Performance Analysis of Fast Sign Detection for Computer Arithmetic Residue Number System: A Survey

Mehul Kumar Pandya[1], Prof. Sachin Bandewar[3]
[1]M-Tech Research Scholar, [2] HOD & Research Guide,
Department of Electronics & Communication Engineering, SSSCE, Bhopal

Abstract-Numbers play a significant role in computer systems. Numbers are the basis and object of computer operations. Remarkably, the main task of computers is computing, which deals with numbers all the time. Humans have been familiar with numbers for thousands of years, whereas the representation of these numbers in computer systems is a new issue. A computer can provide only finite digits for a number representation (fixed word length), though a real number may be composed infinite digits. Because of the trade-offs between word length and hardware size, and between propagation delay and accuracy, various types of number representation have been proposed and adopted. This research article we are presenting the literature review on the Residue Number System (RNS) for performance analysis with emphasis on its arithmetic advantages in computers. The RNS is such an integer system exhibiting the capabilities to support parallel, carry-free addition, borrow-free subtraction, and single step multiplication without partial product.

Keywords:- Computer arithmetic, residue number system, restricted moduli set, sign detection.

I. INTRODUCTION

The origin of Residue Number System (RNS) can be traced to the puzzle given by Sun Tzu [6], a Chinese Mathematician and is illustrated as follows: How can we determine a number that has the remainders 2, 3, and 2 when divided by the numbers 7, 5, and 3, respectively. This puzzle, written in the form of a verse in the third century book, Suanching by the Chinese scholar Sun Tsu, is perhaps the first documented use of number representation using multiple residues. The answer to this puzzle, is outlined in Sun Tzu's historic work. The puzzle essentially asked us to convert the residues RNS into its decimal equivalent. Sun Tsu formulated a method for manipulating these remainders (also known as residues), into integers. This method is regarded today as the Chinese Remainder Theorem (CRT). The CRT, as well as the theory of residue numbers, was set forth in the 19th century by Carl Friedrich Gauss in his celebrated Disquisitions Arithmetical. This over 1700 - year - old number system is making waves in computing recently. Digital systems implemented on residue arithmetic units may play an important role in ultra - speed, dedicated, real - time systems that support pure parallel processing of integer - value data due to its inherent features such as carry free addition, borrow free subtraction, single step multiplication without partial product, parallelisms, and fault tolerant. These interesting properties of RNS have lead to its widespread usage in Digital Signal Processing (DSP) applications such as digital filtering, convolution, correlation, Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), image processing, cryptography, communications, and other highly intensive arithmetic applications. In the following, we give brief explanations on the above stated interesting inherent properties of RNS.

This means that no carry information need be communicated between residue digits. This explains why RNS is applicable in high performance computing and thus widely used in highly intensive DSP applications. In order to fully exploit these RNS parallelisms, arithmetic units that efficiently implement the modular statement must be found. Moduli selection and data conversion are one of the greatest challenges for RNS hardware design since the moduli choice affects the representational efficiency and the complexity of the arithmetic algorithms. To that end, a set of efficient moduli must be chosen and the moduli must be made as small as possible since it is the magnitude of the largest modulus that dictates the speed of the RNS arithmetic operations. Fig. 1 shows that the n output words (corresponding to the number of moduli) that are generated by the binary to RNS converter (the front-end) are processed by the n-parallel processors in the RNS signal processor block producing n output words, which are converted to a conventional binary number by the RNS to binary converter (the back-end).

Generally speaking, any RNS architecture must be interfaced efficiently with a binary/decimal number system and for that purpose data conversions are required. As given in Fig. 1, the input operands must be first converted to RNS (forward conversion) and after the arithmetic operations have been

performed, the output must be presented in the same way as the input (reverse conversion).

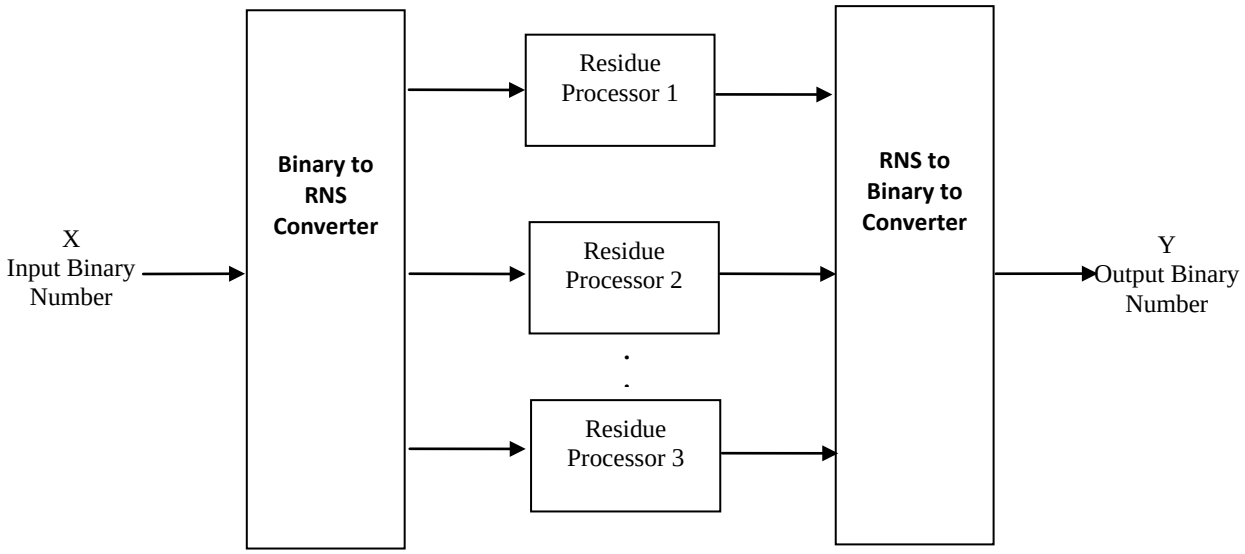

Fig. 1: RNS based Digital Signal Processor

II. RESIDUE NUMBER SYSTEM (RNS)

A residue number system (RNS) [11] represents a large integer using a set of smaller integers, so that computation may be performed more efficiently. The residue number system is defined by the choice of v positive integers m_i ($i = 1, 2, 3 \ldots v$) referred to as moduli. If all the moduli are pair-wise relative primes, any integer N, describing a non-binary message in this letter, can be uniquely and unambiguously represented by the so-called residue sequence $(r_1, r_2 .. r_v)$ in the range $0 < N < M_I$,where $r_i = N$ (mod mi) represents the residue digit of N upon division by mi, and $M_I = \Pi$ mi is the information symbols' dynamic range. Conversely, according to the Chinese Reminder Theorem, for any given v-tuple $(r_1, r_2 .. r_v)$ where $0 \leq r_i < m_i$; there exists one and only one integer N such that $0 \leq N < M_i$ and $r_i = N$ (mod mi) which allows us to recover the message N from the received residue digits.

Residue number system [10] has two inherent features that render the RNS attractive in comparison to conventional weighted number systems, such as for example the binary representation. These features are: The carry-free arithmetic and Lack of ordered significance amongst the residue digits. The first property implies that the operations related to the individual residue digits of different moduli are mutually independent because of the absence of carry information. The second property of the RNS arithmetic implies that some of the residue digits can be discarded without affecting the parameter, provided that a sufficiently "high dynamic range" is retained in the "reduced" system in order to unambiguously contain as the argument below.

III. REVIEW OF LITERATURE

Minghe Xu; Zhenpeng Bian; Ruohe Yao, [1] presented a fast sign detection algorithm for the residue number system moduli set $\{2^{n+1} - 1, 2^n - 1, 2^n\}$. First, a sign detection algorithm for the restricted moduli set is described. The new algorithm allows for parallel implementation and consists exclusively of modulo 2^nadditions. Then, a sign detection unit for the moduli set $\{2^{n+1} - 1, 2^n - 1, 2^n\}$ is proposed based on the new sign detection algorithm. The unit can be implemented using one carry save adder, one comparator and one prefix adder. The experimental results demonstrate that the proposed circuit unit offers 63.8%, 44.9%, and 67.6% savings on average in area, delay and power, respectively, compared with a unit based on one of the best sign detection algorithms.

Tay, T.F.; Chip-Hong Chang; Low, J.Y.S. [6] researched that Scaling is a problematic operation in residue number system (RNS) but a necessary evil in implementing many digital signal processing algorithms for which RNS is particularly good. Existing signed integer RNS scalers entail a dedicated sign detection circuit, which is as complex as the magnitude scaling operation preceding it. In order to correct the incorrectly scaled negative integer in residue form, substantial hardware overheads have been incurred to detect

the range of the residues upon magnitude scaling. In this brief, a fast and area efficient 2^n signed integer RNS scaler for the moduli set $\{2^n-1, 2^n, 2^n+1\}$ is proposed. A complex sign detection circuit has been obviated and replaced by simple logic manipulation of some bit-level information of intermediate magnitude scaling results. Compared with the latest signed integer RNS scalers of comparable dynamic ranges, the proposed architecture achieves at least 21.6% of area saving, 28.8% of speedup, and 32.5% of total power reduction for n ranging from 5 to 8.

Chip-Hong Chang; Kumar, S., [7] investigated a Sign detection is a necessary but non-trivial operation in Residue Number System (RNS) for many digital signal processing applications. Efficient sign detector for the three-moduli set RNS $\{2^n-1,2^n, 2^n+1\}$ has been proposed, but the problem remains unsolved for its extended four moduli sets. This paper presents a new sign detection algorithm dedicated to $\{2^n-1,2^n, 2^n+1,22^n+1\}$ RNS that has a wider dynamic range and higher parallelism. Approach exploits the number theoretic and multiplicative inverse properties in two-residue Chinese Remainder Theorem (CRT) and the New CRT II to halve the bit width of the modulo additions required by a complete reverse conversion. Study shows greater than 60% area reduction and more than 40% speedup for n = 2 to 5 compared with using its most efficient reverse converter for sign detection.

Maji, P.; Rath, G.S., [8] studied that the Residue number system (RNS) is generally an integer number system. The foremost canonical reason for implementation of filter in residue arithmetic is the inherent property of carry-free addition, subtraction and multiplication. As a result authors add, subtract and multiply in unison regardless to the numbers. Hereby, devices operating in this principle are fast and ingest low power. Though, principal limitation of Residue Number System is the slow and complex nature for arithmetic operations viz. division, comparison, sign detection and overflow detection and rejection. In this paper they have described some novel approaches to grapple with the limitations of comparison, sign detection and averting overflow. The selection of moduli in RNS is most important in attaining to solutions of problems as described earlier. Accordingly, a set of moduli is selected. Further in this paper they have used this set of moduli to successfully depict a design approach for 32-bit low-pass finite impulse response (FIR) filter.

Jaberipur, G.; Nejati, S. [9] described the classical RNS moduli set $RNS_C = \{2^n-1, 2^n, 2^n+1\}$ is widely used in digital signal/image processing and generally in computer arithmetic with residue number systems (RNS). This popularity is due to possibility of efficient binary to/from RNS conversions and existence of modulo-$(2^n \pm 1)$ adder architectures that are quite competitive with ordinary modulo-2^n adders. For example, there are modulo-(2^n-1) and -2^n parallel prefix adders with the minimal latency of (3 + 2[log n]) unit gate delay (UGD), while latencies of the fastest existing modulo-$(2^n + 1)$ adders are 1, 2 or 3 UGDs more, depending on the encoding of residues. In particular diminished-1 (D1) representation of residues, in one design, has led to the least latency of (4 + 2[log n]) UGDs. Given that RNS_C addition is undertaken in three parallel computation channels corresponding to the three moduli, it is desirable to device a (3 + 2[log n])-UGD modulo-$(2^n + 1)$ adder as well. so, authors are motivated to improve the performance of the aforementioned least-latency D1 design. To achieve this goal in this paper, they use some of the existing techniques for zero handling associated with D1 representation. UGD measures are supported by the synthesis results, except for less than 5% deviation due to reasonably expected interconnection and routing effects.

Boruah, D.; Saikia, M. [10] presented that the Residue Number System (RNS) is widely used in various applications such as design of cryptoprocessor, digital filters etc. For better performance of these RNS systems conversion module should be fast enough. This paper presents a new reverse converter architecture for a novel five moduli set Residue Number System (RNS) $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1, 2^{n-1} - 1\}$ for even values of n. It exploits the special properties of the numbers of the form $2^n \pm 1$, and extends the dynamic range of the present triple moduli $\{2^n - 1, 2^n, 2^n + 1\}$ based systems. The proposed moduli set has a dynamic range that can represent upto 5n - 1 bit numbers while keeping the moduli small enough and the converter efficient considering computation required. In new Five moduli set Reverse Converter design authors use both the Chinese Remainder Theorem (CRT) and Mixed Radix Conversion (MRC) techniques.

Timarchi, S.; Fazlali, M.; Cotofana, S.D [11] Given the modulo $2^n\pm1$ are the most popular moduli in Residue Number Systems (RNS), a large variety of modulo $2^n\pm1$ adder designs have been proposed based on different number representations. Though, in most of the cases, these encodings do not allow the implementation of a unified adder for all the moduli of the form 2^n-1, 2^n, and 2^n+1. In this paper, authors address the modular addition issue by introducing a new encoding, namely, the stored-unibit RNS. Moreover, authors demonstrate how the proposed representation can be utilized to derive a unified design for

the moduli set $\{2^n-1,2^n,2^n+1\}$. Approach enables a unified design for the moduli set adders, which opens the possibility to design reliable RNS processors with low hardware redundancy. Moreover, the proposed representation can be utilized in conjunction with any fast state of the art binary adder without requiring any extra hardware for end-around-carry addition.

Yanlong Ye; Shang Ma; Jianhao Hu, proposed the high efficient of scaling operation for residue number system (RNS) with VSLI implementation plays an important role in RNS-based information processing systems. With the properties of moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ authors proposed an efficient scaling scheme for these moduli set. Furthermore, the corrective factor for scaling a negative number is also introduced. The analysis shows that the proposed scalar has high area and power consumption performances compared to the cascading scaling scheme. The scalar can be used in the design of RNS-based ALUs and DSP systems.

IV. PROBLEM IDENTIFICATION

The problem of sign determination is one of the main problems that encountered for designing a computer based residue number. Attaching a sign bit to a residue number the magnitude of a residue number is not readable and therefore after adding a positive and negative number, the sign of the result is not immediately can be known. The residue number system is divided in two parts for representing positive and negative integers. For achieving this residue number is converted to its natural number from that it will fall in positive or may be in negative region for the representation. This process is not that much efficient as it is slow and therefore the fast method is needed. Data conversion is also a very big challenge of RNS because the input operands are provided in either standard binary or decimal format and must be converted to RNS before the computation can be performed. Similarly, the final results must be represented in the same way as the input operands, thus RNS to binary/decimal conversion is very essential to a successful RNS design. This implies that RNS based processors make heavy use of data conversions, which are slow processes. For an RNS processor to compete favorable with a conventional processor efficient data converters must be developed so that the RNS speedup will not be nullified by the conversion overhead.

V. CONCLUSION

In this we have gone through some significant researches related to the residue number system, for sign detection. We have involved the research articles which are very essential to get the batter performance of Residue Number system for faster sign detection. As the arithmetic applications grow rapidly, it is important for computer engineers to be well informed of the essentials of computer number systems and arithmetic processes. With the remarkable progress in the very large scale integration (VLSI) circuit technology, many hitherto complex circuits that were unthinkable yesteryears become components easily realizable today. Algorithms that seemed impossible to implement now have attractive implementation possibilities for the future. This means that not only the conventional computer arithmetic's, but also the unconventional ones are worth investigation in new design.

REFERENCES

[1] Minghe Xu; Zhenpeng Bian; Ruohe Yao, "Fast Sign Detection Algorithm for the RNS Moduli Set," in *Very* Large Scale Integration (VLSI) Systems, IEEE Transactions on , vol.23, no.2, pp.379-383, Feb. 2014.

[2] Z. Ulman, "Sign detection and implicit-explicit conversion of numbers in residue arithmetic," IEEE Trans. Comput., vol. 32, no. 6, pp. 590–594, Jun. 1983.

[3] T. V. Vu, "Efficient implementations of the Chinese remainder theorem for sign detection and residue decoding," IEEE Trans. Comput., vol. 34, no. 7, pp. 646–651, Jul. 1985.

[4] E. Al-Radadi and P. Siy, "RNS sign detector based on Chinese remainder theorem II (CRT II)," Comput. Math. Appl., vol. 46, nos. 10–11, pp. 1559–1570, 2003.

[5] M. Akkal and P. Siy, "Optimum RNS sign detection algorithm using MRC-II with special moduli set," J. Syst. Arch., vol. 54, no. 10, pp. 911–918, Oct. 2008.

[6] Tay, T.F.; Chip-Hong Chang; Low, J.Y.S., "Efficient VLSI Implementation of Scaling of Signed Integer in RNS ," in Very Large Scale Integration (VLSI) Systems, IEEE Transactions on , vol.21, no.10, pp.1936-1940, Oct. 2013.

[7] Chip-Hong Chang; Kumar, S., "Area-efficient and fast sign detection for four-moduli set RNS $\{2n-1,2n, 2n+1,22n+1\}$," in Circuits and Systems (ISCAS), 2014 IEEE International Symposium on , vol., no., pp.1540-1543, 1-5 June 2014.

[8] Maji, P.; Rath, G.S., "A novel design approach for low pass finite impulse response filter based on residue number system," in *Electronics Computer Technology (ICECT), 2011 3rd International Conference on* , vol.3, no., pp.74-78, 8-10 April 2011.

[9] Jaberipur, G.; Nejati, S., "Balanced minimal latency RNS addition for moduli set $\{2^n-1, 2^n, 2^n+1\}$," in *Systems, Signals and Image Processing (IWSSIP), 2011 18th International*

Conference on , vol., no., pp.1-7, 16-18 June 2011.

[10] Boruah, D.; Saikia, M., "A novel Reverse Converter design for new Five moduli set RNS," in *Advance Computing Conference (IACC), 2015 IEEE International* , vol., no., pp.337-342, 12-13 June 2015.

[11] Timarchi, S.; Fazlali, M.; Cotofana, S.D., "A unified addition structure for moduli set $\{2^n-1, 2^n, 2^n+1\}$ based on a novel RNS representation," in *Computer Design (ICCD), 2010 IEEE International Conference on* , vol., no., pp.247-252, 3-6 Oct. 2010

[12] Yanlong Ye; Shang Ma; Jianhao Hu, "An Efficient RNS Scaler for Moduli Set," in *Information Science and Engineering, 2008. ISISE '08. International Symposium on* , vol.2, no., pp.511-515, 20-22 Dec. 2008.