World Applied Sciences Journal 4 (3): 332-337, 2008
ISSN 1818-4952
© IDOSI Publications, 2008

High Speed Implementation of r^n Moduli

[1]Somayyeh Jafarali Jassbi, [1]Mehdi Hosseinzadeh, [2]Omid Hashemipour and [2]Keivan Navi

[1]Department of Computer Engineering,
Science and Research Branch, Islamic Azad University, Tehran, Iran
[2]Faculty of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran

Abstract: The Residue Number System (RNS) is non Weighted System. It supports parallel, high speed, low power and secure arithmetic. There are some concerns related to the application of this Number System: reaching the most possible speed and the largest dynamic range and so having bigger moduli. There is a conflict when one wants to resolve all of these problems. 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 is increased in order m^2. With the use of Multi-Level we can solve the largest dynamic range. For having big moduli we can use Multiple-Valued Logic. In this paper combining the Multi-Level Residue Number System and One-Hot Residue Number System and so Multiple-Valued Logic we represent a high speed implementation for r^n moduli.

Key words: Computer arithmetic . Multi-Level Residue Number System (MLRNS) . One-Hot Residue Number System (OHRNS) . Multiple-Valued Logic (MVL) . Multiple-Valued Logic One-Hot Multi-Level Residue Number System (MVLOHMLRNS)

INTRODUCTION

As we know one of the most important goals in VLSI circuit design are reducing power consumption and increasing calculation speed. Residue Number System is one of the methods to reach these goals.

Residue Number System is unconventional and non-Weighted Number System in which the additions, subtractions and multiplication are inherently carry-free. As a result we may add, subtract and multiply numbers in one step regardless of the length of the number involved [1].

Due to its special features, the Residue Number System has many applications in arithmetic functions such as Digital Signal Processing, Digital Filtering, Coding, RSA ciphering system [2], digital communications, Ad-hoc network, storing and retrieving information [3], Error detection and Correction [4,5] and fault tolerant systems. This system is generally used in those areas where addition, subtraction and multiplication operations of numbers are being repeated. Moreover, since in this system the calculations on the remainders are done independently if one error occurs on one remainder it won't be transferred to other moduli. In other words, the architecture of RNS is inherently tolerant against faults and error detection and correction are quite possible.

For having best factors in RNS such as simplicity of moduli selection, having a lower power consumption and so higher calculation speed we can use the combination of Multi- Level Residue Number System and One-Hot Residue Number System that will be examined respectively and after that Multiple-Valued Logic One-Hot Multi-Level Residue Number System that is represented. At the end Multiple-Valued Logic One-Hot Multi-Level Residue Number System will be compared to other Residue Number System from the respective of the simplicity of moduli selection, calculation speed and the expansion of dynamic range and power consumption. Finally an overall conclusion will be represented.

MATERIALS AND METHODS

Multiple-valued logic: Multiple-Valued logic is a non-binary logic and involves the switching between more than 2 states.

It means that Multiple-Valued Logic (MVL) is the ability of a circuit or system to perform math or logic operations in a radix above 2 (binary). Omni base's

Corresponding Author: Dr. Somayyeh Jafarali Jassbi, Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

technology easily enables integrated circuits to operate in ternary (base 3) or ternary (base 4) and can be extended beyond.

MVL solves the limiting problems of today's IC technology: Current leakage, heat dissipation and error rates associated with packing more transistors into less silicon.

Multiple-Valued logic:

- Increases data density and throughput
- Increases functionality by up to 50%*
- Reduces die size & interconnects
- Reduces power consumption by 40-75%* to exceed international standards and requirements.

Residue number system: In the Residue Number System An integer X is represented by an n-tuple $(x_1,x_2,x_3,\ldots,x_n)$ where x_i is a nonnegative integer satisfy $X=m_iq_i+r_i$.This causes an increase in calculation speed and a reduction in its power consumption.

Residue Number System is specified by moduli set like $\{m_1, m_2, m_3,\ldots, m_n\}$ in which all the moduli are positive integers. If all the moduli are relatively pair wise prime the system will have the largest possible dynamic range which equals [a,a+M) in which a is an integer and M is:

$$M=\prod_{i=1}^{n} m_i \tag{1}$$

The integer X in a<=X<a+M has a single representation in Residue Number System which is shown by the set of remainders $(x_1,x_2,x_3,\ldots,x_n)$. In this way:

$$x_i = X \bmod m_i,\ i=1,2,3,\ldots,n \tag{2}$$

In order to reconstructing the specified number X the remainders $(x_1,x_2,x_3,\ldots,x_n)$ the Chinese Remainder Theorem is applied as follows:

$$X=\left\langle \sum_{i=1}^{n} (x_i N_i)_{m_i} \times M_i \right\rangle_M$$

$$M=\prod_{i=1}^{n} M_i$$

$$M_i=\frac{M}{m_i} \quad ,N_i=\left\langle M_i^{-1}\right\rangle_{m_i} ,i=1,2,3,\ldots,n \tag{3}$$

In which $<M_i^{-1}>$ is defined as multiplicative inverse with moduli.

Multi-level residue number system: Considering the impact of Residue Number System in increasing calculation speed, reducing power consumption and increasing the security and fault tolerance, it would be possible to perform arithmetic calculations on each modulus with a new Residue Number System. It is possible to repeat this procedure until we reach very small moduli, in other words this procedure could be repeated in several levels. The system which is achieved form the above mentioned procedure is called Multi-Level Residue Number System. The only restriction that should be considered in Multi-Level Residue is that the Residue Number System dynamic range that is considered for i level of each (i-1) moduli-level should be greater or equal to those moduli.

In this article, for having a more simple representation two-level Residue Number System is being analyzed. It should be mentioned that this method could be generalized to more than two levels.

In two-level Residue Number System, two symmetrical coding key algorithms are used inside each other; therefore the system has a much higher security level than the Residue Number System. The other advantage of two-level Residue Systems is the simple selection of moduli set for a large dynamic range that is by selecting a few large moduli and applying a new Residue Number System with a lower power for second level this capability is achieved. By having few moduli with higher power in the first level; first the need for moduli to be relatively pair wise prime is eliminated and there is no obligation for the moduli to be symmetric and regular, second as the number of moduli is reduced the concerning conversion circuits, become simple and the operation is done rapidly. Also, in the second level since the moduli are small because of the limited propagation of carries, the internal calculations of the Residue Number System are done faster.

The expressions and terminologies used in this article for two-level Residue Number System are as follows:

- $\{m_1, m_2, m_3,\ldots, m_n\}$: The first level Residue Number System moduli.
- $\{m_{i1}, m_{i2}, m_{i3},\ldots, m_{in}\}$: The second level Residue Number System moduli for m_i moduli that i=1,2,3,…,n.
- $\{r_1, r_2, r_3,\ldots, r_n\}$: The weighted number residues in the first level Residue Number System.
- $\{r_{i1}, r_{i2}, r_{i3},\ldots, r_{in}\}$: Residues in the second level of Residue Number System related to i=1,2,3,…,n.

The arithmetic calculations of the Residue Number System manipulates on the remainders of second level.

Two functional operations in the Number System are defined as follows:

$$\{z_{i1}, z_{i2}, z_{i3}, \dots\ z_{in_i}\} = \{x_{i1}, x_{i2}, x_{i3}, \dots\ x_{in_i}\} \circ \{y_{i1}, y_{i2}, y_{i3}, \dots, y_{in_i}\} \quad (4)$$

$$z_{ij} = (x_{ij} \circ y_{ij}) \bmod m_{ij},\ i = 1,2,3,\dots,n$$

And "o" could be addition, subtraction and multiplication. For converting weighted Number System into two-level Residue Number System first, that number should be converted to first level moduli system and then the acquired remainders should be changed into second level Residue Number System. The general diagram is shown in Fig. 1.

In the reverse conversion, n number n_i-Channel CRT that i=1,2,3,…,n is necessary to change the remainders of he second level into the equivalent remainders of the first level and then by using a n-channel CRT it is changed into Weighted Number System. The general diagram is illustrated in Fig. 2 [6].

One-hot residue number system: M_i moduli remainders are from zero to m_i-1 that in One-Hot representation a signal line is dedicated for each of these numbers: The activity of each signal shows the similar remainder with it. One–Hot representation for m_i moduli remainders are shown in Fig. 3.

In this representation system in each moment only one of the lines are active and the remaining lines are inactive. By changing the entrance amount, the amount of two lines changes at maximum level. Therefore the power consumption waste is at minimum level. One-Hot Residue Number System is simple and rapid and has regular and simple structure. In One–Hot representation of remainders, the addition is done by circular shifts. These shifts could be done in several ways and the best one is the Barrel shifter application.

The main and basic element in One-Hot is Barrel shifters. In addition to m_i moduli one of the operands are shifted as the other shifter. In Fig. 4 this operation is represented for moduli 4 by a graph.

In this graph, one of the two operands is the system condition and the other one is the entry to the system. For example if one of the operands is 2, in the graph we give 2 to it, now the other operand will be as follows:

- If it is zero, then the system will remain in position 2.
- If it is 1, then the system will change to position 3.
- If it is 2, then the system will change to position 0.
- If it is 3, then the system will change to position 1.

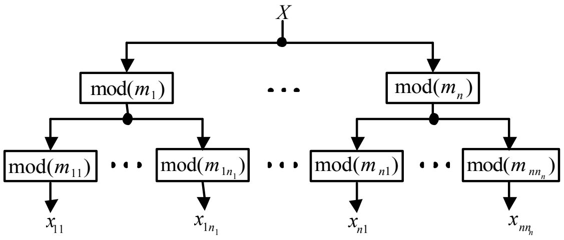


Fig. 1: Converting weighted number system into second level RNS

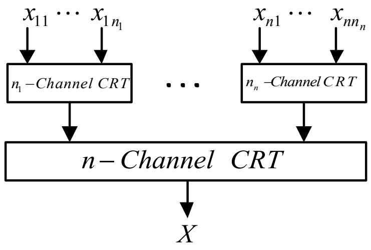


Fig. 2: Converting two-level RNS into weighted number system

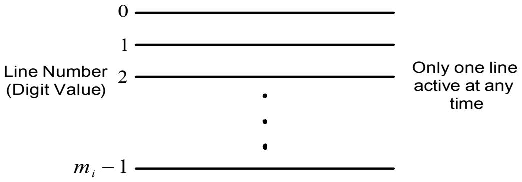


Fig. 3: One-hot representation for m_i remainders

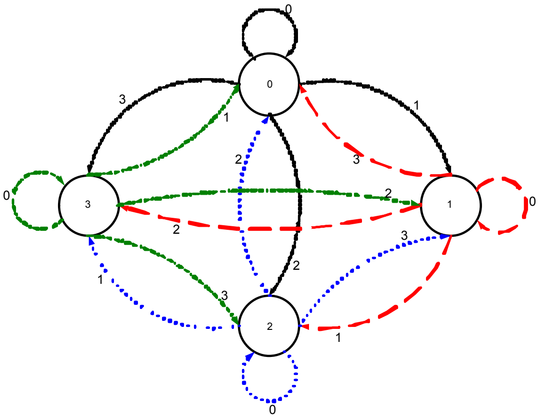
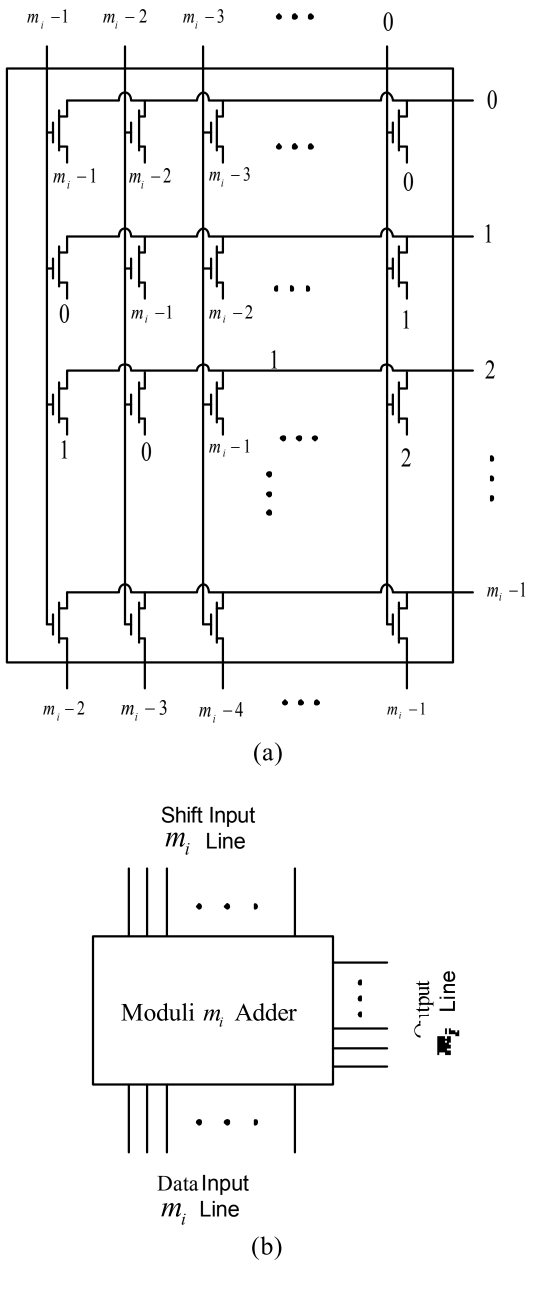


Fig. 4: Addition position for Moduli 4

In Fig. 5a, One-Hot addition is represented in which two entries are named as "data entry" and "shift entry" and in Fig. 5b the total schema is represented.



(a)

(b)

Fig. 5: (a) Additive symbol of On-Hot for m_i moduli
(b) Total schema of Additive symbol of On-Hot for m_i moduli

The shifter transfers the "data entry" to the same extent as "shift entry" and it moves toward output point. The delay of this circuit equals one transistor. In Fig. 6, a One-Hot addition is shown for moduli 5 on transistor level and the transistor delay is shown clearly in this figure.

The subtraction is the same as addition. The only difference is that "data entry" has a reverse shift equal to "entry shift".

One of the important characteristics of this operation is its independence to the type of moduli (2^n, 2^n-1, 2^{n-1}-1), (2^n + 1, 2^n, 2^{n-1}-1), (2^n-3, 2^n+1, 2^n-1, 2^n + 3) collections or (r^n - 1, r^n, r^n-2), (r^a, r^b-2, r^c+1), moduli collections are selected. The main reason for this selection is the simplicity of its circuit implementation. But in One-Hot, the implementation is totally independent of the moduli type [7-9].

One of the short comings of One-Hot System is that it couldn't be implemented for large moduli since the number of transistor are increased. Therefore this system is suitable for small moduli but practically it is not applicable for large moduli.

Multiple-valued logic one-hot multi level residue number system for r^n: As it was illustrated in the earlier part, One-Hot Residue Number System is suitable for small moduli, but for large moduli it is not applicable because the transistors are added in arithmetic calculations. On the other hand, in Multi-Level Residue Number System the arithmetic operations are done on large dynamic range, also in Multiple-Valued logic we have large moduli.

In this article these three techniques are combined with each other and the result is "Multiple-Valued logic One –Hot Multi-Level Residue Number System".

In combining these three techniques, first a moduli collection with large modulus is selected and then for each of these moduli one new Residue System is chosen and the procedure is repeated. Therefore in the final level, one Residue Number System with moduli is gained.

If we consider two numbers A and B as the remainders of the moduli m, then we will have: 0<=A<=m-1, 0<=B<=m-1. For performing addition operation in m moduli first the two numbers should be added therefore the sum would remain in 0<=A+B<=2m-2 range. If the sum of two numbers is equal or greater than the modulus, it is enough to subtract the moduli amount from the sum.

$$\begin{cases} A+B<m & \Rightarrow \quad A+B \\ A+B\geq m & \Rightarrow \quad A+B-m \end{cases} \tag{5}$$

In other words, if the sum equals or is larger than the moduli we will add it to moduli complement and the carry will be thrown away therefore the addition circuit in m circuit in Residue Number System will be illustrated in Fig. 7. The circuit delay is:

$$\tau = 2\tau_{n-Bit-Adder} + \tau_{Or} + \tau_{Mux(2\times 1)} \tag{6}$$

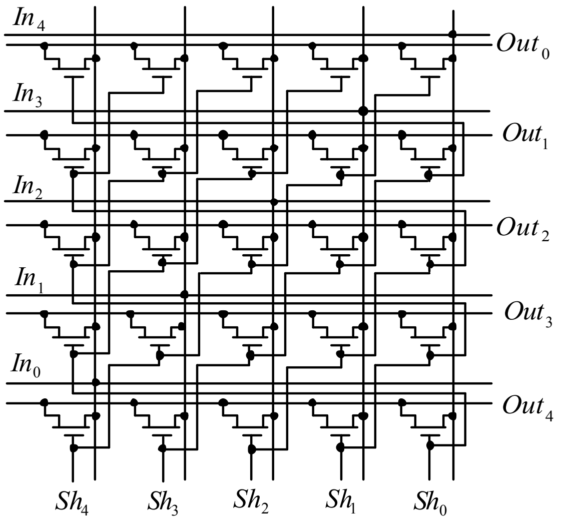


Fig. 6: One-Hot additive for moduli 5

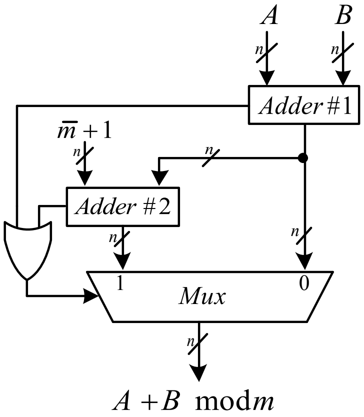


Fig. 7: Addition circuit residue number system in m moduli

By using different techniques such as CSA for adding number 1, in Fig. 7 the three entries could be converted into two outputs and then the addition will be performed in parallel way and also we may use other techniques such as multi-operand additions but it would be too complicated.

Since the circuit delay in One-Hot implementation equals one transistor therefore One-Hot circuits are much faster and also since two signals are active in these circuits the power consumption is low.

For example if we consider the moduli collection of (2^{14}-1,2^{14},2^{14}+1) if One-Hot System is implemented their addition circuit $(2^{14}-1)^2+(2^{14})^2+(2^{14}+1)^2$ transistors will be needed. Now with the new method i.e. by using Multiple-Valued Logic One-Hot Multi-Level Residue Number System we will be able to change its moduli into smaller ones until we reach (3, 4 and 5) moduli. Then this collection will generally need 50 transistors for three moduli, meanwhile it will function much faster (the transistor delay).

But if we work with Residue Number System for these circuits the number of transistors and delay will be more. The delay in the worst case will happen for moduli 5 and will be:

$$\tau = 4\tau_{FA} + \tau_{Or} + \tau_{Mux(2\times 1)}$$

RESULTS AND DISCUSSION

In Table 1 a comparison is made between Multiple-Valued Logic One-Hot Multi-Level system and other Residue Number System. As we see in Table 1, comparing to other Number Systems, we have achieved significant improvement in terms of simplicity of moduli selection, dynamic range, calculation speed and power consumptions.

CONCLUSION

In this article first the Multiple-Valued Logic system and then Residue Number System, Multi-Level Residue Number System and finally One-Hot Residue Number System were examined and after that by combining these Number Systems, Multiple-Valued Logic One-Hot Multi level Residue Number System was represented for r^n.

Residue Number System has some advantages such as the simplicity of moduli selection and large dynamic range. One-Hot Residue Number System also has some

Table 1: Comparing OHMLRNS for r^n with other residue number systems

	RNS	MLRNS	OHRNS	MVLRNS	MVLOHMLRNS
Select the set of moduli	Normal	Simple	Normal	Normal	Simple
Speed of calculate	Normal	Normal	High	High	Very High
Dynamic range	Normal	Large	Normal	Large	Large
Power consumption	Normal	Normal	Low	Low	Very low

advantages such as implementation of low-power circuits and the rapidity of calculations and simple and regular structure, Multiple-Valued Logic has many advantages such as the big moduli, reduces die size & interconnects and reduces power consumption.

One-Hot Residue Number System faces certain obstacles when applying large moduli because the numbers of transistors are added in order to relate the moduli. By combining these three Number Systems and creating Multiple-Valued Logic One-Hot Multi–level Residue Number System we can benefit from the advantages of all for r^n.

REFERENCES

1. Szabo, S. and R.I. Tanaka, 1967. Residue Arithmetic andIts Applications to Computer Technology. New York: McGraw-Hill.
2. Bajard, J.C. and Laurent Imbert, 2004. A Full Implementation RSA in RNS. IEEE Transactions on Computer, 53 (6).
3. Ramirez, J. *et al*., 2002. Fast RNS FPL-Based Communications Receiver Design and Implementation. Proc. 12th Int'l Conf. Field Programmable Logic, pp: 472-481.
4. Krishna, H., K.-Y. Lin and J.-D. Sun, 1992. A coding theory approach to error control in redundant Residue Number Systems - Part I: theory and single error correction. IEEE Trans. Circuits Syst., 39L 8-17.
5. Sun, J.-D. and H. Krishna, 1992. A coding theory approach to error control in redundant Residue Number Systems -Part II: Multiple error detection and correction. IEEE Trans. Circuits Syst., 39: 18-34.
6. Parhami, B., 2001. RNS Representation with Redundant Residues. Proc. of the 35th Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, pp: 1651-1655.
7. Yassine, H.M., 1992. Hierachical Residue Number System suitable for VLSI Arithmetic Architectures. IEEE International Symposium on Circuits and Systems, 2: 811-814.
8. Skavantzos, A. and M. Abdallah, 1999. Implementation Issues of the Two-Level Residue Number System with Pairs of Conjugate Moduli. IEEE Transactions On Signal Processing, 47: (3).
9. Chren, W.A., Jr., 1998. One-Hot Residue Coding for Low Delay-Power Product CMOS Design. IEEE Transactions On Circuits And Systems II: Analog And Digital Signal Processing, 45 (3).