Adder /Subtractor for Residue Moduli

Chandana[1], P.Rajini[2]
M.Tech

***Abstract*- Efficient modular adders and subtractors for arbitrary moduli are key booster of computational speed for high cardinality Residue Number Systems as they rely on arbitrary moduli set to expand the dynamic range. This paper proposes a new unified modular adder/subtractor that possesses a regular structure for any modulus. Compared to the latest modular adder/subtractor, which works for modulus in the forms of 2n±1 the proposed design is on average faster and consumes less hardware area and lower power for 'n' ranging from 4 to 8.**

I. INTRODUCTION

Fourier transform (FFT) and discrete cosine transform (DFT) computations have been made. The design implements modular subtraction by subtracting the subtrahend from the corresponding modulus followed by the modular addition. This method avoids the use of fused adder/subtractor but requires additional constant subtraction, which impacts the speed. The data paths of designs and are heavily occupied by additions and subtractions. The overall speed of the system is thus predominated by how well these modular adders and subtractors Residue Number System (RNS) has become a promising alternative number system for digital system implementation in recent years. The key success for RNS-based computations is its carry-free additions and subtractions in residue domain. Besides, RNS-based computations are also inherently fault tolerant. Attempts to leverage RNS for the acceleration of fast are optimized.Due to the end-around and complementary end-around carry properties, hardware implementations of modular $2^n \pm 1$ addition and subtraction can be made as efficient as their binary counterparts. The problem with this special moduli set is its limited dynamic range or parallelism. In order to expand the dynamic range of the RNS with minimal negative impact on the arithmetic speed, extra coprime moduli of comparable word-length have to be added.

II. PROPOSED UNIFIED MODULAR ADDER/SUBTRACTOR

A. Background

In an RNS formed by N coprime integers $\{m_1, m_2, ..., m_N\}$,an integer X can be represented by using an N-tuple $(x_1, x_2, \ldots, x_N)$, where mi and xi are known as modulus and residue digit,respectively. xi is computed by finding the least non-negative remainder of X divided by mi ($xi = |X|_{mi}$). Let Z be the result of an arithmetic operation acted upon integers, X and Y.

B. Circuit Architecture

Fig. 1 depicts the computations of w and v for m= 11 and n = 4. The terms in dotted-line boxes are used only for the detection of the conditions of $v < 2^n$and $w \geq 2^{n+1}$. They are not involved in the addition operations for $|W|_{2^n}$ and $|V|_{2^n}$.

The computations of w and v consist of two levels of additions. The first level involves the additions of the first three terms, i.e., x+ ($y \oplus s$) + ($2^n \oplus s$) and x + ($y \oplus s$)+($m \oplus s$) , for the computation of w and v, respectively. Since one of the terms is a constant, this first level of additions can be implemented using half-adder-like (HAL) cells.

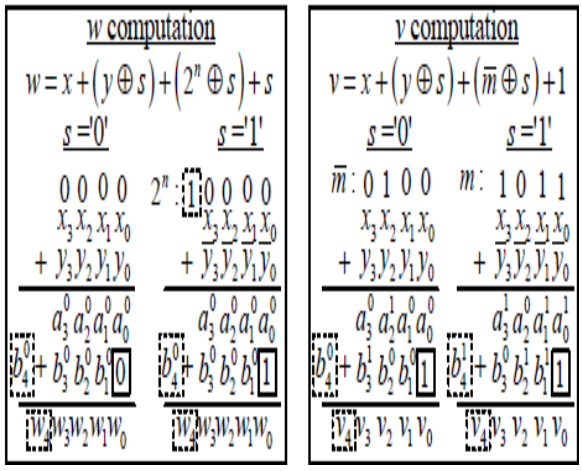

FIG 1.Computation of W and V for m=11 and n=4

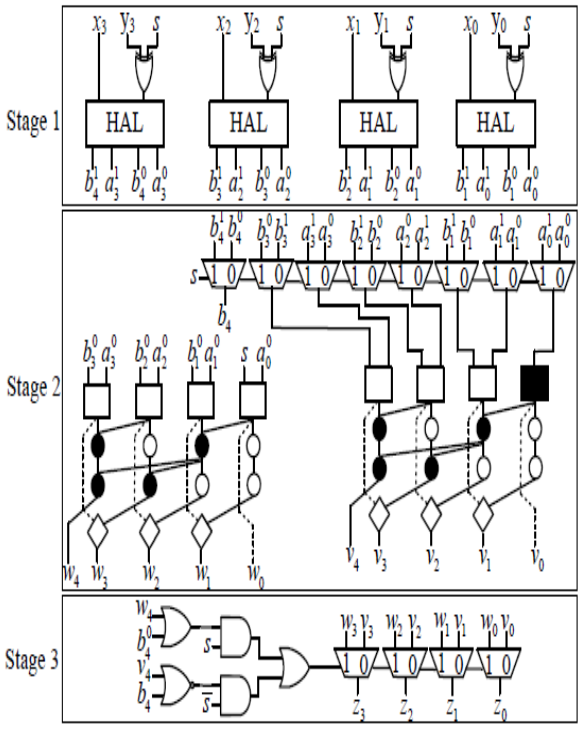

FIG 2. Proposed Modular Adder/Subtractor for m=11 and n=4

In this section, the proposed unified modular adder/subtractor depicted in Fig. 2 is evaluated and compared against the latest design. The designs are first analyzed using unit-gate model before they are synthesized and optimized. Two designs are proposed in, which are Adder/subtractorI and Adder/subtractor II. The former can be implemented for moduli in the forms of 2^n -k and $2^n + k$ but the latter is limited to only moduli of form $2^n + k$ for odd k and has no speed and area advantage when n is less than 12 according to the synthesis result. Therefore, the adder/subtractorsI for moduli 2^n-k is implemented for comparison. The performances of the proposed design and adder/subtractorI are analyzed with n = 4, 5, 6, 7, and 8. For each n, three moduli in the forms of $2^{n-1}+3$, 2^n-2^{n-2} and 2^n-3 are chosen.

C. Unit-Gate Analysis

The unit-gate analysis is performed based on the model, where a two-input monotonic logic gate, such as *AND*, *OR*, *NAND* and *NOR*, is considered to have one unit of area and one unit of delay; Both *XOR* gate and MUX have two units of area and two units of delay; The area and delay of an inverter are assumed to be negligible. In addition, the area and delay of a full adder are counted as seven units and four units, respectively.Each HAL cell in Stage1 of the proposed unified adder/subtractor has four units of area and two units of delay each. Since Stage1 consists of n HAL cells and n *XOR* gates, its total area and delay are 6n units and 4 units, respectively. In Stage 2, two PPAs are required for w and v computations. Since there is only one input at the least significant bit (LSB) position, the propagate, generate and half-sum generation of PPA for v computation can be simplified.

SINTHESYZED RESULTS:

n	m	AREA(μm^2)	DELAY(ns)
		PPA	CPA
4	11	874	666
4	12	718	651

III. CONCLUSION

The simplification of range detection criteria leads to a regular unified modular adder/subtractor architecture. In most cases, the proposed design is faster, smaller and consumes less power than the latest design.

REFERENCES

[1] R. B. Are and K, Rajan, "An RNS based transform architecture for H.264/AVC," in 2008 IEEE Region 10 Conf. (TENCON 2008), Hyderabad, India, Nov. 2008, pp. 1-6.

[2] F. J. Taylor, G. Papadourakis, A. Skavantzos, and A. Stouraitis, "A radix-4 FFT using complex RNS arithmetic," IEEE Trans. Comp., vol. C-34, no. 6,pp. 573–576, Jun. 1985.

[3] P. Fernandez, A.Garcia, J. Ramirez, L. Parrilla, and A. Lloris, "A RNS based matrix-vector-multiply FCT architecture for DCT computation," in Proc. 43rd IEEE Midwest Symp. Circuits Syst., Lansing, MI, Aug. 2000, vol.1, pp. 350–353.

[4] G. Lakhani, ''VLSI design of modulo adders/subtractors,'' in Proc. IEEE Int. Conf. Comp.Design: VLSI Comps. & Processors (ICCD 92), Cambridge,MA , Oct. 1992, pp. 68-71.

[5] C. Efstathiou, I. Voyiatzis, "Handling zero in diminished-1 modulo 2n+1 subtraction", in Proc.

of 3rd Int. Conf. Signals, Circuits and Systems (SCS09), Medenine, Tunisia, Nov. 2009, pp. 1-6.

[6] P. Matutino, H. Pettenghi, R. Chaves, and L. Sousa, ‘‘RNS arithmetic units for modulo {2n ± k},’’ in 2012 15th Euromicro Conf. Digital System Design (DSD), Izmir, Turkey, September 2012, pp. 795 -802.

[7] R. Patel, M. Benaissa, N. Powell, and S. Boussakta, ‘‘Novel power-delayarea- efficient approach to generic modular addition,’’ IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 54, no. 6, pp. 1279--1292, Jun. 2007.

[8] A. A. Hiasat, ‘‘High-speed and reduced-area modular adder structure for RNS,’’ IEEE Trans. Comput., vol. 51, no. 1, pp. 84--89, Jan. 2002.

[9] H. T. Vergos, C. Efstathiou, and D. Nikolos, ‘‘Diminished-one modulo 2n+1 adder design,’’ IEEE Trans. Comput., vol. 51, no. 12, pp. 1389-1399,Dec. 2002.