ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

IMPROVING SYSTEM PERFORMANCE BY USING PREFIX ADDERS IN RNS

M.Augusta Angel[1], **A. Narendrakumar**[2]

Assistant Professor, Department of ECE, VVCOE, Tisaiyanvilai, India[1]

Professor, Department of ECE, VVCOE, Tisaiyanvilai, India[2]

ABSTRACT: over the past few decades, the intense growth of portable communication devices leads to stringent need of efficient system performance. The system performance is upgraded by reducing the computation time. The Residue Number System performs the computations fast and makes use of the power and energy 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 (RNS), Reverse converter, prefix adders, computations.

I. 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. The Residue Number System (RNS) plays a very important role in the world of portable and battery based devices, because of its low power features and delay.

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 are 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.

II. DESIGN METHODOLOGY

This section briefly describes about the proposed adder components such as Parallel prefix adder with modified incremented 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 leads to significant reduction in speed due to the linear increase of delay with the number of bits.

2.1. Residue Number System:

A System which decomposes a large integer and represents it as a set of small integers is called Residue Number System (RNS). The computations are performed as a series of smaller calculations. A Residue Number System (RNS) is defined by a set of relatively prime moduli set $\{k_1, k_2 \cdots k_m\}$, where gcd $(k_i, k_j) = 1$ for $i \neq j$. A weighted binary number X can be represented as $X = (x_1, x_2 \cdots x_n)$, where is given by equation,

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

DOI:10.15662/IJAREEIE.2015.0501001

Such a representation is unique for any integer X in the range [0, K – 1], where K is the dynamic range of the moduli set *{k_1, k_2,…, k_m}*, which is equal to the product of ki *(K = k_1, k_2,…, k_m)* [7].

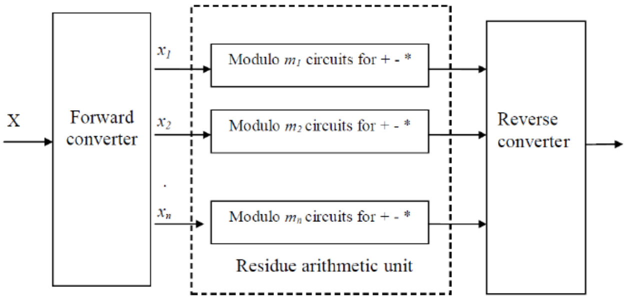

X
Forward converter
x_1
x_2
x_n
Modulo m_1 circuits for + - *
Modulo m_2 circuits for + - *
Modulo m_n circuits for + - *
Residue arithmetic unit
Reverse converter

Figure 1: Block diagram of RNS.

A typical RNS system consists of a forward converter, modulo arithmetic units and a reverse converter. Figure1 shows the block diagram of RNS system. 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 resulted residue number into corresponding weighted binary number.

III. PROPOSED ADDER COMPONENTS

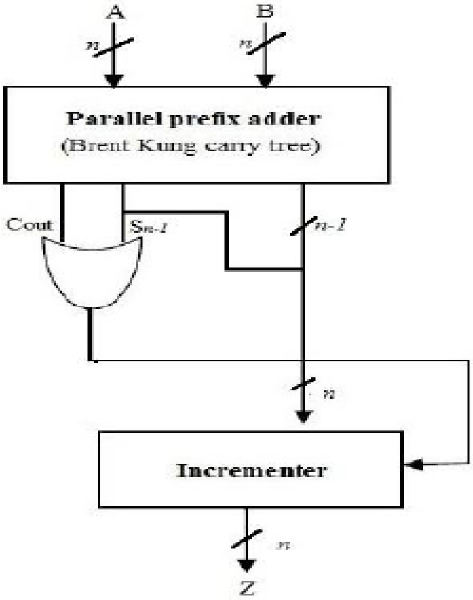


Figure 2: Proposed adder component.

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 figure 2. The figure shows that the proposed adder component consists of parallel prefix adder, OR gate and an incremented 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 incremented produces the n-bit length output based on the OR gate output signals.

The parallel prefix adder block of proposed adder component depicts in the figure3 has three blocks. The square represents the pre-processing stage of the parallel prefix structure that consists of n half adders to produce two signals such as propagate and generate signals.

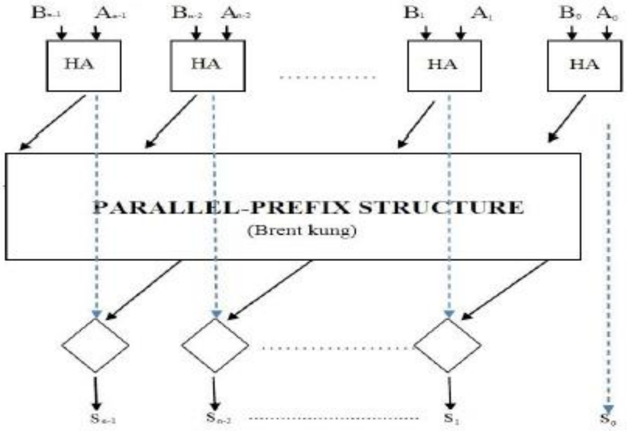


Figure 3: Parallel prefix adder.

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. The diamond block represents the post processing stage which produces the sum output. The input signals are EX-O Red to produce the sum output. The incremented structure in the proposed adder component is used to overcome the problem of double zero representation in reverse converters.

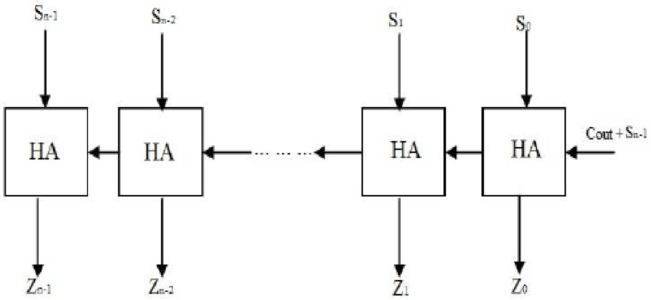


Figure 4: Incremented.

In most of the existing moduli sets of reverse converters modulo $2n - 1$ 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 incremented.

The carry propagate increment stage of proposed adder is depicted in Figure 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 (Cout) and sum output signal (Sn-1) produced by the parallel prefix adder. The incremented 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.

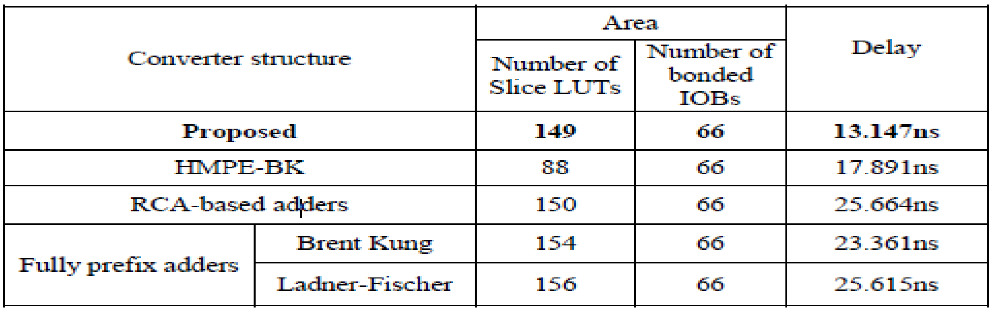
Furthermore, the coordination packet is assumed to be small enough to be transmitted within slot duration. Instead of a common control channel, FHS provides a diversity to be able to find a vacant channel that can be used to transmit and receive the coordination packet. If a hop of FHS, i.e., a channel, is used by the primary system, the other hops of FHS can be tried to be used to coordinate. This can allow the nodes to use K channels to coordinate with each other rather than a single control channel. Whenever any two nodes are within their communication radius, they are assumed to meet with each other and they are called as contacted. In order to announce its existence, each node periodically broadcasts a beacon message to its contacts using FHS. Whenever a hop of FHS, i.e., a channel, is vacant, each node is assumed to receive the beacon messages from their contacts that are transiently in its communication radius.

IV. RESULTS AND DISCUSSIONS

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

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

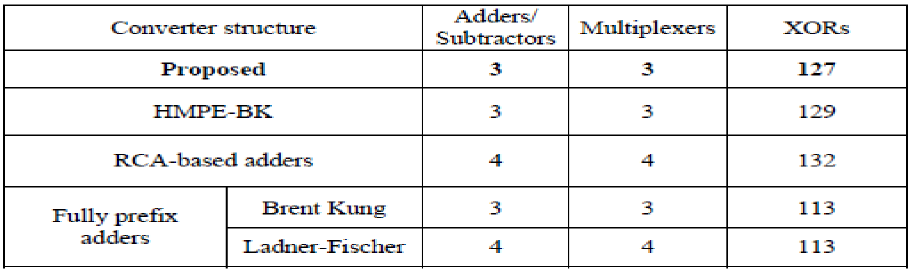
Table 1: Comparison results for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ n=4.



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

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

Table 2: Hardware requirement for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$ n=4.



Converter structure		Adders/ Subtractors	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

Table II summaries the hardware components required by these adders to implement the reverse converter design for the moduli set $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$. 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 $\{2^n - 1, 2^{2n}, 2^n + 1, 2^{2n} + 1\}$for the n value 4.

VI.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] Ananda PV, Premkumar AB, RNS-to-Binary Converters for Two Four-Moduli Sets $2^n + 1$, 2^n-1, 2^n, 2^n+1+1 and $2^n + 1$, 2^n-1, 2^n, 2^n+1 + 1', IEEE Trans. Circuits Syst. I Reg. Papers 2007; 54: 6.

[2] Augusta Angel M, Vijay MM, High Speed RNS-To-Binary Converter Design Using Parallel Prefix Adders. IJIRCCE 2015; 3.

[3] Bajard JC, Didier LS, et al. An RNS montgomery modular multiplication algorithm. IEEE Trans Comput 1998; 47: 766-776.

[4] Bayoumi MA, Jullien GA, and WC. Miller W. C., (1987), 'A VLSI implementation of residue adder', IEEE Trans. Circuits Syst, vol. CAS-34, no. 3, pp. 284-288.

[5] Cao B, Chang CH et al. 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 Fundam. Theory Appl 2003; 50: 1296-1303.

[6] Cao B, Chang CH, et al. (2007), 'A residue-to-binary converter for a new five moduli set', IEEE Trans. Circuits Syst. I, Reg. Papers, 2007; 54: 1041 -1049.

[7] Hiasat AA, VLSI implementation of new arithmetic residue to binary decoders, IEEE Trans. Very Large Scale Integr. (VLSI) Syst, 2005; vol. 13: 153 -158.

[8] Kogge PM, Stone HS, A parallel algorithm for the efficient solution of a general class of recurrence equations. IEEE Trans. Comput., 1973; 22: 783-791.

[9] Molahosseini AS, Navy K, et al. '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 Trans. Circuits Syst. I, Reg. Papers, 2010; 57: 823-835.

[10] Molahosseini AS, Dadkhah C, A new five moduli set for efficient hardware implementation of the reverse converter. IEICE Electron. Exp, 2009; 6: 1006 -1012.

[11] Montgomery PL, Modular multiplication without trial division. Math Comput. 1985; 44: 519-521.

[12] Navi K., Molahosseini AS, et al. How to teach residue number system to computer scientists and engineers. IEEE Trans. Educ 2011; 54: 156-163.

[13] Omondi A, Premkumar B, Residue Number Systems: Theory and Implementations, London, U.K.: Imperial College Press 2007.

[14] Patel RA, Benaissa M, et al. Fast parallel-prefix architectures for modulo 2n1 addition with a single representation of zero', IEEE Trans. Comput. 2007; 56: 1484-1492.

[15] Ramkumar B, Kittur HM, Low power and area efficient carry select adder. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 2012; 20: 371-375.

[16] Sousa L, Antao S, 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 Trans. Circuits Syst. II, 2012; 59: 244-248.

[17] Stine JE, Digital computer arithmetic data path design using Verilog HDL. Kluwer Academic Publishers 2004.

[18] Wang W, Swami MNS et al. (2003) Moduli selection in RNS for efficient VLSI implementation. Proc. IEEE Int. Sump. Circuits Syst 2003; 4: 512-515.

[19] Wang Y, Song X, et al. Adder based residue to binary numbers converters for (2^n 1, 2^n, $2^n + 1$), IEEE Trans. Signal Process 2002; 50: 1772-1779.

[20] Zamhari N, Voon P, et al. Comparison of Parallel Prefix Adder (PPA), Proceedings of the World Congress on Engineering 2012, II WCE 2012, London, UK.

[21] Zarandi AAE, Molahosseini AS, et al. Reverse Converter Design via Parallel-Prefix Adders: Novel Components, Methodology, and Implementations. in IEEE Trans. on VLSI SYSTEMS.