RESEARCH ARTICLE OPEN ACCESS

Towards Efficient Modular Adders based on Reversible Circuits

*Dr.M.Jagadeeswari,
*Head of the Department, ECE, Sri Ramakrishna Engineering College, Tamilnadu, India
Email: jagadeeswari.m@srec.ac.in
**B.Sivadharini, ***V.Rinissha, ****P.Sindhoora
**ECE, Sri Ramakrishna Engineering College, Tamilnadu, India
Email: sivadhrn@gmail.com
***ECE, Sri Ramakrishna Engineering College, Tamilnadu, India
Email: infantrinissha@gmail.com
****ECE, Sri Ramakrishna Engineering College, Tamilnadu, India
Email: sindhoorap.30@gmail.com
Corresponding Author Email: sindhoorap.30@gmail.com, Phone no: +917358829227

--*************************-----------------------------------

Abstract:

Reversible logic is a reckoning standard that has attracted momentous attention in recent years due to its properties that lead to ultra-low-power reliable circuits. Reversible circuits are fundamental in executing quantum computing. Since addition is an essential operation in designing efficient adders it is a key element in the research of reversible circuits. RNS has been an influential tool to come up with parallel and fault-tolerant implementations of computations in which additions and multiplications are assertive. In our project, we have implemented a combination of RNS and reversible logic. The parallelism of RNS is highly influential to increase the accomplishment of reversible computational circuits. Since modulo adders play a pivotal role in any RNS, we here proposed modular adders using reversible logic. The proposed adders have been synthesized using Xilinx tool and from the experimental results it is identified that modulo adders could be designed by means of reversible gates with minimum expenditure in assessment to regular reversible adders.

Keywords — **Residue Number System (RNS), Parallel-Prefix Adder and Reversible circuits.**

--*************************-----------------------------------

I. INTRODUCTION

Researchers in academe and trade believe that Moore's law is ending, and even recently delivered deep-submicron transistors are not considerably additional economical than their previous generations. Therefore, new computing paradigms ought to be investigated to beat the anticipated performance wall which might be reached in 2020. This rebooting of computing should be supported novel strategies at totally different computing levels of style abstraction, together with arithmetic logic gate level, to modify the challenges of the rising applications sort of a deep convolutional neural network (DNN) and internet-of- things (IoT).

Residue range Systems (RNS) has been associate authoritative tool to produce parallel and fault-tolerant implementations of computations wherever additions and multiplications RNS structure assertive. In this work, we've enforced a combination of RNS and reversible logic. The correspondence of RNS is incredibly authoritative to increase the accomplishment of reversible procedure circuits. Since modulo adders RNS structure elementary elements in any RNS, we have enforced standard adders like adders, victimizating reversible logic. RNS is used these days to understand conjointly energy-efficient and high performance implementation of varied rising applications, like deep neural networks, communication networks and cloud storage. This illustration is allowable by the remainder theorem, that asserts that, if N is that the merchandise of the moduli, there is, in associate interval of length N, precisely one whole number having any given set of standard values. A residue numeral system is outlined by a group of k integers, known as the moduli, that RNS structure usually purported to be pairwise coprime (that is, any 2 of them have a greatest common live adequate one), forementioned as a result of the moduli.

The capability of RNS to perform extraodinary parallel and carry-free arithmetic is compatible temperament for taking advantage of the selections of reversible circuits. However, later, all the offered RNS structures RNS structure designed for ASIC implementation, a rethinking of RNS architectures ought to be performed to adapt them to the properties of reversible circuits. The very important part of a neighborhood architecture of RNS systems is standard addition since all elements of RNS together with forward and reverse conversion are supported standard additions. This work presents the first implementation of modulo adders supported by reversible gates. For these typical adders, that RNS structure regularly utilised in RNS structures, parallel-prefix and ripple-carry architectures are measured.

In this work, we tend to propose the joint usage of these two unconventional computing approaches, Residue Number System and Reversible Computing, to understand associate ultra-efficient computing paradigm for the rising applications. The capability of RNS to perform extraodinary parallel and carry-free arithmetic is compatible temperament for taking advantage of the selections of reversible circuits. However, later, all the offered RNS structures RNS structure designed for ASIC implementation, a rethinking of RNS architectures ought to be performed to adapt them to the properties of reversible circuits. The very important part of a neighborhood architecture of RNS systems is standard addition since all elements of RNS together with forward and reverse conversion are supported standard additions.This work presents the first implementation of modulo adders supported by reversible gates. For these typical adders, that RNS structure regularly utilised in RNS structures, parallel-prefix and ripple-carry architectures are measured

II. Residue Number System Architecture

The first step to design a RNS is to pick out a moduli set consistent with the target application constraints and necessities. The moduli set consists of pair-wise comparatively prime numbers , being the dynamic vary the sequence of integers which will be unambiguously depicted in RNS, i.e. Among these moduli, the best one to take care of is that the 2n, is nothing but does not need any specific modular arithmetic, jut the circuits for binary arithmetic.

Apart from that, the foremost frequent co- prime range in moduli sets for RNS is 2n-1, since moduli 2n+1 is additional complicated and its illustration needs an extra bit. The main arithmetic blocks of RNS are the forward convertor, the modular arithmetic within the channels, and therefore the reverse convertor [12]. The forward convertor interprets the weighted binary range (X) to the residues (xi's), consistent with the moduli, as:

$$X \xrightarrow{Forward\ Conversion} (x_1, x_{2.....}\ x_n) \quad (1)$$

Where x_i= X mod m_i=|X|m_i for i = 1…n (2)

Note that mod indicates the rest of the whole number division of X by mi. Then, we should consider two numbers A and B as follows:

$$A=(a_1, a_{2,}a_3 \ldots..a_n) \quad (3)$$

$$B=(b_1, b_{2,}b_3 \ldots..b_n) \quad (4)$$

modulo arithmetic operations are often performed on residues as follows:

$$S = A \bullet B= (a_1, a_{2,}a_3 \ldots..a_n) \quad (5)$$

where

$$S_i = |a_i \bullet b_i|_{m_i}, \bullet \text{€}\{+ , -, \times\} \quad (6)$$

Finally, a reverse converter maps the results in the RNS domain to the regular weighted illustration, by using, as an example, the Chinese remainder theorem (CRT). Other RNS operations like sign detection, magnitude comparison and overflow handling are nonmandatory, consistent with the target application, and more durable to perform within the RNS domain. It ought to be mentioned that general division cannot directly be performed in RNS, however division by a relentless, one among the moduli of the set, i.e. scaling, is simpler to perform.

III. Reversible Gates

Reversible circuits give us a one-to-one mapping among inputs and outputs, thus inputs can be recovered from outputs. This effective feature tends to design efficient low power circuit by saving the power drastically. Regular digital gates are irreversible. Reversible gates can be built as basic structures to design reversible logic circuits. Some of the popular reversible gates are Feynman, Peres and HNG gates.

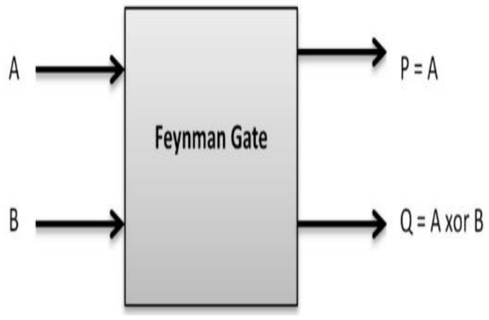

Fig. 1. Feyman gate

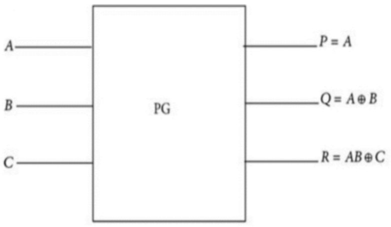

Fig. 2. Peres gate

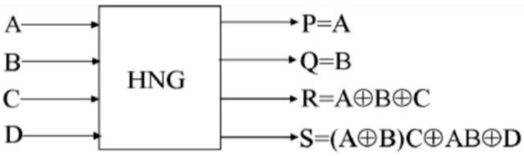

Fig. 3. HNG gate

The Feynman is also called as controlled not (CNOT) gate. It is often utilized in reversible logic circuits because it will provide Ex-OR and also the copy and complement of the input. As reversible gates cannot have advantage of fan-out, these gates shall be used to attain two copies of the similarlv input by making another input of the gate to the zero-logic level. Likewise, by changing the second input of the Feynman to one-logic level, we can attain the copy of another input.

When considering the reversible logic, the input given to the logic are equal their outputs of the gates so as to achieve a one-to-one mapping. This logic processes a set of output bits for every set of unique input bits. This avoids the lack of information which leads to wastage of power. In reversible logic fan-out is impossible and feedback and loops are not entertained.

IV. Modular Adder Design Using Reversible Circuits

This section represents the reversible enactment of three modular adder constructions that are oftentimes applied to RNS.

A. RCA Based Modulo Adder

The Ripple Carry Adders with End Around Carry for modulo ‘2n-1’ addition of two ‘n’ bit numbers wants n Full Adders and n Half Adders in both the first and second stages respectively which is shown in Fig. 4. Like the Carry Select Adder, Full Adders can be realized with HNG gates. Also the Peres gate which is reversible shall be used in place of the Half Adders, where the third input bit is initialized to zero. The total quantum cost of the Ripple Carry Adders with End Around Carry for two ‘n’ bit is 6n+4n=10n because the quantum cost and depth of a single Peres gate is 3. Besides, the final quantum depth of the Ripple Carry Adders with End Around Carry is given as ((3×(n-1)+4+(3×(n-1)+5))Δ. Also, the final garbage output and constant inputs are 3n and 2n, respectively because in both the inputs either one of the inputs of Peres and HNG gates is zero and also two outputs of HNG and one output of Peres gates are not used.

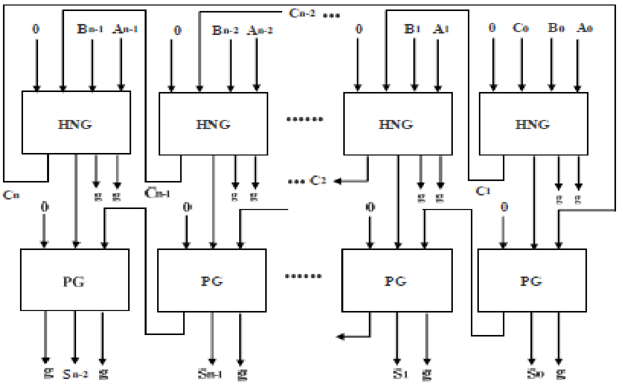

Fig. 4. The Ripple Carry Adder with End Around Carry using HNG and Peres reversible gates.

B. PPA Based Modulo Adder

The important block of a Parallel prefix adder is a carry-computation network that contains gray and black cells. There are various carry-computation networks that can be utilized for constructing Parallel Prefix Adders. The regular parallel-prefix adder structure is based on two popular methods namely Kogge stone adder and Brent-Kung adder. After comparing and analysing their individual characteristics, it is found that the Brent-Kung adder has low quantum cost when compared to the other prefix structures. Because of this advantage, the Brent-Kung adder has been chosen the reason is basic adder to style modulo 2n-1 adder with reversible logic gates.

The Brent-Kung adder has low quantum cost when compared to the other prefix structures which is shown in the Fig. 5. Because of this advantage, the Brent-Kung adder has been chosen the reason is basic adder to style modulo 2n-1 adder with reversible logic gates.

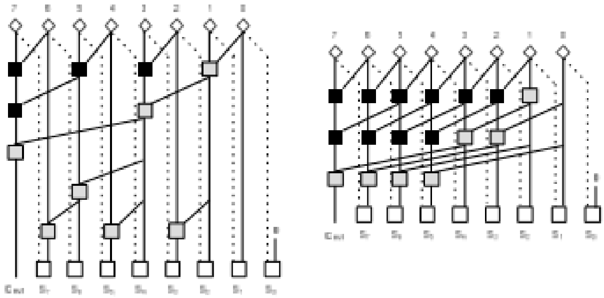

Fig. 5. The regular parallel-prefix adder structure of two types (left side) BrentKung and (right side) Kogge-Stone

The modulo 2n-1 Parallel prefix adder contains generate and propagate signal generation, prefix carry-computation network and post process to come up with the entire carry and add bits. The reversible logic implementation of Brent-Kung adder with the carry-computation network is completed. The propagate and generate signals ought to be computed exploitation the input bits.

$$P_i = a_i \oplus b_i$$
$$g_i = a_i\ b_i$$

This process can be easily simply done by a Peres gate with the next input made to zero. The propagate and generate signals can be achieved using the carry computation network.

$$P_{i:j} = P_{[i:k]}\ P_{[k-1:j]}$$
$$G_{[i:j]} = G_{[i:k]} + P_{[i:k]}\ G_{[k-1:jj]} = G_{[i:k]} \oplus P_{[i:k]}\ G_{[k-1:j]}$$

The black cell produce G[i:j] and P[i:j] using two peres gate. P[i:k] is repeated by considering the fan-out gate in the black cell. Besides, the grey cell simply wants one Peres gate. G[i:0] can be generated by a single peres gate in the grey cell.

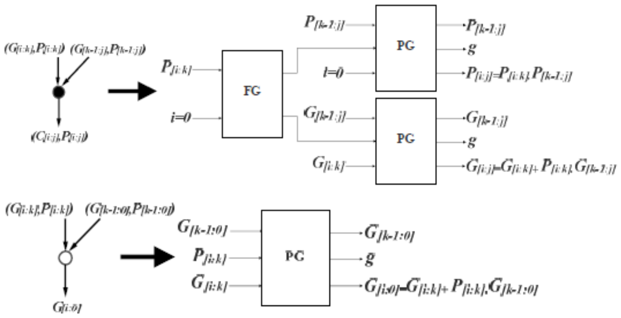

Fig. 6. The internal prefix cells implementation using Peres gates

The Post processing part involves a row of black cells to generate the *Cout*, i.e. End around Carry to the carries situated in the middle which is then processed by the sum cells. This generates the sum. The black cells in the final level are not similar to those that are in the internal cells because they have three inputs. Peres gates are effectively used to realize those cells. Feynman gates are used to generate the sum as only the Ex-OR gates are required.

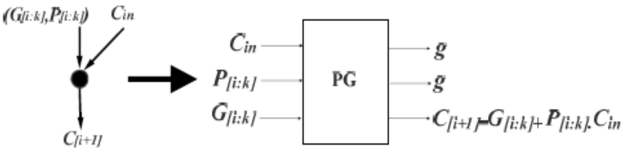

Fig. 7. The black cell used in the End Around Carry level of the parallel prefix modular adder.

Finally, as shown in Fig. 5, the Post processing part involves a row of black cells to generate the *Cout* , i.e. End around Carry to the carries situated in the middle which is then processed by the sum cells . This generates the sum. The black cells in the final level are not similar to those that are in the internal cells because they have three inputs. Peres gates are effectively used to realize those cells. Feynman gates are used to generate the sum as only the Ex-OR gates are required. The total amount of quantum price and depth likewise as a wide range of constant inputs and garbage outputs in case of the regular Brent-Kung adder is calculated. Therefore, it is simply necessary to introduce one level of black cells to derive the quantum depth and quantum price for the projected modular adder.

V. Perfomance Comparison

The Area, Power and Delay of the different modulo adders and the total quantum cost and depth as well as number of constant inputs and garbage outputs are presented in Table I and II respectively. It is observed that the projected 2n-1 modulo adders have higher price and depth than the equivalent binary adders. Therefore, it is concluded that planning prefix-based modular adder leads to less overhead than RCA-based style, in reversible logic. Besides, it can be seen PPA based modulo adder which is quite frequently used in RNS circuits, can be implemented quite efficiently using reversible gates.

VI. Conclusion

This work presents the reversible design of modular adders which acts as the basic and elementary component of RNS based architectures. It is shown that a modular 2n-1 parallel prefix adder is often designed using small overheads when compared to the other modular adders. On analyzing the synthesized results, we can observe that the proposed modular Brent-kung adder is efficient among all the other modular adders when considering the area, power, quantum cost and depth. So, we can conclude that the proposed modular Brent kung adder is better in terms of all the parameters observed such as area, power, quantum cost, quantum depth and therefore is the efficient modular adder.

VII. Future Works

Now every day accuracy is the main goal to achieve with this fast processing environment and it will conjointly consumes less energy, previous conventional circuits are non reversible and due to which during communication of information when there is loss of information circuit dissipates energy because of reload of data in between communication channel from input to output vectors. As reversibility recovers energy loss and prevent bit error by together with fault tolerant mechanism. Reversiblity is gaining abundant quality in quantum computing. Thus we have got to make a circuit under optimized way in manner that it will be price effective within the sense of Gate price, delay, garbage and quantum cost taking all these in account we have to design the optimized circuit which are reversible and have capability to detect and correct the error throughout data transmission.

Table I Performance Comparison of Efficient Parameters of Reversible Modulo Adders

S.NO	TITLE	AREA(Gate count)	POWER (mW)	DELAY(ns)
1	Ripple Carry adder	156	499	24.170
2	Kogge stone adder	276	735	18.412
3	Brent Kung Adder	204	512	22.600

Table II Performance Comparison of Circuit Parameters of Reversible Modulo Adder

S.NO	TITLE	QUANTUM COST	QUANTUM DEPTH	CONSTANT INPUTS	GARBAGE OUTPUTS
1	Ripple Carry Adder	80	51	16	24
2	Kogge stone Adder	144	14	24	33
3	Brent Kung Adder	134	14	8	29

REFERENCES

[1] A. S. Molahosseini, A. Asadpoor, A. A. E. Zarandi and L.Sousa,(2018),"Towards Efficient Modular Adders based on Reversible Circuits," *IEEE International Symposium on Circuits and Systems (ISCAS),* Florence, 2018, pp. 1 -5.

[2] Alioto P, (2017),” Enabling the Internet of Things: From Integrated Circuits to Integrated Systems”, Springer.

[3] Chang C.H, Molahosseini A.S, Emrani Zarandi A.A, and Tay T.F,(2015), “RNS: A New Paradigm to Datapath Optimization for Low-Power and High-Performance Digital Signal Processing Applications,” *IEEE Circuits and Systems Magazine*, Volume 15, no. 4, pages (26-44).

[4] Conte T.M, DeBenedictis E.P, Gargini P.A, and Track E, (2017) “Rebooting Computing: The Road Ahead,” Computer, Volume 50, no. 1, pages (20-29).

[5] DeBenedictis E.P, Mee J.K, and Frank M.P, (2017) “The Opportunities and Controversies of Reversible Computing,” Computer, Volume 50, no. 6, pages (76-80).

[6] Hiasat A, (2017) “An Efficient Reverse Converter for the Three-Moduli Set (2^{n+1}-1, 2^n, 2^n-1),” *IEEE Transactions on Circuits and Systems-II*, Volume 64, no. 8.

[7] Kirti Batish, Shruti Pathak, Raghav Gupta, (2018) “Comparative Analysis for Performance Evaluation of Full Adders Using Reversible Logic Gates”, *International Conference on Intelligent Circuits and Systems.*

[8] Molahosseini A.S, Zarandi A.A.E, Martins P and Sousa L, (2017)“A Multifunctional Unit for Designing Efficient RNS-based Datapaths”,*IEEE Access*, accepted.

[9] Morrison, Matthew, Ranganathan, Nagarajan, (2011) “Design of a Reversible ALU Based on Novel Programmable Reversible Logic Gate Structures”, *IEEE Computer Society Annual Symposium on VLSI (ISVLSI),* Volume 56, pages (126-131).

[10] R. Chaves and L. Sousa,(2017) "Improving residue number system multiplication with more balanced moduli sets and enhanced modular arithmetic structures," in *IET Computers & Digital Techniques*, vol. 1, no. 5, pp. 472-480.

[11] Sousa L, Antão S, and Martins P, (2016) “Combining Residue Arithmetic to Design Efficient Cryptographic Circuits and Systems,” *IEEE Circuits and Systems Magazine*, Volume 16, no. 4, pages (6-32).

[12] Taha S.M.R, (2016),” Reversible Logic Synthesis Methodologies with Application to Quantum Computing”, Springer.

[13] Thapliyal, H, Ranganathan, N, (March 2011) “A new reversible design of BCD adder,” Design, Automation & Test in Europe Conference & Exhibition (DATE), Volume 15, pages (1-18).

[14] Vudadha C, (2012) “Design and Analysis of Reversible Ripple, Prefix and Prefix-Ripple Hybrid Adders,” *IEEE Computer Society Annual Symposium on VLSI (ISVLSI).*