{2n}-1|_{2^{2n}+1})$ = 1 and gcd$(2^{2n+1}, 2^{2n}+1)$ = gcd $(2^{2n}+1, |2^{2n+1}|_{2^{2n}+1})$ = 1.Thus from these results it can be concluded that the moduli set contains relatively prime moduli and it is a valid RNS moduli set.

Theorem 2*:* For the given three moduli set$\{P_1,P_2,P_3\}$ = $\{2^{2n+1}, 2^{2n}-1, 2^{2n}+1\}$,the number X can be derived from its corresponding residues (x_1,x_2,x_3) by

$$X = x_1 + 2^{2n+1}|2^{2n-1}(x_2 - x_1)|_{2^{2n-1}} + (2^{2n}+1)(2^{2n}-1)\,Z_2 \quad (6)$$

Where $Z_2 = |((2^{2n}+1)(2^{2n}-1))^{-1}|_{2^{2n+1}}\,(x_3 - Z_1)|_{2^{2n+1}}$ (7)

and let us consider $Z_1 = x_1 + 2^{2n+1}|2^{2n-1}(x_2 - x_1)|_{2^{2n-1}}$ (8)

Proof: By substituting $P_1 = 2^{2n+1}, P_2 = 2^{2n}+1, P_3 = 2^{2n}-1$ from theorem 1 into Eq(2) we get Eq (6).

The following properties are required for the derivation of backward converter and used for further simplification to decrease hardware complexity. [9]

Property 1*:* Modulo $(2^p - 1)$ multiplication of a residue number by 2^k, where p and k are positive integers, is equivalent to k bit circular left shifting.

Property 2*:* A negative number in modulo $(2^p - 1)$ is equivalent to the one's compliment of the number, which is obtained by subtracting the number from $(2^p - 1)$.

Proposed moduli set

$$x_1 = x_{1,2n} \dots \dots \dots \dots \dots \dots . x_{1,0} \quad (9)$$

$$x_2 = x_{2,2n-1} \dots \dots \dots \dots \dots \dots . x_{2,0} \quad (10)$$

$$x_3 = x_{3,2n} \dots \dots \dots \dots \dots \dots . x_{3,0} \quad (11)$$

From Eq(6) we know that

$$X = x_1 + 2^{2n+1}|2^{2n-1}(x_2 - x_1)|_{2^{2n-1}} + (2^{2n}+1)(2^{2n}-1)\,Z_2$$

We simplify Eq(6) as follows

Let us consider moduli set $\{2^{2n}+1, 2^{2n}-1\}$ and $Z_1 = (x_1, x_2)$

Then using MRC algorithm for two moduli set $\{2^{2n}+1, 2^{2n}-1\}$

$$Z_1 = a_1 + a_2\,P_1$$

$$= x_1 + 2^{2n+1}|2^{2n-1}(x_2 - x_1)|_{2^{2n-1}} \quad (12)$$

Let us assume $H = |2^{2n-1}(x_2 - x_1)|_{2^{2n-1}}|$ and can be subdivided into V_1 and V_2

Then $V_1 = |2^{2n-1}\,x_2|\,2^{2n}\text{-}1 = |2^{2n-1}(x_{2,2n-1} \dots x_{2,0})|_{2^{2n-1}}$

$$= x_{2,0}\,\underbrace{x_{2,2n-1} \dots x_{2,1}}_{2n-1} \quad (13)$$

$$V_2 = |2^{2n-1}(-x_1)|_{2^{2n-1}}$$

It can be further simplified as $V_2' = |-2^{2n-1}(2^{2n})(0 \dots 0\,x_{1,2n}|_{2^{2n-1}}$

$$= |\text{-}2^{2n-1}(0 \dots 0\,x_{1,2n})|2^{2n-1} = x_{1,2n}\underbrace{1 \dots 1}_{2n-1} \quad (14)$$

$$V_2'' = |\text{-}2^{2n-1}(x_{1,2n-1} \dots x_{1,0})|_{2^{2n-1}}$$

$$= \bar{x}_{1,0}\underbrace{\bar{x}_{1,2n-1} \dots \dots . \bar{x}_{1,1}}_{2n-1} \quad (15)$$

$$Z_1 = x_1 + (2^{2n}+1)H = x_1 + 2^{2n}H + H$$

$$Z_1 = \underbrace{H_{2n-1} \dots H_0}_{2n}\,\underbrace{x_{1,2n} \dots x_{1,0}}_{2n} + H_{2n-1} \dots H_0 \quad (16)$$

Next consider composite Moduli Set $\{(2^{2n}+1)(2^{2n}-1), 2^{2n+1}\}$

Let x = (Z_1, x_3)

Using MRC

$$X = Z_1 + (2^{2n}+1)(2^{2n}-1)\,Z_2 \quad (17)$$

Where $Z_2 = |((2^{2n}+1)(2^{2n}-1))^{-1}|_{2^{2n+1}}\,(x_3 - Z_1)|_{2^{2n+1}}$

$$Z_2 = |(2^{2n+1}-1)\,((x_3 - Z_1)|_{2^{2n+1}}$$

$$= |\text{-}(x_3 - Z_1)|\,2^{2n+1}$$

$$= |\text{-}(x_3 - x_1 - (2^{2n}+1)H\,|\,2^{2n+1}$$

$$Z_2 = |-x_3 + x_1 + (2^{2n}+1)H\,|_{2^{2n+1}} \quad (18)$$

$$U_1 = |-x_3|_{2^{2n+1}} = \underbrace{\bar{x}_{3,2n}, \ldots \bar{x}_{3,0}}_{2n+1} + 1 \quad (19)$$

$$U_2 = |x_1|_{2^{2n+1}} = \underbrace{x_{1,2n} \ldots x_{1,0}}_{2n+1} \quad (20)$$

$$U_3 = |(2^{2n+1})H\,|_{2^{2n+1}} = |H_{2n-1} \ldots H_0\ H_{2n-1} \ldots H_0\,|_{2^{2n+1}} = \underbrace{H_0\ H_{2n-1} \ldots H_0}_{2n+1} \quad (21)$$

$$Z_2 = |U_1 + U_2 + U_3|_{(2^{2n+1})} \quad (22)$$

Then from Eq(10) we get the final equation as follows

$$X = Z_1 + (2^{4n}-1)Z_2 \quad (23)$$
$$= A+B$$

Where $A = Z_1 + 2^{4n}Z_2 = \underbrace{Z_{2,2n} \ldots . Z_{2,1} Z_{2,0}}_{2n+1} \underbrace{Z_{1,4n-1} \ldots Z_{1,1} Z_{1,0}}_{4n}$ (24)

$B = -Z_2 = \underbrace{1 \ldots 11}_{4n} \underbrace{\overline{Z}_{2,2n} \ldots . \overline{Z}_{2,1}\ \overline{Z}_{2,0}}_{2n+1}$ (25)

Hardware implementation:

The hardware structure of the proposed backward converter is shown in Fig.1 and for efficient design implementation it is on solely adders based i.e. CSAs with End Around Carry (EAC) and CPAs only. Implementation is based on equations Eq (06), Eq(16), Eq(22) and Eq(23).The operand preparation unit prepares the required operands in equations Eq(13),Eq(14),Eq(15),Eq(19) and Eq(20) by simple manipulation of the routing of the bits of residues. The computation of final equation Eq(23) requires addition of (2n+1) bits of B and A with the help of a (2n+1) Carry Propagate Adder .

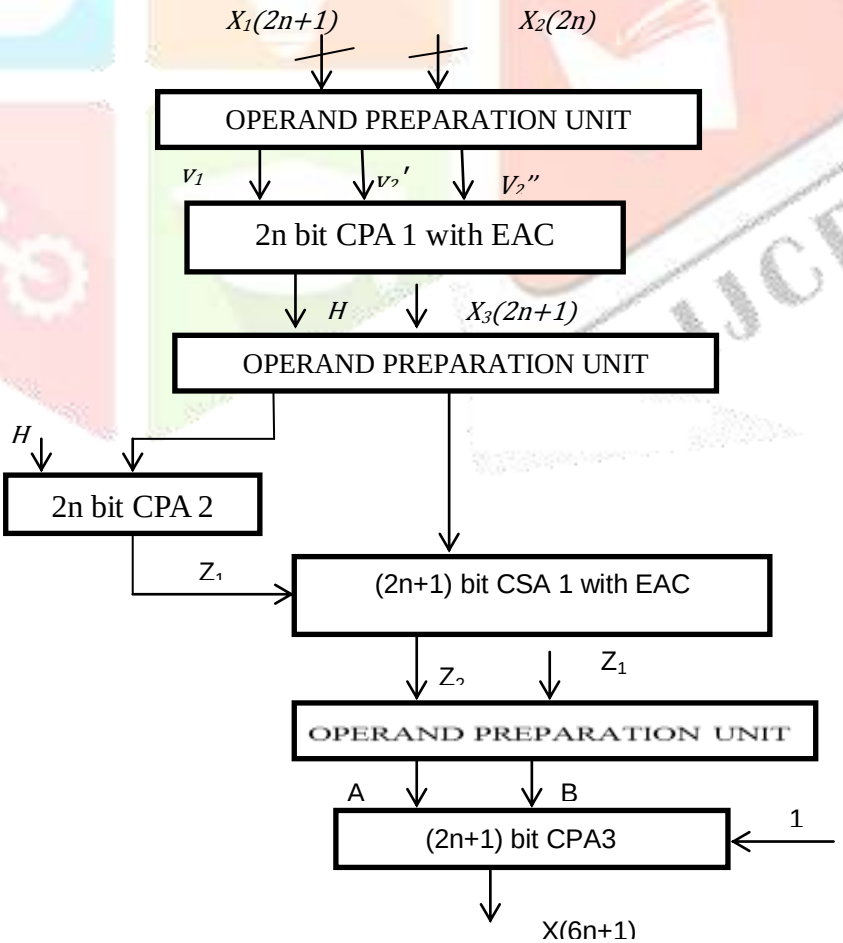

Figure 1: Proposed Backward Converter Architecture

IV. PERFORMANCE ANALYSIS

The performance of the proposed backward converter is evaluated theoretically in terms of conversion delay and area time complexity. The hardware utilization of the proposal is computed in terms of adders i.e. Full Adders (FAs) and Half Adders (HAs). The performance of the proposed converter is evaluated by comparing it with equivalent state of the art presented in [2], [4] and [6] in terms of hardware cost and conversion delay. The results of this comparison are presented in Table 1. It shows that the proposed converter performs faster than all the other existing converters.

Table 1: Table of Comparison

BACKWARD CONVERTERS	DYNAMIC RANGE BITS	DELAY	Time Complexity
[2]	6n	$(8n+1)t_{FA}+t_{NOT}$	$208\ n^2$
[4]	6n	$(11n+4)t_{FA}+t_{NOT}$	$187n^2$
[6]	6n	$(8n+3)t_{FA}+t_{NOT}$	$256n^2$
PROPOSED	6n	$(6n+3)t_{FA}+t_{NOT}$	$115n^2$

V. CONCLUSION

In this paper an effective MRC based backward converter architecture for the novel balanced moduli set $\{2^{2n}+1, 2^{2n}-1, 2^{2n+1}\}$ is presented. It has 6n-bit dynamic range and the design has been simplified by using purely adders i.e. CSAs and CPAs. The theoretical evaluation has suggested that it outperforms the best known similar state of the art equivalent converters in terms of delay metric.

REFERENCES

[1] S. J. Piestrak, "A high speed realization of a residue to binary converter," IEEE Trans. Circuits Syst. II, Analog. Digit. Signal Process., Vol. 42, No. 10, pp. 661–663, Oct. 1995.

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

[3] Bankas E.K.,Gbolagade K.A.,Cotofana S.D. "An effective New CRT based reverse converter for a novel moduli set$\{2^{2n+1}-1, 2^{2n+1}, 2^{2n}-1\}$" . IEEE Transactions on Application-Specific Systems, Architectures & Processors (ASAP) pp.142-146.June , 2013.

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

[5] Y.Wang, "Residue to binary converters based on new chinese remainder theorems", IEEETrans.Circuits Syst. II,Analog. Digit.Signal Process.,Vol.47,No.3,pp.197-205,Mar.2000.

[6] Ch.Divya"An Power Efficient RNS Backward converter for Novel Moduli Set", International Journal of computational Engineering & Management Vol. 17,Issue 6,November 2014.

[7] Keivan navi,Amir Sabbagh Molahosseini, Mohammad esmaeil doust. "How to teach residue number system to computer scientists and engineers",IEEE Trans.Education,Vol.54.No.1,Feb 2011.

[8] M.A.Soderstrand, W.K. Jenkins, G.A.Jullien, and F.J.Taylor, "Residue Number System Arithmetic: Modern Applications In Digital Signal Processing". Piscataway ,NJ:IEEE Press,1986.

[9] A.Omondi and B. Premkumar. Residue Number Systems: Theory and Implementation, Imperial College Press, London, 2007.

[10] Fred J. Taylor, "Residue Arithmetic: A Tutorial with Examples", IEEE Trans. on Computer, pp. 50~62, May 1984.