A Review Analysis Of Reverse Converter Based On Rns In Signal Processing

Daphni S, Vijula Grace K.S

Abstract: In digital processing techniques, the fundamental operations such as sum, division can be carried out by several categories of adders with different sum times, requirements of area and power consumption. The Residue number system (RNS) based processor mainly used in many digital signal processing applications which mainly consists of reverse conversion (residue to binary) process. This paper analyzed the design o Reverse Converter which based upon the RNS of DSP applications with various adders and algorithms. Now a days a role of RNS based processor is an essential in many signal processing applications. From the analysis, it shows that the Hybrid modulo Parallel–prefix Excess-one adder (HMPE) with Chinese Remainder Theorem (CRT) Reverse Converter design is well suitable for better performance on the aspects of delay and area.

Keywords : Parallel Prefix Adder, Carry Propagate Adder, Residue Number System, Mixed Radix Conversion, End around Carry, Ripple Carry Adder.

1. INTRODUCTION

Generally, the digital functions are carried out by binary number system. In any digital based processors addition is the basic operations that can be done using different types of adders CLA, CPA and PPA with dissimilar summation times, area occupation and power consumption. Now a days, the RNS based processor plays an important role in many digital signal processing applications. This type of processor consists of two conversions namely Forward (binary to residue conversion) and Reverse (Residue to binary conversion) Conversions. This paper only takes the reverse converter design because the Reverse conversion plays a main role and essential, wants to be hardware and time proficient. It regularly used to achieve the tasks like comparison, sign detection and scaling. In Residue number system moduli, the numbers ranging from 0 and M-1 can be individually denoted by the residues. Thus a huge number can be signified by the many smaller numbers called residues which achieved as the balances when the specific number is separated by the moduli. The RNS based reverse conversion design mainly applicable for signal processing and cryptography. The most of the RNS based processors need smaller word length for modulo operations so that the basic process such as the multiplication, addition can be done faster.

- *1Daphni S, 2Vijula Grace K.S*
  Research Scholar, Department of Electronics Communication Engineering Noorul Islam University, Thuckalay. Kumaracoil, India. daphnithavasumony@gmail.com
- *2Assistant Professor, Department of Electronics and Communication Engineering*
- *Noorul Islam University, Thuckalay. Kumaracoil, India. vijulasundar@gmail.com*

This paper is structured as follows, in section 2; it analyses the applications of RNS design, in section 3; it explains the different types of algorithms used in reverse converter design, in section 4; it defines the various types of adders used in reverse converter design. The last section is concluded with the analysis results and discussion.

2. APPLICATIONS OF RNS DESIGN

In DSP - Digital signal processing and cryptography applications, the RNS based processors able to propose carry free and fully parallel arithmetic operations.

2.1. RNS in Signal Processing:

The applications of RNS in signal processing are discussed first. The RNS design is mainly used in FIR (Finite Impulse

Response) filters in the field of signal processing. FIR filters depends upon Read Only Memory multipliers by Residue Number System have been defined by Jenkins and Leon [1]. In that design, the FIR filter operation is given by the following equation,

$$y(i) = \sum_{j=0}^{N-1} h(j)\, s(i-j)$$

The above FIR filter equation is done in Residue Number System for all the j moduli.

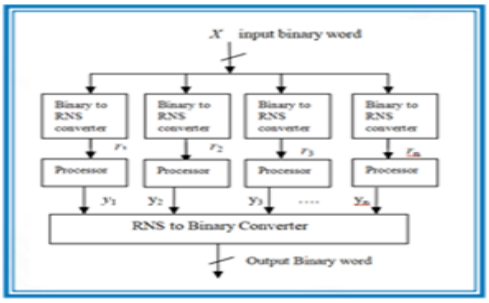

***Fig.1**. RNS based processor*

The RNS design is used in RNS based processor. The general RNS based processor is shown in Fig.1. Ramirez et al. [23] have designed a Residue Number System enabled Digital Signal Processing by four moduli set using SIMD architecture. The forward and reverse converters were external from chip. The adder/subtractor is constructed by a

cascade design. The Look Up Tables - LUTs and index adder are used to realize the multiplier. In addition the RNS is applied in DFT, FFT, DWT, DCT [3] and communications systems [2] in the field of signal processing.

2.2. RNS in Cryptography:

Next application of RNS design is in cryptography. The necessity of firmly retrieving the data and keeping the data from illegal people is well predictable usually [4]. Cryptographic applications like Elliptic curve cryptography, RSA encryption, Diffie-Hellman Key exchange etc., are required the modulo exponentiation and multiplication of big values with bit large sizes (160-2048 bits) normally. Two general methods are depends on Montgomery multiplication and Barrett reduction. Though, to do the process (XY) mod N for a solo modulus, Residue Number System using a number of less word sizes moduli can be engaged. This theme has established newly significant consideration. Some more applications of RNS in cryptography like Montgomery Modular Multiplication, Modulo Multiplication Using Barrett's Technique, RNS Montgomery Multiplication and Exponentiation, Pairing Processors Using RNS, and Elliptic Curve Cryptography Using RNS [5-9].

3. ALGORITHMS USED IN RNS BASED REVERSE CONVERTER DESIGN

There are few fundamental conventional algorithms to convert a value from Residue Number System to binary form. These algorithms are mainly depends on CRT and MRC [10]. Recently few innovative techniques have been familiarized based on the fundamental methods such as New CRT-I, CRT-II and Mixed-Radix CRT.

3.1. CRT & MRC Based Reverse conversion:

CRT can be proficiently used the three and four moduli sets e.g. $\{2^n -1, 2^n, 2^n + 1\}$, $\{2^n-1, 2^n, 2^n+1, 2^{2n} + 1\}$ and $\{2^{2n}-1, 2^n, 2^{2n} + 1\}$, $\{2^n-1, 2^n, 2^{n+1} -1\}$, $\{2^n-1, 2^n, 2^{n-1}-1\}$ where n bits of the decoded number X are straight offered as residue. Few examples of reverse converter design based on CRT are given in the reference [11-13]. The MRC algorithm is consecutive and includes modulo multiplication and modulo subtractions by means of multiplicative inverses of one modulus corresponds to the balance moduli [14]. In each step, one mixed radix digit d_i is calculated and there is no essential for last modulo reduction. Some example illustrates the MRC technique is given in the reference [15-17]. The final step wants product of bigger numbers. This MRC algorithm uses the pipelined technique. Bi and Gross [18] have defined a Mixed-Radix CRT for reverse conversion. Some of the RNS based on these new techniques CRT-I and CRT-II is given in the reference [19-22]. The benefit of this design is the option for parallel calculation of several MRC digits allowing high speed evaluation of two numbers at the expenses of hardware since several Mixed Radix digits and division using the multiplication of moduli and taking only the integer value are bulky.

4. ADDERS USED IN RNS BASED REVERSE CONVERTER DESIGN:

The RNS based processor consists of arithmetic units for modulo addition in the reverse conversion process. Primarily, the reverse conversion calculations are measured using famous adder architectures, like CSAs and ripple-carry architectures. By using of these adders delay can be reduced and the utilization of area can be increased. The usage of CSA with End around Carry - EAC methodology is used for the simplified addition [15]. To compromise both area and delay, the CPA with EAC adders is used for modulo addition in the reverse conversion process [17]. Generally CPA is very expensive due to high hardware requirements. Since this is not suitable for the higher order bits. To recover the problem for the usage previous adders, recently the parallel prefix adders are used for the addition in the reverse conversion process for higher order bits [22]. Normally, the PPA is used for the better in delay performance since the speed of the process automatically increased but this having the high power consumption. This paper [13] described HMPE adder for the simplified reverse conversion structure for the analysis up to 16 bits. The area and delay performance for the various types of adders is given in Table.1.

***Table.1**. Comparison analysis of area and delay for various types of adders:*

Adders type	*area((μm^2))*		*Delay (ns)*	
	12	*16*	*12*	*16*
RCA based adders	*4098.2*	*5353.9*	*0.91*	*1.093*
Fully prefix adders	*7087*	*9800.3*	*0.268*	*0.292*
HMPE-KS	*6950.9*	*8987*	*0.294*	*0.442*
HMPE-SK	*4903.9*	*6525*	*0.416*	*0.456*
HMPE-BK	*5018.8*	*6478.9*	*0.285*	*0.455*

From the analysis, the delay can be reduced by the usage of parallel prefix adders, and based upon the area and delay based the HMPE PPA structure adders is well suitable for reverse conversion.

***Table.2**. Power analysis by the usage of various types of adders*

Adders type	*Power (mW)*		*PDP*	
	12	*16*	*12*	*16*
RCA based adders	*6.382*	*6.997*	*5.81*	*7.65*
Fully prefix adders	*39.99*	*53.85*	*10.72*	*15.72*
HMPE-KS	*37.56*	*26.52*	*11.04*	*11.72*

HMPE-SK	*16.75 19.87*	*6.97 9.06*
HMPE-BK	*27.59 20.48*	*7.86 9.32*

From table 2, it clears that the power consumption is maximum for PPA than other adders since the delay is less so that the PDP is reduced automatically. Finally from all the analysis result, the overall performance of reverse conversion process is better by the usage of PPA.

5 CONCLUSION

This paper has reviewed various analysis of RNS based Reverse converter design with different algorithms and the usage of adders in signal processing applications. From the algorithm analysis, many of the converter design based upon the CRT, MRC algorithm, and New CRT methods. For the better performance in reverse conversion arithmetic units, the HMPE adder is better that is cleared by the analysed result. But the power consumption is increased. In future, the reverse converter will design for higher order bits (32 or 64) include HMPE adders with power reduction techniques.

6 REFERENCES

[1] W.K. Jenkins, B.J. Leon, "The use of residue number systems in the design of finite impulse response digital filters," in IEEE Trans. Circuits Syst. CAS-24, 191–201 (1977).

[2] L.L. Yang, L. Hanzo, "A residue number system based parallel communication scheme using orthogonal signaling: part I—system outline," IEEE Trans. Veh. Technol. 51, 1534–1546 (2002).

[3] P.G. Fernandez et.al, "A new implementation of the discrete cosine transform in the residue number system," in Proceedings of 33rd Asilomar Conference on Signals, Systems and Computers vol. 2, pp. 1302–1306 (1999).

[4] W. Stallings, "Cryptography and Network Security, Principles and Practices," in 6th edn. (Pearson, Upper Saddle River, 2013)

[5] P. Barrett, "Implementing the Rivest-Shamir-Adleman Public Key algorithm on a standard Digital Signal Processor," in Proceedings of Annual Cryptology Conference on Advances in Cryptology, (CRYPTO'86), pp. 311–323 (1986).

[6] C.K. Koc, T. Acar, B.S. Kaliski Jr, "Analyzing and comparing Montgomery Multiplication Algorithms," in IEEE Micro, pp. 26–33 (1996).

[7] K.C. Posch, R. Posch, "Modulo reduction in residue Number Systems," IEEE Trans. Parallel Distrib. Syst. 6, 449–454 (1995).

[8] D.M. Schinianakis, A.P. Kakarountas, T. Stouraitis, "A new approach to elliptic curve cryptography: an RNS architecture," in IEEE MELECON, Benalma´dena (Ma´laga), Spain, pp. 1241–1245, 16–19 May 2006.

[9] J. Groth, A. Sahai, "Efficient non-interactive proof systems for bilinear groups," in 27th Annual International Conference on Advances in Cryptology, Eurocrypt 2008, pp. 415–432 (2008).

[10] P.V. Ananda Mohan "Residue number sustem theory and applications," (Springer International Publishing Switzerland, 2016).

[11] Arash Hariria , Keivan Navib, Reza Rastegarc.,"A new high dynamic range moduli set with efficient reverse converter," Elsevier:Computers and Mathematics with Applications(2008).

[12] Kalyanaraman Karthik and Nicholas Chan Hua Vun.,"Efficient Reverse Converters Designs for RNS based Digital Signal Processing Systems," IEEE 2nd Global Conference on Consumer Electronics-GCCE(2013).

[13] Azadeh Alsadat Emrani Zarandi, Amir Sabbagh Molahosseini and et.al., "Reverse Converter Design via Parallel-Prefix Adders:Novel Components, Methodology, and Implementations," IEEE Transactions on Very Large Scale Integration (VLSI) Systems (2014).

[14] H.M. Yassine, W.R. Moore, "Improved Mixed radix conversion for residue number system architectures," Proc. IEE Part G 138, 120–124 (1991).

[15] Amir Sabbagh Molahosseini, Sara Sezavar and Keivan Navi.,"A New Design of Reverse Converter for a Three-Moduli Set," International symposium on intelligent signal processing & communication systems - ISPACS(2009).

[16] Marcin Wesolowski, Piotr Patronik, Krzysztof Berezowski, Janusz Biernat.,"Design of a Novel Flexible 4-moduli RNS and Reverse Converter," ISSC., (2012).

[17] Leonel Sousa, Samuel Antão, and Ricardo Chaves.," On the Design of RNS Reverse Converters for the Four-Moduli Set $\{2^n + 1, 2^n - 1, 2^n, 2^{n+1} + 1\}$," IEEE Transactions on Very Large Scale Integration (VLSI) Systems (2013).

[18] S. Bi, W.J. Gross, "The Mixed-Radix Chinese Remainder Theorem and its applications to Residue comparison," IEEE Trans. Comput. 57, 1624–1632 (2008).

[19] Amir Sabbagh Molahosseini, Keivan Navi, Omid Hashemipour, Ali Jalali.,"An efficient architecture for designing reverse converters based on a general three-moduli set," Elsevier:Journal of Systems Architecture(2008).

[20] Amir Sabbagh Molahosseini and Keivan Navi.,"A Reverse Converter for the Enhanced Moduli Set $\{2^n–1, 2^n+1, 2^{2n}, 2^{2n+1}–1\}$ Using CRT and MRC," IEEE Annual Symposium on VLSI(2010).

[21] Yuan-Ching Kuo, Ming-Hwa Sheu, Siang-Min Siao, Cheng-Yi Huang and Tzu-Hsiung Chen., "New reverse converter design of Moduli Set {2n, 2n+1-1, 2n-1},"Second International Conference on Innovations in Bio-inspired Computing and Applications(2011).

[22] Hector Pettenghi, Ricardo Chaves, and Leonel Sousa.,"Method to Design General RNS Reverse Converters for Extended Moduli Sets," IEEE Transactions on Circuits And Systems—II: Express Briefs(2013).
[23] J. Ramirez, A. Garcia, S. Lopez-Buedo, A. Lloris, "RNS-enabled digital signal processor design," Electron. Lett. 38, 266–268 (2002).