© 2014 IJIRT | Volume 1 Issue 7 | ISSN: 2349-6002

A New Algorithm 2^n-2^k-1 for Residue Number System

Ch. Satyaveni[1], M. Shiva Kumar[2]
[1]*M.Tech, ECE Dept, M.R.C.E, Hyderabad,*
[2]*M.Tech, Asst. Professor, M.R.C.E. Hyderabad,*

***Abstract*— The Residue Number System (RNS) is a non weighted system. It supports parallel, high speed, low power and secure arithmetic. Detecting overflow in RNS systems is very important, because if overflow is not detected properly, an incorrect result may be considered as a correct answer. The previously proposed methods or algorithms for detecting overflow need to residue comparison or complete convert of numbers from RNS to binary. Modular adder is one of the key components for the application of residue number system (RNS). Modulo set with the form of 2^n-2^k-1 ($1 \le k \le n - 2$) can offer excellent balance among the RNS channels for multi-channels RNS processing. In this paper, a novel algorithm and its VLSI implementation structure are proposed for modulo 2^n-2^k-1 adder. In the proposed algorithm, parallel prefix operation and carry correction techniques are adopted to eliminate the re-computation of carries. Any existing parallel prefix structure can be used in the proposed structure. Thus, we can get flexible tradeoff between area and delay with the proposed structure. Compared with same type modular adder with traditional structures, the proposed modulo 2^n-2^k-1 adder offers better performance in delay and area.**

***Index Terms*— Carry correction, modular adder, parallel prefix, residue number system (RNS), VLSI.**

I. INTRODUCTION

Residue number systems (RNS) have been for a long time a topic of intensive research. Their usefulness has been demonstrated, especially for computations where additions, subtractions and multiplications dominate, because such operations can be done independently for each residue digit without carry propagation [1]. Other operations such as overflow detection, sign detection, magnitude comparison and division in RNS are very difficult and time consuming [2, 3]. However, above mentioned operations are essential in certain applications, e.g. in exact arithmetic or computational geometry, where residue arithmetic is applied [4]. RESIDUE number system (RNS) is an ancient numerical representation system. It is recorded in one of Chinese arithmetical masterpieces, the Sun Tzu Suan Jing, in the 4th century and transferred to European known as Chinese Remainder Theorem (CRT) in the 12th century. RNS is a non-weighted numerical representation system and has carry-free property in multiplication and addition operations. In recent years, it has been received intensive study in the very large scale integration circuits (VLSI) design for digital signal processing (DSP) systems with high speed and low power consumption [1]–[4].

Modular adder is one of the key modules for RNS-based DSP systems. For the general modular adder, Bayoumi proposed a scheme for arbitrary modulus by using two cascaded binary adders [5]. However, the delay is the sum of the two binary adders. Several literatures constructed several modular adders with two parallel binary adders to calculate A+B and A+B+T [6], [7]. This method can achieve less delay but needs about twice area of binary adder. Dugdale proposed a method to construct a type of general modular adders with a reused binary adder [9]. The shortage of this structure is that it will use two operation cycles to perform one modular addition. The area or delay of these modular adders mentioned above is twice or more than that of binary adder. In recent studies, a few modular adders with better area and delay performance are presented. Hiasat proposed a class of modular adders in which any regular Carry Look-Ahead (CLA)—based binary adder can be used in the final stage [10].

However, it needs an extra CLA unit to get the carry-out bit of A+B+T before the final CLA addition. As a result, the structure does not reduce the delay significantly. The ELMMA algorithm proposed by Patel et al. [11] uses two carry computation modules for A+B and A+B+T in which some carry computation units can be shared. The area reduction of this scheme is dominated by the form of. In the worst case, almost two independent carry generation modules are needed. Patel et al. [12] also proposed several algorithms which can generate carries fastly. A new number representation for modulo addition is proposed in [8]. However, its outputs are represented in special format. Thus, the extra area and delay are needed to perform the conversion from the special representation to binary number representation or all operations should be performed in this number representation format in RNS-based systems.

On the other hand, the complexity of the special modular adder is much less than that of general modular adder, since

the structure of the special modular adder can be further optimized according to the modulus. The effective modular adders for modulo 2^n-1 and 2^n+1 modulo have drawn much more attention than other kinds of modular adders [13], [14]. [15] And [16] proposed architecture for modulo 2^n+1 adder based on "diminished-1" number representation. [17] and [18] presented a structure for modulo 2^n +1 and 2^n-1 based on parallel prefix and carry correction, respectively. A similar architecture with [7] for modulo 2^n±3 adder is also proposed in [19]. In [20], Patel et al. described an implementation structure for modulo 2^n -2^n -1adder based on the technique of carry offset, which is only required to obtain the carry information of A+B+T. In order to obtain the carries required in the modular addition, each carry of A+B+T has to be modified according to the utmost carry of A+B+T. In this case, the redundant modules of carry computation are eliminated, but the structure of carry computation is fixed and can only perform the special modular addition, that is, modulo addition.

One of the important issues is the selection of moduli sets in RNS-based application. In addition and multiplication intensive systems, residue channels are always expected as many as possible when the dynamic range is fixed, that is, the word length of individual residue can be reduced to achieve better speed performance. Meanwhile, the width of each channel is also expected as close as possible to get similar critical path delay.

That is the balance between each residue channel. Moreover, the complexity of modular adder should be evaluated carefully in residue radix selection. At present, it is possible to get high performance modular adders for a few moduli radixes, such as modulo and modulo . But these moduli radixes are not always suitable to construct multi-channel RNS with fine channel balance. For example, it is hard to construct a multichannel moduli set with and to achieve co-prime and fine balance between channels. However, the modulus with the form of have the prominent advantage in constructing multi-channel moduli sets with fine balance [21]. We can find several methods for moduli set selection with this type residue.

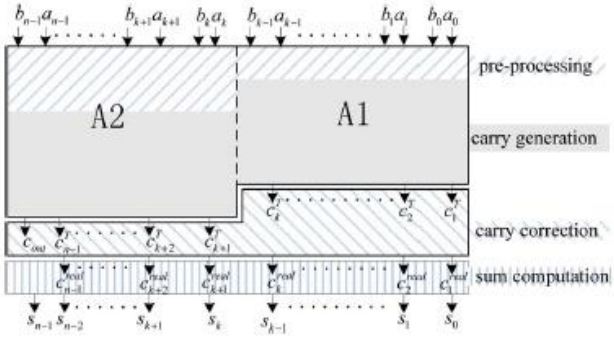
II. DWT SOLUTIONS ENHANCED BY THE RNS

The design of wavelet filter banks using the RNS, presents new opportunities. If the wavelet filters coefficients are fixed a priori, the LUT-based modulo multiplier represents the most efficient solution to meeting low-latency and hardware efficiency [8]. However, if the wavelet filter coefficients are to be run-time programmable, then the solution may require an unacceptably large number of LUTs to cover all coefficient instances [13].

The use of index-transformation multipliers [15, 16], and re-timing techniques leads to DWT filter banks designs requiring a single $2^{nj} \times$ n j LUT for each filter coefficient, where n j = [$\log_a$(mj)], is the modulus word width. Figure 1 shows the design based on index transformations of a modulo mj channel, for an octave-i 8-tap decomposition filter bank. The input sequence |a(i−1) n |mj is decomposed into even and odd sequences that are converted to the index-domain by means of two LUTs storing the j function. Some circuitry is added to the input to detect zero values of the input sequences. Notice that clearable registers have been added to make zero the filter products in case zero is detected in the even- and odd indexed sequences. The reason for this is that multiplication by zero is not defined in the index domain and must be considered to be a special case. After the filter products are computed in the index-domain, the LUT storing the function −1 j maps the indices back to the RNS domain, and the remaining filtering or addition stage is carried out by a modular adder tree. The system exhibits symmetry for the computation of the approximation and detail sequences. The complete RNS design consists of a number of parallel channels whose combined word width is sufficient to ensure that the dynamic range requirements are met.

III. PROPOSED MODULO 2^n-2^k-1 ADDER:

As shown in Fig. the proposed modulo adder is composed of four modules, pre-processing unit, carry generation unit, carry correction unit, and sum computation unit. In Fig., different shade represents different processing units. The proposed modular adder can be divided into two general binary adders, A1 and A2 in Fig., with carry correction and sum computation module according to the characteristics of correction for modulus $\boldsymbol{2^n-2^k-1}$. We can get the carries Cireal used in the final stage through correcting CiT the carries of, which can be computed by any existing prefix structure with proper pre-processing. At last, we can get the final modular addition result from and partial sum information.

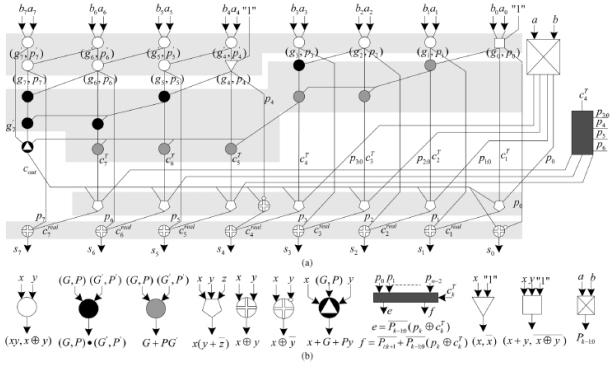


The proposed architecture shown in Fig. 2 can avoid the calculation of carries information for A+B+T and A+B separately. Thus, the area and delay in VLSI implementation can be reduced. Meanwhile, the proposed scheme offers flexible tradeoff of area and delay with different parallel prefix structures.

IV. RELATED WORK

One of the fastest and most efficient RNS comparator for the moduli set {2n-1, 2n, 2n+1} are introduced in references [17] and [19] respectively. In a generic approach, after a residue to binary convert, comparison operation can be done by using n or (n +1) bits comparator which has a delay of residue to binary converter plus delay of a (n +1) bit Binary Comparator (BC) proposed technique is compared with other methods. The most effective overflow detection circuit based on reverse converters can be built on the base on Converter I from [20]. In Converter I and also Converters II and III from [20], the minimum delay is O(n) whereas, delay of proposed method is factor of O(log2 n).

The proposed approach for overflow detection in moduli set {2n-1, 2n, 2n+1} is faster than previous works. However, the hardware cost of the presented method is more. It is essential to remark that, although the proposed design consumes more hardware but it demonstrates significant improvement in terms of delay, especially for large n. Furthermore, our proposed method detects overflow without applying a complete comparator or reverse converter.



V. CONCLUSION

In this paper, a new class of modulo 2^n-2^k-1 adder is proposed. The proposed structure is consisted of four units, the pre-processing, the carry computation, the carry correction and the sum computation unit. The performance analysis and comparison show that the proposed algorithm can construct a new class of general modular adder with better performance in delay or "area*delay". It has some main features as following:

The way using twice carry corrections improves the performance of area and timing in VLSI implementation and reduces the redundant units for parallel computation of A+B+T and A+B in the traditional modular adders.

Any existing prefix tree can be used in this structure. That means fine tradeoff property between area and delay for the proposed scheme. The synthesis results also show that our scheme can be optimized to work at faster operation frequency. Furthermore, the modulus with the form of 2^n-2^k-1 $(1 \le k \le n-2)$ facilitates the construction of a new class of RNS with larger dynamic and more balanced complexity among each residue channel. The work of this paper provides an alternative scheme of modular adder design for this type of RNS.

REFERENCES

[1] S. Ma, J. H. Hu, L. Zhang, and L. Xiang, "An efficient RNS parity checker for moduli set and its applications," Sci. in China, Ser. F: Inform. Sci., vol. 51, no. 10, pp. 1563–1571, Oct. 2008.

[2] Y. Liu and E.M.-K. Lai, "Design and implementation of an RNS-based 2-D DWT processor," IEEE Trans. Consum, Electron., vol. 50, no. 1, pp. 376–385, Feb. 2004.

[3] P. Patronik, K. Berezowski, S. J. Piestrak, J. Biernat, and A. Shrivastava, "Fast and energy-efficient constant-coefficient FIR filters using residue number system," in

Proc. Int. Symp. Low Power Electronics and Design (ISLPED), 2011, pp. 385–390.
[4] J. C. Bajard, L. S. Didier, and T. Hilaire, " -direct form transposed and residue number systems for filter implementations," in Proc. IEEE 54th Int. Midwest Symp. Circuits and Systems (MWSCAS), 2011, pp. 1–4.
[5] M. Bayoumi, G. Jullien, and W. Miller, "A VLSI implementation of residue adders," IEEE Trans. Circuits Syst., vol. CAS-34, no. 3, pp. 284–288, Mar. 1987.
[6] S. J. Piestrak, "Design of residue generators and multi operand modular adders using carry-save adders," IEEE Trans. Comput,, vol. 43, no. 1, pp. 68–77, Jan. 1994.
[7] H. Vergos, "On the design of efficient modular adders," J. Circuits, Syst., and Comput., vol. 14, no. 5, pp. 965–972, Oct. 2005.
[8] G. Jaberipur, B. Parhami, and S. Nejati, "On building general modular adders from standard binary arithmetic components," in Proc. 45th Asilomar Conf. Signals, Systems, and Computers, 2011, pp. 6–9.
[9] M. Dugdale, "VLSI implementation of residue adders based on binary adders," IEEE Trans. Circuits Syst. II: Analog Digit. Signal Process. vol. 39, no. 5, pp. 325–329, May 1992.
[10] A. A. Hiasat, "High-speed and reduced-area modular adder structures for RNS," IEEE Trans. Comput,, vol. 51, no. 1, pp. 84–89, Jan. 2002.
[11] R. A. Patel, M. Benaissa, N. Powell, and S. Boussakta, "ELMMA: A new low power high-speed adder for RNS," in Proc. IEEE Workshop on Signal Processing Systems, Oct. 2004, pp. 95–100.
[12] R. A. Patel, M. Benaissa, N. Powell, and S. Boussakta, "Novel power-delay-area-efficient approach to generic modular addition," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 54, no. 6, pp. 1279–1292, Jun. 2007.
[13] E. Vassalos, D. Bakalis, and H. T. Vergos, "Modulo 2^n+1 arithmetic units with embedded diminished-to-normal conversion," in Proc. 14th Euromicro Conf. Digital System Design (DSD), 2011, pp. 468–475.
[14] G. Jaberipur and S. Nejati, "Balanced minimal latency RNS addition for moduli set $\{2^n-1, 2^n, 2n+1\}$,," in Proc. 18th Int. Conf. Systems, Signals and Image Processing (IWSSIP), 2011, pp. 1–7.
[15] H. T. Vergos and C. Efstathiou, "A unifying approach for weighted and diminished-1 modulo 2^n+1 addition," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 55, no. 10, pp. 1041–1045, Oct. 2008.
[16] S. H. Lin and M. H. Sheu, "VLSI design of diminished-one modulo 2^n +1 adder using circular carry selection," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 55, no. 9, pp. 897–901, Sep. 2008.
[17] C. Efstathiou, H. T. Vergos, and D. Nikolos, "Fast parallel-prefix modulo 2^n+1 adders," IEEE Trans. Comput., vol. 53, no. 9, pp. 1211–1216, Sep. 2004.
[18] R. A. Patel and S. Boussakta, "Fast parallel-prefix architectures for modulo 2^n-1 addition with a single representation of zero," IEEE Trans. Comput., vol. 56, no. 11, pp. 1484–1492, Nov. 2007.
[19] P. M. Matutino, R. Chaves, and L. Sousa, "Arithmetic units for RNS moduli $\boldsymbol{2^n}$ -3 and $\boldsymbol{2^n}$ +3 operations," in Proc. 13th Euromicro Conf. Digital System Design: Architecture, Methods and Tools (DSD), 2010, pp. 243–246.
[20] R. A. Patel, M. Benaissa, and S. Boussakta, "Fast modulo $\boldsymbol{2^n-(2^n-2+1)}$ addition: A new class of adder for RNS," IEEE Trans. Comput., vol. 56, no. 4, pp. 572–576, Apr. 2007.

AUTHOR DETAILS:

First Author: ***Ch. Satyaveni*** received B.Tech Degree in Electronics and Communication Engineering from Malineni Lakshmaiah Women's Engineering College in the year of 2012. She is currently M.Tech student in Em & VLSI Design from Malla Reddy College of Engineering. And her research interested areas in the field of High-speed low-power DSP technology with VLSI, NoC, Wireless Communications, and Software Radio.

Second Author: ***M. Shiva Kumar*** working as an Assistant Professor in Malla Reddy College of Engineering. He has completed his M.Tech and he has 6+ years of teaching experience. His research interested areas are High-speed low-power DSP technology with VLSI, NoC, Wireless Communications, and Software Radio.