ISSN: 2395-1680 (ONLINE)
DOI: 10.21917/ijme.2016.0044

IMPROVING SYSTEM PERFORMANCE BY USING PREFIX ADDERS IN RNS

M. Augusta Angel[1] and A. Narendra Kumar[2]
Department of Electronics and Communication Engineering, V V College of Engineering, India
E-mail: [1]augusangel@gmail.com, [2]nandhume@gmail.com

Abstract

Over the past few decades, the intense growth of portable communication devices has led to stringent need of efficient system performance. The system performance is upgraded by reducing the computation time using the Residue Number System. Since, it performs the complex computation efficiently. In this paper, the modified prefix adders are proposed to perform the fast modulo computations and make use of the available resources. The projected modulo adders computes the complex modulo operations in reverse conversion process of RNS independently and in parallel without carry propagation. This results in better performance than the other typical adder components in terms of area and delay.

Keywords:

Residue Number System, Reverse Converter, Prefix Adders, Computations

1. INTRODUCTION

Today the embedded systems are transformed from simple single function control systems to complex multipurpose computing platforms. The battery-powered devices require cheap, high performance and power efficient embedded processors. Hence there is a space to develop a system that performs computations fast and make use of the power and energy efficiently. In most arithmetic systems, the speed is limited by the nature of the building block that makes logic decisions. Carry independent arithmetic called the Residue arithmetic representation is a way of approaching a famous bound on the speed at which addition and multiplication can be performed.

Portable and battery based devices widely makes use of the Residue Number System (RNS) because of its low power features and reduced delay compared to other computation system. The major issues in designing an efficient RNS are moduli set selection, Forward conversion, Residue arithmetic unit and Reverse conversion. While compared to other parts of RNS, the reverse converter has complex structures. The selection of moduli sets and conversion techniques plays vital role in reverse conversion performance.

In this paper, the proposed component is implemented in $\{2^n -1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ moduli sets of reverse converter design and the performances are compared for $n = 4$, in terms of area and delay with other existing adder structures.

2. RELATED WORKS

The conversion of residue number to binary number in RNS reverse converter presents a significantly higher hurdle that offsets the performance gained in the RNS. The reverse conversion algorithms are based primarily on the Chinese remainder theorem or mixed-radix conversion [1] [6] [7]. Generally, the Chinese remainder theorem CRT uses a large modulo M adder, where M is the product of all moduli, whereas MRC is a series of sequential step that usually requires a number of lookup tables [3]. Practically, both the methods are inefficient in case of system with large dynamic range. Another problem in reverse converter design is moduli set selection. Moduli sets are carefully selected to reduce the hardware complexity in the implementation of reverse converters. In [12] Wang proposed a new and uniform algorithm, designed using the New Chinese Remainder Theorems for the RNS to binary conversion. The 2n-bit adder-based converter is faster and requires very less hardware when compared to its previous methods [11]. A.S. Molahosseini et al. [6] presented a simple residue-to-binary conversion algorithm based on the New Chinese Remainder Theorem (NCRT) for new 4-moduli set $\{2^n - 1, 2^n, 2^n + 1, 2^{2n} + 1\}$. The new reverse converter completely gets rid of the need for modulo multiplication and allows further optimization opportunity in a simple MOMA realization [2]. They are more efficient than the reverse converter for the 3-moduli set $\{2^n - 1, 2^n, 2^n + 1\}$, for applications requiring a large dynamic range and high parallelism. These moduli sets consist of simple moduli which can lead to efficient implementation of the reverse converter.

L. Sousa and S. Antao [10], modified the moduli set $\{2^n + 1, 2^n - 1, 2^n, 2^{2n+1} - 1\}$ with $5n$ bits dynamic ranges to $\{2^n + 1, 2^n - 1, 2^{2n}, 2^{2n+1} - 1\}$ with $6n$ bits dynamic range. They have proposed a method for designing reverse converters to apply the mixed-radix (MR) conversion (MRC) successively to moduli subsets with two elements, to unify the design of reverse converters for the four moduli sets and to achieve efficient converters for large dynamic range.

In all these proposed system there arise a problem of double zero representation when the 2^n-1 modulo addition in these moduli sets are implemented using typical carry adders. In general, modulo 2^n-1 addition is performed using a carry propagate adder (CPA) with end-around-carry (EAC) [12], which produces a double representation of zero, that is, both the positive zero representation {00,...,0} and the negative zero representation {11,...,1} are produced. The single representation of zero is not necessarily required during the intermediate stages of RNS computation. It also adds a complexity to the design. During computation, if the all 1s representation of zero has an unexpected rise, that leads to additional unwanted signals; it results in high power dissipation

Some modulo 2^n-1 adder in residue to binary converters require single zero representation for efficient moduli sets Hence, investigations leading to optimized single-zero representing modulo 2^n-1 adder are required for the optimized implementation of DSP and communications systems using RNS. New algorithms for modulo 2^n-1 addition with single zero representation has been presented in [8].

The algorithms and the corresponding architectures have been derived by assuming carry input is one in the first stage of the addition. The recursive effect of generating and propagating signals at each prefix level is the main reason for the high power consumption and area overhead of these adders. An optimized approach proposed by [8] uses an extra prefix level to add the output carries. However, this method suffers from high fan-out; hence it is used only for trivial width operands. However, by using a binary-to-excess-one converter (BEC) [9] we could eliminate the additional prefix level as well as the BEC can be modified to fix the double-representation of zero issue [14].

The organization of the paper is as follows. In the next section, the design methodology and the RNS structure are explained. In section 3, we introduce the modified parallel prefix adder based RNS reverse converter and its functionality. The Problem of Zero representation is also addressed. In section 4, the performance of proposed adder structure is analyzed with the existing typical carry adders. The section 5 concludes the paper.

3. DESIGN METHODOLOGY

This section briefly describes the proposed adder components such as Parallel prefix adder with modified incrementer structure. The RNS reverse conversion formulations based on the Chinese remainder theorem or other improved techniques and approaches are computed directly using well known adder architectures such as Carry Save Adder (CSAs) and Ripple Carry Architectures (RCA). But this has led to significant reduction in speed due to the linear increase of delay with the number of bits.

3.1 RESIDUE NUMBER SYSTEM

To overcome the problem of computational complexity the Residue Number System (RNS) divides a large integer into a set of small integers and performs computation as a series of smaller calculations. A Residue Number System (RNS) is defined by a set of relatively prime moduli set $\{k_1, k_2,...,k_m\}$, where gcd $(k_i, k_j) = 1$ for $i \neq j$. A weighted binary number X can be represented as $X = (x_1, x_2\ldots x_n)$, where x_i is given by equation,

$$x_i = X \bmod k_i = |X|_{k_i}\ 0 \leq x_i < k_i$$

Such a representation is unique for any integer X in the range $[0, K\text{-}1]$, where K is the dynamic range of the moduli set $\{k_1, k_2, k_m\}$, which is equal to the product of k_i $(K = k_1, k_{2,}\ k_m)$ [4].

A typical RNS system has three units. They are,

1. Binary to residue conversion unit
2. Residue modulo arithmetic units
3. Residue to binary conversion unit

The block diagram of RNS system is shown in Fig.1. In which the forward converter converts the weighted binary operands into residue representations. The residue arithmetic unit consists of modulo k_i circuits to perform arithmetic computations like addition, subtraction, and multiplication on residue numbers in parallel without any carry signal propagation between the residue digits. Next, the reverse converter converts the resultant residue number into corresponding weighted binary number.

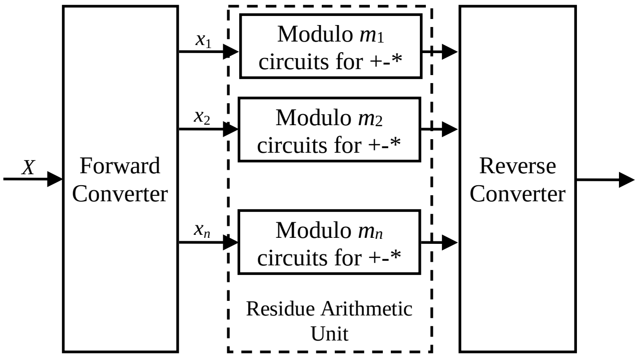
X
Forward Converter
x_1
x_2
x_n
Modulo m_1 circuits for +-*
Modulo m_2 circuits for +-*
Modulo m_n circuits for +-*
Residue Arithmetic Unit
Reverse Converter

Fig.1. Block diagram of RNS

4. PROPOSED ADDER COMPONENTS

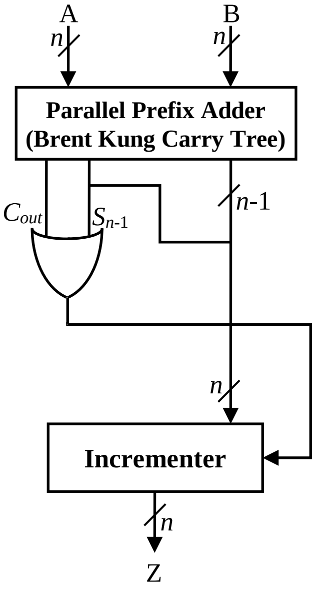

Fig.2. Proposed Adder Component

This section describes a new adder component which is then employed in reverse converter design for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ to determine the required performance. The proposed adder component is shown in Fig.2. The figure shows that the proposed adder component consists of parallel prefix adder, OR gate and an incrementer in order to eliminate the problem of double zero representation. For the OR gate the MSB bit of sum output and the carry output of the parallel prefix structure are given as input. The incrementer produces the n-bit length output based on the OR gate output signals.

The parallel prefix adder block of proposed adder component, depicted in the Fig.3 has three blocks. The square represents the preprocessing stage of the parallel prefix structure that consists of n half adders to produce two signals such as propagate and generate signals.

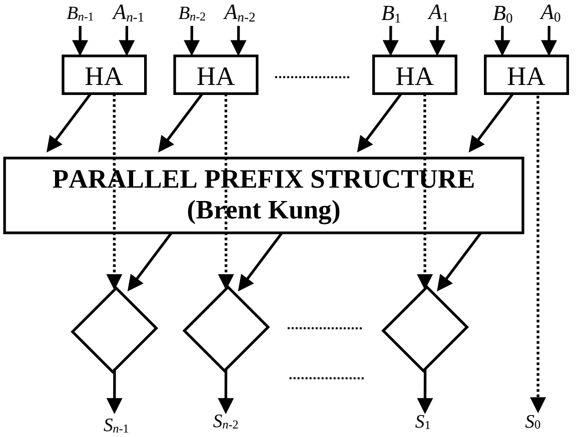

Fig.3. Parallel prefix adder

The Brent Kung parallel prefix carry structure is used as the carry tree to calculate the carry signal parallel, since it provides minimum fan out and delay. When compared to other parallel prefix structures, the Brent-Kung adder has minimum number of nodes, which results in reduced area [13]. The diamond block represents the post processing stage which produces the sum output. The input signals are EX-ORed to produce the sum output. The incrementer structure in the proposed adder component is used to overcome the problem of double zero representation in reverse converters.

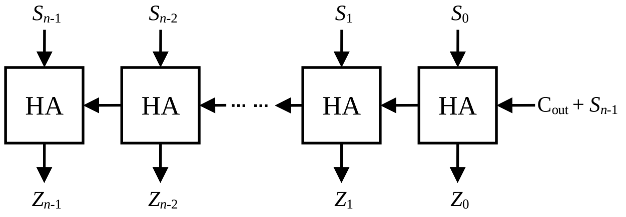

Fig.4. Incrementer

In most of the existing moduli sets of reverse converters modulo 2^n-1 is a fundamental operation. The typical Carry Propagate Adders are used to perform these addition operations. But it results in a problem of double representation of zero which is not desirable in reverse converters. To overcome this problem the proposed adder component is designed with an incrementer.

The carry propagate increment stage of proposed adder is depicted in Fig.4. It consists of '*n*' number of half adders. It increments the sum output of the prefix adders based on the control signal. The control signals are generated by using the carry out (C_{out}) and sum output signal (S_{n-1}) is produced by the parallel prefix adder. The incrementer takes the sum output of the parallel prefix adder as input. Based on the control signals the sum result is conditionally incremented so as to ensure the single zero representation.

5. RESULTS AND DISCUSSIONS

The proposed adder is enrolled in the reverse converters for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ [5]. The proposed parallel prefix structure is designed with incrementer structure for desired performance.

The performance of the proposed adder component is compared with other typical adder components, which are also employed in the reverse converters for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ [5]. The obtained result is compared in terms of area and delay. It also includes the hardware complexity of these adder components.

Table.1. Comparison Results

Converter structure		Area		Delay (ns)
		Number of slice LUTs	Number of bonded IOBs	
Proposed		149	66	13.147
HMPE-BK		88	66	17.891
RCA- based adders		150	66	25.664
Fully prefix adders	Brent Kung	154	66	23.361
	Ladner-Fischer	156	66	25.615

The Table.1 summarizes the performance of adders in terms of area and delay when it is employed in reverse converter design for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$.

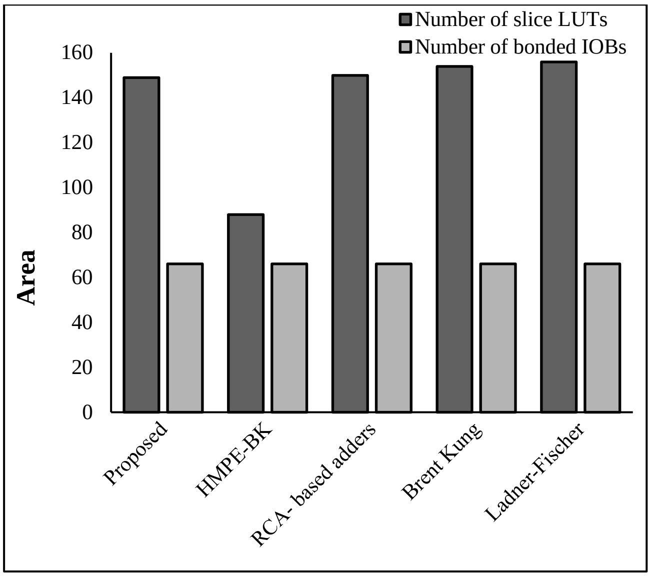

Fig.5. Graphical representation of the result obtained in terms of area for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$

From the table it is clear that the proposed component provides fast arithmetic modulo operation when compared to other adder based reverse converter design. But it uses more area when compared than HMPE structure, However it is efficient than all other adder based designs. The graphical representation of the result obtained in terms of area for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ proposed in [5] is shown in Fig.5.

The Table.2 summarizes the hardware components required by the adders when implemented in the reverse converter design for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ proposed in [5].

Table.2. Hardware Requirements

Converter structure		Adders/ Subtractor	Multiplexers	XORs
Proposed		3	3	127
HMPE-BK		3	3	129
RCA based adders		4	4	132
Fully prefix adders	Brent Kung	3	3	113
	Ladner-Fischer	4	4	113

The proposed component requires second less amount of hardware components when compared to other existing adder components when employed in RNS reverse converter design for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ [5] for the n value 4. The graphical representation of the obtained result in terms of delay for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ proposed in [5] is shown in Fig.6.

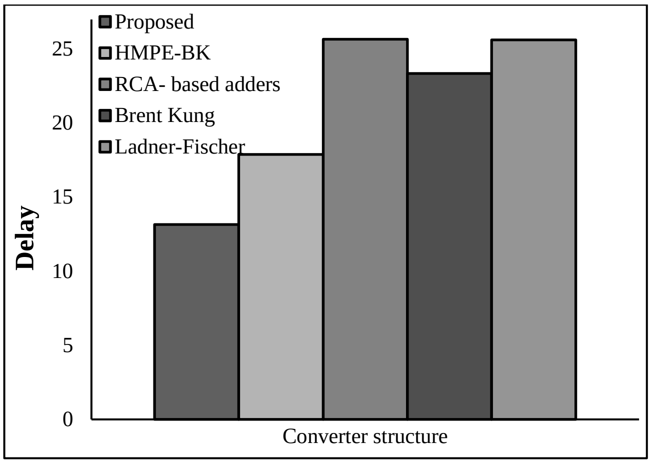

Fig.6. Graphical representation of delay comparison for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ $n = 4$

6. CONCLUSION

The RNS has wide applications, since it provides advantageous high speed and low power implementation. To increase its performance further, the computation should be done as faster as possible. In such a way, the proposed RNS modulo adders employed in reverse converter architectures provided better performance than other adder components when employed in reverse converse design for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$. In future, for secure image processing, the RNS image coding can be used since, it provides high speed and low power implementation. In addition to this, RNS is also used in computer arithmetic and cryptography.

REFERENCES

[1] M. Augusta Angel and M.M. Vijay, "High Speed RNS-To-Binary Converter Design using Parallel Prefix Adders", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3, No. 1, pp. 138-143, 2015.

[2] J.C. Bajard, L.S. Didier and P. Kornerup, "An RNS Montgomery Modular Multiplication Algorithm", *IEEE Transactions on Computers*, Vol. 47, No. 7, pp. 766-776, 1998.

[3] 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 Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 50, No. 10, pp. 1296-1303, 2003.

[4] A.A. Hiasat, "VLSI Implementation of New Arithmetic Residue to Binary Decoders", *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 13, No. 1, pp.153-158, 2005.

[5] A.S. Molahosseini, K. Navy, C. Dadkhah, O. Kavehei and S. Timarchi, "Efficient Reverse Converter Designs for the New 4-Moduli Sets $\{2^{n-1}, 2^n, 2^{n+1}, 2^{2n+1}-1\}$ and $\{2^{n-1}, 2^{n+1}, 2^{2n}, 2^{2n+1}\}$ based on New CRTs", *IEEE Transactions on Circuits and Systems Part I: Regular Papers*, Vol. 57, No. 4, pp. 823-835, 2010.

[6] K. Navi, A.S. Molahosseini and M. Esmaeildoust, "How to Teach Residue Number System to Computer Scientists and Engineers", *IEEE Transactions on Education*, Vol. 54, No. 1, pp. 156-163, 2011.

[7] Amos Omondi and Benjamin Premkumar, "*Residue Number Systems: Theory and Implementation*", Imperial College Press, 2007.

[8] R.A. Patel, M. Benaissa and S. Boussakta, "Fast Parallel-Prefix Architectures for Modulo 2^{n-1} Addition with a Single Representation of Zero", *IEEE Transactions on Computers*, Vol. 56, No. 11, pp. 1484-1492, 2007.

[9] B. Ramkumar and H.M. Kittur, "Low Power and Area Efficient Carry Select Adder", *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 20, No. 2, pp. 371-375, 2012.

[10] L. Sousa and S. 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 Part II: Regular Papers*, Vol. 59, No. 4, pp. 244-248, 2012, 2012.

[11] Wei Wang, M.N.S. Swami and M.O. Ahmad, "Moduli Selection in RNS for Efficient VLSI Implementation", *Proceedings of International Symposium on Circuits and Systems*, Vol. 4, pp. 512-515, 2003.

[12] Yuke Wang, Xiaoyu Song, Mostapha Aboulhamid and Hong Shen, "Adder based Residue to Binary Numbers Converters for $(2^{n-1}, 2^n, 2^{n+1})$", *IEEE Transactions on Signal Processing*, Vol. 50, No. 7, pp. 1772-1779, 2002.

[13] Nurdiani Zamhari, Peter Voon, Kuryati Kipli, Kho Lee Chin and Maimun Huja Husin, "Comparison of Parallel Prefix Adder (PPA)", *Proceedings of the World Congress on Engineering*, Vol. 2, pp. 1-3, 2012.

[14] A.A.E. Zarandi, A.S. Molahosseini, M. Hosseinzadeh, S. Sorouri, S. Anto and L. Sousa, "Reverse Converter Design via Parallel-Prefix Adders: Novel Components, Methodology, and Implementations", *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 23, No. 2, pp. 374-378, 2014.