# A Review on Residue Module Arithmetic's Adder and Sub-tractor using Reversible Gate 

Pragya Mishra*, Prof. Nishi Pandey** and Dr. Neelesh Gupta***<br>*M. Tech. Scholar, Department of Electronics and Communication, Truba College of Science and Technology, Bhopal<br>**_***Department of Electronics and Communication, Truba College of Science and Technology, Bhopal


#### Abstract

Due to the increasing spread of digital computing, investigation of various number representation systems in the digital field seems necessary. In general, the number representation systems regarding their applications can be classified in two areas: general-purpose and specific-purpose. Binary Digit Residue Number System (BD-RNS) is one of the specific-purpose and optimized number system. In Residue Number System-based systems, how to select moduli set and evaluate its performance is an important issue. The objective of this study is to propose a systemic performance evaluation method for RNS based on the properties of moduli set. By abstracting the inherent properties of moduli sets, such as the complexity of arithmetic units, utilization ratio of dynamic range, parallelism and balance between residue channels, this method can provide advices on moduli set selection and carry out performanceestimation before circuit's implementation.


Keywords: CMOS Technology, Reversible Gate, Feynman Gate, Peres Gate.

## Introduction

Residue Number System (RNS) is a non-weighted numerical system, in which a large integer is divided into several small integers. These small integers are computed independently and concurrently in multiplication and addition operations. There is no carry propagation between residue channels.
RNS is used in cryptography firstly, and then it is received intensive researches in digital signal processing (DSP) systems with intensive multiplication and addition operations.
For many RNS-based applications, the moduli set are the main factor for implementation complexity. This is because the complexity of modular multiplication and addition are related to the form of moduli set. Besides, the complexities of the operations, such as forward and backward conversion, scaling and sign detection, etc., also depend on the moduli set form. Many specific fonns of moduli set has been proposed. The commonly used three-channel muduli sets are proposed in [1-3].
In recent years, efficient schemes for modulo adder have been studied intensively [11]-[13]. Generally, modulo $2^{n} \square 1$ 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, used Booth encoding to realize, but depart from the diminished-1 arithmetic, which leads to a complex architecture with large area and delay requirements. For the second category, proposed diminished-1 adder with n-bit input operands. The adders 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.
The proposed new modulo adder 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.
The 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 $2+1$ adder by inverted $n$-bit adder.
Actually, the design in this letter is not the first reversible version ALU. Also gave an ALU design by generalizing the V shape design which can achieve five basic arithmetic-logical operations on two n -bit operands, but the structure is so simple that some functions cannot even get the right results, for example, we cannot calculate the ADD operation only using the bitwise exclusive-or of the two n-bit arguments| $\mathrm{A}>$ and| $\mathrm{B}>$ without considering the carry bit or only by setting the carry bit to the TRUE. The goal of this letter is to build a multi-functional circuit reasonably that conditionally performs one
of several possible arithmetic-logical operations on two operands $\mid \mathrm{A}>$ and $\mid \mathrm{B}>$ depending on control input data instructions. The following section is based on the assumption that the readers are familiar with the basics of reversible logic [5].

## Literature Review

Adib Armand et al. [1], Due to the increasing spread of digital computing, investigation of various number representation systems in the digital field seem necessary. In general, the number representation systems regarding their applications can be classified in two areas: general- purpose and specific-purpose. Binary Signed-Digit Residue Number System (BSD-RNS) is one of the specific-purpose and optimized number system. In fact with blending RNS that decreases the length of operands and BSD that has redundancy property, we can achieve BSD-RNS that can perform calculation in parallel. On the other hand, due to limited access to the energy resources, reducing power consumption can also increase system popularity. The addition unit as a basic computational unit can play an important role in overall system performance. Therefore, in this paper, it is intended first to introduce three basic adder structures for BSDRNS. Then we propose low power adders for the moduli set $\{2 \mathrm{n}-1,2 \mathrm{n}, 2 \mathrm{n}+1\}$ based on 2's complement, 1 -out-of-3, and Pos-Neg BSDRNS number system. Compared to conventional structure of BSD-RNS adders, proposed adders have $10 \%, 70 \%$, and $21 \%$ less power than the existing efficient BSD-RNS adders for 2's complement, 1 -out-of-3, and Pos-Neg encoding, respectively.

Jian Wang et al. [2], in Residue Number System-based systems, how to select moduli set and evaluate its performance is an important issue. The objective of this study is to propose a systemic performance evaluation method for RNS based on the properties of moduli set. By abstracting the inherent properties of moduli sets, such as the complexity of arithmetic units, utilization ratio of dynamic range, parallelism and balance between residue channels, this method can provide advices on moduli set selection and carry out performance estimation before circuit's implementation. Furthermore, we also propose a new multi-channel moduli set by introducing a new radix component in this paper. Performance analysis and comparison results show that the proposed multi-channel moduli set has better performance of dynamic range utilization ratio, parallelism and balance than that of the commonly used moduli set with the same number of channels.

Shugang Wei et al. [3], in this paper, high-speed Signed- Digit (SD) architectures of binary-to-residue and residue- to-binary conversions for residue number system (RNS) with the moduli set ( $2 \mathrm{n}, 2 \mathrm{n}-1,2 \mathrm{n}+1$ ) are proposed. The complexity of the conversions and residue arithmetic operations has been greatly reduced by using compact forms for the multiplicative inverse and the fast residue SD addition algorithm. The relationships of the proposed binary to- residue and residue-to-binary conversions using the residue SD numbers result in simpler hardware requirements for the converters. The primary advantage of our methods is that our conversions and arithmetic operations utilize the modulo m SD adders (MSDAs) only and the proposed basic circuits have high speed structures in a constant delay time.
I. B. K. Raju et al. [4], guy has done wonders in his race from the Stone Age to the supersonic age. Those wonders can be understood from the cutting-edge technologies. Technological improvements are getting a element and parcel of this world. An increasing number of technologies with lot of capabilities and advantages are springing up. Reversible logic is one such rising concept. One of the most important characteristics of reversible circuits is their less strength intake. as the generation improves, the variety of components and as a result the variety of transistors packed directly to the chip also will increase. Reversible common sense has a extensive software in low electricity VLSI circuits.
H.R. Bhagyalakshmi et al. [5], on this paper, we suggest the layout of two vectors testable sequential circuits primarily based on conservative common sense gates. The proposed sequential circuits based on conservative logic gates outperform the sequential circuits implemented in classical gates in phrases of testability. Any sequential circuit primarily based on conservative good judgment gates can be tested for classical unidirectional stuck-at faults the use of only two check vectors. The 2 test vectors are all 1's, and all zero's. The designs of two vectors testable latches, grasp-slave flip- flops and double area prompted (DET) flip-flops are provided. The significance of the proposed paintings lies inside the reality that it presents the design of reversible sequential circuits completely testable for any stuck-at fault by means of best two check vectors, thereby eliminating the want for any kind of scan-path access to internal reminiscence cells. The reversible design of the DET flip-flop is proposed for the first time within the literature. We also confirmed the application of the proposed technique in the direction of a hundred\% fault insurance for single missing/extra cellular defect within the quantum-dot cellular automata (QCA) layout of the Fredkin gate.

Akanksha Dixit et al. [6], this has led to the development of reversible gates. BCD is a fundamental building block of a central processing unit (CPU) in any computing system; reversible arithmetic unit has a high power optimization on the offer. By using suitable control logic to one of the input variables of parallel adder, various arithmetic operations can be realized. BCD based on a Reversible low power control unit for arithmetic \& logic operations is proposed.

In our design, the full Adders are realized using synthesizable, low quantum cost, low garbage output Peres gates. This paper presents a novel design of Arithmetic \& Logical Unit using Reversible control unit. This Reversible BCD has been modeled and verified using Verilog and Quartus II 5.0 simulator. Comparative results are presented in terms of number of gates, number of garbage outputs, number of constant inputs and Quantum cost.

Mr. Abhishek Gupta et al. [7], the proposed BCD configuration is checked and its points of interest over the main existing BCD outline are quantitatively analyzed. Reversible rationale is generally being considered as the potential rationale configuration style for usage in present day nanotechnology and quantum figuring with negligible effect on physical entropy. Late advances in reversible rationale take into account enhanced quantum PC calculations and plans for comparing PC architectures. Huge commitments have been made in the writing towards the configuration of reversible rationale door structures and number-crunching units, nonetheless, there are very few endeavors coordinated towards the outline of reversible BCDs. The outline of two programmable reversible rationale door structures focused at BCD execution and their utilization in the acknowledgment of a proficient reversible BCD is illustrated. The proposed BCD configuration is confirmed and its preferences over the main existing BCD outline are quantitatively investigated.
H. Thapliyal et al. [8], reversible logic has received great attention in the recent years due to its ability to reduce the power dissipation which is the main requirement in low power digital design. It has wide applications in advanced computing, low power design, Optical information processing,. Conventional digital circuits dissipate a significant amount of energy because bits of information are erased during the logic operations. Thus, if logic gates are designed such that the information bits are not destroyed, the power consumption can be reduced dramatically. The information bits are not lost in case of a reversible computation. This has led to the development of reversible gates. BCD is a fundamental building block of a central processing unit (CPU) in any computing system; reversible arithmetic unit has a high power optimization on the offer. By using suitable control logic to one of the input variables of parallel adder, various arithmetic operations can be realized. BCD based on a Reversible low power control unit for arithmetic \& logic operations is proposed. In our design, the full Adders are realized using synthesizable, low quantum cost, low garbage output Peres gates. This paper presents a novel design of Arithmetic \& Logical Unit using Reversible control unit. This Reversible BCD has been modeled and verified using Verilog and Quartus II 5.0 simulator. Comparative results are presented in terms of number of gates, number of garbage outputs, number of constant inputs and Quantum cost.

## Problem Formulation

We tackle the problem of finding a basis of literature review residue adder whose adder is large gerbang output and ancilla input to enable targeted computations for a given residue moduli bit size and a given architecture. After going throw the review of various existing work taken in the residue number the following problem formulation:

- Real time data processing necessitates the use of special purpose hardware which involves hardware efficiency as well as high speed.
- Those architectures which involves reversible gate, for example residue signed adder has less regular architecture due to complex routing and requires large silicon area.


## Residue Number

For conventional logic circuits there exists much research, even whole books, dedicated to the design and implementation of computer arithmetic. This is definitely not the case for reversible logic. The constraint that the circuits must be garbage-free is what makes it an interesting research problem, but most proposed designs (both hand-made and CAD generated) still implement the conventional algorithms with garbage. They use the reversible gates, but as their sole goal is to reduce logic size or number of garbage bits for a specific fixed-size circuit, very little knowledge is actually gained from this approach. However, arithmetic functions often have some inherent properties that can be exploited to make a very regular circuit design. A good example is the ripple-carry adder, where only a redesign gave the garbage-free V-shaped adder; a redesign that none of the automatic approaches can find. In many cases the arithmetic function itself must also be redefined, such that it can be expressed reversibly. Here our current work on multiplication is the obvious example. With this in mind, we need more design work on good garbage-free implementations of reversible circuits.
To convert the decimal number 29 to a residue number, we compute:

$$
\begin{aligned}
& \mathrm{R}_{5} 29 \bmod 5=4 \\
& \mathrm{R}_{3} 29 \bmod 3=2 \\
& \mathrm{R}_{2} 29 \bmod 2=1
\end{aligned}
$$

The decimal number 29 is represented by in the above residue number system.

The main advantage of the residue number system is the absence of carriers between columns in addition and in multiplication.

## Residue Addition

Addition can be accomplished by simply adding (or subtracting) the small integer values, modulo their specific moduli. That is,

$$
\begin{gathered}
\mathrm{C}=\mathrm{A}+\mathrm{B} \bmod \mathrm{M} \text { Can be calculated in RNS as } \\
\mathrm{Ci}=\mathrm{ai}+\mathrm{bi}
\end{gathered}
$$

One does not have to check for overflow in these operations.

## Residue Subtractor

Addition can be accomplished by simply adding (or subtracting) the small integer values, modulo their specific moduli. That is,

Can be calculated in RNS as

$$
\begin{gathered}
C=A-B \bmod M \\
C_{i}=a_{i}-b_{i}
\end{gathered}
$$

One does not have to check for overflow in these operations.
As We know, the addition arithmetic operation [1] represent the basic operation that is used by all of us in a daily basis, and this basic operation is one that enable us to implement another more complex mathematical operations such as subtraction, multiplication and division. The literature of the mathematics proposed many types of mathematics; the most commonly used and known is the traditional mathematics where the arithmetic functions performed directly on integer or floating point operands. Another type that is known as a modular arithmetic has been proposed where the arithmetic functions are executed on the residues of the input operands with respect to a set of modulo. This simple definition of the modular arithmetic [2,3] reveals to us that there should be some way to represent the conventional numbers in such a way that will allow us to perform this type of mathematics. This kind of representation is called a Residual Numbering System (RNS). We propose an RNS-Based two-operand digital adder [1, 2]; we abbreviate it as RNS-Adder. This adder is based on RNS (Residual Numbering System) in which an integer is represented by an ordered set of residues. This scheme is preferable in high speed computing systems since the high-independency among the set of residues. Thus, instead of working on large operands, working on residues which are definitely smaller ones eases some arithmetic operations like addition, subtraction, and multiplication. Fig. 1 depicts shortly the design of a complete RNS-adder module.


Figure1: The main components of RNS adder
An important issue that must be taken into consideration when designing RNS-based digital system is the representation of
inputs and outputs. Unfortunately, we used to use decimal numbering system in our life, and no one can force us to use another one. Thus, despite the efficiency of RNS in many arithmetic operations like addition and multiplication it's useless unless there is a technique to convert the conventional represented inputs to RNS (forward conversion) and the RNS results to conventional output (reverse conversion). Another issue in designing RNS-based arithmetic systems is the set of moduli used. As we will show that the basic principle in the computation of residues is division, with the moduli as the divisors. But division is an expensive operation in hardware and so is rarely used in the computation of residues. Division can be avoided in the case of using special set of moduli. This also simplifies the implementation of the modules but with some mathematical tricks.

## Reversible Gate

Reversible common sense is gaining importance in regions of CMOS layout because of its low energy dissipation. The traditional gates like AND, OR, XOR are all irreversible gates. Recall the case of conventional AND gate. It consists of inputs and one output. As an end result, one bit is misplaced every time a computation is completed. In line with the reality desk shown in Fig.1, there are three inputs (1, zero), $(0,1)$ and (zero, 0) that corresponds to an output zero. Subsequently it isn't feasible to determine a unique enter that resulted in the output 0 . with a view to make a gate reversible additional input and output strains are brought in order that a one to at least one mapping exists between the enter and output. This prevents the loss of statistics that is predominant purpose of strength dissipation in irreversible circuits. The enter that is introduced to an mxn characteristic to make it reversible is known as consistent enter (CI). All the outputs of a reversible circuit want not are used within the circuit. The ones outputs that aren't used within the circuit are called as garbage output (cross). The wide variety of garbage output for a specific reversible gate is not constant. The 2 fundamental constraints of reversible common sense circuit is
$>$ Fan out not allowed
$>$ Feedbacks or loops not allowed.

## Basic Reversible Gates

Numerous reversible gates have come out within the latest years. The maximum fundamental reversible gate is the Feynman gate and is shown in Fig.1. It is the most effective $2 \times 2$ reversible gate to be had and is typically used for fan out functions. Do not forget the input B as consistent. When B is 0 , the gate acts as a copying gate or a buffer where both the output lines comprise the enter A . while B is one, the complement of A is acquired on the output Q . The $3 \times 3$ reversible gates consist of Toffoli gate, Fredkin gate, New gate and Peres gate, all of which can be used to recognize various Boolean features. Fredkin gate is shown in Fig.2.The 4 x 4 reversible gates include TSG gate, MKG gate, HNG gate, PFAG gate etc.


Figure 2: Feynman gate


Figure 3: Fredkin gate
Figure 3 shows the TSG gate. Some of the $4 x 4$ gates are designed for implementing some important combinational functions in addition to the basic functions. Most of the above mentioned gates can be used in the design of reversible adders.


Figure 4: Peres gate
Several $4 \times 4$ and $5 \times 5$ gates have been described in the literature targeting low cost and delay which may be implemented in a programmable manner to produce a high number of logical calculations. The HNG gate, presented in [10], produces the following logical output calculations:

$$
\begin{gathered}
P=A \\
Q=B \\
R=A \oplus B \oplus C \\
S=(A \oplus B) \cdot C \oplus(A B \oplus D)
\end{gathered}
$$

The quantum cost and delay of the HNG is 6 . When $D=0$, the logical calculations produced on the $R$ and $S$ outputs are the required sum and carry-out operations for a full adder. A new programmable $4 x 4$ reversible logic structure - Peres AndOr (PAOG) gate - is presented which produces outputs

$$
\begin{gathered}
P=A \\
Q=A \oplus B \\
R=A B \oplus C \\
S=(A B \oplus C) \cdot C \oplus((A \oplus B) \oplus D)
\end{gathered}
$$

Fig. 5 shows the block diagram of the PAOG gate. This gate is an extension of the Peres gate for ALU realization.


Figure 5: Block Diagram of the PAOG


Figure 6: Block Diagram of DPG Gate

$$
\begin{gathered}
P=B \\
Q=A^{\prime} C+A D \\
R=(A \oplus B)(C \oplus D) \oplus C D \\
S=B \oplus C \oplus D
\end{gathered}
$$

## Proposed Methodology

The proposed algorithm can be implemented easily as shown in figure 6 . This implementation is easy to build if we have a modules called modulo adders. Thus we have to implement these modules from reversible gate.


Figure 7: Flow Chart of 4-bit Reversible Residue Adder
The proposed implementation is programmed (Described) and implemented using VHDL language which is a Hardware Description Language that was developed by the Institute of Electrical and Electronic Engineers (IEEE) as a standard language for describing the structure and behavior of digital electronic systems. It has many features appropriate for describing the behavior of electronic components ranging from simple logic gates to complete microprocessors and custom chips. Features of VHDL allow electrical aspects of circuit behavior (such as rise and fall times of signals, delays through gates, and functional operation) to be precisely described. The resulting VHDL simulation models can then be used as building blocks in larger circuits (using schematics, block diagrams, or system-level VHDL descriptions) for the purpose of simulation. As a compiling and simulation tool for VHDL, we used the ModelSim XE III 6.2 g which is known as a powerful tool developed by Mentor Graphics Company to offer an appropriate environment to validate the functional correctness of the design hardware.

## Expected Outcome

The proposed implementation is programmed (Described) and implemented using VHDL language which is a Hardware Description Language that was developed by the Institute of Electrical and Electronic Engineers (IEEE) as a standard language for describing the structure and behavior of digital electronic systems. It has many features appropriate for describing the behavior of electronic components ranging from simple logic gates to complete microprocessors and custom chips. The resulting VHDL simulation models can then be used as building blocks in larger circuits (using schematics, block diagrams, or system-level VHDL descriptions) for the purpose of simulation.


Figure 8: Flow Chart of 4-bit Reversible Residue Sub- tractor
1 Design residue adder and subtractor using different types of reversible gate.
2 Design different types of programmable reversible gate and compared.
3 Design free garbage based architecture using different types of input and compared existing algorithm.
4 Hand calculation of delay and area in residue adder and multiplier in different inputs.
5 All the modules design to different device family i.e. Spartan-3, Virtex-4 and Virtex-7.

## Conclusion

This paper has presented a high-speed residue binary number adder and converters between binary and residue numbers for moduli $n$. In the proposed method, only some fast binary additions are used for the arithmetic operations and the conversions. The design results show that the performance of proposed circuits will comparable with binary architectures and the schemes are high-speed architectures.

## References

[1] Adib Armand and Somayeh Timarchi, "Low Power Design of Binary Signed Digit Residue Number System Adder", 2016 24th Iranian Conference on Electrical Engineering (ICEE).
[2] Jian Wang, Shang Ma, Ze-guo Yang and Jianhao Hu, "A Systemic Performance Evaluation Method for Residue Number System", 20162nd IEEE International Conference on Computer and Communications.
[3] Shugang Wei, "Fast Signed-Digit Arithmetic Circuits for Residue Number Systems", 978-1-5090-0246-7/15/\$31.00 ©2015 IEEE.
[4] I. B. K. Raju, P. Rajesh Kumar and P. Bhaskara Rao, "Residue Arithmetic's using Reversible Logic Gates", Devices, Circuits and Systems (ICDCS), 2014 2nd International Conference on 10.1109/ICDCSyst.2014.6926193.
[5] H.R. Bhagyalakshmi and M.K. Venkatesha, "Optimized reversible BCD adder using new reversible logic gates", Journal of Computing, vol. 2, no. 2, 2010.
[6] A. D'amora, "Reducing power dissipation in complex digital filters by using the quadratic residue number system", Conf. Record 34th Asil. Conf. Signals SystComput. (ACSSC 2000), vol. 2, pp. 879-883, 2000.
[7] H. Thapliyal, N. Ran-Ganathan and S. Kotiyal, "Design of Testable Reversible Sequential Circuits", IEEE Transactions on VLSI, pp. 1-9, 2012.
[8] H. Thapliyal and N. Ranganathan, "Design of reversible latches optimized for quantum cost delay and garbage outputs", Proceedings of the Twenty Third IEEE International Conference on VLSI Design, pp. 235-240, 2010.
[9] H. Thapliyal and N. Ranganathan, "Testable reversible latches for molecular qca", Proceedings of the Eighth IEEE Conference on Nanotechnology, pp. 699-702, 2008.
[10] M. Chuang and C. Wang, "Reversible sequential element designs", Proceedings of the IEEE Asia and South Pacific Design Automation Conference, pp. 420-425, 2007.
[11] [11] S. Kumar Sastry Hari, S. Shroff, S. Noor Mahammad and V. Kamakoti, "Efficient building blocks for reversible sequential circuit design", Proceedings of the Forty Ninth IEEE International Midwest Symposium on Circuits and Systems, pp. 437441, 2006.
[12] J.E. Rice, "A New Look at Reversible Memory Elements", Proceedings of the IEEE International Symposium on Circuits and Systems, pp. 243-246, 2006.
[13] Amos Omondi and Benlamin Premkumar, Residue Number Susyem Theory and Implementation, Imperial College Press, 2007, pp. 1-134.
[14] Milos D. ERCEGOVAC, Tomas LANG, Digital Arithmetic, Morgan Kaufmann Publishers, by Elsevier Science (USA), Vol1, Ch2, pages (51-136), 2004.
[15] Mary Jane Irwin, ComputerArithmetic, "www.cse.psu.edu/ mji"s, Spring, 2005, CSE 575.
[16] Martin Horauer and Dietmar Loy, Adder Synthesis, Institute of Computer Technology., University of Technology Vienna, Emails: horauer,loy@ict.tuwien.ac.at, Supported by the Austrian Science Foundation (FWF).
[17] Linda Null,Julia Lobur, The Essentials of Computer Organization and Architecture, Textbook, Pennsylvania State University, Jones and Bartlett Publishers, Canada, 2003.

