HDL Implementation of Five Moduli Residue Number System

Tukur Gupta, Shamim Akhter, Anandita Srivastava, Saurabh Chaturvedi

Abstract*: The demand for residue number system (RNS) is increasing day by day because of its high speed and fault tolerant characteristics. RNS encodes a large number into group of small numbers, which consequently increases the overall data processing rate. This paper presents an analysis of the forward converter designed using ripple carry adder (RCA), carry save adder (CSA), and half adder-like (HAL), for the figure of merits area, delay, and power for five moduli set: 2^n-1, 2^n, 2^n+1, 2^{n+1}-1, and 2^{n-1}-1 with the standard cells at 90 nm technology. The designing of different blocks has been done in Verilog-HDL. The area, delay, and power of the implemented circuits are obtained using the Synopsys Design Compiler at 90 nm technology node, while VCS is used for verification. It is observed that the area of the architecture using CSA is less, whereas power utilization and timing behavior are better in HAL.

***Index Terms*: Carry save Adder (CSA), forward converter, modular addition, modular multiplication, residue number system (RNS),**

I. INTRODUCTION

Residue number system (RNS) has achieved certain popularity especially in digital signal processing because of its carry free and fault tolerant behavior [1], [2]. In RNS domain, the representation of an integer number is done as a set of small binary numbers, known as residues. The residues are processed separately, therefore the faults in one block cannot affect the other blocks of the circuit. The present paper has analyzed different architectures of forward converter using three binary adders, including ripple carry adder (RCA), carry save adder (CSA) and half adder-like (HAL) adder for the set of five moduli: 2^N-1, 2^N, 2^N+1, 2^{N+1}-1, and 2^{N-1}-1 proposed in [3]. The rest of this paper is arranged as follows: Section II discusses the overview of RNS. Section III presents the forward converter design for set of five moduli. Section IV describes the simulation and synthesis results, and Section V concludes the paper.

II. OVERVIEW OF RNS

RNS is used to simplify the mathematical operations [1]. In RNS, suppose a co-prime moduli set is represented as {m1, m2, m3, … mn} and an integer X is represented as a set of residues with respect to the moduli as {x1, x2, x3, … xn}.

$$x_i = (X \bmod m_i), \text{ if } X>0$$

$$= (M-|X|) \bmod m_i, \text{ otherwise,}$$

where M, the multiplication of all moduli, is known as the dynamic range. Moduli sets are classified into two categories: arbitrary and special. The lookup tables (LUTs) and combinational logic circuits are used in the implementation of the converters based on arbitrary moduli set [1], [2], whereas the implementation of the converters based on special moduli set does not necessarily need LUTs. The converters based on special moduli set require less hardware, and they exhibits small delays. However, the complexity of the hardware is dependent on the selected type of moduli set.In general, the signals which are in binary or in analog form need techniques for the conversion in RNS representation for data processing. The technique by which the binary numbers are converted in RNS form is known as forward conversion. The efficient forward converter is that in which area, power, and delay are optimized.

III. FORWARD CONVERTER DESIGN FOR FIVE MODULI SET

Section III presents the special moduli set proposed in [3]. The first three moduli in this set are basic special three moduli 2^N-1, 2^N, and 2^N+1, and other two are the extension of moduli 2^N-1 form. This is a balanced moduli set with large dynamic range of 5^N-1.

Let $m_1 = 2^N-1$, $m_2 = 2^N$, $m_3 = 2^N+1$, $m_4 = 2^{N-1}-1$, and $m_5 = 2^{N+1}-1$.

The computation of the residues r_1, r_2, r_3, r_4, and r_5 for a number X with all five moduli is given as [3]:

$$r_2 \text{ w.r.t. } 2^N = B_3 \quad (1)$$

$$r_1 \text{ w.r.t. } 2^N-1 = |B_1 + B_2 + B_3|_{2^N-1} \quad (2)$$

$$r_3 \text{ w.r.t. } 2^N+1 = |B_1 - B_2 + B_3|_{2^N+1} \quad (3)$$

For above computation, X is divided into N-bits each to represent X as $B_1B_2B_3$, with B_1 formed by the MSB's N-bit followed by B_2 and then B_3 formed by LSB's N-bit. For computing the residue for 2^{N-1}-1, the number X is divided into N-1 bits to form X as $B_1B_2B_3B_4$ with B_1 formed by the MSB's N-1 bits followed by B_2, B_3, and then B_4 formed by LSB's N-1 bits.

$$r_4 \text{ w.r.t. } 2^{N-1}-1 = |B_1 + B_2 + B_3 + B_4|_{2^{N-1}-1} \quad (4)$$

Similarly, for computing the residue for 2^{N+1}–1, X is divided into N+1 bits to form X as $B_1B_2B_3B_4$ with B_1 formed by the MSB's N+1 bits followed by B_2, B_3, and then B_4 formed by LSB's N+1 bits.

Revised Manuscript Received on July 05, 2019.

Tukur Gupta, Ph.D. Scholar, Deptt. of ECE, Jaypee Institute of Information Technology, NOIDA, India

Shamim Akhter, Assistant Professor, Deptt. of ECE, Jaypee Institute of Information Technology, NOIDA, India

Anandita Srivastava, M.Tech. (ECE), Jaypee Institute of Information Technology, NOIDA, India

Saurabh Chaturvedi, Assistant Professor, Deptt. of ECE, Jaypee Institute of Information Technology, NOIDA, India

r_5 w.r.t. 2^{N+1}-1 = $|B_1 + B_2 + B_3 + B_4|_{2^{N+1}-1}$ (5)

On the basis of (1) to (5), the schematic of the five moduli set is illustrated in Fig. 1.

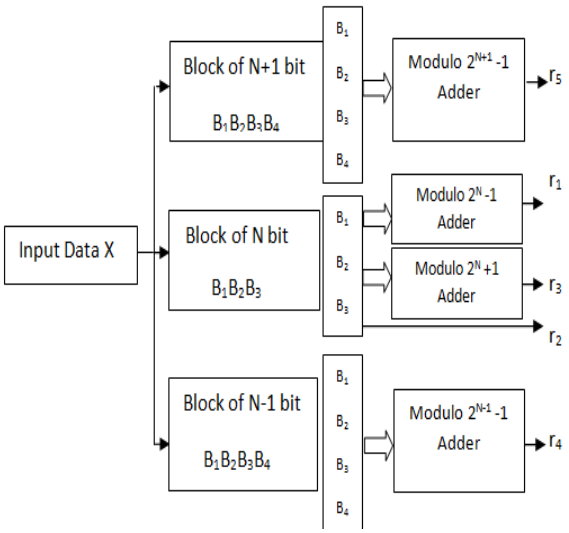


Fig. 1. Schematic of forward converter based on five moduli.

Modulo adder is used as a basic building block in the design of a forward converter. Various architectures of the modulo adders are proposed in literature [1]-[5].

Fig. 2 depicts the basic structure of a modulo adder, which is designed using the RCAs [1]. The circuit can be used by replacing m by different moduli. As shown in (3), there is a requirement of a modulo subtractor for 2^N+1 moduli.

Fig. 3 demonstrates the schematic diagram of a modulo adder using CSA [6]-[8] for simultaneously adding three operands.

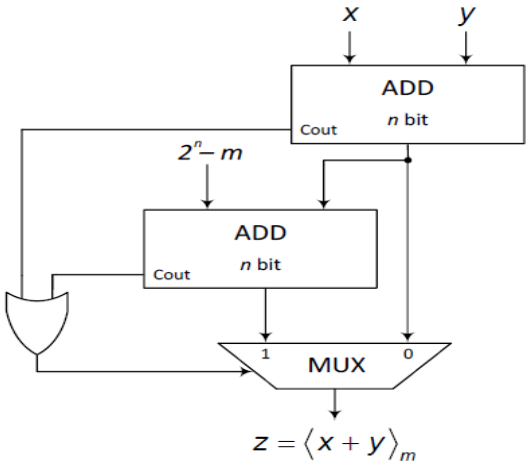


Fig. 2. General structure of a modulo adder [1].

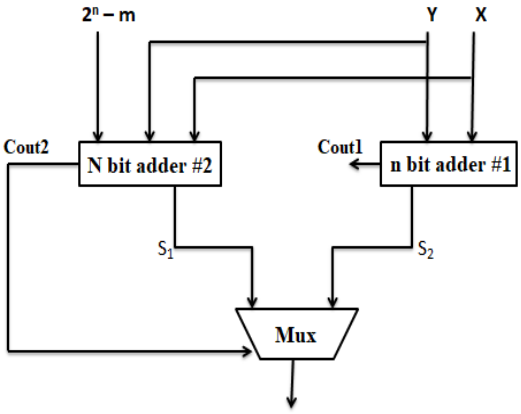


Fig. 3. Modulo adder using CSA.

Based on area, power, and delay parameters, the comparative performance analysis of different modulo adders of Fig.1 is done using the adders like RCA, CSA, and HAL adder. A HAL cell is a mixture of CSA and carry look-ahead adder [4], [5].

IV. SIMULATION AND SYNTHESIS RESULTS

The implementation of five moduli set is done using Verilog-HDL for N=4, i.e. five moduli set: 15, 16, 17, 31, and 7.The simulation waveform is shown Fig. 4. For each clock cycle, the input data is converted into residues. For the first input data 1127, the residues are 2, 7, 5, 11, and 0. The complete block diagram generated after synthesis is shown in Fig. 5 for the design using RCA. Fig. 6 shows the CSA-based mod-15 calculator unit.

The choice of the moduli is very important in RNS because it decides the efficiency of the forward converters. The performance analysis in terms of area, power, and delay is done using the 90 nm standard cells in Synopsys Design Compiler for different moduli set individually and jointly and presented in Table I and II, respectively.

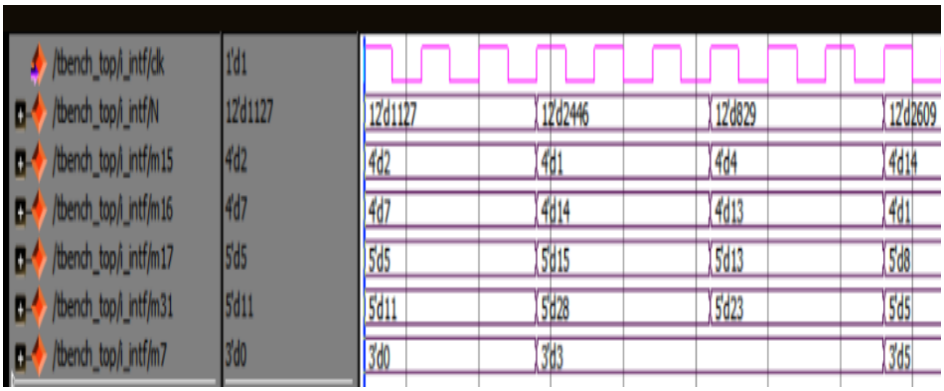
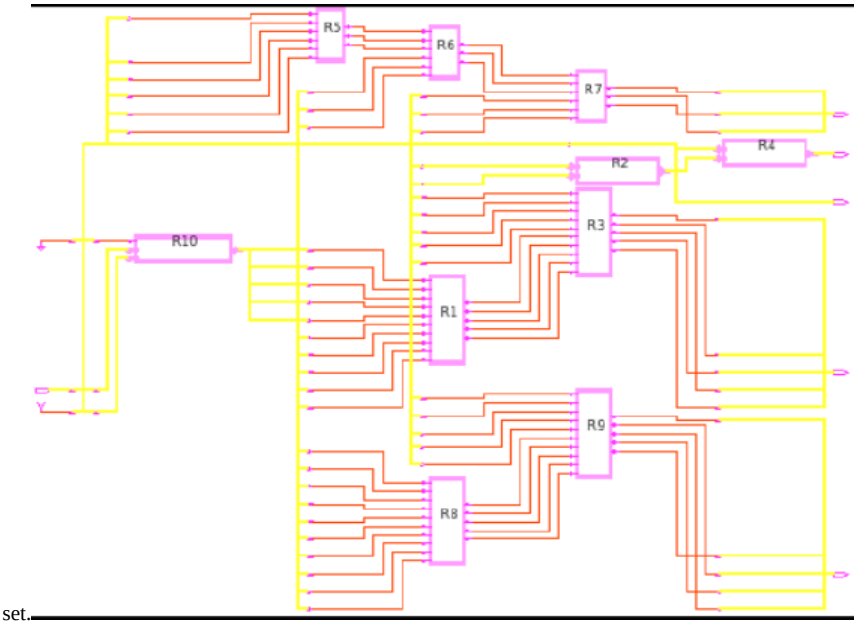


Fig. 4. Simulation waveform for five moduli.



set.

Fig. 5. Schematic of five moduli RNS forward converter using RCA.

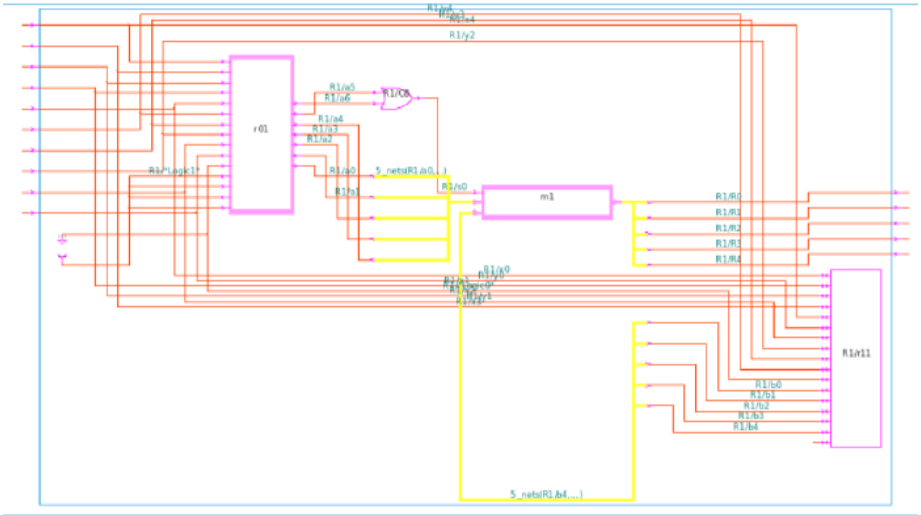


Fig. 6. Schematic of CSA-based mod-15 unit.

TABLE I. Comparative analysis based on RCA, CSA, and HAL for individual moduli

	RCA-based			CSA-based			HAL-based		
	Area (μm^2)	Power (μW)	Delay (ns)	Area (μm^2)	Power (μW)	Delay (ns)	Area (μm^2)	Power (μW)	Delay (ns)
MOD 7	278.323	151.168	1.86	376.934	130.275	1.45	233.165	079.885	1.36
MOD 15	368.640	203.445	2.26	512.410	186.591	1.63	318.874	113.484	1.76
MOD 17	514.252	210.635	2.76	597.197	187.377	1.80	528.077	182.403	2.26
MOD 31	458.957	216.631	2.27	597.197	187.377	1.80	384.307	140.011	2.10

Figs. 7(a)-(c) show area, power, and delay, respectively for different module set for various adder architectures.

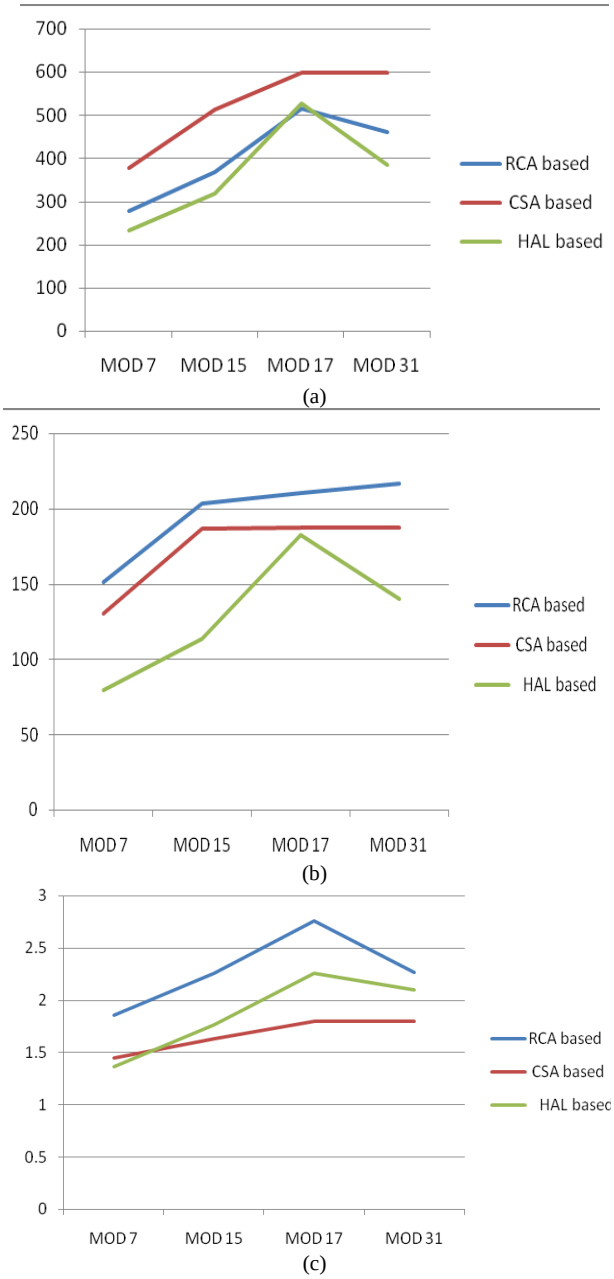


Fig.7. Performance comparision of forward converters using different adders: (a) area, (b) power and (c) delay.

I. CONCLUSION

TABLE II. Comparative analysis based on RCA, CSA, and HAL for complete five moduli forward converter

Parameters	Using RCA	Using CSA	Using HAL
Area (μm^2)	3584	4735	3397
Power (μW)	1.73×10^3	2.1×10^3	1.4×10^3
Delay (ns)	5.49	4.57	4.65

This paper compares three architectures of forward converter in RNS of five moduli using modular adders based on RCA, CSA, and HAL. From the performance comparison table, it is observed that the area of forward converter using CSA and HAL architectures is less than that of RCA by 15% and 10%, respectively. Therefore, CSA is more area efficient. Nonetheless, the forward converter based on HAL is advantageous compared to other architectures in terms of power and delay.Some other types of adders can also be explored for comparison as discussed in [7]-[10]. Moreover, modulo multiplication based on different special moduli set can be applied using Vedic mathematics for fast multiplication in RNS domain [11], [12]. In addition, modulo multiplication can also be implemented using serial multipliers [13].

REFERENCES

1. A. Omondi and B. Premkumar, *Residue number systems: Theory and implementation*, 1st ed. London: Imperial College Press, 2007.
2. S. Akhter, G. Raturi, and S. Khan, "Analysis and design of residue number system based building blocks," in *Proc. IEEE 2018 International Conference on Signal Processing and Integrated Networks*, 2018, pp. 441-445.
3. D. Boruah and M. Saikia, "A pure combinational logic gate based forward converter for new five moduli set RNS," in *Proc. IEEE 2015 International Conference on Advances in Computing and Communication Engineering*, 2015, pp. 301-307.
4. A. A. Hiasat, "High-speed and reduced-area modular adder structures for RNS," *IEEE Transactions on Computers*, vol. 51, no. 1, pp. 84-89, Jan. 2002.
5. A. A. Hiasat, "General modular adder designs for residue number system applications," *IET Circuits, Devices & Systems*, vol. 12, no. 4, pp. 424-431, Aug. 2018.
6. B. K. Mohanty and S. K. Patel, "Area-delay-power efficient carry-select adder," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 61, no. 6, pp. 418-422, Jun. 2014.
7. V. K. Saini, S. Akhter, and T. Chauhan, "Implementation, test pattern generation, and comparative analysis of different adder circuits," *VLSI Design*, vol. 2016, pp. 1-8, 2016.

8. S. Akhter, V. Saini, and J. Saini, "Analysis of Vedic multiplier using various adder topologies," in *Proc. IEEE 2017 International Conference on Signal Processing and Integrated Networks*, 2017, pp. 173-176.
9. S. Akhter, S. Chaturvedi, and K. Pardhasardi, "CMOS implementation of efficient 16-bit square root carry-select adder," in *Proc. IEEE 2015 International Conference on Signal Processing and Integrated Networks*, 2015, pp. 891-896.
10. H. Goyal and S. Akhter, "VHDL implementation of fast multiplier based on Vedic mathematic using modified square root carry select adder," *International Journal of Computer Applications*, vol. 127, no. 2, pp. 24-27, Oct. 2015.
11. S. Akhter, "VHDL implementation of fast N×N multiplier based on Vedic mathematics," in *Proc. 18th European Conference on Circuit Theory and Design*, 2007, pp. 472-475.
12. S. Akhter and S. Chaturvedi, "Modified binary multiplier circuit based on Vedic mathematics," in *Proc. IEEE 2019 International Conference on Signal Processing and Integrated Networks*, 2019, pp. 234-237.
13. S. Akhter and S. Chaturvedi, "HDL based implementation of N×N bit-serial multiplier," in *Proc. IEEE 2014 International Conference on Signal Processing and Integrated Networks*, 2014, pp. 470-474.

AUTHORS PROFILE

Tukur Gupta has received her B.Tech degree in Electronics and Communication Engineering (ECE) from Gautam Buddha Technical University (Formerly, Uttar Pradesh Technical University, Lucknow) in 2010 and the M.Tech (Microelectronics & Embedded Technology) from Jaypee Institute of Information Technology (JIIT), NOIDA in 2015. She is currently pursuing PhD in VLSI Design from Jaypee Institute of Information Technology, NOIDA. She has 6 years of industrial and teaching experience. Her research interests include VLSI design, low-power design.

Shamim Akhter did B.Tech (ECE) from AMU Aligarh (2001), M.Tech (VLSI) from IIT Delhi (2003) and PhD from JIIT Noida (2015). His research interest is VLSI signal processing.

Anandita Srivastava did B.Tech from NIET (AKTU) in electronics and communication (2016) and M.Tech (2019) from JIIT NOIDA with specialization in Microelectronics and Embedded Technology.

Saurabh Chaturvedi obtained his B.Tech. degree in ECE from JIIT, NOIDA (2005), M.Tech. degree in VLSI Design from the Guru Gobind Singh Indraprastha University, Delhi, India (2008), and Ph.D. degree from the University of Johannesburg, South Africa (2018).