Advances in Wireless Communications and Networks
2016; 2(1): 11-14
http://www.sciencepublishinggroup.com/j/awcn
doi: 10.11648/j.awcn.20160201.12

An Improved Redundant Residue Number System Based Error Detection and Correction Scheme for the Moduli Set $\{2^{2n} + 1, 2^{n+1} + 1, 2^{n+1} – 1, 2^n + 1, 2^n\}$

Salifu Abdul-Mumin[1], Kazeem Alagbe Gbolagade[2]

[1]Department of Computer Science University for Development Studies, Navrongo, Ghana

[2]Department of Computer Science College of Information and Communication Tech, Kwara State University, Malete, Nigeria

Email address:

smumin@uds.edu.gh (S. Abdul-Mumin), Kazeem.gbolagade@kwasu.edu.ng (K. A. Gbolagade)

To cite this article:

Salifu Abdul-Mumin, Kazeem Alagbe Gbolagade. An Improved Redundant Residue Number System Based Error Detection and Correction Scheme for the Moduli Set $\{22^n + 1, 2^{n+1} + 1, 2^{n+1} – 1, 2^n + 1, 2^n\}$. *Advances in Wireless Communications and Networks*. Vol. 2, No. 1, 2016, pp. 11-14. doi: 10.11648/j.awcn.20160201.12

Received: October 6, 2016; **Accepted**: November 4, 2016; **Published**: December 5, 2016

Abstract: Data integrity has tremendous effects on any data communication system's performance. Communication systems are probabilistic in nature and may fail due to errors generated during the transmission process. These errors are generated due to various factors as noise, heat and other disturbance from neighboring systems. In this paper, an error detection and correction scheme based on redundant residue number system is presented. A novel 5-moduli set $\{2^{2n} + 1, 2^{n+1} + 1, 2^{n+1} – 1, 2^n + 1, 2^n\}$, for n even, is utilized. The first three moduli is the information moduli set while the last two moduli are redundant that are used for the error detection and correction. Consequently, an error detection and correction algorithm is proposed. The number of iterations in the error correction scheme has been tremendously reduced which in turn reduces the design complexity and also decreases the propagation delay.

Keywords: Data Communication, Error Detection and Correction, Redundant Residue Number System

1. Introduction

A tremendous technological transformation during the last two decades has provided a potential growth in the area of digital communication and lot of newer applications and technologies are coming up every day. The modern telecommunication industry demands higher capacity networks with high data rate, higher transmission speed and reliable medium of communication [1]. Communication traffic volumes have been increasing rapidly, especially due to the widespread proliferation of the Internet Protocol (IP), accelerating the need for large-capacity backbone networks. The integrity of such volume of information passing through modern digital systems such as filters and arithmetic units is of utmost importance [2]. This paper seeks to employ the advantages of Residue Number System (RNS) to achieve reliable and efficient transmission of data through these systems. Many communication channels are subject to channel noise and other impairments, and thus errors may be introduced during data transmission. The integrity of data has tremendous effects on the performance of any data acquisitions system. Noise and other disturbances can often degrade the information or data transmitted from these systems [3]. With the business of e-commerce, e-governance and other related computer networks, applications on their peak, more sensitive information is being passed around on computer networks. Financial and identity information are at a higher risk of being modified due to transmission errors as users take advantage of the ease of doing business and carrying out daily transactions through computer networks [4]. Communication channels are stochastic in nature and are prone to transmission impairments. The ability to still function and deliver user information without severe degradation in an unreliable transmission system is of importance to the success story of data communication. The general form for obtaining error detection and correction is to add some redundancy bits to the transmitted message. The receiver will use the redundancy bits to check for consistency of the delivered message, and to recover the original message if the transmitted message is deemed to be corrupted. There are two Error detection and correction schemes; systematic and non-systematic. In a systematic scheme, the transmitter

sends the original data, and attaches a fixed number of check bits, which are derived from the data bits by some deterministic algorithm. If error detection is required, the receiver applies the same algorithm to the received data bits and compares its output with the received check bits; if the values do not match, an error has occurred at some point during the transmission. In a non-systematic scheme, the original message is transformed into an encoded message that has at least as many bits as the original message.

Properties of Redundant Residue Number System have been used for detecting and correcting potential errors during the transmission process. Similar scheme was presented in [3]. Our proposed system is very straight forward and it is not complex to implement. The number of iterations in the correction scheme have been tremendously reduced which in turn reduces the design complexity and decreases the propagation delay.

In this paper, an error detection and correction scheme based on redundant residue number system is presented. A novel 5-moduli set $\{2^{2n} + 1, 2^{n+1} + 1, 2^{n+1} – 1, 2^n + 1, 2^n\}$, for n even, is utilized. The first three moduli is the information moduli set while the last two moduli are redundant that are used for the error detection and correction. Consequently, an error detection and correction algorithm is proposed. The number of iterations in the error correction scheme has been tremendously reduced which in turn reduces the design complexity and also decreases the propagation delay.

The rest of the paper is organized as follows: Section A discusses the background and some terminologies used, Section B gave the basic concepts of Redundant Residue Number system, Section C showed RRNS is useful for error detection and correction, Section D demonstrated the proposed algorithm, Section E presented a performance evaluation with the state of art, and the paper is concluded in Section F.

2. Background and Terminologies

In this section, the various key terms and the terminologies used in this work is discussed. During the ancient study of number system, computer scientist rediscovered RNS, who sought to exploit their good properties in the implementation of fast arithmetic and fault-tolerant computing. This 1700-year-old number system has been attracting a great deal of attention recently. Digital systems structured into residue arithmetic units may play an important role in ultra-speed, dedicated, real-time systems that support pure parallel processing of integer-valued data. It is a "carry free" system that performs addition, subtraction, and multiplication as concurrent (parallel) operations, sidestepping one of the principal arithmetic delays managing carry information [5]. The residue representations carry no weight-information hence an error in any digit-position in a given representation does not affect other digit-positions. [3] There are however problems with RNS that have limited their practical implementation; these are sign detection, magnitude comparison, overflow detection, division and other complex arithmetic operations like square root, exponentiation etc.

RNS is defined in terms of a set of relatively prime moduli. If P denotes the moduli set, then

$$P = \{m_1, m_2, ...m_k\}, GCD(m_i, m_j) = 1,$$

for $i \neq j$. Any integer X in the range [0, M) where

$$M = \Pi_{i=1}^{k} m_i \tag{1}$$

can be uniquely and unambiguously represented by the residue sequence: $X \leftrightarrow (x_1, x_2\ x_k)$ where

$$\begin{aligned} x_i &= X \bmod m_i, \\ i &= 1, 2, ..., k \end{aligned} \tag{2}$$

Is the residue modulus mi of X. The range [0, M) is called dynamic range or the legitimate range of X. [6] [7].

Given a residue sequence (x_1, x_2, x_k), the corresponding integer X in [0, M) can be uniquely recovered from the k residues using the Chinese Remainder Theorem (CRT). According to the CRT, for any given k-tuple (x_1, x_2, x_k), where $0 \leq xi < mi$; i = 1, 2,.k, then the value of X can be found from the residue using;

$$X = \left| \sum_{i=1}^{k} M_i \left| M_i^{-1} r_i \right|_{m_i} \right|_M \tag{3}$$

Where from equation (1), $M = \Pi_{i=1}^{k} m_i$

$$M_i = \frac{M}{m_i} \tag{4}$$

M_i^{-1} is referred to as the multiplicative inverse corresponding to mi. [8].

3. Redundant Residue Number System (RRNS)

An RRNS is defined as a chosen RNS with additional redundant moduli. Each redundant modulus is generally greater than any of the moduli of the chosen moduli set. Assuming the standard RNS consists of the moduli set of {m1, m2, mk}, the corresponding RRNS consists of a moduli set of $\{m_1, m_2, m_k, m_{k+2r}\}$ ($r \geq 1$) [3] [9] [10].

The RRNS has error detection and correction capability. By using 2r ($r \geq 1$) redundant moduli, r errors can be detected and corrected [3].

The residues in RNS will serve as several channels for data communication (fault tolerant; each digit result is completely independent).

4. Rrns as Used in Error Detection and Correction

RNS are also useful in error detection and correction. This

apparent, given the independence of digits in a residue-number representation: an error in one digit does not corrupt any other digits. In general, the use of redundant moduli, that is extra moduli that play no role in determining the dynamic range, facilitates both error detection and correction. The error detection and correction is done at the reverse converse of the general RNS processor. Therefore the algorithm is incorporated in a reverse converter. But even without redundant moduli, fault-tolerance is possible, since computation can still continue after the isolation of faulty digit-positions, provided that a smaller dynamic range is acceptable [3].

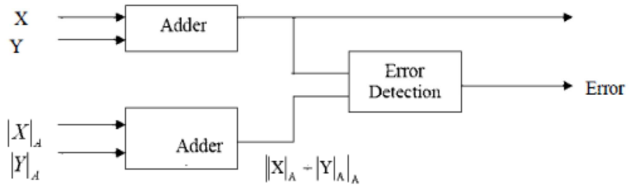

Figure 1. *Circuit Error Detection [3].*

5. Proposed Algorithm

The algorithm has been proposed using the moduli set: $\{2^{2n} + 1, 2^{n+1} + 1, 2^{n+1} - 1, 2^n + 1, 2^n\}$ for n even Where $\{2^{n+1} - 1, 2^n + 1, 2^n\}$ is the information moduli set and $\{2^{2n} + 1, 2^{n+1} + 1\}$ is the redundant moduli set.

To illustrate the following detection and correction mechanism, consider n = 2. The moduli set will be (17, 9, 7, 5, 4) where (7, 5, 4) is the information moduli set and (17, 9) is the redundant moduli set.

If a message X = 21 is to be transmitted using the moduli set above, the transmitted residues will be given as21 = (0, 1, 1)RNS (7 |5 |4). Let (0, 1, 1) = (x2, x1, x0). Assuming there is an error in the transmission channel due to either noise or other transmission impairments, and x0 is changed to 3which resulted in the received residue to be like (0, 1, 3).

Using the mixed-radix conversion, X is obtained as follows:

Let the corresponding mixed-radix values, be (z_2, z_1, z_0). But $x_0 = z_0 = 3$

Subtracting 3 and dividing by 4, will give the following

$$(4, 3, 0)/4 = (4, 3, 0) * (2, 4, -) = (1, 2, -). \text{ Therefore } z_1 = 2$$

Subtracting 2 and dividing by 5, will give the following

$$(6, 0, -)/5 = (6, 0, -) * (3, -, -) = (4, -, -). \text{ Therefore } z_2 = 4$$

$$\text{Therefore } (0.\ 1, 3)_{RNS(7 \mid 5 \mid 4)} = (4, 2, 3)_{MRS((7 \mid 5 \mid 4)}$$

$$X = 4 * (5 * 4) + 2 * (4) + 3 = 91$$

For detection of the error, take 91mod9 = 1 which is not 3 as required. The second residue can be further found by the second redundant modulus by 91mod17 = 6 which is not 4. It can therefore be concluded that an error has occurred in the transmission of X = 21.

For the correction of the error, the modulus that generated the error must be identified. The error was either generated by m_2, or m_1 or m_0. So a test on each of the information moduli with the two redundant moduli will present the following:

$$(m_4, m_3, m_0), (m_4, m_3, m_1) \text{ and } (m_4, m_3, m_2)$$

$$\text{For } (m_4, m_3, m_0),\ X = 21 = (4, 3, 3)_{RNS(17 \mid 9 \mid 4)}.$$

Note: The residue, 3 is replaced with the residue, 1due to the error generated from m_0 during the transmission. Using the MRC, X can be obtained as follow:

$X_0 = z_0 = 3$. So subtracting 3 and diving 4, will lead to the following: (1, 0, 0) /4 = (1, 0, 0) * (13, 7, -) = (13, 0, -). Therefore z1 = 0. So subtracting 0 and dividing 9, will present,

$$(13, 0,-) / 9 = (13, 0, -) * (2, - -) = (9, -, -). \text{ Therefore } z_2 = 9$$

Hence,

$$(4, 3, 3)_{RNS(17 \mid 9 \mid 4)} = (9, 0, 3)_{MRS(17 \mid 9 \mid 4)}$$

$$X = 4 * (9 * 4) + 0 * (4) + 3 = 147$$

For (m_4, m_3, m_1), $X = 21 = (4, 3, 1)_{RNS(17 \mid 9 \mid 5)}$. Using the MRC, X can be obtained as follows:

X0 = z0 = 1. Subtracting 1 and dividing by 5, will result to (3, 2, 0) / 5 = (3, 2, 0) * (7, 2, -) = (4, 4, -). Therefore z1 = 4. Subtracting 4 and dividing 9,

$$(0, 0, -) / 9 = (0, 0, -) * (2, -, -) = (0, -, -). \text{ Therefore } z2 = 0$$

$$\text{Therefore } (4, 3, 1)RNS(17 \mid 9 \mid 5) = (0, 4, 1)MRS(17 \mid 9 \mid 5)$$

$$X = 0 * (9 * 5) + 4* (5) + 1 = 21$$

For (m_4, m_3, m_2), $X = 21 = (4, 3, 0)_{RNS(17 \mid 9 \mid 7)}$. Using the MRC, X can be obtained as follows:

$X_0 = Z_0 = 0$. Subtracting 0 and dividing 7, will lead to the following; (4, 3, 0) / 7 = (4, 3, 0) * (5, 4, -) = (3, 3, -). Implies z1 = 3. Subtracting 3 and dividing 9,

$$(0, 0, -) / 9 = (0, 0, -) * (2, -, -) = (0, -, -). \text{ Implies } z2 = 0$$

$$\text{Therefore } (4, 3, 0)_{RNS(17 \mid 9 \mid 7)} = (0, 3, 0)_{MRS(17 \mid 9 \mid 7)}$$

$$X = 0 * (9 * 7) + 3* (7) + 0 = 21$$

It can henceforth be observe that the error was generated by m_0. It is concluded that the correct result is 21 and that there was an error in x_0, which can be corrected by computing.

$$X_0 = 21 \pmod 4 = 1$$

6. Performance Analysis

Results of this paper are compared to the results in [3] where the number of iterations performed in order to correct a single error with 5- moduli set is ten; that is a complete recombination. This has a total of k (k-1)/2 number of iterations/recombination, where k is the number of moduli

set. This means the correction algorithm in RRNS with k moduli set has an asymptotic complexity in the order of O (k^2). In this paper however, only three combinations or iterations are required. This has a total of (k + 1)/2 for k being odd and (k + 2)/2 for k being even number of iterations/recombination. Therefore the correction algorithm in RRNS with k moduli set has an asymptotic complexity in the order of O (k). Hence, given the same conditions for the error detection and correction at the reverse conversion, the delay in this scheme is expected to be reduced to about 70%. The amount of memory also needed to design this architecture is expected to reduce significantly.

7. Conclusion

Errors are inevitable in data communication due to various factors like noise, heat, interference in the communication circuits. Thus, there is need for fast error detection and correction schemes. This proposed scheme detects and corrects a single error using RRNS. Five-length moduli set have been proposed where the first three moduli set is the information moduli and the last two is the redundant moduli for error detection and correction. The proposed scheme have only three recombination or iterations to detect and correct a transmission error whiles the state of the will need ten recombination or iterations. As such, the proposed scheme is very simple and straightforward and the time it will take to correct an error is relatively lesser than other detection and correction schemes.

References

[1] D. K. Sharma, A. Mishra & Rajiv Saxena, Analog and Digital Modulation Techniques: An Overview TECHNIA-International Journal of Computing Science and Communication Technologies, VOL. 3, NO. 1, July 2010. (ISSN 0974-3375)

[2] Vik Tor Goh and Mohammad Umar Siddiqi, Multiple Error Detection and Correction Based on Redundant Residue Number Systems, IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 56, NO. 3, MARCH 2008

[3] M. Roshanzadeh, A. Ghaffari and S. Saqaeeyan, Using Residue Number Systems for Improving QoS and Error Detection & Correction in Wireless Sensor Networks, Communication Software and Networks (ICCSN), May 2011 IEEE 3rd International Conference on Page: 1-5

[4] Salifu Abdul-Mumin, Detection of Man-in-the-Middle attack in Computer Network i-manager's Journal on Communication Engineering and Systems, Vol. 2 No. 1 November 2012 - January 2013

[5] Fred J. Taylor, Residue Arithmetic: A Tutorial with Examples, IEEE Computer Society Press Los Alamitos, CA, USA Volume 17 Issue 5, May 1984 Pages 50-62

[6] K. A. Gbolagade, An Efficient MRC based RNS-to-Binary Converter for the moduli set, $\{2^{2n+1}-1, 2^n, 2^{2n}-1\}$, AIMS SA, 2011

[7] Amir Sabbagh Molahosseini and Keivan Navi, New Arithmetic Residue to Binary Converters International Journal of Computer Sciences and Engineering Systems, Vol.1, No.4, October 2007 CSES International ©2007 ISSN 0973-4406

[8] Duc-Minh Pham, A. B. Premkumar and A. S. Madhukumar, Error Detection and Correction in Communication Channels Using Inverse Gray RSNS Code, IEE Transactions on Communications 59(4): 975-986 April 2011

[9] Jenn-Dong Sun and Hari Krishna, Fast Algorithm for Multiple Errors Detection and Correction in Redundant Residue Number System Journal of Circuit, Systems and Signal Processing December Volume 12, Issue Issue 4, pp 503-531, 1993

[10] Hari Krisna, Kuo-Yu Lin, and Jenn-Dong Sun, A coding Theory Approach to Error Control in Redundant Residue Number Systems- Part I: Theory and Single Error Correction, IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing Vol 39 issue 1 pp 8-17 Jan 1992