International Journal of LNCT, Vol 2(5)
ISSN (Online): 2456-9895

A review on residue module arithmetic's adder and sub-tractor

Pradeep Upadhyay[1] and Ramanand Singh[2]
M. Tech. Scholar, LNCT, Bhopal[1]
Assistant Professor, LNCT, Bhopal[2]

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 performance estimation before circuit's implementation.

Keywords

CMOS technology, Reversible gate, Feynman gate, Peres gate.

1.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+1 adder can be divided into three categories, depending on the type of operands that they accept and output:

a) The result and both inputs use weighted representation;
b) The result and both inputs use diminished-1 representation;
c) 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^n+1 adder by inverted n-bit adder.

All things considered, the outline in this letter isn't the primary reversible variant ALU. Likewise gave an ALU configuration by summing up the V-shape plan which can accomplish five fundamental number juggling sensible tasks on two n-bit operands, yet the structure is simple to the point that a few capacities can't get the correct outcomes, for instance, we can't figure the ADD activity just utilizing the bitwise restrictive or of the two n-bit arguments| A > and| B > without considering the convey bit or just by setting the convey bit to the TRUE. The objective of this

letter is to construct a multi-utilitarian circuit sensibly that restrictively performs one of a few conceivable number juggling coherent tasks on two operands | A > and | B > relying upon control input information guidelines. The accompanying area depends on the presumption that the perusers know about the nuts and bolts of reversible rationale [5].

2.Literature review

Uttam Narendra Thakur et al. [1], today the most interesting research topic in theoretical point of view is Residue Number System (RNS). Its significance originates from the lack of carry propagation between its arithmetic units. To implement any modular process, the important step is the conversion from a residue number system (RNS) to binary. In modern telecommunication system and multimedia applications, the use of RNS increases day by day due to its many advantages such as low power consumption, high speed, very precise etc. Usually the translation of the output from residue to binary is the vital point in successful realizations of application specific architectures based on residual arithmetic. In this paper a novel architecture of parallel forward conversion (Residue to Binary number system) for signed number has been proposed successfully. This article also highlighted the mapping of this projected architecture on FPGA and shown it is very efficient on FPGA technology.

Adib Armand et al. [2], because of the expanding spread of computerized figuring, examination of different number portrayal frameworks in the advanced field appear to be fundamental. As a rule, the number portrayal frameworks in regards to their applications can be grouped in two regions: universally useful and particular reason. Parallel Signed-Digit Residue Number System (BSD-RNS) is one of the particular reason and upgraded number framework. Indeed with mixing RNS that declines the length of operands and BSD that has excess property, we can accomplish BSD-RNS that can perform figuring in parallel. Then again, because of restricted access to the vitality assets, lessening power utilization can likewise expand framework prominence. The expansion unit as an essential computational unit can assume a critical part in general framework execution. Subsequently, in this paper, it is expected first to present three fundamental viper structures for BSDRNS. At that point we propose low power adders for the moduli set {2n-1,2n, 2n+1} in view of 2's supplement, 1-out-of-3, and Pos-Neg BSDRNS number framework. Contrasted with regular structure of BSD-RNS adders, proposed adders have 10%, 70%, and 21% less power than the current proficient BSD-RNS adders for 2's supplement, 1-out-of-3, and Pos-Neg encoding, individually.

Jian Wang et al. [3], 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. [4], 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 $(2n, 2n-1, 2n + 1)$ 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. [5], 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. [6], 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.

D'Amora A et al. [7], 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.

Thapliyal H et al. [8], 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. [9], 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.

3.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.

4.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:

R_5 29 mod 5 = 4

R_3 29 mod 3 = 2

R_2 29 mod 2 = 1

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,

$C = A + B \mod M$

Can be calculated in RNS as

$C_i = a_i + b_i$
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,

$C = A - B \mod M$

Can be calculated in RNS as
$C_i = a_i - b_i$
One does not have to check for overflow in these operations.

As We probably am aware, the expansion number juggling activity [1] speak to the fundamental task that is utilized by every one of us in a consistent schedule, and this essential activity is one that empower us to execute another more mind boggling numerical activities, for example, subtraction, duplication and division. The writing of the science proposed numerous sorts of math; the most generally utilized and known is the conventional arithmetic where the number juggling capacities performed specifically on whole number or drifting point operands. Another composes that is known as a secluded number juggling has been proposed where the number-crunching capacities are executed on the buildups of the info operands regarding an arrangement of modulo. This straightforward meaning of the secluded number-crunching [2, 3] uncovers to us that there ought to be some approach to speak to the regular numbers such that will enable us to play out this sort of arithmetic. This sort of portrayal is known as a Residual Numbering System (RNS). We propose a RNS-Based two-operand advanced snake [1, 2]; we abridge it as RNS-Adder. This snake depends on RNS (Residual Numbering System) in which a whole number is spoken to by an arranged arrangement of deposits. This plan is ideal in fast figuring frameworks since the high-independency among the arrangement of deposits. Thus, instead of working on large operands, working on residues which are definitely smaller ones eases

some arithmetic operations like addition, subtraction, and multiplication. Figure 1 depicts shortly the design of a complete RNS-adder module.

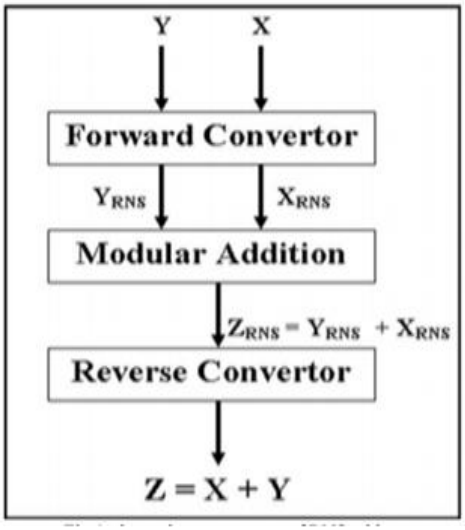

Figure1 The main components of RNS adder

An essential issue that must be thought about when planning RNS-based computerized framework is the portrayal of information sources and yields. Lamentably, we used to utilize decimal numbering framework in our life, and nobody can constrain us to utilize another. In this manner, in spite of the effectiveness of RNS in numerous number juggling activities like expansion and augmentation it's futile unless there is a procedure to change over the regular spoke to contributions to RNS (forward transformation) and the RNS results to ordinary yield (turn around transformation). Another issue in outlining RNS-based number juggling frameworks is the arrangement of moduli utilized. As we will demonstrate that the essential rule in the calculation of deposits is division, with the moduli as the divisors. Yet, division is a costly activity in equipment as is once in a while utilized as a part of the calculation of buildups. Division can be maintained a strategic distance from on account of utilizing uncommon arrangement of moduli. This additionally rearranges the usage of the modules yet with some scientific traps.

5.Proposed methodology

The proposed algorithm can be implemented easily as shown in Figure 2. This implementation is easy to build if we have a modules called modulo adders. Thus we have to implement these modules from reversible gate.

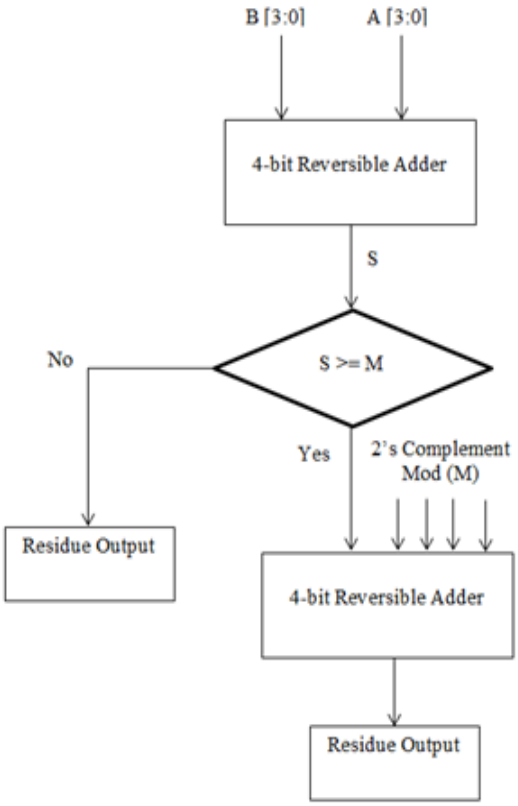

Figure 2 Flow Chart of 4-bit Reversible Residue Adder

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[14-15]. 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 6.2i 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.

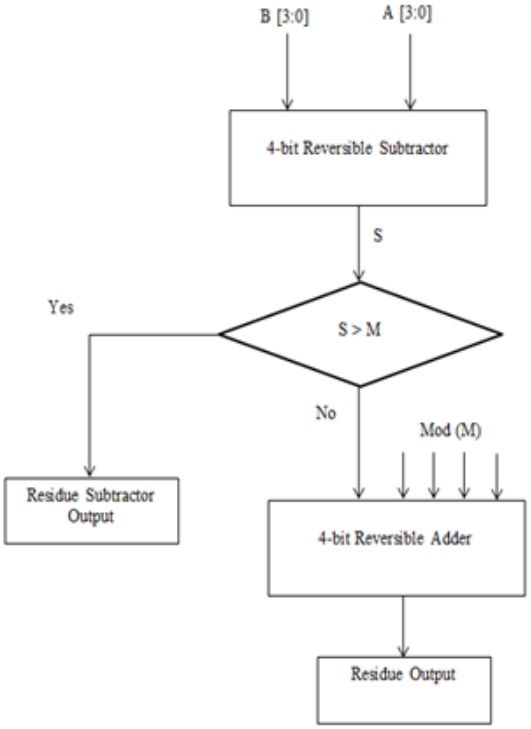

Figure 3 Flow Chart of 4-bit Reversible Residue Subtractor

6.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.

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.

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] Thakur UN, Mallick S, Moitra RM, Kotal M, Zakaria S, Chakraborty A, Pramanik S, Mukherjee D, Mukherjee C. FPGA based effecient architecture for conversion of binay to residue number system. In information technology, electronics and mobile communication conference (IEMCON), 8th IEEE Annual 2017 (pp. 700-4). IEEE.

[2] Armand A, Timarchi S. Low power design of binary signed digit residue number system adder. In electrical engineering (ICEE), 24th iranian conference on 2016 (pp. 844-8). IEEE.

[3] Wang J, Ma S, Yang ZG, Hu J. A systemic performance evaluation method for Residue Number System. In computer and communications (ICCC), 2nd IEEE International Conference on 2016 (pp. 321-5). IEEE.

[4] Wei S. Fast signed-digit arithmetic circuits for residue number systems. In Electronics, Circuits, and Systems (ICECS), 2015 IEEE International Conference on 2015 (pp. 344-7). IEEE.

[5] Raju IB, Kumar PR, Rao PB. Residue arithmetic's using reversible logic gates. In devices, circuits and systems (ICDCS), 2nd international conference on 2014 (pp. 1-6). IEEE.

[6] Bhagyalakshmi HR, Venkatesha MK. Optimized reversible BCD adder using new reversible logic gates. arXiv preprint arXiv:1002.3994. 2010.

[7] D'Amora A, Nannarelli A, Re M, Cardarilli GC. Reducing power dissipation in complex digital filters by using the quadratic residue number system. In signals, systems and computers, 2000. Conference record of the thirty-fourth asilomar conference on 2000 (pp. 879-83). IEEE.

[8] Thapliyal H, Ranganathan N, Kotiyal S. Design of testable reversible sequential circuits. ieee transactions on very large scale integration (vlsi) systems. 2013; 21(7):1201-9.

[9] Thapliyal H, Ranganathan N. Design of reversible latches optimized for quantum cost, delay and garbage outputs. In VLSI Design, 2010. VLSID'10. 23rd International Conference on 2010 (pp. 235-40). IEEE.

[10] Thapliyal H, Ranganathan N. Testable reversible latches for molecular QCA. In nanotechnology. NANO'08. 8th IEEE Conference on 2008 (pp. 699-702). IEEE.

[11] Chuang ML, Wang CY. Synthesis of reversible sequential elements. ACM Journal on Emerging

Technologies in Computing Systems (JETC). 2008; 3(4):4.
[12] Hari SK, Shroff S, Mahammad SN, Kamakoti V. Efficient building blocks for reversible sequential circuit design. In circuits and systems, 2006. MWSCAS'06. 49th IEEE International Midwest Symposium on 2006 (pp. 437-41). IEEE.
[13] Rice JE. A new look at reversible memory elements. In circuits and systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International Symposium on 2006 (pp. 4-pp). IEEE.
[14] Szabo NS, Tanaka RI. Residue arithmetic and its applications to computer technology. McGraw-Hill; 1967.
[15] Ling R. The mobile connection: The cell phone's impact on society. Elsevier; 2004 Jun 25.