ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Sign detection algorithm using carry look ahead adder for the RNS Module Set 2n+1,2n-1,2n.

P.Umamaheswari
MTech Student
Department of ECE
AnuBose Institute Of Technology(ABIT)
Paloncha, Khammam, India

B.Sowmya
Assistant Professor
Department of ECE
AnuBose Institute Of Technology(ABIT)
Paloncha, Khammam, India

ABSTRACT: ***The Residue Number System (RNS) is a non-weighted system that is very efficient in digital signal processing and communicational applications. The previous proposed methods for the residue to binary (R/B) conversions are based on the Chinese Reminder Theorem (CRT) or Mixed Radix Conversion (MRC). These theorems are difficult to implement. In this paper, we present a new high-speed ROM-less residue to binary converter for the three moduli set of {2n 1, 2n−, 2n 1}.+ Our technique unlike previous methods uses the grouping numbers in dynamic representation range M which its delay is much less than other converters.***

Keywords: ***residue number system, reverse converter, moduli set {2n 1, 2n−, 2n+1}, group number.***

INTRODUCTION:

Residue Number System is an unconventional system. In this system, an integer X is represented by its reminder modulo a number of different bases. These residue numbers are smaller than the original number in the conventional system, so computations can be done with more speed and low power [1]. The advantages of RNS for implementing digital signal processors for certain applications such as FIR filtering are well-known [2-5]. Some of the more recent applications have been for 1-D filtering [6-8], 2-D filtering [9], video filtering [10], RSA cryptography [11-14], Elliptic curve cryptography [15], m-ary orthogonal keyed communication scheme [16], general purpose RISC DSP [17] and Image processing [18]. The RNS is determined using a set of relative pair wise prime integers positive co-prime integers {m1, m2, …, mn} as moduli set. The dynamic range M of that system is given as a product of the moduli mi where 1 can be uniquely−Any integer X between 0 and M represented as (x1, x2, …, xn). The residues ,|| mi Xx=i also called residue digits, are defined as (2) mxmXx ii≤< i =i .0,mod The two most important issues for the residue arithmetic are the choice of moduli sets and the conversion of residue to binary numbers. The choice of moduli set in RNS is of continuing interest. Early designs of RNS based processors were largely based on ROMs which used small set of mutually prime integers to realize a large dynamic range. However, the R/B converters for the general moduli sets are hardware intensive and implemented based on LUTs (Look-up tables). The access time of the LUTs and the need to read these iteratively have made the implementations inefficient for ASIC realization for RNS with large dynamic range. Hence, the more recent trend has been to use moduli sets which can help to eliminate the ROMs. These are known as power-of-two related moduli sets or “conversionfriendly” moduli sets [19].

Existing System:

I performed efficiently with limited amount or even without ROM. The periodicity properties exhibited by three moduli of this RNS result in superb performance of the binary to residue converter and modulo addition even for large n [27].

Section 2 describes how the conversion of RNS to binary system using the new approach. Section3 presents the hardware implementation and in section 4, the proposed design is compared with other reported converters.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Proposed System:

For residue to binary conversion in moduli set {2n -1, 2n , 2 n +1}, we distribute the numbers in dynamic representation range M into several groups and subgroups which a part of this novel idea is presented in [28]. Since, residue representation of X in above moduli set is corresponding with (x1, x2, x3), then the three residues denotes as:

$$x_1 = X \bmod 2^n - 1 = \underbrace{x_{1,n-1}x_{1,n-2}\ldots x_{1,0}}_{n}$$

$$x_2 = X \bmod 2^n = \underbrace{x_{2,n-1}x_{2,n-2}\ldots x_{2,0}}_{n}$$

$$x_3 = X \bmod 2^n + 1 = \underbrace{x_{3,n}x_{3,n-1}\ldots x_{3,0}}_{n+1}$$

So, the group number of any residue number in the considered moduli set obtains according to Figure 1.

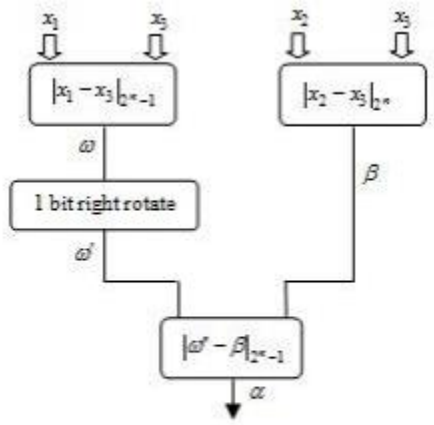

Fig. 1 Group Number Detection.

Table 1: Distribution of Numbers in subgroups

Number	*Subgroup*
$0 \rightarrow 2^n$	0
$2^n+1 \rightarrow 2(2^n+1)-1$	1
$2^n(2^n+1) \rightarrow 3(2^n+1)-1$	2
⋮	
$(2^n-1)(2^n+1) \rightarrow 2^n(2^n+1)-1$	2^n-1

$$\upsilon = |x_1 - x_3|_{2^n-1} \Rightarrow \begin{cases} 0 \le X < 2^n+1, & \omega = 0 \\ 2^n+1 \le X < 2(2^n+1), & \omega = 2 \\ 2(2^n+1) \le X < 3(2^n+1), & \omega = 4 \\ \vdots & \\ (2^{n-1}-1)(2^n+1) \le X < 2^{n-1}(2^n+1) & \omega = 2^n-2 \\ 2^{n-1}(2^n+1) \le X < (2^{n-1}+1)(2^n+1), & \omega = 1 \\ \vdots & \\ (2^n-2)(2^n+1) \le X < (2^n-1)(2^n+1), & \omega = 2^n-3 \\ (2^n-1)(2^n+1) \le X < 2^n(2^n+1), & \omega = 0. \end{cases} \quad (7)$$

According to (7) and with regard to the product result from moduli subtraction in each group be appeared first, odd values and afterward even respectively. Since, in order to accomplishment of arithmetic operations should values increasingly, so it is achievableωbe arranged the = 0,ωthrough one bit right rotate. Therefore, if assume 2, 4, 6, …, 2n - 2, 1, 3, .., 2n - 3, after 1-bit right rotate, = 0, 1, 2, …, 2n′ωwe get - 3, 2n - 2.

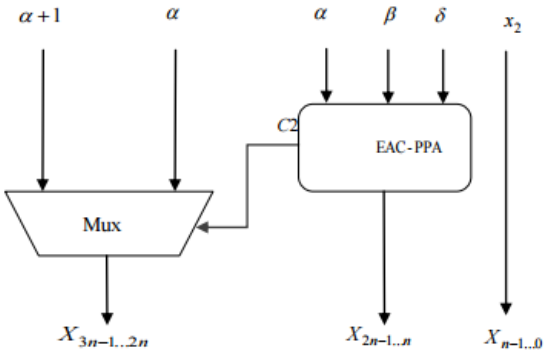

Fig. 2 reverse conversion unit

Hardware Structure

The group detection function is determined by Eq.(8) as . 12− = nαωβ −′ is computedαAccording to [28], since as a residue modulo 2n -1 then, instead of subtracting 12− nβ we can add its additive inverse modulo 2n -1. An additive inverse modulo 2n -1 is simply a negation of binary representation.

Proposed method for the numbers conversion from residue system to binary system is implemented with parallel prefix structure including parallel-prefix adder and end-around-carry prefix adder, both of which are

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

introduced in [29]. A parallel prefix adder and also parallel prefix adder with end-around-carry are built from elements shown in Figure 3.

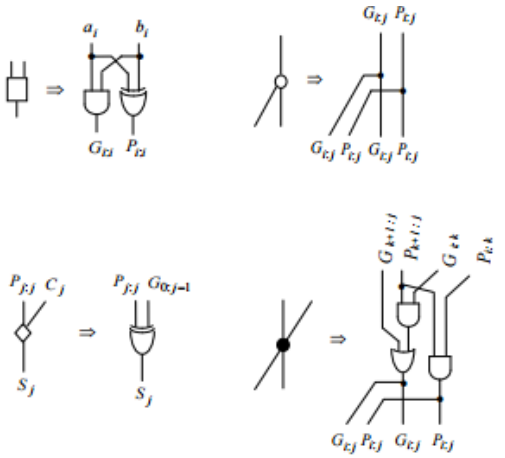

Fig. 3 Blocks of prefix adder structure [30].

The signals G : ji and P: ji are the carry generation and propagation functions from the position i to j. For an addition of two binary vectors −01 n ...aa and −01 n ...bb and for jki ,<< these functions can be expressed by logic equations

$$G_{i:i} = a_i \cdot b_i$$
$$P_{i:i} = a_i \oplus b_i$$
$$G_{i:j} = G_{i:k} \cdot P_{k+1:j} + G_{k+1:j}$$
$$P_{i:j} = P_{i:k} \cdot P_{k+1:j}.$$

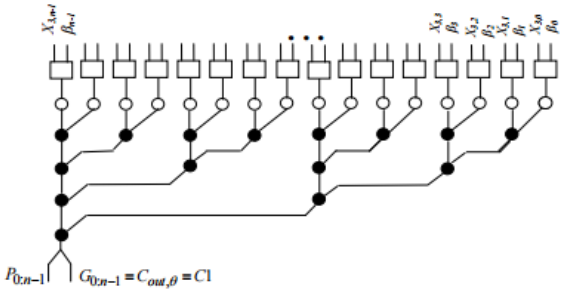

Fig. 4. Carry Generation Unit for n=16

The carry generation unit use (n - 1) black nodes and n input nodes (denoted as square). Its area and time can be expressed as

$$A_2 = 3n + 3(n-1) = 6n - 3$$
$$T_2 = 2\log_2 n + 2 \quad (27)$$

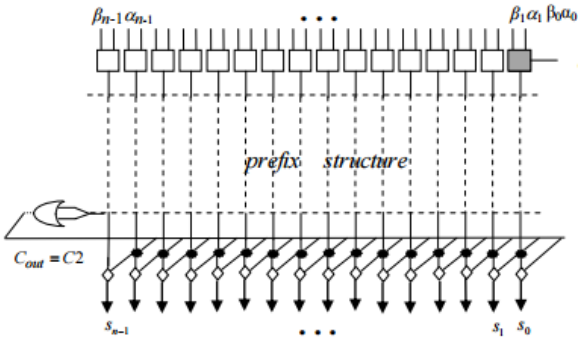

Fig. 5 EAC-PPA

The requirements for the above adder is as follows: n input nods, n output nodes (denoted as lozenge), (n - 1) black node, one additional gate. Notice that first input node is a full adder with area of 4 unit and delay of 2 unit more than half adder. The prefix part of circuit from [29] requires the delay of log2 2 n logic levels and also, the area of log)2/3(2 nn . The AT parameters for the shown circuit in Figure 5

$$A_3 = 8n + \frac{3}{2} n \log_2 n + 2$$
$$T_3 = 2\log_2 n + 8.$$

It is shown in EAC-PPA circuit that delay of generation of C2 is equal to 6log2n + 17. According to Fig. 2, the most significant n bits of X in + 1. The output carryα or αbinary system is given by signal from the circuit shown in Fig. 5 be called C2 is αselecting line of multiplexer which determine whether + 1. In order to computation ofαbe directed to output or , beα + 1, is sufficient after the value determination of α add with 1. + 1 perform the function ofαTherefore, the circuit adding 1 to a n-bit input number. Consider 0+1=en-1en-2… e1e0.α1αn-2…αn-1α+1=α0,α1αn-2…αn-1α=α We have the following equation, which imply that the circuit plus 1 requires n-1 XOR gates and n AND gates plus 1 inverter. 0αe0= ⊕1α, e1= 0,α1α

Conclusions

Reverse converter is one of the most important issues in residue number system. In this paper, a novel and

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

fast algorithm for the conversion of numbers given in RNS {2n -1, 2n , 2n +1} is presented. Our proposed technique is based on grouping numbers which has significant reduction in delay, compared to other methods. Furthermore, it accomplishes reverse conversion without applying the generic approaches such as CRT and MRC.

REFERENCES:

[1] E. Gholami, R. Farshidi, M. Hosseinzadeh and K. Navi, "High speed residue number system comparison for the moduli set {2n -1, 2n , 2n +1}", Journal of communication and computer, Vol. 6, No. 3, 2009, pp. 40-46.

[2] N. Szabo, R. Tanaka, "Residue arithmetic and its applications to computer technology", New York: MCGraw-Hill, 1967.

[3] M. Soderstrand, M.A.W. Jenkins, G. Jullien and F. Taylor, "Residue number system arithmetic: Modern Applications in Signal Processing", New York: IEEE Press, 1986.

[4] P.V. Ananda Mohan, "Residue number system: algorithms and Architectures", New York: kluwer Academic Publishers, 2002.

[5] F. Taylor, "Residue arithmetic: a tutorial with examples", IEEE Comput Mag, 1984, pp. 50-62.

[6] W. Freking, K. Parhi, "Low-power FIR digital filters using residue arithmetic", In: Conference of the 31st Asilomar conference on signals, systems and computers, 1997.

[7] A. D'Amora, et al, "Residue power dissipation in complex digital filters by using the quadratic residue number system", In: Conference of the 34th Asilomar conference on signals, systems and computers, Vol. 2, 2000, pp.

[8] G. Cardarill, et al, "Low-power implementation of polyphase filters in Quadratic Residue Number System", In: Proceedings of the IEEE international symposium on circuits and systems, vol. 2, 2004, pp. 725-8,

[9] N. Shanbag, R. Siferd, "A single-chip pipelined 2-D FIR filter using residue Arithmetic. IEEE J SolidState Circuits, 1991, pp. 796-805.

[10] T. Toivonen, J. Heikkila, "Video filtering with format number theoretic transforms using residue number system", IEEE Trans Circuits Syst Video Technol, 2006, pp. 128-38.

[11] J. Schwemmlein, K. Posch , P. Reinhard, "RNS modulo reduction upon a restricted base value set and its applicability to RSA cryptography", 1978, pp. 637-50.

[12] H. Nozaki, M. Motoyama, A. Shimbo and S. Kawamura, "Implementation of RSA algorithms based on RNS Montgomery multiplications", Springer, 2001, pp. 364-76.

[13] J-C. Bajard, L. Kornerup, "An RNS Montgomery modular multiplication algorithm", IEEE Trans Comput, 1998, pp. 769-74.

[14] J-C. Bajard, L. Imbert, "a full RNS Implementation RSA", IEEE Trans Comput 2004, pp. 769-74.

[15] D. Schinianakis, A. Kakarountas, T. Stouraitis, "A new approach to elliptic curve cryptography: an RNS architecture", IEEE Mediterranean electrotechnical