International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:1, No:7, 2007

A Novel Multiple Valued Logic OHRNS Modulo r^n Adder Circuit

Mehdi Hosseinzadeh, Somayyeh Jafarali Jassbi, and Keivan Navi

***Abstract*—**Residue Number System (RNS) is a modular representation and is proved to be an instrumental tool in many digital signal processing (DSP) applications which require high-speed computations. RNS is an integer and non weighted number system; it can support parallel, carry-free, high-speed and low power arithmetic. A very interesting correspondence exists between the concepts of Multiple Valued Logic (MVL) and Residue Number Arithmetic. If the number of levels used to represent MVL signals is chosen to be consistent with the moduli which create the finite rings in the RNS, MVL becomes a very natural representation for the RNS. There are two concerns related to the application of this Number System: reaching the most possible speed and the largest dynamic range. There is a conflict when one wants to resolve both these problem. That is augmenting the dynamic range results in reducing the speed in the same time. For achieving the most performance a method is considered named "One-Hot Residue Number System" in this implementation the propagation is only equal to one transistor delay. The problem with this method is the huge increase in the number of transistors they are increased in order m^2. In real application this is practically impossible. In this paper combining the Multiple Valued Logic and One-Hot Residue Number System we represent a new method to resolve both of these two problems.

In this paper we represent a novel design of an OHRNS-based adder circuit. This circuit is useable for Multiple Valued Logic moduli, in comparison to other RNS design; this circuit has considerably improved the number of transistors and power consumption.

***Keywords*—**Computer Arithmetic, Residue Number System, Multiple Valued Logic, One-Hot, VLSI.

I. Introduction

DIFFERENT number systems have been developed since the evolution of computers. These systems focus on simplifying the basic mathematical operations in order to assist in making the computer more powerful. One of these systems, which has a great potential in Digital Signal Processing and other applications that deal with integers only, is the Residue Number System. Residue Number System arithmetic is widely used in the DSP and digital real-time computing systems, because the arithmetic addition, subtraction and multiplication may be executed in RNS very fast without the need for carry.

Manuscript received August 27, 2007.

M. Hosseinzadeh and S. J. Jassbi are with the Islamic Azad University Science and Research Branch, Tehran, Iran (e-mails: hosseinzadeh@sr.iau.ac.ir, a.jassbi@sr.iau.ac.ir).

K. Navi is with the Faculty of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran (e-mail: navi@sbu.ac.ir).

VLSI digital systems are used in numerous applications in DSP, telecommunication and cryptography. The objective of VLSI digital design is to continuously reduce the cost and improve the performance of the VLSI digital systems in terms of complexity, speed and power, one method of designing high-speed, low-power VLSI digital systems is using the Residue Number System. The RNS has limited carry chain and offers high-speed operations. The high-speed gained by the RNS parallelism can then be traded-off for low-power consumption. In a low-power ASIC or FPGA implementation of VLSI digital systems, the RNS-based structures provide a promising future [1,2].

The system also offers some useful properties for error detection and error correction and fault tolerance in digital systems. Important areas of application of the RNS include:

- Digital Signal Processing
- Fast Fourier Transform (FFT)
- Digital Filters
- Ad-Hoc Networks
- Digital Communication
- Real Time Processing
- RSA Cryptosystem
- Error Detection and Correction Algorithm [3-9].

In many earlier publications, different authors propose the moduli sets: $\{r^n-2, r^n-1, r^n\}$ $\{r^a, r^b-1, r^c+1\}$ $\{r^n-1, r^n, r^n+1\}$, where n is a positive integer [10-12]. Regarding these examples r^n is the most important modulo frequently cited in the RNS literature; hence in this article we work on addition of r^n beside the fact that it is highly used in designing RNS systems, it has a simple adder circuit and simple converter that don't need any supplement hardware.

The One-Hot Residue Number System allows the implementation of high-speed simple adders and multipliers. Among its many advantages are fast low-power addition, multiplication, and moduli conversion, as well as hardware-free constant multiplication. Adders and multipliers are barrel shifter-based and, therefore, regular and simple. Constant multiplication is done without redundant circuitry, using a reordering of digit representations called a signal transposition (ST). In addition to its speed and power-reduction advantages, this operation offers the further advantage of chip area reduction with the advent of advanced IC technologies possessing as many as eight layers of metal. Moduli conversion is also fast and simple, using (at worst case) a logic depth of one, and, at best, no hardware at all [13].

On the one hand in some applications we need the large dynamic ranges such as RSA and DSP for more security and

accuracy, and on the other hand barrel shifter based One-Hot Residue arithmetic circuits consume a chip area that is $O(m^2)$, where m is the modulo size.

In this paper we represent a novel design of an OHRNS-based adder circuit. This circuit is useable for large moduli in comparison to other RNS design; this circuit has considerably improved the number of transistors and power consumption.

The organization of this paper is as follows; in section II recollect MVL. Section III and IV contains brief introductions to Residue Number System operation and One-Hot RNS and adder circuit respectively. In section V we have proposed a Novel One-Hot Residue Number System adder circuit. Section VI and VII contains our comparison and conclusion respectively.

II. Multiple Valued Logic

Despite binary logic in which logical levels are restricted to two possible states, namely false and true, there exists an alternative named Multiple Valued Logic [14]. In this system, theoretically, one can define an unlimited number of logical levels, but in reality it is limited and this limitation mainly depends on the used technology. In Multiple Valued Logic with r levels comprising $\{0,1,2,\dots,r-1\}$, we can introduce a new area.

It is obvious that the positional weights of any two succeeding columns are power of r. Fig. 1 represents the positional value of each location.

$$\begin{array}{c} a_{n-1}a_{n-2}a_{n-3}\ \dots\ a_2a_1a_0 \\ \downarrow\ \downarrow\ \downarrow\ \ \dots\ \ \downarrow\ \downarrow\ \downarrow \\ r^{n-1}r^{n-2}r^{n-3}\ \dots\ r^2r^1\ r^0 \end{array}$$

Fig. 1 Positional weight value of each location

Each location in an MVL component can store much more information than a binary logic component can, the dynamic range of the moduli set $\{r^n-2, r^n-1, r^n\}$ is much greater than its equivalent in the binary representation. Now the question is how to present the related hardware which is clearly answered in [15]. For example if we compare two different moduli sets with equal number of locations, the results illustrated in Table I will be obtained.

TABLE I
Comparison of Dynamic Range and Number of Location

Moduli set	Number of position	M
$\{r^n-2, r^n-1, r^n\}$	$3n$	$r^{3n}-3r^{2n}+2r^n$
$\{2^n-1, 2^n, 2^{n-1}-1\}$	$3n$	$2^{3n-1}-1.5(2^{2n})+2^n$
$\{2^n-1, 2^n, 2^n+1\}$	$3n+1$	$2^{3n}-2^n$

TABLE II
Comparison of Dynamic with Different n

M / n	5	10
$3^{3n}-3^{2n+1}+2\times3^n$	14172246	$\cong 2\times10^{14}$
$2^{3n-1}-1.5\times2^{2n}+2^n$	14880	$\cong 5\times10^{8}$
$2^{3n}-2^n$	32736	$\cong 10^{9}$

In Table II, r is selected equal to 3 and a comparison is done.

Based on these comparisons, we conclude that the MVL with the same number of locations has much more dynamic range.

III. Residue Number System Operation

RNS is defined by a set of relative pair wise prime integers $\{m_1, m_2, m_3, \dots, m_n\}$, with dynamic range $M=\prod_{i=1}^{n} m_i$. Any integer X belonging to $Z_m=\{0,1,2,\dots,M-1\}$ has a unique RNS representation given by:

$$X \xrightarrow{RNS} (x_1, x_2, x_3, \dots, x_n) \tag{1}$$

Where

$$x_i = \langle X \rangle_{m_i},\ i=1,2,3,\dots,n \tag{2}$$

While $\langle x \rangle_{m_i}$ denotes the operation $x \bmod m_i$. If the integers X and Y have RNS representations $(x_1, x_2, x_3, \dots, x_n)$ and $(y_1, y_2, y_3, \dots, y_n)$ respectively, then the RNS representation of $Z = X \circ Y$ (where $\circ$ denotes addition, subtraction, or multiplication) is given by:

$$Z \xrightarrow{RNS} (z_1, z_2, z_3, \dots, z_n)$$
$$z_i = \langle x_i \circ y_i \rangle_{m_i},\quad i=1,2,3,\dots,n \tag{3}$$

Equation (3) demonstrates the parallel, carry-free nature of the RNS [13-17]. The reconstruction of X from its residues $(x_1, x_2, x_3, \dots, x_n)$ is based on the Chinese Remainder Theorem (CRT) shown by:

$$X = \left\langle \sum_{i=1}^{n} \langle x_i . N_i \rangle_{m_i} \times M_i \right\rangle_M$$
$$M = \prod_{i=1}^{n} m_i \tag{4}$$

where:

$$M_i = \frac{M}{m_i},\ N_i = \langle M_i^{-1} \rangle_{m_i},\ i=1,2,3,\dots,n \tag{5}$$

The notation $\langle M_i^{-1} \rangle_{m_i}$ in (5) denotes the multiplicative inverse of M_i modulo m_i [16,17].

IV. One-Hot RNS and Adder

A. One-Hot RNS

The advantages obtained when the One-Hot is used to represent the digits of an RNS are so compelling that it is given the resulting "number system" the new name "One-Hot Residue Number System," even though, strictly speaking, it is still the RNS with the same arithmetic. The advantages include the use of barrel shifters for the basic operations (which possess superior DP-products and operand independent delays compared to binary implementations), simple and regular layout of arithmetic circuits, and zero-cost implementation (by signal transposition) of inverse and index calculation and moduli conversion. Lower DP-products result from the fact that signal activity factors are near-minimal and fewer critical path transistors in referred papers [18,19].

The One-Hot representation for the i[th] residue digit x_i is depicted in Fig. 2, only the single line corresponding to the digit value is asserted (driven high) at any time. Furthermore, during a change in digit value, at most two lines change their value. This is the minimal possible activity factor and means that the power dissipation is small.

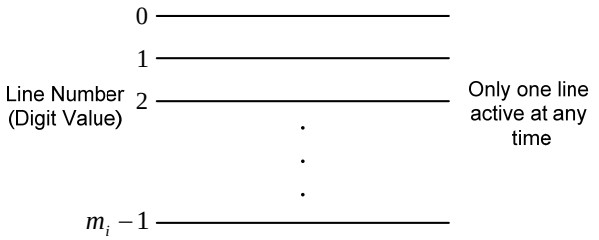


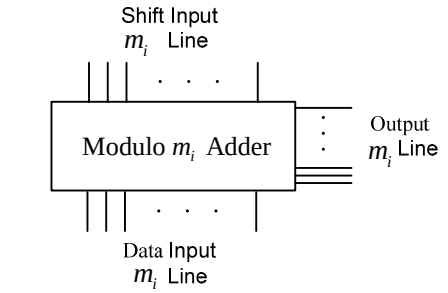
Fig. 2 OHRNS representation for digit x_i

With this One-Hot representation of the residue digits, addition can be performed by cyclic shifts ("rotations"). One of the operands (the "data" operand) is rotated by an amount equal to the other's (the "shift" operand) value. The rotation can be performed by one of several types of circuits; in our work we have chosen to use barrel shifters. These circuits compute all possible rotations in parallel and pass when required the appropriate one to the output.

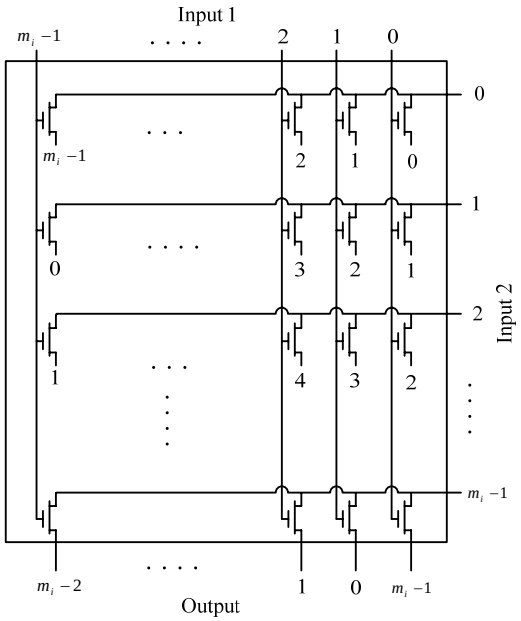
B. OHRNS Adder

In this section, we present OHRNS adders. OHRNS adders employ barrel shifters as their basic computational elements. This is possible because, for One-Hot encoded operands, modulo m_i addition are a cyclic permutation of one operand by the other.

A modulo m_i OHRNS adder is shown in Fig. 3, in Fig. 3(a), the two inputs are denoted as "shift" and "data" to make the internal operation [Fig. 3(b)] more easily understood. The barrel shifter generates, in parallel, all possible rotations of the data input, and selects one of them for output. Which one is selected is determined by the shift input.



(a)



(b)

Fig. 3 OHRNS adder: (a) symbol and (b) architecture

As an example, the moduli 5 OHRNS adder model using the OB level restoration method is shown in Fig. 4. The TG version differs in that it uses transmission gates in place of the pass transistors, and lacks the dual output buffers. Furthermore, the complements of the shift inputs are generated by inverters, one per line, in order to drive the control inputs of the transmission gates.

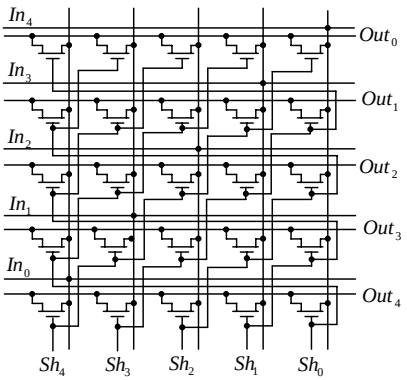


Fig. 4 Modulo 5 OHRNS adder model

V. A Novel One-Hot RNS Adder Circuit

In this section we represent a novel adder circuit for r^n modulo on the basis of One-Hot schema. If we consider A as a remainder of r^n modulo then A is n-digit adder and $o \le A \le r^n$.

On this base:

$$m = r^n \Rightarrow 0 \le A < m = r^n \text{ (n is even)}$$
$$A = \left(a_{n-1} \dots a_{(n/2)} a_{(n/2)-1} \dots a_2 a_1 a_0\right)_r = \beta_1 \beta_0$$
$$(\beta_1)_{P_2} = \left(a_{n-1} \dots a_{(n/2)}\right)_r \quad (6)$$
$$(\beta_0)_{P_1} = \left(a_{(n/2)-1} \dots a_2 a_1 a_0\right)_r$$
$$P_1 = P_2 = r^{(n/2)}$$

$$m = r^n \Rightarrow 0 \le A < m = r^n \text{ (n is odd)}$$
$$A = \left(a_{n-1} \dots a_{(n+3)/2} a_{(n+1)/2} \dots a_2 a_1 a_0\right)_r = \beta_1 \beta_0$$
$$(\beta_1)_{P_2} = \left(a_{n-1} \dots a_{(n+3)/2}\right)_r \quad (7)$$
$$(\beta_0)_{P_1} = \left(a_{(n+1)/2} \dots a_2 a_1 a_0\right)_r$$
$$P_1 = r^{(n+1/2)},\ P_2 = r^{(n-1/2)}$$

According to equations 6 and 7 $(B)_p$ denotes the number of B in radix P.

With the use of equations 6 and 7 we achieve a novel represent for every remainder on the basis of $B_1 B_o$ which $o \le B_0 \le p_1$, $o \le B_1 \le p_2$ and on this base B_1 is a high order part and B_0 is a low order part for novel representation.

We add up the high order and low order parts independently based on One-Hot RNS, but we need to add up the carry propagated from the lower part to the result of the addition of higher part (note that an adder in the base r, carry in can be $\{0, 1, 2, \dots, r-1\}$).

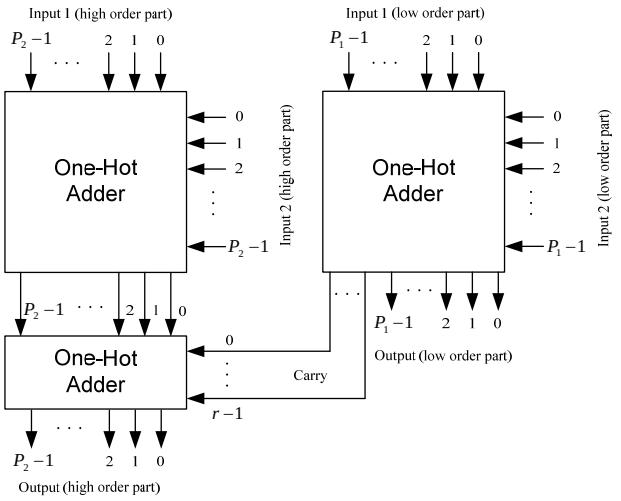


Fig. 5 Symbol of Novel Adder

As illustrated in Fig. 5 each pass transistor has two outputs. One is used to drive carry signal and the other for sum.

In this section in order to clarify the proposed subjects, we give example.

Example 1: $m = 3^4 = 81$

If $m = 3^4 = 81$ then the remainder of each modulo will be presented in four digit in binary representation. Its equivalent Multiple Valued Logic representation in radix 4 need only two locations as illustrated in Fig. 6.

$$A \in \{0, 1, 2, \dots, 81\}$$
$$A = a_3 a_2 a_1 a_0 = \beta_0 \beta_1$$
$$a_i \in \{0, 1, 2\},\quad i = 0, 1, 2, 3$$
$$(\beta_0)_{3^2} = (a_3 a_2)_3,\quad (\beta_1)_{3^2} = (a_1 a_0)_3$$
$$(\beta)_p \in \{0, 1, 2, \dots, p-1\}_p$$

Table III shows its related remainder in binary and Ternary Valued Logic representation.

TABLE III
Representation of Remainder of $m = 3^4 = 81$

Decimal	Ternary Valued Logic				New Representation	
0	0	0	0	0	0	0
1	0	0	0	1	0	1
2	0	0	0	2	0	2
3	0	0	1	0	0	3
⋮	⋮	⋮	⋮	⋮	⋮	⋮
8	0	0	2	2	0	8
9	0	1	0	0	1	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
77	2	2	1	2	4	3
78	2	2	2	0	4	2
79	2	2	2	1	4	3
80	2	2	2	2	4	4

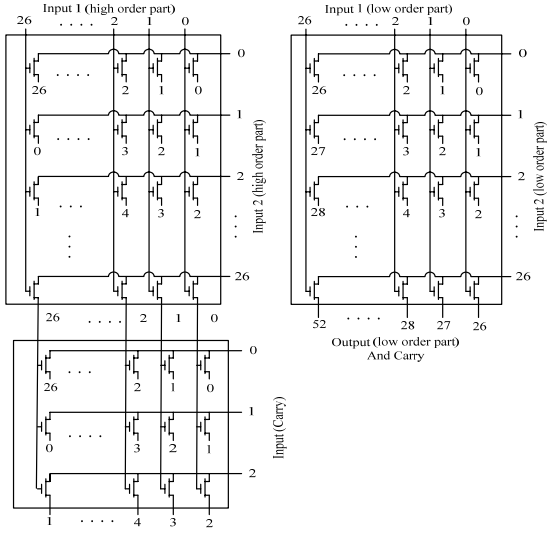


Fig. 6 Novel Adder for $m = 3^4 = 81$

Number of transistors: 1539 and Delay: 2 transistors

VI. Comparison

We compare the conventional OHRNS to the proposed OHRNS, in terms of propagation delay and the number of transistors.

Conventional One-Hot Adder:

Number of transistors: $\left(r^n\right)^2 = r^{2n}$

Delay: 1 transistor

Idea:

Number of transistors:

$$\begin{cases} \left(\left(r^{(n/2)}\right)^2 \times 2\right) + \left(r \times r^{(n/2)}\right) = 2 \times r^n + r^{(n/2)+1} & n \text{ is even} \\ \left(r^{(n-1)/2}\right)^2 + \left(r^{(n+1)/2}\right)^2 + \left(2 \times r^{(n-1)/2}\right) & n \text{ is odd} \end{cases}$$

Delay: 2 transistors (8)

VII. Conclusion

According to equations 8 we conclude that the novel proposed circuit demonstrates some significant improvement in terms of the number of transistor used and the corresponding chip area.

This improvement is proportional to the square-root of the number of transistors and hence chips area of the conventional One-Hot adder.

References

[1] H. Garner, "The Residue Number System," *IEEE Transactions Electronic Computer*, Vol. 8, pp.140-147, 1959.

[2] N. Szabo and R. Tanaka, Residue arithmetic and its applications to computer technology, (New York, McGraw-Hill, 1967).

[3] R. Conway and J. Nelson, "Improved RNS FIR Filter Architectures," *IEEE Transactions on Circuits and Systems II*, Vol. 51, No. 1, pp. 26-28, 2004.

[4] P. G. Fernandez, et al., "A RNS-Based Matrix-Vector-Multiply FCT Architecture for DCT Computation," *Proc. 43rd IEEE Midwest Symposium on Circuits and Systems*, pp. 350-353, 2000.

[5] A. D. Re, A. Nannareli and M. Re, "A Tools for Arithmetic Generation of RTL-Level VHDL Description of RNS FIR Filters," *IEEE Proceeding of the Design, Automation and Test in Europe Conference and Exhibition*, pp. 686-687, 2004.

[6] W. L. Freking and K. K. Parhi, "Low-power FIR digital filters using residue arithmetic," *31st Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA*, Vol. 1, pp. 739–43. 1997.

[7] F. Taylor, "A Single Modulus ALU for Signal Processing," *IEEE Transactions on Acoustics, Speech, Signal Processing*, Vol. 33, pp. 1302-1315, 1985.

[8] S. Yen, S. Kim, S. Lim and S. Moon, "RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis," *IEEE Transactions On Computers*, Vol. XX, No. Y, pp. 461-472, 2003.

[9] J. Ramirez, et al., "Fast RNS FPL-Based Communications Receiver Design and Implementation," *Proc. 12th Int'l Conf. Field Programmable Logic*, pp. 472-481, 2002.

[10] M. Hosseinzadeh, K. Navi and S. Gorgin**,** "A New Moduli Set for RNS: $\{r^n - 2, r^n - 1, r^n\}$," *International Conference on Electrical Engineering 2007***,** Apr. 11-12, 2007.

[11] M. Abdallah and A. Skavantzos, "On Multi Moduli Residue Number Systems with Moduli of Forms $(r^a, r^b - 1, r^c + 1)$," *IEEE Transactions Circuits System I: Regular Paper*, Vol. 52, No. 7, Jul. 2005.

[12] I. Kouretus and V Puliourus, "High-Radix Redundant Circuits for Modulo $r^n - 1, r^n$ or $r^n + 1$," Proceedings of the 2003 International Symposium on Circuits and Systems, Vol 5, 2003.

[13] A. Chren, Jr., "One-Hot Residue Coding for Low Delay-Power Product CMOS Design," *IEEE Transactions On Circuits And Systems II: Analog And Digital Signal Processing*, Vol. 45, No. 3, Mar. 1998.

[14] S. L. Hurst, "Multiple-Valued Logic – Its status and its future," *IEEE Transaction on Computers*, pp. 1160-1179, 1984.

[15] A. F. Gonzalez, and P. Mazumdar, Redundant Arithmetic, "Algorithms and Implementations," *Integration: The VLSI Journal*, Vol. 30, No. 1, pp. 13-53, 2000.

[16] M. Hosseinzadeh, K. Navi and S. Timarchi, "Design Residue Number System Circuits in Current mode," *14th Iranian Conference of Electrical Engineering*, 2006.

[17] M. Hosseinzadeh, K. Navi and S. Timarchi, "New Design of 4-3 Compressor," 11th *International CSI Computer Conference of Iran*, 2006.

[18] S. Hanzawa, T. Sakata, K. Kajigaya, R. Takemura, and T. Kawahara, "A Large-Scale and Low-Power CAM Architecture Featuring a One-Hot-Spot Block Code for IP-Address Lookup in a Network Router," *IEEE Journal of Solid-State Circuits*, Vol. 40, No. 4, Apr. 2005.

[19] W. A. Chren., "Delta–Sigma Modulator with Large OSR Using the One-Hot Residue Number System," *IEEE Transactions on Circuits and Systems—II: Analog and Digital Signal Processing*, Vol. 46, No. 8, Aug. 1999.