Diminished-One Modulo 2^n +1 Adder Using Circular Carry Selection

Aiswarya S
Dept. of ECE
New Horizon College of Engineering and Technology
Bangalore, India

***Abstract*—The diminished-one modulo 2^n+1 addition is an important arithmetic operation for a high-performance residue number system. This paper, is an attempt to implement a new circular-carry-selection (CCS) technique for modulo 2^n+1addition in the diminished-one number domain. The architecture design of CCS modular adder is simple and regular for various bit-width inputs.**

Keywords— modulo 2^n+1 addition, residue number system, circular-carry-selection

I. INTRODUCTION

The proposed CCS diminished-one modulo adder has been introduced and developed to derive the most compromising design in terms of area, delay and power. For a large bit-width requirement, this CCS modular adder is realized by the combination of CCS addition blocks, CCG and MUX to lead into the simple and efficient. The VLSI implementation of CCS modular adder indeed has better area-delay and delay-power performances over conventional designs.

II. DIMINISHED ONE MODULO 2^n+1 ADDER

A. *Residue number system*

Residue number system (RNS) is a non-weighted number system which exhibits a parallel carry-free arithmetic feature in digital signal processing. RNS is used in the implementation of fast arithmetic and fault-tolerant computing. Three properties of RNS make them well suited for these. The first is absence of carry-propagation in addition and multiplication, carry-propagation being the most significant speed-limiting factor in these operations. The second is, since the residue representations carry no weight-information, an error in any digit-position in a given representation does not affect other digit-positions. And ¬¬ third is that there is no significant-ordering of digits in an RNS representation, which means that faulty digit-positions may be discarded with no effect other than a reduction in dynamic range.

A great deal of computing now takes place in embedded processors, such as those found in mobile devices, and for these high speed and low-power consumption are critical; the absence of carry-propagation facilitates the realization of high-speed, low-power arithmetic. Also, computer chips are now getting to be so dense that full testing will no longer be possible; so fault-tolerance and the general area of computational integrity have again become more important. Lastly, there has been progress in the implementation of the difficult arithmetic operations. In any case, RNS is extremely good for many applications such as digital signal processing, communication engineering, computer security (cryptography), image processing, speech processing, and transforms in which the critical arithmetic operations are addition and multiplication.

In an RNS based application, every number X is represented by a sequence of residues $X_1, X_2, \ldots X_M$., where Xi is X mod Pi , Pi should be $1 \le i \le M$, the base of the RNS should be pair wise relative prime integers. A two operand RNS operation, suppose ◇,

$$(Z_1, Z_2, \ldots Z_M)=(X_1, X_2, \ldots X_M) \diamond (Y_1, Y_2, \ldots Y_M),$$

$$Z_i =(X_i \diamond Y_i) \bmod pi$$

For most RNS applications ◇ is either addition, subtraction, or multiplication. Since the computation of Zi only depends upon Xi, Yi, and pi, each Zi is computed in parallel in a separate arithmetic unit, often called channel. Moduli choices of the form $\{2^n-1, 2^n, 2^n+1\}$ have received significant attention because they offer very efficient circuits in the area x time.

Addition in such systems is performed using three channels. Because they have efficient combinational convertors to and from the binary system.

B. *Modulo 2^n+1 Arithmetic*

Many moduli sets such as {2n-1, 2n, 2n +1}, {2n-1, 2n, 2n +1, 22n +1}, and {2n-1, 2n, 2n +1, 2n-1 +1}, etc. are frequently utilized for designing successful RNS-based DSP applications. Among these moduli sets, the arithmetic in modulo 2^n-1 type or 2^n type channel only handles 'n' bit operands and the corresponding modulo operation is easy to design. On the contrary, the arithmetic in modulo 2^n+1 type channel computes 'n+1' bit operands and its modulo operation is more complex to implement, such that it mainly dominates the performance of the whole RNS system in terms of area, delay and power. Therefore, the 2^n+1 type modulus is the significant and complicated modular element in many moduli sets.

In this paper the focus is on the design subject of an efficient modulo 2^n+1 addition. Given two 'n+1' bit inputs A and B in the range $[0, 2^n]$, the modulo 2^n+1 addition is defined

By <A+B> 2^n+1 .The diminished-one number arithmetic was adopted to design an efficient modulo 2^n+1 adder. For a diminished-one modulo adder, the inputs A and B are decreased by one to obtain diminished-one data A*=A-1 and B*=B-1 which have n-bit width. The representation of 0 is

treated in a special way. Therefore, the diminished-one modulo 2^n+1 addition can be designed by n-bit adder and modulo function. This leads to the resulting modular adder be suitable for constructing a high-speed RNS addition.

Several architectures have been proposed for modulo $2^n + 1$ arithmetic components for each of the two representations, including parallel-adders, multi-operand adders and residue generators.

For modulo $(2^n +1)$ addition, the diminished one number system is often used, where the number A is represented by $A^{\prime}= A-1$ and the value 0 is not used or treated separately (i.e., requires an additional zero indication bit which is omitted here)

Ordinary addition in this number system looks as follows:

$A+B=S$

$(A^{\prime}+1)+(B^{\prime}+1)=S^{\prime}+1$

$A^{\prime}+B^{\prime}+1=S^{\prime}$

The sum of a diminished-1 modulo adder is derived according to the following cases:

- When none of the input operands is zero (az, bz ≠ 0) their number parts $A^{\prime}$ and $B^{\prime}$ are added modulo 2n +1. This operation as discussed in the following, can be handled by CLA.
- When one of the two inputs is zero the result is equal to the non-zero operand.
- When both operands are zero the result is zero.

In any case that the result is equal to 0 (cases 1 or 3), the zero-indication bit of the sum needs to be set and the number part of the sum should be equal to the all-zero vector. According to the above, a true modulo addition in a diminished-1 adder is needed only in case 1, while in the other cases the sum is known in advance.

When none of the input operands is zero, az, bz ≠1, the number part of the diminished-1 sum is derived by the number parts $A^{\prime}$ and $B^{\prime}$ of the input operands as follows:

$(A^{\prime}+B^{\prime}+1) \bmod (2^n+1) = A^{\prime}+B^{\prime}+1- (2^n+1)$ is

$= (A^{\prime}+B^{\prime}) \bmod 2^n$, if $A^{\prime}+B^{\prime}+1 \geq 2^n$

$=A^{\prime}+B^{\prime}+1$, otherwise

The sum $A^{\prime}+B^{\prime}$ is incremented if $A^{\prime}+B^{\prime}+1 < 2n$, i.e., if cout = 0. Thus, modulo (2^n+1) addition can be realized by the CCS in DS-CLA with cin = cout (i.e., with an inverter in the carry feedback path)

$(A^{\prime}+B^{\prime}+1) \bmod (2^n+1) = (A^{\prime}+B^{\prime}+C^{\prime}out) \bmod 2^n$

The diminished one number representation, however, often requires the conversion from and to the normal number representation using incrementation / decrementation, which might be too expensive when compared to its advantages.

III. Implementation Conventional 2^16+1 Adder Using CLA Technique

Here the modulo $2^n + 1$ addition of A and B, hereafter denoted by $|A+B|_{2^n+1}$,

Where A*=an-1*,…,a1*, a0* and B*=bn-1*,…,b1*, b0* are two (n + 1)-bit binary numbers in the range [0, 2n], we have that.

$|A+B|_{2^n+1} = A + B – (2^n + 1)$, if $A + B \geq (2^n + 1)$

$|A+B|_{2^n+1} = A + B,$ otherwise

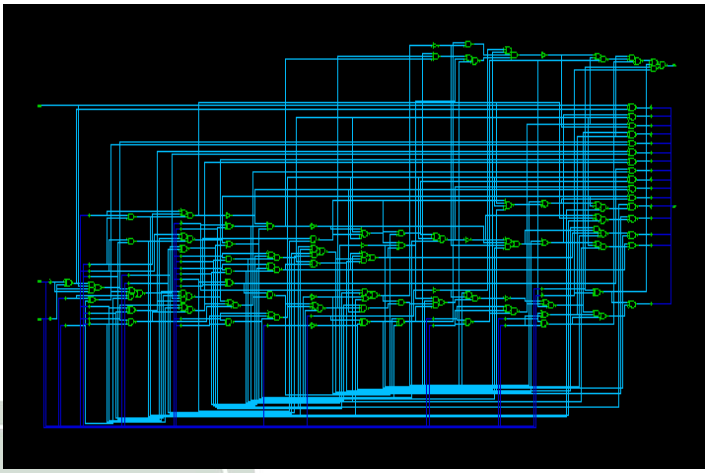

Fig. 1. 2^16+1 Adder Using Carry Look Ahead Adder Technique On Synopsis® Design-Vision.

In this conventional CLA, the area and the power consumption were found to be much larger and also the logic elements used here is quite large. So, introducing a new CCS technique for diminished one modulo 2^n+1 adder.

IV. Implementation Of The Proposed Diminished One Modulo 2^n+1 Adder Using CCS Technique

Assume that two -bit diminished-one operands are

A* =A-1 and B*=B-1 ie,

A-1=an-1*,…,a1*, a0* and B-1=bn-1*,…,b1*, b0*

The sum derived by performing modulo 2^n+1 addition of A* and B* can be changed into the uncomplicated function with performing modulo 2^n addition as the following expression:

$S^* = <A^*+B^*+(Cn-1)^{\rightarrow}> 2^n$

Where Cn-1 is regarded as an original carry-out bit of (A*+B*) .Denote the carry generate term and the carry propagate term as

gi* = ai*.bi*

pi* = ai* bi* where stands for XOR function.

According to CLA function, the carry term of Ci* is derived by

$C_i^*=g_i^*+$

$$\sum_{j=0}^{i-1}\left(\prod_{k=j+1}^{i} pk*\right) gj* + c* - 1 \left(\prod_{k=0}^{i}\right.$$

for i=0,. . . ,n-1.

where c*-1 is the carry-in bit. Based on CCS technique, we set $c^*-1=(Cn-1)^{\rightarrow}$

The Boolean function of each sum bit can be expressed as follows:

$S_i^* = C_{i-1}^* \oplus P_i^* = (g_{i-1}^* + \sum_{j=0}^{i-2}(\prod_{k=j+1}^{i-1} pk^*)gj^* + \overrightarrow{Cn-1}\prod_{k=0}^{i-1} pi) \oplus P^*$

Where $C_{n-1} = g^*_{n-1} +$ Since $\epsilon \{0,1\}$.

we have, $s_i^* = \{s^*_{i,1} = (g^*_{i-1} + \sum_{j=0}^{i-2}(\prod_{k=j+1}^{i-1} pk^*)gj^* + \prod_{k=0}^{i-1} pk^*) \oplus pi$

if $c_{n-1} = s_i^* = \{ s^*_{i,0} = (g^*_{i-1} + \sum_{j=0}^{i-2}(\prod_{k=j+1}^{i-1} pk^*)gj$, if $c_{n-1}=1$

Here a new circular-carry-selection (CCS) technique is presented to design an efficient diminished-one modulo adder. The proposed CCS modular adder simply consists of dual-sum carry look-ahead (DS-CLA) adder, circular-carry generator (CCG) and multiplexer (MUX). The DS-CLA adder is designed to generate two different modulo sums in parallel. The carry-out bit computed by CCG is then used to circularly control the MUX for obtaining the correct modulo result.

We can easily design a DS-CLA adder to produce S*i,1 and S*i,0 two sums and since they have the same term

$g_{i-1}^* + \sum_{j=0}^{i-2}(\prod_{k=j+1}^{i-1} pk^*)gj$

.ie, they can share the circuit from the view point of hardware design. At the same time, Cn-1 generated by the CLA function is circularly used to control MUX for getting the correct outputs S*'s. The block diagram of CCS diminished-one modulo 2^n+1 adder is shown in Fig. 2, which is simple and regular. Fig. 2 shows the detailed logic design for CCS diminished-one modulo 2^4+1 adder.

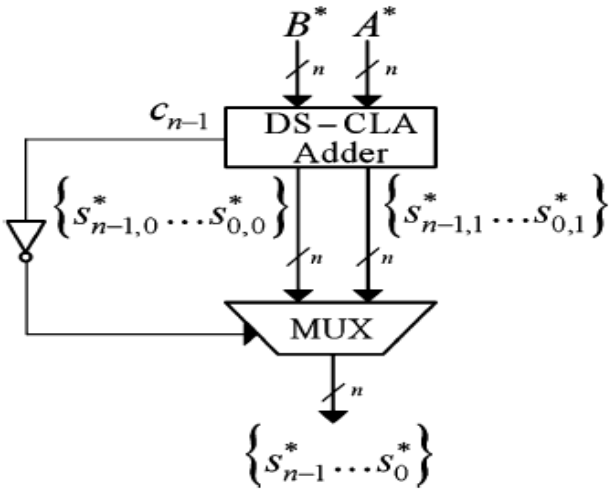

Fig. 2. Block Diagram Of CCS Diminished One Modulo 2^n+1 Adder.

A. *Implementation Of Modulo 2^4+1 Adder Using CCS Technique*

Here will demonstrate one example.

Suppose $n = 4$

$A = 6$,

$B = 3$,

$A* = 5 = 0101$,

$B* = 2 = 0010$,

$S^* = \langle A^*+B^*+\rangle_{2^n} = (5+2+1) \bmod (16) = 8 = 1000_2$.

The carry propagate term $p*$ and the carry generate term $g*c$ can then be obtained as

$p* = 0111$

$g* = 0000$

Then the modulo sum is computed with the help of $Cn-1$. Here $Cn-1=C_3=0$;

The modulo sum is $S^*_{i,1}$

$S^*_{3,1} = (g_2^*+p_2^*g_1^*+p_2^*p_1^*g_0^*+p_2^*p_1^*p_0^*) \oplus p_3^*=1 \oplus 0=1$

$S^*_{2,1} = (g_1^*+p_1^*g_0^*+p_1^*p_0^*) \oplus p_2^*=1 \oplus 1=0$

$S^*_{1,1} = (g_0^*+p_0^*) \oplus p_1^*=1 \oplus 1=0$

$S^*_{0,1} = p_0^*=0$

$S^*=1000$

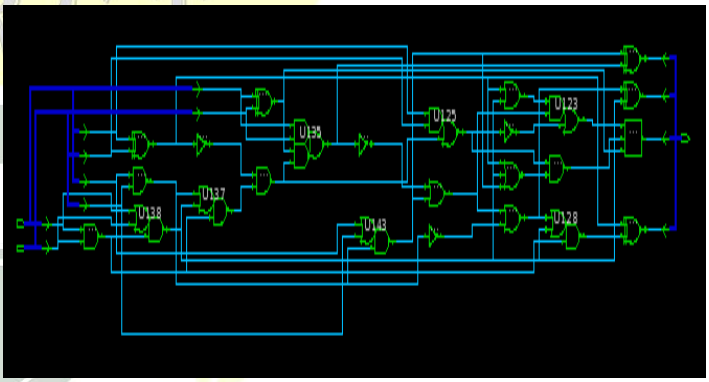

Fig. 3. Logic Circuit Of CCS Diminished One Modulo 2^4+1 Adder.

B. *Implementation of the low power with reduced area modulo 2^16+1 adder using ccs technique*

In order to speed up the CCS modular adder for the large dimension of 'n' , we partition the n-bit CCS modular adder in to m 'r 'bit CCS addition blocks and a fast CCG where n= m x r . Fig. 4 illustrates the general (m x r)-bit CCS modular adder architecture. Both input data are divided into block inputs are:

A * = {Am-1*,…, A0*} and B * = {Bm-1*,…, B0*}

where,

At* = a* (t+1) r-1,…, a* tr+1 a* t r and Bt* = b* (t+1) r-1,…, b* tr+1 b* t r

For t = 0, 1, 2, ……,(m-1).

The block sum is St* = s* (t+1) r-1,…, s* tr+1 s* t r

derived by A*t +B* t + k* t-1

V. RESULTS

Design view On Synopsis® Design-Vision :

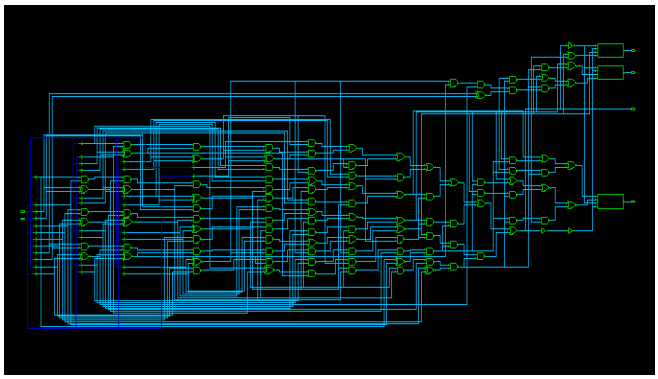

Fig. 4. CCS Diminished One Modulo 2^16+1 Adder On Synopsis® Design-Vision.

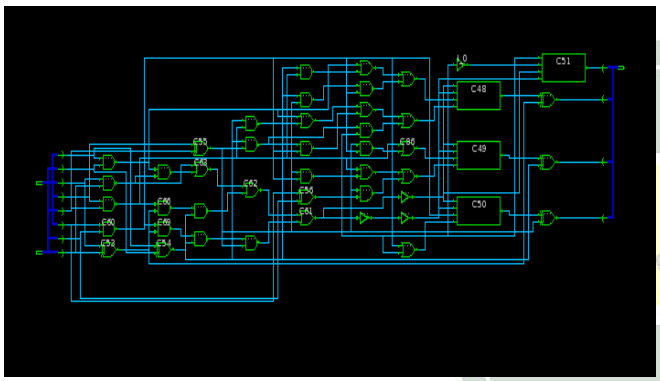

Fig. 5. Modified CCS Diminished One Modulo 2^4+1 Adder On Synopsis® Design-Vision.

TABLE I. COMPARISON BETWEEN DIMINISHED ONE MODULO 2^16+1 ADDER USING CLA AND WITH CCS

	AREA (cells)	POWER (µW)	DELAY (nSec)
Modulo 2^16+1 Using CLA	184	33.3226	13.08
Modulo 2^16+1 Using 4x4 CCS	83	11.1618	17.58

TABLE II. COMPARISON BETWEEN DIMINISHED ONE MODULO 2^4+1 ADDER WITH MODIFIED DIMINISHED ONE MODULO 2^4+1 ADDER(USING CCS)

	AREA(cells)	POWER(µW)	DELAY(nSec)
Modulo 2^4+1 Adder	46	9.4128	9.15
Modified	39	6.47	7.96

REFERENCES

[1] 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.

[2] R. Zimmermann, "Efficient VLSI implementation of Modulo 2^n+1 addition and multiplication," in Proc. 14th IEEE Symp. Computer Arithmetic, Apr. 1999, pp. 158–167.

[3] H. T. Vergos, C. Efstathiou, and D. Nikolos, "Diminished-one modulo 2^n+1 adder design," IEEE Trans. Comput., vol. 51, no. 12, pp. 1389–1399, Dec. 2002.

[4] L.M. Leibowitz, "A simplified binary arithmetic for the fermat number transform," IEEE Trans. Acous., Speech, Signal Process., vol. 24, pp. 356–359, 1976.

[5] Harvey l. Garnert ," The residue number system", IEEE transactions on electronic computers, pp.143-159,june.1959.