An Extensive Review on Fast Sign Detection Algorithm for the RNS Moduli Set $\{2^{n+1} - 1, 2^n - 1, 2^n\}$

Nirbhay Hardaha[1], Dr. Rita Jain[2]

[1]M-Tech Research Scholar, [2]Research Guide Department of Electronics & Communication Engineering, LNCT, Bhopal

Abstract - Some redundant number systems, such as the residue number system, have interesting and potentially useful characteristics in the arithmetic operations of multiplication, addition and subtraction. In a conventionally weighted number system, the n^{th} digit in the sum is dependent upon the n^{th} digits of the two operands and the carry from the lesser significant digits.

Index Terms— Computer arithmetic, residue number system, restricted moduli set, sign detection.

I. INTRODUCTION

In this age of universal electronic connectivity, of electronic eavesdropping and fraud, it is of utmost importance to store information securely. This leads to a heightened awareness to protect the data from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Cryptography plays a major role in mobile phone communications, e-commerce, sending private emails, transmitting financial information, security of ATM cards, computer passwords and electronic commerce, digital signature and so on.

One possible way to speed up multiplication modulo a large number is to rely on Residue Number Systems (RNS) to represent the operands. RNS has been an important field of research in arithmetic operations, due to its great potential for accelerating arithmetic computations, by breaking the arithmetic on large numbers to arithmetic on a set of smaller numbers. Thus, the carry-free and parallel nature of residue arithmetic makes RNS a powerful candidate for fast solutions to long integer arithmetic. However, applying the RNS to the long integer modular multiplication problem is not straightforward. The main difficulty is induced by the fact that the modulus used in RSA cryptosystem is a product of two prime numbers, which precludes coincidently with the dynamic range of a many moduli RNS base.[2]

The RNS is a very old number system. It was found 1500 years ago by a Chinese scholar Sun Tzu. Since the last five decades, RNS features have been rediscovered and thus the interest in this system has been renewed. The researchers have used the RNS in order to benefit from its features in designing high-speed and fault-tolerance applications.

The interest in RNS arithmetic has started since 1950's. The first hardware based on the RNS was built in 1967. The work in this field continued and many improvements in all areas of the RNS have arisen, in order to enhance its features, resolve its related problems and find suitable applications that benefit from RNS's features. Most of the early designs of RNS were based on Read-Only Memories (ROM). However, the great advance in Very Large Scale Integration (VLSI) technology paved the way for new approaches in designing RNS systems. New trends to design non-ROM based RNS have appeared. Subsequently, much work was devoted for special moduli sets. Excellent results in terms of computational speed have been achieved in 2000.

The fundamental idea of the RNS is based on uniquely representing large binary numbers using a set of smaller residues, which results in carry-free, high-speed and parallel arithmetic. This system is based on modulus operation, where the divider is called modulo and the remainder of the division operation is called residue.

The principal aspect that distinguishes the RNS from other number systems is that the standard arithmetic operations; addition, subtraction and multiplication are easily implemented, whereas operations such as division, root, comparison, scaling and overflow and sign detection are much more difficult. Therefore, the RNS is extremely useful in applications that require a large number of addition and multiplication, and a minimum number of comparisons, divisions and scaling. In other words, the RNS is preferable in applications in which additions and multiplications are critical. Such applications are Digital Signal Processing (DSP), image processing, speech processing, cryptography and transforms.

The advantage of RNS is the absence of carry propagation between digits, which results in high-speed arithmetic needed in embedded processors. Another important feature of RNS is the digit independence, so an error in a digit

does not propagate to other digits, which results in no error propagation, hence providing fault-tolerant system. In addition, the RNS can be very efficient in complex-number arithmetic, because it simplifies and reduces the number of multiplications needed.

All these features increase the scientific tendency toward the RNS especially for DSP applications. However, the RNS is still not popular in general-purpose processors, due the aforementioned difficulties.

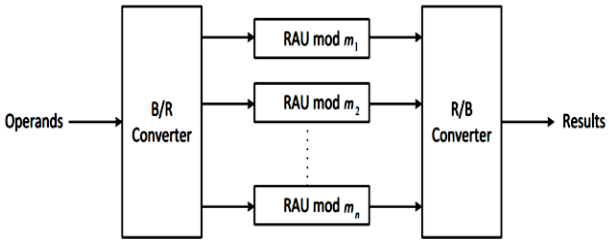

Fig. 1.1: The architecture of the residue number system

The basic RNS processor's architecture is shown in Fig. 1.1. It consists of three main components; a forward converter (binary to residue converter), that converts the binary number to *n* equivalent RNS residues, corresponding to the *n* moduli. The *n* residues are then processed using n parallel Residue Arithmetic Units (RAU); each of them corresponds to one modulo. The *n* outputs of these units represented in RNS are then converted back into their binary equivalent, by utilizing the reverse converter (residue to binary converter).

The most important issues that must be taking into account when designing an RNS system are, a proper moduli set selection, forward conversion, residue arithmetic units and reverse conversion.

II. LITERATURE REVIEW

M. Xu, Z. Bian and R. Yao, [1] This brief presents 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^n additions. 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.

N. Szabo, [2] The problem of sign determination in no redundant residue systems is investigated. A general theorem is derived establishing necessary conditions for sign detection, and the use of this theorem is demonstrated through specific examples. It is shown that for a particular system organization these same conditions are also sufficient for sign detection. An implementation of this last system is presented for four moduli.

Z. D. Ulman, [3] A new method of sign detection is proposed. The advantage of this method is a possibility of simultaneous execution of two operations: residue to mixed-radix conversion of the number magnitude and sign detection in one and the same circuit (implicit-explicit conversion).

Thu Van Vu, [4] Two conversion techniques based on the Chinese remainder theorem are developed for use in residue number systems. The new implementations are fast and simple mainly because adders modulo a large and arbitrary integer M are effectively replaced by binary adders and possibly a lookup table of small address space. Although different in form, both techniques share the same principle that an appropriate representation of the summands must be employed in order to evaluate a sum modulo M efficiently. The first technique reduces the sum modulo M in the conversion formula to a sum modulo 2 through the use of fractional representation, which also exposes the sign bit of numbers. Thus, this technique is particularly useful for sign detection and for any operation requiring a comparison with a binary fraction of M. The other technique is preferable for the full conversion from residues to unsigned or 2's complement integers. By expressing the summands in terms of quotients and remainders with respect to a properly chosen divisor, the second technique systematically replaces the sum modulo M by two binary sums, one accumulating the quotients modulo a power of 2 and the other accumulating the remainders the ordinary way. A final recombination step is required but is easily implemented with a small lookup table and binary adders.

T. Tomczak, [5] In this paper, authors propose a fast algorithm for sign-extraction of a number given in the Residue Number System $(2^{n-1},2^n,2^{n+1})$. The algorithm can be implemented using three n-bit wide additions, two of which can be done in parallel. It can be used in a wide variety of problems, i.e., in algorithms for dividing numbers in the RNS, or in evaluating the sign of determinant in computational geometry, etc.

P. V. A. Mohan, [6] In this brief, the design of residue number system (RNS) to binary converters for a new powers-of-two related three-moduli set $\{2^{n+1} - 1, 2^n, 2^{n-1}\}$ is considered. This moduli set uses moduli of uniform word length (n to n + 1 bits). It is derived from a previously investigated four-moduli set $\{2^{n-1}, 2^n, 2^{n+1}, 2^n$

$^{+1}$ - 1}. Three RNS-to-binary converters are proposed for these moduli set: one using mixed radix conversion and the other two using Chinese remainder theorem. Detailed architectures of the three converters as well as comparison with some earlier proposed converters for three-moduli sets with uniform word length and the four-moduli set $\{2^{n-1}, 2^n, 2^{n+1}, 2^{n+1} - 1\}$ are presented.

III. PROBLEM IDENTIFICATION

In this brief, a fast sign detection algorithm is presented for restricted moduli set including the modulo 2^n. The proposed algorithm allows for parallel implementation and consists exclusively of modulo 2^n additions. A sign detection unit for the moduli set $\{2^{n+1} - 1, 2^n - 1, 2^n\}$ is proposed based on the proposed sign detection algorithm. The experimental results demonstrate that the proposed circuit achieves significant improvements in terms of area, delay, and power.

IV. PROPOSED SYSTEM MODEL

Choosing proper moduli set greatly affects the performance of the whole system. The prevalent issue is that as the number of moduli increases the speed of the residue arithmetic units increases, whereas the residue-to-binary converters become slower and more complex.

Due to the fact that binary to residue converters are rather simple, little work has been dedicated to enhance their performance. Since my research dealt with special moduli sets rather than general moduli sets, the utilized components to obtain residues with respect to the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ are presented.

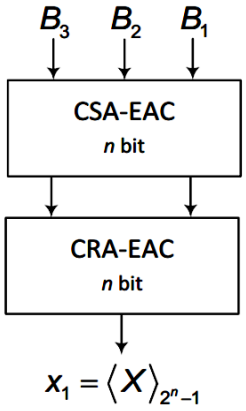

Fig. 1.2: Proposed binary to residue converter – modulo $(2^n - 1)$ channel. [3]

Since the majority of moduli sets have moduli of the following forms $(2^k - 1)$, (2^k) or $(2^k + 1)$, thus, the illustrated forward converters can be used to obtain the RNS representation with respect to any of those sets.

The most straightforward residue to obtain from binary is the one with respect to modulo 2^n. This residue represents the least n bits of the binary number. Thus, no adders or any logical components are needed. However, computing a residue with respect to modulo $(2^n - 1)$, demands two consecutive modulo $(2^n - 1)$ adders. Instead of using this structure, a carry save adder with end around carry (CSA-EAC) followed by carry ripple adder with end around carry (CRA-EAC) can perfectly fulfill the task.[5]

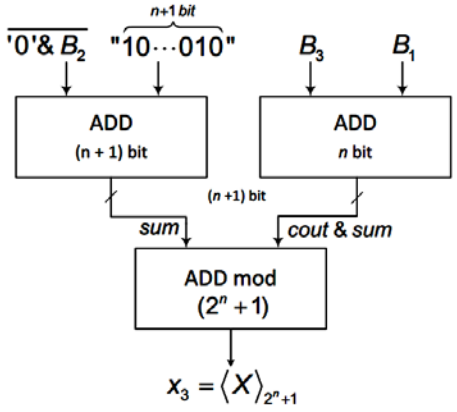

Fig. 1.3: Proposed binary to residue converter – modulo $(2^n + 1)$ channel. [4]

The most difficult residue to obtain is the one with respect to $(2^n + 1)$ modulo. Typically, this one requires modulo $(2^n + 1)$ subtractor followed by modulo $(2^n + 1)$ adder. This structure is rather complicated, since both components are complex and time consuming.

V. CONCLUSION

A Redundant Binary Representation (RBR) is a numeral system that uses more bits than needed to represent a single binary digit so that most numbers have several representations. An RBR is unlike usual binary numeral systems, including two's complement, which use a single bit for each digit. Many of an RBR's properties differ from those of regular binary representation systems. Most importantly, an RBR allows addition without using a typical carry. When compared to non-redundant representation, an RBR makes bitwise logical operation slower, but arithmetic operations are faster when a greater bit width is used. Usually, each digit has its own sign that is not necessarily the same as the sign of the number represented. When digits have signs, that RBR is also a signed-digit representation.

REFERENCES

[1] M. Xu, Z. Bian and R. Yao, "Fast Sign Detection Algorithm for the RNS Moduli Set $\{2^{n+1}-1, 2^{n-1}, 2^n\}$," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 23, no. 2, pp. 379-383, Feb. 2015.

[2] N. Szabo, "Sign Detection in Nonredundant Residue Systems," in IRE Transactions on Electronic Computers, vol. EC-11, no. 4, pp. 494-500, Aug. 1962.

[3] Z. D. Ulman, "Sign Detection and Implicit-Explicit Conversion of Numbers in Residue Arithmetic," in IEEE Transactions on Computers, vol. C-32, no. 6, pp. 590-594, June 1983.

[4] Thu Van Vu, "Efficient Implementations of the Chinese Remainder Theorem for Sign Detection and Residue Decoding," in IEEE Transactions on Computers, vol. C-34, no. 7, pp. 646-651, July 1985.

[5] T. Tomczak, "Fast Sign Detection for RNS (2^{n-1},2^n,2^{n+1}) ," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 55, no. 6, pp. 1502-1511, July 2008.

[6] P. V. A. Mohan, "RNS-To-Binary Converter for a New Three-Moduli Set {2n+1−1,2n,2n−1}," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 54, no. 9, pp. 775-779, Sept. 2007.

[7] 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.

[8] 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.

[9] S. Bi and W. Gross, “The mixed-radix Chinese remainder theorem and its applications to residue comparison,” IEEE Trans. Comput., vol. 57, no. 12, pp. 1624–1632, Dec. 2008.

[10] S. Piestrak, “Design of residue generators and multioperand modular adders using carry-save adders,” IEEE Trans. Comput., vol. 43, no. 1, pp. 68–77, Jan. 1994.

[11] R. Zimmermann, “Efficient VLSI implementation of modulo (2n ± 1) addition and multiplication,” in Proc. 14th IEEE Symp. Comput. Arithmetic, 1999, pp. 158–167.

[12] K. Furuya, “Design methodologies of comparators based on parallel hardware algorithms,” in Proc. 10th ISCIT, Oct. 2010, pp. 591–596.