International Journal of Engineering Research and General Science Volume 4, Issue 1, January-February, 2016
ISSN 2091-2730

Review paper on VLSI Design of modulo 2^n □1 Adder using Residue Number System

Author- 1- Sonali Singh(PG Scholar VLSI, RKDF IST Bhopal M.P
2- Mr. Manish Trivedi (HOD EC Department, RKDF IST Bhopal M.P)

Abstract— Modular adder is one of the key components for the application of residue number system (RNS). Moduli set with the form of 2^n +1 can offer excellent balance among the RNS channels for multi-channels RNS processing. As one of the processor's ALU performance issues, the carry propagation during the addition operation limits the speed of arithmetic operation. In this paper review on 2^n +1 addition in the residue number system. The architecture design of CCS modular adder is simple and regular for various bit-width inputs. The review modulo adder in the aforementioned paper consists of a dual-sum carry look-ahead (DS-CLA) adder, a circular carry generator, and a multiplexer, which can reduce both number of slice and maximum combination path delay (MCPD).

Keywords: -Modulo Adder, Residue Number System (RNS), and VLSI design

I. INTRODUCTION

Residue number systems (RNS) [1]-[2] reduces the delay of carries propagation, thus suitable for the implementation of high-speed digital signal processing devices. Some arithmetic operations, such as addition and multiplication, can be carried out more efficiently in RNS than in conventional two's complement systems. RNS has been adopted in the design of Digital Signal Processors (DSP) [3]-[4], Finite Impulse Response (FIR) filters [5], image processing units [6], Discrete Cosine Transform (DCT) processors [7], communication components [8], cryptography [9], and other DSP applications. In recent years, efficient schemes for modulo multipliers have
been studied intensively. Generally, modulo 2^n □1 adder can
be divided into three categories, depending on the type of operands that they accept and output:

i. the result and both inputs use weighted representation;
ii. the result and both inputs use diminished-1 representation;
iii. the result and one input use weighted representation, while the other input uses diminished-1.

For the first category, Zimmermann et al. [8] used Booth

encoding to realize, but depart from the diminished-arithmetic, which leads to a complex architecture with large
area and delay requirements. For the second category, Wang *et al.* [9] proposed diminished-1 multipliers with -bit input operands. The multipliers use a non-Booth recoding and a zero partial-product counting circuit. The main drawback in this architecture was handling of zero inputs and results were not considered.

P. Rajender , R.Srinivas published a research with title " Design of Novel Digital Adder Design Based On Residue Number System" They proposed in their research that Modular adder is one of the key components for the application of residue number system (RNS). Module set with the form can offer excellent balance among the RNS channels for multi-channels RNS processing. A novel algorithm and its VLSI implementation structure were 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.

In a recent paper by Lin and Sheu, the authors have proposed a new circular-carry-selection technique that is applied in the design of an efficient diminished-one modulo 2*n* + 1 adder. The proposed modulo adder in the aforementioned paper consists of a dual-sum carry look-ahead (DS-CLA) adder, a circular carry generator, and a multiplexer, which can reduce both area–time (AT) and time–power (TP) products compared with previous modulo adders. However, in our investigation, there will be incorrect results on the calculation of modulo addition because the carry-in of the DS-CLA adder is equal to zero. To remedy this drawback, we propose the corrected architecture of the DS-CLA adder based on the equations proposed in the aforementioned paper, which can perform correct modulo addition. The complexity of the corrected architecture is almost the same as the one proposed by Lin and Sheu but with less area cost, which can also have the same merits of both AT and TP products.

Curiger et al. [10] proposed new modulo multipliers by using the third category. This architecture use ROM based look-up methods are competitive. The main drawback in this architecture increasing n-bit, they become infeasible due to excessive memory requirements. Also proposed for the third category architecture and reduce the memory requirement and speed up. The new architecture is based on n-bit

addition and radix-4 booth algorithm, which is efficient and regular. We are replaced diminished-1 modulo 2^n □1 adder by inverted n-bit adder.

The remainder of the paper is organized as follows: mathematical formulation of Diminished-1 number representation computation of modulo multiplier is presented in Section II. The proposed structures are presented in Section III. Hardware and time complexity of the proposed structures are discussed and compared with the existing structures in Section IV. Conclusion is presented in Section V.

II. DIMINISHED -1 NUMBER REPRESENTATION

The modulo $2^n + 1$ arithmetic operations require (n+1) bit operands. To avoid (n+1)-bit circuits, the diminished-1 number system [15] has been adopted. Let $d[A]$ be the diminished-1 representation of the normal binary number $A \in [0, 2^n$, namely

$$d[A] = |A - 1|_{2^n+1} \quad \text{(i)}$$

In (i), when, $A \neq 0, d[A] \in [0, 2^n - 1$ is an n -bit number, therefore (n+1) -bit circuits can be avoided in this case. However,

$$A = 0, d[A] = d[0] = |-1|_{2^n+1} = 2^n \quad \text{(ii)}$$

is an (n+1) -bit number. This leads to special treatment for d [0]. The diminished-1 arithmetic operations [15] are defined as

$$d[-A] = \overline{d[A]}, if\ d[A] \in [0, 2^n - 1] \quad \text{(iii)}$$

$$d[A + B] = |d[A] + d[B] + 1|_{2^n+1} \quad \text{(iv)}$$

$$d[A - B] = \left|d[A] + \overline{d[B]} + 1\right|_{2^n+1} \quad \text{(v)}$$

$$d[AB] = |d[A] \times d[B] + d[A] + d[B]|_{2^n+1} = |d[A] \times B + B - 1|_{2^n+1} \quad \text{(vi)}$$

$$d[2^k, A] = iCLS(d[A], k) \quad \text{(vii)}$$

$$d[-2^k, A] = iCLS(\overline{d[A]}, k) \quad \text{(viii)}$$

Where $\overline{d[A]}$ represents the one's complement of d [A]. In (vii) and (viii) iCLS (d[a], k) is the k -bit left-circular shift of in which the bits circulated into the LSB are complemented.

III. VARIOUS MODULO ADDER

A proposed architecture consists of the partial products generator (PPG), the correction tern generator (CTG), the inverted end-around-carry carry save adder (EAC CSA) and 2-stage inverted n-bit adder. Based on this architecture, a solution which is more effective is proposed. The encoding scheme accordant with the radix-4 Booth recoding [15], the partial product generator (PPG) can be constructed with the well-known Booth encoder (BE) and Booth selector (BS). The different blocks used in PPG and EAC CSA are taken from [15].

In this paper, we modified BE block which take successive overlapping triplets ($b_{2i-1} b_{2i} b_{2i+1}$) and encodes each as an element of the set {-2,-1, 0, 1 2}. Each BE block produces 3 bits: 1x, 2x and Sign. The 3 bits along with the multiplicand are used to form partial products.

The CTG produces which has the form ($.....0x_{i+1}\ 0x_i\ .....0x_1\ 0x_0$) with $x_i \in \{0,1\}$. Since the 2i-th bit x_i is 1 when the BE_i block encodes 0, otherwise x_i is 0, one XNOR gate accepting the 1x and 2x bits of the block can generate the 2i-th bit x_i .

The inverted EAC CSA tree can reduce the Partial Products to two numbers. The CSA tree is usually constructed with full adders (FA).Then the final two numbers from the tree is passed through the 2 -stage inverted n-bit adder. The 2-stage inverted n-bit adder is consisting of two rows of adders. First row consist of n-bit ripple carry adder of one half adder and (n-1) full adders and the second row consist of n-bit ripple carry adder of n half adders, as shown in fig.(3).

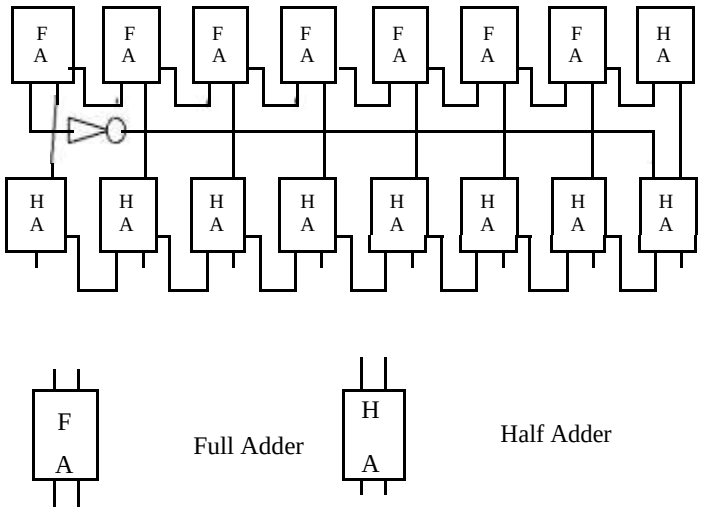

Fig.3. 2-Stage Inverted n-bit Adder

In othertechniques the modulo $2^n - 2^k$ -1 adder is s composed of four modules, pre-processing unit, carry generation unit, carry correction unit, and sum computation unit.

B. Carry Generation Unit

In carry generation unit, the carries C_i^T (i= 1, 2, 3…n) of can be obtained with the carry generation and carry propagation bits from the pre-processing unit. Any existing prefix structure can be used to get the carries.

It is worth pointing out that the carry-out bit of SCSA in the pre-processing unit, is not involved in the prefix computation. Instead, C_{SCSA} combined with the carry-out bit of the prefix tree is required to determine the carry-out bit of A+B+T (denoted as C_{out})

$$C_{out} = C_{SCSA} \cdot C_n^T$$

C. Carry Correction Unit

The carry correction unit is used to get the real carries for each bit needed in the final sum computation stage. In order to reduce the area, we get the carries of A+B by correcting the carries of A+B+T in the carry correction unit.

We first derive the relation of C_i^0 and C_i^1 (i=0, 1, 2, 3 …n) in binary addition. Where and arethecarry outputs of prefix tree when the lowest carry in is ―0‖ and ―1‖, respectively.

D. The Sum Computation

Generally, the sum computation is as same as that in prefix based binary adder. However, is the correction result when C_{out} is taken into account. That is, if C_{out}=0, is the carry bit of A+B. Otherwise, it is the carry bit of A+B+T. Thus, the partial sum bits of A+B and A+B+T are both required in the final sum computation.

IV. RESULT AND SIMULATION

The architecture has very low hardware complexity compared to [5], which consist of modulo $2^n + 1$ adder. In the architecture, we use the 2-stage inverted n-bit adder. And calculate the output for 8, 12bit.

We compare the CCS diminished-one modulo adder against two previous designs of parallel-prefix modular adder [10] and select-prefix modular adder [11], which are regarded as the fastest and the most AT efficient designs among the existing solutions.

In order to get more accurate performance evaluation, we design the existing modulo $2^n - 2^k$ - 1 adder with Sklansky prefix tree and the other modulo adders mentioned in Table I with VHDL

AREA OF MODULO 2^n-2^k-1 ADDER BASED ON UNIT-GATE MODEL

Modules	AND	OR	XOR
Pre-processing	2n-k-2	1	2n-k-1
Carry generation	$2N_P$-n+k-1	N_P+1	0
Carry Correction	n-1	n-1	0
Sum Computation	0		N+1

V. CONCLUSION

The aspire behind the system is to design a high speed adder with low power consumption and low surface area. The structure will be consisted of four units, the pre-processing, the carry computation, the carry correction and the sum computation unit. The tradeoff property between area and delay is proposed in this scheme. The synthesis results will be check on Xilix Software. Although 2^n +1 is proposed in this synopsis but we can change the scheme if result will not match our expectations. This work aims to build an Efficient Hardware Design for an Adder based on Residual Numbering System (RNS), with a pre-specified special set of moduli to simplify the implementation for the purpose of proving the feasibility of its usage.

REFERENCES:

[1] P. V. Ananda Mohan, *Residue Number Systems: Algorithms and Architectures*, Kluwer, Academic Publishers, 2002.

[2] Omondi, and B.Premkumar,Residue Number System: Theory and Implementation,*Imperial College Press*,2007

[3] R. Chaves, L. Sousa, "RDSP: a RISC DSP based residue number system", *in Proc. Euromicro Symposium on Digital System Design (DSD)*, pp. 128–135, Sept. 2003.

[4] J. Ramirez, A. Garcia, S. Lopez-Buedo, and A. Lloris, "RNS-enabled digital signal processor design", *Electronics Letters*, vol. 38, no. 6, pp. 266–268, March 2002.

[5] G. L. Bernocchi, G. C. Cardarilli, A. D. Re, A. Nannarelli, M. Re,"Low-power adaptive filter based on RNS components", *in Proc. ofthe Int. Symposium on Circuits and Systems (ISCAS)*, pp. 3211–3214, 2007.

[6] F. Marino, E. Stella, A. Branca, N. Veneziani, and A. Distante, "Specialized Hardware for Real-Time Navigation", *Real-Time Imaging*, vol. 7, no. 1, pp. 91-108, Feb. 2001.

[7] P. G. Fernandez, and A. Lloris, "RNS-based implementation of 8x8 point 2D-DCT over field-programmable devices", *Electronics Letters*, vol. 39, no. 1, pp. 21-23, Jan. 2003.

[8] U. Meyer-Baese,A. Garcia, and F. Taylor, "Implementation of a communications channelizer using FPGAs and RNS arithmetic", *Journal of VLSI Signal Processing*, vol. 28, no. 1-2, pp. 115-128, June 2001.

[9] J. C. Bajard, and L. Imbert, "A full RNS implementation of RSA", *IEEE Trans. Comput*., vol. 53, no 6, pp. 769–774, June 2004.

[10] Y. Liu, and E.M.-K Lai, "Design and implementation of an RNSbased 2-D DWT processor", *IEEE Trans. on Consumer Electronics*, vol. 50, no. 1, pp. 376-385, Feb. 2004.

[11] R. Zimmermann,―Efficient VLSI implementation of modulo (2^n □1) addition and multiplication,‖ in *Proc. 14th IEEE Symp. Comput. Arithm.*, Adelaide, Australia, Apr. 1999, pp. 158–167.

[12] Z.Wang, G. A. Jullien, andW. C.Miller, ―An efficient tree architecture for modulo (2^n □1) multiplication,‖ *J. VLSI Signal Process. Syst.*, vol.14, no. 3, pp. 241–248, Dec. 1996.

[13] A. Curiger, H. Bonnenberg, and H. Kaeslin, ―Regular VLSI architectures for multiplication modulo (2^n □1) ,‖ *IEEE J. Solid-State Circuits*,vol. 26, no. 7, pp. 990–994, Jul. 1991.

[14] L. Leibowitz,―A simplified binary arithmetic for the fermat number transform,‖ *IEEE Trans. Acoust., Speech, Signal Process.*, vol. ASSP-24, pp. 356–359, May 1976.

[15] J.W.Chen, R.H.Yao and W.J.Wu,Efficient ―modulo (2^n □1) multipliers,‖ *IEEE Trans. VLSI systems*., vol. 19, no 12, pp. 2149–2157, Dec. 2011