Advanced Production and Industrial Engineering
R.M. Singari and P.K. Kankar (Eds.)

doi:10.3233/ATDE220717

Residue and Quadratic Residue Number System Based on Converters

[1]B.V.V.D Sainath, [2]K. Sangeet Kumar and [3]G. Rama Naidu

[1,2]Department of ECE, Aditya College of Engineering, Surampalem, India
[3]Department of ECE, Aditya Engineering College, Surampalem, India
[3] ramanaidu.gangu@aec.edu.in

Abstract. The quick growth of easy communication technologies concluded the last several decades has led in the establishment of strict standards for the functioning of productive systems. The system execution is improved by reducing computation time with the “Residue Number System (RNS)”. It is extensively castoff in “signal processing” “numeral analysis”, and “cryptoanalysis”, and an exact graph-based technique for designing perfect converters from binary framework to RNS to “Quadratic RNS (QRNS)” as well as, on the other hand, employing complete adder as the primary building blocks are shown. The measured adder is a critical component of the RNS system. In this work, it tries to summarized possible prospect of converters by using RNS adder and QRNS adders.

Keywords: Residue Number System (RNS), Converter, Quadratic Residue Number System (QRNS), Adder, RNS adder

1. Introduction

More efficient arithmetic algorithms and better VLSI structures are required for high-speed “Digital Signal Processing (DSP)” devices [1]. The numbering system used has a significant impact on how an arithmetic method is implemented in hardware. The “Logarithm Number System (LNS)” [4] and “Residue Number System (RNS)” are non-conventional numbering systems that are carry free, fault isolating, and modular. RNS is a historically significant numerical representation scheme [2]. The most important prime component of a Residue number system is modular adders. Moduli in the procedure of 2n-2k-1 can provide the right mix of channels in a multichannel RNS processing system [3]. The cell required in each scenario consists of a Connector topology and information flow structure are critical to determining a circuit's function [4]. For many years, the Residue Number System (RNS) has made it tempting to implement a variety of specific high-performance digital signal processing (DSP) systems [5].

VLSI designs are becoming more popular as high-speed digital signal processing (DSP) devices become available. The use of hardware for an arithmetic calculation could be a preference for a specific numbering system. The use of RNS, QRNS, and other number systems is determined by ROMs [6]. In general, these executions are expensive, intermediate, and necessitate a lot of space, a lot of power, and a lot of hardware complexity. Researcher’s numerous converters are based on mathematical concepts like scaling or the properties of specific moduli sets. Communication analysts are accustomed to doing computations over narrow areas [7]. These computations are now used in a variety of coding schemes [8].

The RNS has received significant attention in arithmetic calculation and signal processing applications such as rapid Fourier transformations, digital filtering, and image processing over the last decade [9, 11]. Because of its strong performance in increase and gather intensive algorithms, residue number framework (RNS) arithmetic is garnering attention in the field of DSP frameworks [12, 13]. RNS can perform DSP calculations faster than other arithmetic systems [14, 15]. In the field of signal and image processing, many numerical challenges must be dealt with in real time. The amount of information provided in these computations is enormous [16, 17]. Because of its low control features and shorter latency when compared to other computation systems, the Residue Number Framework (RNS) is widely used in portable and battery-powered devices. The majority of digital signal processing (DSP) applications, the fundamental prepared methods within the calculations, as a rule, incorporate in a variety of applications [18-22].

2. Related Work

Systematic review of available literatures are as follows. In 1982, a range of essential signal processing procedures were shown using systolic displays of 1-bit cell. This approach has a variety of significant silicon innovation applications, which are briefly addressed [1, 14]. VLSI floating point pipeline processor CORDIC is fast. was used in a wide variety of high-speed multiprocessor applications. The paper [2, 15] details applications such Examples of these technologies include speech recognition, matrices, antenna arrays, and computer graphics [16]. A 1.0-um p-well CMOS inventor devised and built a bit level pipeline 12x12 2’s complement multiplier with a 27-b gatherer. The use of productive clock and output buffer techniques, required for high-speed timing and board-level integration interface was demonstrated [17].

It was possible that this was the quickest known residue-to-binary converter for any nontrivial. The development of a fast residue-to-binary converter was made possible thanks to Rescan. The residue-to-binary converters for the three-module RNS 2, 2, 1 are described in [18, 19]. VLSI RNS architectures can be synthesized utilizing a graph-based method and a few FA-based designs for internal product step processors operating in limited rings. A graph-based technique could be utilized to develop VLSI RNS converters from the double framework to the RNS with complete adders. These innovative designs could have a significant impact on DSP applications [21, 22].

The amount of the numbers involved determines the pace of mathematical operations in the year 2000. Both the CRT and the RNS have been considered. The new CRTs on display will open up a plethora of new possibilities for sophisticated RNS research [5]. Researchers demonstrated new RNS-based SIMD RISC CPU design and synthesis. A SIMD architecture is used to study RNS arithmetic execution, while a smaller instruction set allows a three-level microprogrammed modified control unit to be used [6, 7]. RNS image coding, which provides high speed and low power implementation, can be utilized for secure image processing in 2016. In addition, RNS is used in cryptography and computer arithmetic [9, 10].

An adder with moduli set 2n–2k was evaluated in 2016 to provide random numbers with the acceptable unpredictability quality for cryptographic applications, and a random number generator based on this adder was presented. Multichannel RNS processing employs moduli in the form of 2n – 2k are optimum [11].

3. Methodology

3.1. Residue number system

The RNS divides huge numbers into a set of little integers and performs computation as a sequence of small operations to solve the problem of computational complexity. A RNS is made up of moderately prime moduli $K_1, K_2,...,K_m$, with gcd = 1 for i and j. $X = (X_1, X_2,... X_n)$, where X_i is decided by condition, is a weighted binary number.

$$xi = X \bmod k_i = |X|_{ki}\ 0 \leq x_i < k_i \qquad (1)$$

For any number X in the range [0, K-1], where K is the dynamic extension of the moduli set k1, k2, km, which is break even with the item of ki (K = k1, k2, km), this sort of representation is beneficial.

The RNS system is made up of three components. Specifically:

- Binary to residue conversion unit
- Residue modulo arithmetic units
- The residual of a binary conversion unit

The block diagram of the RNS system is shown in Figure. The weighted binary operands are converted into residue representations via the forward converter. The residue arithmetic unit is made up of modulo ki circuits that conduct arithmetic operations on residue numbers in parallel without requiring any carry signal propagation between the residue digits. On the other hand, the switching converter converts the generated residue number into a comparing weighted binary number shown in figure 1.

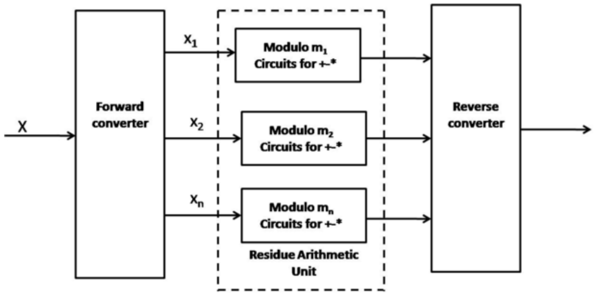
X
Forward converter
X1
X2
Xn
Modulo m1 Circuits for +-*
Modulo m2 Circuits for +-*
Modulo mn Circuits for +-*
Residue Arithmetic Unit
Reverse converter

Figure 1. Block diagram of RNS

3.2. Processor Architecture

A high-performance DSP processor based on RNS arithmetic is developed, manufactured, and synthesized in order to study the implications of RNS for general-purpose DSP applications. In the proposed RNS-based DSP's RISC SIMD inner architecture, a single programmed runs across several data sets. A block diagram of a CPU's architecture is shown in the image. Running application shows how RNS-output

|y| 256, |y| 251 and |y| 241 are transformed into residue digits using the built-in measurement processors. Decoding data from an internal ROM is performed by each of the four 32-bit dynamic range modulo processors in the control unit simultaneously. You'll need addressing registers to get to the channel data memory.

4. Results and Discussion: Modulo ‘m’ processor architecture

Each modulo m processor is illustrated in this diagram. Galois field index-based multipliers required the insertion of three more prime moduli. The modulus set was expanded to include all of the primes so that Galois field index-based multipliers could be built. Each RNS channel has a dedicated memory area for data-intensive algorithm implementation. The system has a 16-level stack sampler (SS), 256x8 RAM, eight 8-bit registers, and 256x8 RAM for the input port. The SS's addressable first-in-first-out can help DSP algorithms that require z-1 delays (FIFO). For recording reasons, each channel has its own input and output ports. A modular adder/subtract and a MAC unit make up the arithmetic unit. The arithmetic unit uses eight registers or a single stack sampler address as operands. The prime modulus adder/subtractor is built using the Galois field index multiplier [3] and a modulo m - 1 index adder.

RNS arithmetic uses N-tuples to represent integers, where each digit of the base m is represented by an N-tuple (0, 1,...).. The digit Xi = Xmi is used to denote M(N-1). Modulo m is represented by F m. N parallel channels must be utilized for each computation. IPSPm is the abbreviation for IPSPs established for each channel in the proposed approach. The best approach to describe what it accomplishes is to use the term "function."

$$Y_{out} = \langle Y + \langle A \times X \rangle m \rangle m \qquad (2)$$

We can use the following method to determine the number of recursions and the length of each recursion's output: In the second step, At the end of the process, Yr is turned into its residue modulo m value. This map was created with a single n-bit adder. This design is broken down into three parts since there are three phases. Because it belongs to the weak single assignment code family of algorithms, each block can be implemented as an array processor.

With the cell topologies based on RNS FA, the designers can meet a wide range of design requirements. Using hardware and area-time complexity, the proposed converters' performance is evaluated. The efficiency of the implementation is also assessed by analyzing the converter's throughput. For each implementation, the number of transistors required is utilized as a starting point for the number of transistors needed. There should be 28 transistors in an FA built using CMOS technology. Short word lengths or tiny moduli lower the number of transistors required by 25 percent to 70 percent. If you have greater moduli and longer word lengths, the drop can be up to 99.7 percent. For a narrow band of very small moduli, some converters have a hardware increase ranging from 1% to 20%. Binary to RNS and QRNS converters benefit from a large improvement in area-time products. Binary to RNS and RNS to QRNS converters, on the other hand, have a 46% to 95% reduction.

5. Conclusion

Using a measured adder, this paper presents a current plan approach for random number generators that may be implemented in software. Shift registers and modular adders are used in the solution that is proposed. To make matters more complicated, the modular adder is broken into four sections: pre-processing; calculation; correction; and sum computation. The designs and combination of a new SIMD RISC processor created on RNS have been demonstrated in this paper. On the basis of expensive multiply/add requirements, we devised a general method for executing DSP operations over finite rings based on finite rings. Bit-slicing the elementary internal creation sum processors are used to implement the BIPSP.

References

[1] Stouraitis, T. "Efficient convertors for residue and quadratic-residue number systems." *IEE Proceedings G (Circuits, Devices and Systems)* 139.6 (1992): 626-634.

[2] Skavantzos, Alexander. "An efficient residue to weighted converter for a new residue number system." *Proceedings of the 8th Great Lakes Symposium on VLSI (Cat. No. 98TB100222)*. IEEE, 1998.

[3] Mohan, PV Ananda. *Residue number systems: algorithms and architectures*. Springer Science & Business Media, 2002.

[4] B. Venkata Dharani, Sneha M. Joseph, Sanjeev Kumar, Durgesh Nandan, "Booth Multiplier: The Systematic Study", In: Kumar A., Mozar S. (eds) ICCCE 2020. Lecture Notes in Electrical Engineering, vol 698. Pp. 943-956, Springer, Singapore. https://doi.org/10.1007/978-981-15-7961-5_88

[5] Singh, Mahesh K., Narendra Singh, and A. K. Singh. "Speaker's voice characteristics and similarity measurement using Euclidean distances." *2019 International Conference on Signal Processing and Communication (ICSC)*. IEEE, 2019.

[6] Cardarilli, Gian Carlo, et al. "Low-power implementation of polyphase filters in quadratic residue number system." 2004 IEEE International Symposium on Circuits and Systems (IEEE Cat. No. 04CH37512). Vol. 2. IEEE, 2004.

[7] Singh, M., Nandan, D., & Kumar, S. (2019). Statistical Analysis of Lower and Raised Pitch Voice Signal and Its Efficiency Calculation. *Traitement du Signal*, *36*(5), 455-461.

[8] Balaji, V. Nithin, P. Bala Srinivas, and Mahesh K. Singh. "Neuromorphic advancements architecture design and its implementations technique." *Materials Today: Proceedings* 51 (2022): 850-853.

[9] Jyothi, Karri Divya, M. S. R. Sekhar, and Sanjeev Kumar. "Applications of Statistical Machine Learning Algorithms in Agriculture Management Processes." *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*. IEEE, 2021.

[10] Soderstrand, M., C. Vernia, and Jui-Hua Chang. "An improved residue number system digital-to-analog converter." *IEEE transactions on circuits and systems* 30.12 (1983): 903-907.

[11] Toivonen, Tuukka, and Janne Heikkila. "Video filtering with Fermat number theoretic transforms using residue number system." *IEEE Transactions on Circuits and Systems for Video Technology* 16.1 (2005): 92-101.

[12] Kanchana, V., Surendra Nath, and Mahesh K. Singh. "A study of internet of things oriented smart medical systems." *Materials Today: Proceedings* 51 (2022): 961-964.

[13] Brundana, M. S. S., et al. "Successive Approximation Compressor for Efficient FIR Filters in C-MOS VLSI Design." *2021 6th International Conference for Convergence in Technology (I2CT)*. IEEE, 2021.

[14] Ramírez, J., et al. "A new architecture to compute the discrete cosine transform using the quadratic residue number system." 2000 IEEE International Symposium on Circuits and Systems (ISCAS). Vol. 5. IEEE, 2000.

[15] Singh, Mahesh K., A. K. Singh, and Narendra Singh. "Acoustic comparison of electronics disguised voice using different semitones." *Int J Eng Technol (UAE)* 7.2 (2018): 98.

[16] Younes, Dina, and Pavel Steffan. "A comparative study on different moduli sets in residue number system." *2012 International Conference on Computer Systems and Industrial Informatics*. IEEE, 2012.

[17] Singh, Mahesh K., A. K. Singh, and Narendra Singh. "Multimedia utilization of non-computerized disguised voice and acoustic similarity measurement." *Multimedia Tools and Applications* 79.47 (2020): 35537-35552.

[18] McCanny, J. V., & McWhirter, J. G. (1982). Implementation of signal processing functions using 1-bit systolic arrays. Electronics Letters, 18(6), 241-243.

[19] Priya, B. Jyothi, Parvateesam Kunda, and Sanjeev Kumar. "Design and Implementation of Smart Real-Time Billing, GSM, and GPS-Based Theft Monitoring and Accident Notification Systems." *Proceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications*. Springer, Singapore, 2021.

[20] Veerendra, G., et al. "Detecting plant Diseases, quantifying and classifying digital image processing techniques." *Materials Today: Proceedings* 51 (2022): 837-841.

[21] Ramya, Korla, et al. "Compressive Sensing and Contourlet Transform Applications in Speech Signal." *ICCCE 2020*. Springer, Singapore, 2021. 833-842.

[22] Purushothaman, A., & Divya, S. Performance Comparison of RNS Modular Adder Based On Existing Parallel Prefix Trees And Random Number Generator Design.