Restricted Moduli Symmetrical Signed Residue Addition: Part I

First M. N. Daikpor, Second O. Adegbenro, Member, IEEE

Abstract — In this paper we propose a scheme for the design of a Symmetrical Multiple Valued Logic (SMVL) arithmetic circuit based on the use of restricted moduli Symmetrical Signed digit Residue Number system (SSRNS). Sign and overflow detection as well as magnitude comparison operations are accomplished without recourse to the traditional complex Mixed Radix number System (MRS) conversion process and multiplicative inverse computation. The method is particularly general purpose systems oriented. Addition operations are executed economically, fast and at constant speed.

Keywords — **conversion, carry-free, full adder, magnitude, number system, symmetrical-signed-residue, weighted.**

I. Introduction

PRACTICALLY all human endeavours today are Information and Communication Technology Systems (ICTS) driven. These systems rely on high speed, secured and trusted communication gadgets whose operations depend on special classes of very big integer arithmetic circuits. The type of arithmetic operations employed in these devices is not only fixed point but also must be carry-free. The method of number representation is a critical design factor in order to attain the desired high-speed operations of these circuits; designers still have to find optimal ways of managing carry propagation chains [1], [2].

It has long been established that the non-redundant non-weighted Residue Number System (RNS) and the weighted highly redundant Signed-Digit Number System (SDNS), attract fast and efficient arithmetic. [2], [3], [4], [5], [6]. However, RNS arithmetic is beset with complex conversion procedure, difficult sign detection, cost intensive overflow detection and magnitude comparison strategies that require Mixed Radix number System (MRS) and practically none in-existence simple division algorithm. Hence, RNS arithmetic found application in special areas such as: error correction, fault tolerance and digital filter design, power dissipation reduction in VLSI design, fast Fourier transform structures and cryptography [7], [8], [9], [10], [11]. On the other hand, the SDNS representation in addition to the above benefits of RNS provides a means of presenting operands at higher radices thereby supporting SMVL systems design which find application in image processing, robotic, and finite field arithmetic [6], [7]. The SDSN drawback is that it requires more character digits for operands representation. Thus in systems of high frequency addition operation this requirement is a setback in terms of circuit power consumption.

It is already established that combined Signed Digit (SD) and Residue Number (RN) arithmetic could result in reduced carry propagation delay and power consumption but the deployment of this in fast arithmetic circuit design is still at its infancy. For example the related arithmetic circuits in [2] are parameterized to provide basic building blocks for binary logic signal VLSI processors. Binary logic VLSI circuit's main objective is miniaturization with improved circuit complexity all at reduced cost. The Multiple Valued Logic (MVL) systems extend the horizon of this objective by virtue of its higher information per line capacity. Very recently, a Symmetrical Multiple Valued Logic (SMVL) developed from Restricted radix-7 Quaternary Signed Digit (Rr7SqSd) number system has been proposed [7]. It is highly probable that an interesting cross line could evolve when the character digit set of a symmetrical SDNS coalesces with a symmetrical signed digit RNS character digit set.

The proposed SSRNS addition scheme widens the scope of RNS arithmetic application by removing the inherent bottle neck in RNS arithmetic operations namely: sign detection, overflow detection and magnitude comparison. This contribution will thus make RNS arithmetic possible for use in general purpose digital systems. The organization of the remaining part of this paper is as follows. The background to this paper is presented in section II. Section III presents the SSRNS and the conversion procedures. SSRNS addition is presented in section IV.

II. BACKGROUND

Exegesis of RNS arithmetic can be found in popular works such as [2], [4], and [5]. Similar works on Signed-Digit Number System (SDNS) arithmetic can be found in [6]. The concept of restricted radix-7 Symmetrical quaternary Signed-digit number system (Rr7SqSd) and its arithmetic is in the most recent works of [7], [12], [13], and [14]. Hence, by extension restricted radix-5 Symmetrical ternary Signed-digit (Rr5StSd) number system with the character digit set $L \in \{-2,-1,0,1,2\}$ and Restricted radix-3

Corresponding First M. N. Daikpor, is with Faculty of Engineering, Department of Electrical and Electronics Engineering, University of Lagos, Akoka Lagos , Nigeria e-mail michaelnnaseimodaikpor@rocketmail.com
Second O. Adegbenro, is with the Centre for Energy Efficiency and Conservation University of Lagos, Akoka Lagos , Nigeria e-mail wole _adegbenro@yahoo.com

Symmetrical binary Signed-digit (Rr3SbSd) number system exist with the character digit set $L \in \{-1,0,1\}$.

III. THE SSRNS

The number system we are proposing here provides a cross over point between the SDNS and the RNS. It therefore possesses the properties of the two number systems as it is composed of symmetrical signed residues numbers x_k, of the moduli set $p_1 p_2 .. p_k .. p_n$. A symmetrical signed residue number x_k, is a unique representation of the signed integer x, such that for a set of unsigned relative prime moduli set $P_k; k = 1,2,..,n$ the signed integer x can be described as

$$x = (x_1 | x_2 | .. \, | .x_n |) SSRNS (P_1 | P_1 | ... \, | .P_N |) \qquad (1)$$

for all $|x| \in [-M, M]$, where: $x_k = x \bmod p_k$, $|M| = \prod_1^n p_k$ and if ζ_k is a restrictor $\leq |p_k - 1|$ of modulo p_k residues then the SSRNS digit x_{p_k} takes the values

$$x_{p_k} \in \left(\left(\overline{p_k - (\zeta_k - 1)}\right), , \bar{1}, 01, , (p_k - (\zeta_k - 1))\right) \quad (2)$$

Now for bridging Rr7SqSd and SSRNS we take as an example $k = 3$ and the relative prime moduli set as $(7|5|3|)$ which provide a unique representation of any signed integer x, in the dynamic range $-105 < x < 105$. It then follows that with $(\zeta_7, \zeta_5, \zeta_3) = (3,2,1)$

$$\left.\begin{aligned} x_{7_k} &\in \{-3,-2,-1,0,1,2,3\} \\ x_{5_k} &\in \{-2,-1,0,1,2\} \\ x_{3_k} &\in \{-1,0,1\} \end{aligned}\right\} \qquad (3)$$

The following procedures apply for the specified cases.

A. Decimal to SSRNS conversion

1. Obtain the $radix - M/2$ form $X^* = X^*_{m-1} X^*_{m-2} .... X^*_0$, of the number.
2. For each X^*_i, compute the RNS residue $T_{i_k} = X^*_i \bmod p_k$.
3. Represent T_{i_k} in SSRNS i.e. $t_{i,l} = f(T_{i_k})$ and $l \in \{1,2,3\}$

Hence, $X = \{X^*_i\} = (t_{i,1} t_{i,2} t_{i,5}) SSRNS (7|5|3)$,

e,g $X = 65$; $X_i = (2|1|\bar{1}) SSRNS (7|5|3)$.

B. Rr7SqSd to SSRNS

1.Partition the given number $X_{Rr7SqSd} = x_{Rj-1} x_{Rj-2} .... x_{Rj0}$ where $x_{Rj-i} \in \{-3,-2,-1,0,1,2,3\}$, from the right into m groups of 3-Rr7SqSd

$$x_{Rj,3} x_{ij2} x_{j,1} = (\alpha_j \beta_j \lambda_j),$$
$$-172 < \alpha_j, \beta_j, \lambda_j < 172$$
$$\alpha, \beta, \lambda \in \{-3,-2,-1,0,1,2,3\}.$$

2.Compute the SSRNS equivalent $t_{R1j}, t_{R2j}, t_{R3j}$ of the Rr7SqSd j^{th} partition $\alpha_j \beta_j \lambda_j$ as follows;

$$\left.\begin{aligned} t_{Rj1} &= \lambda_j \\ t_{R2j} &= (7(7\alpha_j + \beta_j) + \lambda_j) \bmod p_2 \\ t_{R3j} &= |(\alpha_j + \beta_j + \lambda_j)| \bmod p_3 \end{aligned}\right\} \qquad (4)$$

e.g.

$$1\bar{3}23 = 213_{10} = 2|3_{Radix-M/2} = (22\bar{1}|30\bar{1}) SSRNS (7|5|3).$$

C. SSRNS to decimal

Rather than using the Mixed Radix number System (MRS) , multiplicative or Look Up Tables (LUT) the following formular is developed heuristically. If $p_1 p_2 ... p_k$ is a set of relatively prime moduli in the interval $\left(-\frac{M}{2}, \frac{M}{2}\right)$ $M = 2\prod_{k=1}^{l} p_k$ then there exist the set of integers $u_{1,}, ..., u_k$, $-\frac{M}{2} \leq u_i \leq \frac{M}{2}$ such that

$$u_i \bmod p_j = \begin{cases} \pm 1 \;\; ; \text{ if } i = j \\ \\ 0 \;\; ; \text{if } i \neq j \end{cases} \qquad (5)$$

Satisfying the equation (10)

$$u_1 + ... + u_l = \frac{M}{2} + 1 \text{ or } u_1 - \frac{M}{2} + .. + u_l - \frac{M}{2} = -(M-1) \text{ ;for } u_1 \bmod p_1 = ... = u_l \bmod p_l = 1 \qquad (6)$$

Similarly,

$$-u_1 - ... - u_l = -\left(\frac{M}{2} + 1\right) \text{ or } \frac{M}{2} - u_1 + .. + \frac{M}{2} - u_l = M - 1 \text{ ; for } u_1 \bmod p_1 = .. = u_l \bmod p_l = -1 \qquad (7)$$

If the decimal equivalent of the SSRNS digits $t_1 t_2 .... t_l$ is φ_i $-157 \leq \varphi_i \leq 157$ and denoting $\mu_k = u_k \bmod p_k$, $k = 1,2,..,l$ then,

$$\left(\mu_1 \prod_{h=2}^{l} p_h\right) \bmod p_1 = 1 \Rightarrow \mu_1 = 1$$

....

$$\left(\mu_m \prod_{h^*=1}^{m-1} p_{h^*} \prod_{h=m+1}^{l} p_h\right) \bmod p_m = 1 \Rightarrow \mu_m = 1 \quad (8)$$

....

$$\left(\mu_l \prod_{h=1}^{l-1} p_h\right) \bmod p_l = 1 \Rightarrow \mu_l = l-1$$

provided: $u_k = \mu_k \frac{M/2}{p_k}$. Consequently,

$$\varphi = \sum_{k=1}^{l} \mu_k \frac{M/2}{p_k} t_k = \sum_{k}^{l} u_k t_k \qquad (9)$$

For $l_{\max} = 3$; $\mu_1 = 1$, $\mu_2 = 1$ and $\mu_3 = 2$ therefore; $u_1 = 15$, $u_2 = 21$ and $u_3 = 70$. Hence,

$$\varphi_i = (15t_1 + 21t_2 + 70t_3) \qquad (10)$$

Long SSRNS digits strings are partitioned into g groups of $3-SSRNS$ digits and

$$\varphi = \sum_{i=0}^{g-1} \varphi_i = \sum_{i=0}^{g-1} (15t_{1i} + 21t_{2i} + 70t_{3i})\left(M/2\right)^i \quad (11)$$

IV. SSRNS ADDITION SCHEME

In this contribution we are more concerned with very big integer operand SSRNS addition operations that are operands are converted to $radix-M/2$ number system character digits and subsequently to SSRNS. We describe the addition operation by equation (12)

$$\left.\begin{array}{l} \delta_{ip} = \begin{cases} \bar{1} & ; \text{if } \alpha_{ip} + \beta_{ip} < \bar{a}_p \\ 1 & ; \text{if} \alpha_{ip} + \beta_{ip} > a_p \\ 0 & ; \text{otherwise} \end{cases} \\ \gamma_{ip} = \alpha_{ip} + \beta_{ip} - p\delta_{ip} \\ a_p \in (3,2,1)RNS(7|5|3) \end{array}\right\} \qquad (12)$$

Where $\alpha_{ip_k}, \beta_{ip_k}$ are operand pairs and γ_{ip_k} sum of the signed $radix-M/2$ character digits in the SSRNS representation addition operation. $\alpha_{7i,}\beta_{i7}, \gamma_{7i} = \{x_{7_k}\}$, $\alpha_{5i}, \beta_{5i}, \gamma_{5i} = \{x_{5_k}\}$, and $\alpha_{3i}, \beta_{3i}, \gamma_{3i} = \{x_{3_k}\}$ as earlier defined in equation (3). There are inherent problems here, i) since the addition is $radix-M/2$ pair-wise there is danger of the weighted number systems equivalent of operand's $radix-M/2$ character digit-partitions to acquire varying signs that may lead to inaccurate computed final result. ii) The magnitude ψ_o,of any operand participating in an SSRNS arithmetic lies in the dynamic range $-M/2 < \psi_o < M/2$ just as that of the computed sum φ_s lies in the interval $[-M, M]$. The implication of these observations is that there is bound to be numerical trimming of any computed sum magnitude that lies outside the SSRNS dynamic range. This of course can bring about fictitious sums of the addition operation. Which means long SSRNS digit input string addition schemes must have mechanism for identifying/detecting $radix-M/2$ -partition sign, operand-pair and result pairs parity (odd or even) status, extend of partition sum overflows detection and it's reporting. Existing methods of solving these difficult-to-handle problems in the RNS domain [8], [9] as earlier enunciated require conversion of the RNS operands to MRS domain for computability as well as multiplication inverse computations.

In this paper, these problems are again solved heuristically in a very simple way using the Rr7SqSd addition. The $Radix-M/2$ character digits input stream of operands appear both in 3-Rr7SqSd and in the corresponding 3-SSRNS digits packet streams. The 3-Rr7SqSd operand-pairs are added together per Rr7SqSd in parallel in a four level Rr7SqSd addition operation described by equation (13)

$$\left.\begin{array}{l} z_i = \alpha_i + \beta_i \\ \delta_i = \begin{cases} -1 & ; \text{If } z_i < \bar{a} \\ 1 & ; \text{ if } z_i > a \\ 0 & ; \text{if } otherwise \end{cases} \\ \tau_i = z_i - 7\,\delta_i \\ \lambda_i = \tau_i + \delta_{i-1} \end{array}\right\} \qquad (13)$$

where: $\alpha_i, \beta_i, \tau_i, \lambda_i \{-3,-2,-1,0,1,2,3\}$ and δ_i, δ_{i-1} Є { -1,0,1}. The addition accomplishes the magnitude comparison aspect. The sign of the i^{th} $radix-M/2$ character digit pair Rr7SqSd addition operation is the sign of the most significant Rr7SqSd . of that partition and the corresponding outputs $\lambda_{i=} = \delta_i$, $\lambda_{i,3}$, $\lambda_{i,2}$ and $\lambda_{i,1}$ facilitates overflow discussion making. The actual $radix-M/2$ character digit-pair addition operation is executed in SSRNS domain modulo-wise using equation (16). Overflows appear just as inter-radix carries.

One immediate area of application for the SSRNS arithmetic circuits is in SMVL systems where the processing signal profile, rather than the binary logic, is the Rr7SqSd logic levels. The Rr7SqSd number system being weighted is susceptible to carry propagation chains that adversely affect system operation speed. To avoid this problem, we embed SSRNS addition procedure in Rr7SqSd addition operation. Long Rr7SqSd-input-string operands $x_i = x_{i_3}, x_{i_2}, x_{i_1}$, $y_i = y_{i_3}, y_{i_2}, y_{i_1}$ are divided into *m*-groups of 3-Rr7SqSd each with $-171 \le x_i, y_i \le 171$. Let $-342 \le z_i \le 342$, be the sum of the i^{th} partition addition be such that $z_i = z_{i3}z_{i2}z_{i1}$, $z_{il} \in \{-3,-2,-1,0,1,2,3\}$ $l \in \{3,2,1\}$. In the SSRNS domain, two $radix - {}^{M}\!/_{2}$ character digits are required to represent x_i, y_i and z_i. Taking $(\theta_{0i}\theta_{1i}),(\vartheta_{0i}\vartheta_{1i})$ and $(\gamma_{0i}\gamma_{1i})$ as x_i, y_i and z_i then $-\left({}^{M}\!/_{2}-1\right) \le \theta_{1i}, \vartheta_{1i}, \gamma_{1i} \le \left({}^{M}\!/_{2}-1\right)$, $-1 \le \theta_{0i}\vartheta_{0i} \le 1$ and $-3 \le \gamma_{0i} \le 3$. To reduce cost and enhance operation speed operands are first represented in $radix - {}^{M}\!/_{2}$ character digits and then each $radix - {}^{M}\!/_{2}$ character digit is converted to both Rr7SqSd and SSRNS presentations. In terms of $radix - {}^{M}\!/_{2}$ the addition process is represented by equations (17), (18) and (19)

$$\gamma_{1i} = \theta_{1i} + \vartheta_{1i} \tag{17}$$

$$c_i = \begin{cases} \pm 1\,; \text{if}\, \gamma_{1i} \ge {}^{M}\!/_{2} \text{ or } = \pm\left({}^{M}\!/_{2}-1\right), \\ \gamma_{1i} = \pm {}^{M}\!/_{2} - 1, \gamma_{1i-1} \text{ and } c_{i-2} = \pm 1 \\ \\ 0 \quad ;\text{Otherwise} \end{cases} \tag{18}$$

$$\gamma_{1,i+1} = \begin{cases} \gamma_{1i+1} \mp l\,{}^{M}\!/_{2}\,; \text{if } c_i = \pm 1 \\ \\ \gamma_{1i+1} \quad ; \text{ otherwise} \end{cases} \tag{19}$$

Where $l \in \{-3,-2,-1,0,1,2,3\}$ corresponding to $\{-315,-210,-105,0,105,210,315\}$ and $\theta_{1p} \in \{\alpha_{7i}, \alpha_{5i}, \alpha_{i3}\}, \vartheta_{1p} \in \{\beta_{7i}, \beta_{5i}, \beta_{3i}\}$.

Computational experiments conducted showed 50% operation execution speed increment using this detection-compare-migrate-and-return for alignment approach. There is a 75% increase in speed when magnitude alignment is also carried out in the SSRNS domain though with a higher complexity trade-off. The approach does not need a Chinese Remainder Theory (CRT) and the Extended Euclidean Algorithm (EEA) for backward conversion operation.

REFERENCES

[1] R. Zimmermann, "Lecture notes on computer arithmetic: principles, architectures and VLSI design," Integrated system Laboratory, Swiss Federal Institute of Technology (ETH), CH-8092 Zurich, Switzerland. March 16, 1999. http://www.iis.ee.ethz.ch/

[2] A. Lindstrom, M. Nordseth, L. Bentsson and A. Omondi,"Arithmetic circuits combing residue and signed-digit representations," in Proc. of the 8th Asia-Pacific Computer Systems Architecture conference (ACSAC"2003) Aizu-Wakamatsu City Japan , Sept. 2003, Published by Springer-verlag in lecture Notes in Computer Science(LNCS) Vol. 2823.

[3] S. Shieh and C. Wu, "Asymmetric high-radix signed-digit number system for carry-free addition- Accepted for publication," Journal of Information Science and Engineering 19, February 24, 2003, pp. 1015-1039.

[4] B. Parhami, "RNS Representations with redundant residues- Invited Paper," IEEE (2001) 0-7803-7147-X/01/$10.00, pp. 1651-1655.

[5] S. Wei, "Number conversions between RNS and mixed-radix number system based on modulo (2^p-1) signed-digit arithmetic," Proc. SBCCT'05 September 4-7, 2005, Florianopolis, Brazil, ACM 1-59593-174-0/05/0009, pp. 160- 165.

[6] M. Kameyama and Tatsuo Higuchi, "Design of a radix- 4 signed-digit arithmetic circuit for digital filters,"Proc. of the 12th IEEE International Symposium on multiple-Valued Logic, North-western University, Evanston, IL. USA 1980, pp 272 -277.

[7] M.N Daikpor and O. Adegbenro," Radix - 7 signed digit element finite field arithmetic," Proc of the IEEE International conference on signal processing and communication, Dubai November 2007, pp 708 – 711.

[8] C. K. Cheng, "CSE: Computer arithmetic algorithms and hardware design lecture 2: redundant and residue number systems," 2006, http://cseweb. ucsd.edu/classes/fa06/cse246/lect2.pdf.

[9] N. Stamenkovic, "Digital FIR filter architecture based on residue number system," FACTA UNIVERSITATIS (NIS) Ser.:ELEC.ENERG. vol.22, N0. 1, April 2009, pp 125-140.

[10] M. Hosseinzadeh, S. Jafarali and K Navi., "A novel multiple valued logic OHRNS modulo r^n adder circuit," Proc of World academy of Science, Engineering and Technology, Vol. 25 November 2007 ISSN 1307-6884, pp 128 – 132.

[11] F. Barsi and P Maestrini, "Error correcting properties of redundant residue number systems," IEEE Transactions on Computers, Vol. C-22.N0. 3, March 1973, pp 307 – 314.

[12] B.Tseng, G.A. Jullien and W. Miller, "Implementing FFT structures Using the Residue Number System," IEEE Transactions on Computer, vol. C-28, N0 11, November 1979, pp 831 – 845.

[13] F. J. Taylor, "A VLSI Residue Arithmetic Multiplier," IEEE Transactions on Computers, Vol. C-31, N0. 6, June 1982, pp 540 – 546.

[14] V. Parlours and T. Strouraitis, "Novel High-radix Residue Number System Architectures, " IEEE transaction circuits and systems-II Analog and Digital Processing , Vol. 47, N0. 10 October 2000, pp 1059 -1073.

[15] M.N. Daikpor and O. Adegbenro, "Efficient carry-free Rr7SqSd addition algorithm". Proc of the 3rd International Conference on Emerging Trends, Research directions and Training Requirements of the 21st century Electrical and Electronics Engineering, University of Lagos . 22nd to 24th, July 2009. Pp 102- 107.