American Journal of Applied Sciences

Original Research Paper

A Novel Exploitation of Errors in Redundant Residue Number System Architecture

Yaw Afriyie

Department of Accounting, School of Business and Law, University for Development Studies, Wa, Ghana

Article history
Received: 19-09-2020
Revised: 16-10-2020
Accepted: 20-11-2020

Email: yfriyie@uds.edu.gh

Abstract: Residue Number System (RNS) is an unweighted number system that symbolizes big integers with smaller numbers. It can perform operations in particular addition and multiplication in parallel. Because of this property, RNS is extensively used in communication, Finite Impulse Response (FIR), cryptography and signal processing devices. The transfer of data in digital channels is very important for some critical applications where accuracy is very important. In this study, we proposed a novel algorithm that is premised on the Hamming Distance (HD) and one of the reverse conversion methods, which is, the Chinese Remainder Theorem (CRT) and) as a joint technique for the detection and correction of multiple bit errors in RNS. The proposed algorithm provides a more efficient technique that improves on the hardware size and increases the processing speed with fewer iterations when compared with other state-of-the-art schemes. The work analyses the area and delay of the hardware architecture and compared with other similar schemes. The results indicated the effectiveness of our proposed scheme in terms of the area and delay specifications.

Keywords: Residue Number System, Hamming Distance, Digital Signal Processing, Mixed Radix Conversion, Computer Architecture

Introduction

In this era of technology, a good number of error-control methods are developed to ensure the efficient, fast and reliable transfer of non-erroneous data in modern digital systems such as digital processors and arithmetic units. An identifiable challenge in the transfer of data is caused by noise that can result in an error (s) in a transmission channel (Afriyie and Daabo, 2018a). Fault tolerance is, therefore, needful to be able to allow faulty channels to continue to operate through error detection and correction mechanisms (Afriyie and Daabo, 2018b) the concept of fault tolerance regarding security in transmission channels cannot be left unattended. There are three main concepts of information security namely confidentiality, integrity and availability. Faults can be classified as transient where error happens for a very short moment. With intermittent faults, it appears repeatedly for a specific period and permanent faults however can only be prevented when the parts that have affected transmission channels need to be replaced (Jonsson, 1996).

Error-correcting codes in RNS are attractive because of their inherent features. RNS provides the speed of arithmetic computations because of its unweighted and unparalleled characteristics compared to the conventional number systems. Residue Number System (RNS) is a non-positional, unweighted number system that does not spread error from one residual digit to the other (Daabo and Gbolagade, 2014). Over the past decade, RNS has received and continues to receive considerable attention in digital systems such as image processing, cryptography and digital filtering. The reason for its widespread is its notable properties for instance modularity, fault tolerance, parallelism and its carry-free operations (Beame *et al*., 1986; Leighton, 1992; Taylor, 1984; Soderstrand *et al*., 1986). Several works proposed by scholars in error detection and correction in RNS have been done on single and multiple error detection and correction schemes. Several works in the existing literature on the detection and correction of errors are based on the traditional Chinese Remainder Theorem (CRT) and the Mixed Radix Conversion (MRC) (Wang, 1998; 2000). There are two most important issues for the residue arithmetic in RNS, which include the selection of the moduli set and lastly the conversion of the residue digits to binary numbers. An RNS is based on the traditional moduli set $\{2^n-1, 2^n, 2^n+1\}$ has become popular that is expected to play a very good role in RNS digital processing (Ashur *et al*., 1995). A

number of conversion schemes for $\{2^n\text{-}1, 2^n, 2^n, +1\}$ have been done in (Jenkins, 1978; Taylor and Ramnarynan, 1981; Andraos and Ahmad, 1988; Ibrahim and Saloum, 1988; Vinnakota and Rao, 1994; Piestrak, 1995; Bhardwaj *et al*., 1998; Conway and Nelson, 1999). Yau and Liu (1973) developed an algorithm that detected and corrected single and burst error respectively in Redundant Residue Number System (RRNS). However, their algorithm requires no look-up tables. The hardware implementation of that proposed algorithm had memory space that was faster than the algorithm proposed in earlier works. A similar algorithm that is based on the CRT presented by (Goh and Siddiqui, 2008) detects and corrects multiple bit errors in RRNS The integrity and reliability of data have major special effects on the performance of any data in any transmission line. Factors such as noises and disturbances can also affect transmission lines by reducing the reliability of the data. With the provision of the desired fault tolerance, a system will continue to perform its desired functions. Figure 1 shows the structure of Encoder in error detection and correction proposed by Olabanji *et al*. (2016).

There are two (2) main principles of improving the reliability of Computing Systems (CS) that is resident in the positional number systems through: (1) Increasing the reliability of individual elements of the CS and (2) introducing different types of redundancy (Tay and Chang, 2017; Phalakarn and Surarerks, 2018). It evident that introducing redundancy when applying available elements is the surest way in increasing the reliability of CS. The existence of fault tolerant features in the computing systems helps to increase the reliability of the CS. The existence of fault tolerant features of the CS can be achieved as a result of the application of two main methods namely the Active Fault Tolerance (AFT) and the Passive Fault Tolerant (PFT). Some studies done by (Yatskiv and Tsavolyk, 2017; Krasnobaev *et al*., 2019) indicate the use of PFT technique that helps in the improvement of reliability in CS that is widely used in positional number systems. There is however lack of studies conducted using residue classes in achieving fault tolerance and also improving the reliability of CS that is based on the application of AFT. The main goal of this study is to propose the design of effective fault tolerant structure using residue classes to detect and correct multiple bit errors by applying the AFT technique. Begli *et al*. (2019) proposed a framework that detects attacks by employing machine learning techniques and Support Vector Machines (SVM). Their findings showed the efficiency of the proposed framework in detecting faults in critical infrastructures.

Fundamentals of Residue Arithmetics

Residue Number System is characterized by a set of k pairwise relatively prime positive integers, i.e., the greatest common divisor $gcd\,(m_i, m_t) = 1$ with $i \neq j$, $m_1, m_2 \ldots m_{k\text{-}1}, m_k$ called the moduli, that is formed in increasing, i.e., $m_1 < m_2 <\ldots m_{k\text{-}1} < m_k$ (Afriyie and Daabo, 2018a). Their products represent the interval [0, M) referred to as the legitimate range that defines the useful computational range of the number system, that is:

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

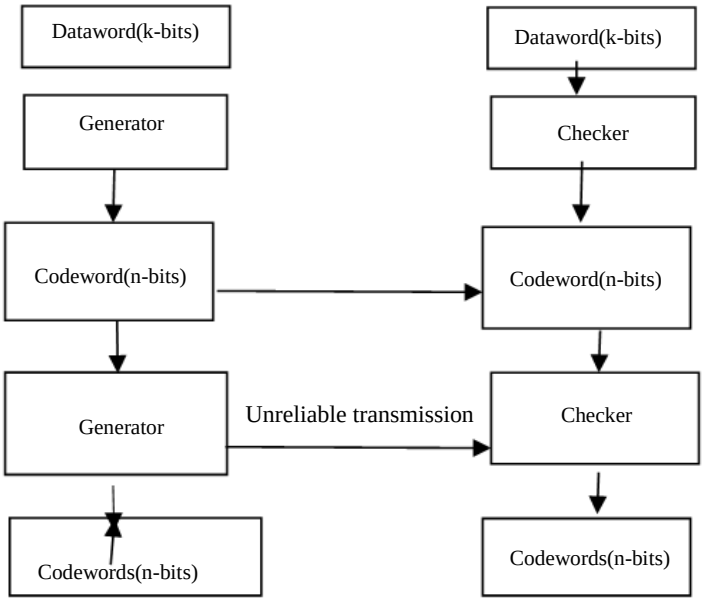

Fig. 1: Structure of encoder in error detection and correction

In representing signed numbers in RNS, the dynamic range is defined as [-(*M*-1)/2, (*M*-1)/2] if *M* is odd and *M*/2 if *M* is even. Every natural integer *X*, in the legitimate range, can be represented by a set of residues r_1, r_2,…r_{k-1}, r_k where:

$$r_i \equiv X \left(\mathrm{mod}\right) m_i \tag{2}$$

$|X|$ m_i represents *X* modulo m_i with $i\epsilon$ [1, *m*]. RNS has a carry-free feature that works on addition, subtraction and multiplication operations. These operations can be achieved independently in RNS concerning the moduli. As a result of the carry-free property of RNS, the three operations specifically addition, subtraction and multiplication are possible to be performed concerning the moduli i.e.:

$$\begin{aligned} &x_1, x_2 \ldots x_k * x_k * y_1, y_2 \ldots y_k = z_1, z_2 \\ &z_k, z_i \equiv \left| x_i * y_i \right| m_i \end{aligned} \tag{3}$$

Hence, * indicates the basic operations. As a result, RNS can provide fast arithmetic.

In achieving redundancy for the reason of detecting errors in digital channels, redundant moduli are added to the existing moduli as spare. By adding (*u*-*w*) redundant moduli (m_{n+1}, m_{n+2}, … m_n) to the *v* information moduli (m_1, m_2, m_3, …m_n), an RRNS (*u*, *w*) code is possible to be generated. The process of achieving this is called RRNS encoding. An integer *S* can be represented in the RRNS form as:

$$S = \left\{ r_1, r_2, r_3, \ldots, r_w, r_{w+1}, \ldots, r_u \right\} \tag{4}$$

where, (m_1, m_2, m_3, … m_n) are known as the information moduli and (m_{w+1}, m_{w+2}, m_{w+3}… m_w) indicating the redundant moduli set. Similarly, the residues, (r_1, r_2, … r_3, r_w) show the information residues and (r_{w+1}, r_{w+2}, r_{w+3} … r_w) are called the redundant residues.

In the process of decoding in RRNS, if some of the spare residues are not used, an integer can be correctly recovered if the existing residue digits are without errors. For RRNS, all moduli are pairwise relatively prime and the representation of this system is equal to:

$$\left[0, \prod_{i=1}^{h+r} m_i \right) \tag{5}$$

Information and Non-redundant for any moduli set are given as:

$$M_r = \prod_{i=1}^{n} m_i$$

$$M_s = \prod_{i=n+1}^{m} m_i$$

Hence, the equation below describes the dynamic range:

$$R = \prod_{i=1}^{n} m_i * \prod_{i=n+1}^{m} m_i = \prod_{i=1}^{m} m_i$$

Also, in determining the Euclidian algorithm, we have:

$$\begin{aligned} &\gcd(a,b) = \gcd(b, |a|_b = 1 \\ &\gcd\left(\left| (2^n) \right|, 2^n + 1 \right) = 1 \\ &\gcd\left(\left| (2^n - 2) \right|, 2^{2n} + 2^n \right) = 1 \end{aligned}$$

Theorem 1

RRNS, (*u*-*w*, *v*) code has a detection capability of (*u*-*w*-*v*) errors and an error correction capability of (*u*-*w*-*v*)/2. The code rate of an RRNS is defined as:

$$R_C = \frac{K_b}{\sum_{j=1}^{u} K_b} \tag{6}$$

where, $K_b = \lfloor \log_2 M_r \rfloor$ and $K_{bj} = \lfloor \log_2 m_j, \rfloor$ where (*j* = 1, 2, 3, …*u*) are the moduli. During the transfer of data, the number of extra bits and the code rate for error detection and correction can be varied. The spare moduli are added to the information bits. This, therefore, affects the code rate by decreasing it and the error correction capability is enhanced. In RNS, the number of non-zero elements in a vector is defined as its hamming weight. Let K_i and K_j be code vectors, then the hamming distance $d(K_i, K_j)$ is defined as the number of bits in which two code vectors K_j and K_j differ. H_D is the minimum of the hamming distances:

$$H_D = \min\left(d\left(y_{i,} y_j \right); y_i \neq Y_j \right). \tag{7}$$

Theorem 2

The minimum Hamming distance (*d*) of an RRNS (*u*, *w*) code is defined as *d* = *u*-*w* + 1provided (m_1, < m_2 < m_3 <… < m_u).

Theorem 3

The minimum distance of an RRNS code is $d_{\min}$, if and only if the product of redundant moduli satisfies these relations:

$$\max\left\{\prod_{i=1}^{d_{\min}} m_{ji}\right\} > M_{n-k} \geq \max\left\{\prod_{i=1}^{d_{\min}-1} m_{ji}\right\} \quad (8)$$

where, $M_{n-k} = \prod_{j=k+1}^{n} m_j$ shows the product of the extra moduli of the code and m_{ji} is of n moduli of the RRNS code, for $1 \leq j_i \leq n$.

Theorem 4

An RRNS code y that is premised on an extra RNS has a minimum hamming weight $wt_{\min} \geq \alpha + 1$ and a minimum distance $d_{\min} = r + 1$.

Theorem 5

For an extra moduli bit in RNS, the error detection capability c_d, $c_d = d\text{-}1$ and the error correction capability $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ where, $\lfloor x \rfloor$ is the largest integer value smaller than x (Ashur *et al*., 1995). That is, RRNS (u, w) code can detect up to (u-w) residue digits and correct up to $t = \left\lfloor \frac{u-w}{2} \right\rfloor$ residual digits. This implies that single and multiple error detection and correction algorithms are possible to be implemented when u and w are carefully selected. This study focuses on detecting and correcting multiple bit errors in RRNS with (u-w = 2).

It is important to determine the optimal set $\{m_o\}_{OPT}$ of modules from the set of the possible respective moduli set m_{n+1}, m_{n+2}, m_{n+3}, …, m_{n+k} at which the reliability of the CS $R^{(n/k)}RC(t)$ of the CS will be maximum. In achieving the optimality of the moduli set $\{m_o\}_{OPTs}$, it is important to frame and solve the problem of inverse of the optimal reservation in the residues. The inverse optimal reservation problem in the residues is mathematically formulated as (Ushakov, 2013):

$$\begin{cases} K^{(a+b)}RC(t)[t = const] \rightarrow \max; \\ \left(V^n TNS \geq P^{(a+c)}RC\right); \end{cases} \quad (9)$$

where, c is the maximum possible number of control bases m_{n+1}, m_{n+2}, m_{n+3}, …, m_{n+k}; $\left\{m_{(a+b)}\right\}_{OPT}\left(f = \overline{1,2,...,k}\right)$ indicates the optimal control bases. In ensuring the possibility of maximum reliability value $K^{\left(\frac{a}{b}\right)}RC(t)$ computing system in RC. With this, the condition that is set must be achieved:

$$V^c RC \leq V^n TNS - V^m RC \quad (10)$$

Conversion

The MRC and CRT are the main approaches that are mainly used in conversion processing (Sun and Krishna, 1992). This study will be limited to the CRT and the HD techniques because the CRT offers the real-time signal processing time as a result of its parallel means of conversion and there is a constant limit to this approach (Soderstrand *et al*., 1986). The process of converting from conventional representations to RNS is known as forward conversion whilst converting from the RNS to the conventional representations is known as the reverse conversion.

The residue to conventional number representation is done mainly by the MRC or the CRT (James and Pa, 2015);

To compute numbers X from its corresponding residues, the CRT technique can be used which is given in Eq. (11):

$$X = \left| \sum_{i=1}^{N} \rho_i \left| \omega_i x_i \right|_{m_i} \right|_M \quad (11)$$

where:

$$M = \prod_{i=1}^{N} m_i \quad (12)$$

$$\rho_i = \frac{M}{m_i} \quad (13)$$

$$\left| \omega_i * x_i \right|_{m_i} = 1 \quad (14)$$

This research paper provides an efficient and novel algorithm for the detection and correction of multiple bit errors for the moduli set $\{2^n\text{-}1, 2^n, 2^n\text{+}1, 2^{n+1}\text{-}1, 2^{2n}\text{-}3, 2^{n2}\text{+}1\}$.

Proposed Methods

This part of the paper presents a new scheme for detecting and correcting multiple bit errors in RRNS in the stated moduli set.

Proposed Algorithm

The proposed method is based on the algorithm outlined given below:

1. Calculate $\bar{y}$ from the received vector y using Eq. (11)

2. Execute the needed number of iterations using $C_t^n = \frac{n!}{(n-t)!t!}$ by dropping two residues at a time
3. If $\bar{y}$ falls within the legitimate range, stop and output $\bar{y}$. Declare there are no errors
4. If $\bar{y}$ is not within the legitimate range, compute the residual vector y and the HD $d(r_i, y)$ If $d(r_i, y)$ stop and output the result
5. If $d(r_i, y) > t$, indicate that there are more than t errors and stop

Using the CRT, it is possible to compute for the original integer message as a way of recovering it from the set of residues received. Hence, to recover the original integer message involves only the modulo operations for some iterations. The algorithm is premised on the CRT and the HD.

From the stated moduli set $S = \{2^n\text{-}1, 2^n, 2^n\text{+}1, 2^{n+1}\text{-}1, 2^{2n}\text{-}3, 2^{n2}\text{+}1\}$ where, $m_1 = 2^n\text{-}1$, $m^2 = 2^n$, $m_3 = 2^n\text{+}1$, $m_4 = 2^{n+1} - 1$, $m_5 = 2^{2n} = 3$ and $m_6 = 2^{2n}\text{+}1$.

The multiplicative inverses for the CRT based on the same moduli set are computed as follows:

$$\left|m_1^{-1}\right| m_2 = \left|(2^n - 1)^{-1}\right|_{2^n} = -1 \tag{15}$$

$$\left|m_2^{-1}\right| m_3 = \left|(2^n)^{-1}\right|_{2^n+1} = 1 \tag{16}$$

$$\left|m_3^{-1}\right| m_4 = \left|(2^n + 1)^{-1}\right|_{2^{n+1}-1} = 2^n \tag{17}$$

$$\left|m_3^{-1}\right| m_5 = \left|(2^n + 1)^{-1}\right|_{2^{2n}-3} = 2^n \tag{18}$$

$$\left|m_4^{-1}\right| m_5 = \left|(2^{n+1} - 1)^{-1}\right|_{2^{2n}-3} = 2^{n+1} - 6 \tag{19}$$

$$\left|m_2^{-1}\right| m_4 = \left|(2^n)^{-1}\right|_{2^{n+1}-1} = 2^n - 1 \tag{20}$$

$$\left|m_3^{-1}\right|_{m_6} = \left|(2^n + 1)^{-1}\right|_{2^{2n}+1} = 2^n + 3 \tag{21}$$

$$\left|m_4^{-1}\right| m_6 = \left|(2^{n+1} - 1)^{-1}\right|_{2^{2n}+1} = 2^{n+1} - 3 \tag{22}$$

$$\left|m_5^{-1}\right| m_6 = \left|(2^{2n} - 3)^{-1}\right|_{2^{2n}+1} = 2^{2n} - 12 \tag{23}$$

Equation (15) - (23) project the formulations using the CRT in detecting the affected integer message. This study purposely employs the CRT for implementation of the hardware architecture. Generally, the CRT is specified usually as.

For the values n_1 to n_6, for the moduli set, $S = \{2^n\text{-}1, 2^n, 2^n\text{+}1, 2^{n+1}\text{-}1, 2^{2n}\text{-}3, 2^{2n}\text{+}1\}$ gives:

$$X_{123456} = \left|\sum_{i=1}^{6} X_i \left|M_i^{-1}\right|_{m_i} * M_i\right|_M \tag{24}$$

Based on the proposed algorithm, the amount of parts for the duplicate CS in the positional number system can be determined by the mathematical expression in equation:

$$V^{(z)}2PNS = 2.8.z \tag{25}$$

For the triple CS, it can also be mathematically expressed as:

$$V^{(z)}3PNS = 3.8.z \tag{26}$$

Equation (25) and (26) can generally be expressed as:

$$R^{(n/k)}RC(t) = \sum_{i=0}^{k} A^i n + kB_i^{n+k-i} \\ (t)\sum_{j=0}^{i}(-1)^i D_i^j B_i^j(t) \tag{27}$$

The probability of the fault tolerant activity of the CS can be obtained on the residues from Eq. (27).

Hardware Implementation

In implementation of the hardware, the considered moduli set $S = \{2^n\text{-}1, 2^n\}$ for the hardware architecture for the non-redundant component is considered. The corresponding binary representation of the residues have a bit level representation as x_1 and x_2 which further give:

$$x_1 = (x_{1,n-1}, x_{1,n-2} \ldots x_1, x_{1,0})_2 \tag{28}$$

$$x_2 = (x_{2,n}, x_{2,n-1} \ldots x_2, x_{2,0})_2 \tag{29}$$

and the redundant part as:

$$x_3 = x_{3,n,} x_{3,n-1,} x_{3,n-2,} \ldots x_{3,0} \tag{30}$$

$$x_4 = x_{4,n+1,n-1,n-2} \ldots x_{4,0} \tag{31}$$

$$x_5 = x_{5,2n,}x_{5,2n-1,}x_{5,2n-2,}\ldots x_{5,0} \tag{32}$$

$$x_6 = x_{6,2n,}x_{6,2n-1,}x_{6,2n-2,}\ldots x_{6,0} \tag{33}$$

Thus CRT technique gives:

$$X_{123456} = \left|x_1\left|M_1^{-1}\right|_{m_1} * M_1 + x_2\left|M_2^{-1}\right|_{m_2} * M_2 + x_3\left|M_3^{-1}\right|_{m_3} *M_3 + x_4\left|M_4^{-1}\right|_{m_4} * M_4 + x_5\left|M_5^{-1}\right|_{m_5} * M_5 + x_6\left|M_6^{-1}\right|_{m_6} * M_6\right|_M \tag{34}$$

The dynamic range, (M) for the non-redundant parts from the Eq. (24) gives:

$$M = m_1m_2 = \left(2^n - 1\right)\left(2^n\right) \tag{35}$$

$$M_1 = \left(2^n\right)\left(2^n + 1\right) \tag{36}$$

$$M_2 = \left(2^n - 1\right)\left(2^n + 1\right) \tag{37}$$

The multiplicative inverses for expanding Eq. (19) are shown in Eq. (15) to (23).

Expanding (24) with the dynamic ranges and its respective multiplicative inverses for the non-redundant part provide:

$$X_{12} = \left|x_1((2^n)(2^n - 1) + x_2((2^n - 1)(2^n))\right|_{(2^n-1)(2^n)} \tag{38}$$

The correct integer message for the non-redundant part that is, X_{12} is known from the Eq. (38) when any of the residue digits have errors in the non-redundant part.

Results

The architectural area of the proposed method is built from the stated moduli set using Carry Propagate Adders (CPAs) and simple adders. To detect and correct multiple bit errors in RNS, the residues are converted to a correct integer message using the traditional CRT and the HD as a joint. In a situation where an error occurs during data transmission in digital lines, the redundant part is called to aid in detecting and correcting residue errors that are premised on the proposed algorithm presented in this study. The erroneous residue digits are calculated about Eq. (8). The schematic architecture as shown in Fig. 2 depicts that there are three regular Carry Propagate Adders (CPAs), that are needed to build the architecture with a bit length of ($8n$ *bite*) as regards to the delay for the proposed schematic architecture, the CPAs execute a computational speed of D_{FA} for of the CPAs each and need a total architecture size of ($8n$) Δ_{FA}. The proposed architecture needs a total area of ($2n$+2) D_{FA}. The schematic diagram for the proposed method is shown in Fig. 2.

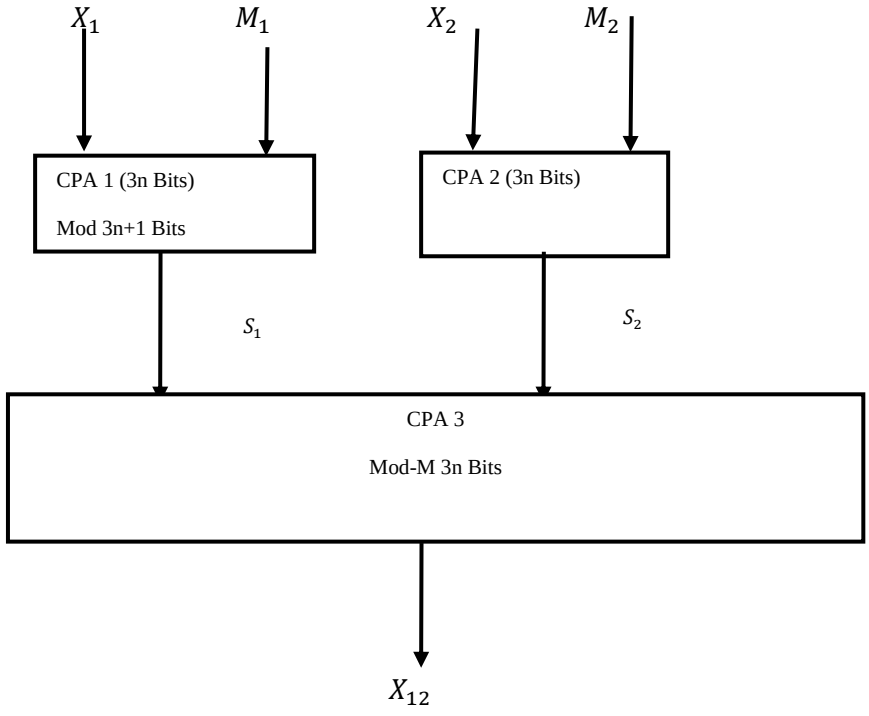

Fig. 2: Block diagram showing the RC for the non-redundant part X_{12}

DOI: 10.3844/ajassp.2021.96.106

Results and Discussion

In this section, we present the analysis of the results proposed in this study against other existing state-of-the-art works. Table 2 and 3 show the proposed algorithm with the other existing algorithms based on the area and delay of the architecture.

Numerical Results

We can now illustrate some numerical examples for the new method in this study.

Considering an RNS code (n, k) where n indicates the length of the code and k represents the dimension of the RNS code with the moduli set (m_1, m_2, m_3, m_4, m_5, m_6) = (3,4,5,7,13,17) where, m_1 and m_2 are non-redundant moduli, m_3, m_4, m_5 and m_6 are the redundant moduli. For instance, considering the integer message y = 11, for its residue digits, are y_i = (2, 3, 1, 4, 11, 17). The range of legitimacy = M_L = 3*4 = 12 and the illegitimate range = M_1 = 5*7*13*17 = 7735. Let us accept that in the process of calculation of the integer message, the second and sixth residues are in error respectively, i.e., two errors (t = 2). These residues in error have propagated into y during transfer in the digital channels using A_1 = 2 and B_2 = 6 as error locations. The codevector after the computation of the computation using the CRT gives, $\bar{y}_i = \left(2,\bar{5},1,4,11,13,\bar{7}\right)$.

The decoding process gives:

$$y_1y_2y_3y_4 - X_{1234} = 221$$
$$y_1y_2y_3y_5 - X_{1235} = 401$$
$$y_1y_2y_4y_5 - X_{1245} = 557$$
$$y_1y_3y_4y_5 - X_{1345} = 11^*$$
$$y_2y_3y_4y_5 - X_{2345} = 1441$$
$$y_1y_2y_3y_6 - X_{1236} = 41$$
$$y_1y_2y_4y_6 - X_{1246} = 1061$$
$$y_1y_3y_4y_6 - X_{1346} = 275$$
$$y_2y_3y_4y_6 - X_{2346} = 1061$$
$$y_1y_2y_5y_6 - X_{1256} = 245$$
$$y_1y_3y_5y_6 - X_{1356} = 1259$$
$$y_2y_3y_5y_6 - X_{2356} = 3781$$
$$y_1y_4y_5y_6 - X_{1456} = 3560$$
$$y_2y_4y_5y_6 - X_{2456} = 2013$$
$$y_3y_4y_5y_6 - X_{3456} = 4886$$

From the above results, it is observed that whenever y_2 and y_6 are used in the computation they give an illegitimate integer and also lies outside the legitimate range namely X_{1234}, X_{1235}, X_{1245}, X_{2345}, X_{1236}, X_{1246}, X_{1346}, X_{2346}, X_{1256}, X_{1356}, X_{2356}, X_{1456}, X_{2456}, X_{2456} and X_{3456}. Whenever the residue digits y_2 and y_6 were dropped in the computation of X_{1345}, the integer message recovered is 11 and also lies within the legitimate range.

The legitimate integers are y_2 and y_6 are the residue digits in error. It can be concluded that, the correct integer value is 11 and there were errors in y_2 and y_6. The integer values y_2 and y_6 can be corrected by computing y_2 = 11 *mod* 4 = 3 and y_6 and y_6 = 11 *mod* 17 = 11.

Table 1 shows the HD between any two code vectors that are computed based on theorem 5 of the HD theorems from the paper. From the comparison involving the residue vectors and the Hamming Distances, the only value that lies in the legitimate range and has a Hamming Distance $d(r_i, y)$ which is less than or equal to 2 i.e., ($t \leq 2$) is 11. This indicates that the proposed algorithm has detected and corrected the transmitted integer message correctly. The proposed technique is simple and provides an efficient way, which makes the integer message, recovered avoiding the use of large integers.

The paper presented a novel and simple scheme that detects and corrects multiple bit errors in RRNS architecture. For the evaluation of the proposed technique, it is compared to known best-known state-of-the-art schemes that also work on errors in RNS. The paper-based on the proposed algorithm provides a faster encoding and decoding schemes because of the generalized moduli set. The generalized moduli set provides an efficient Dynamic Range. The theoretical analysis performed between the proposed and other known schemes indicated that the proposed technique had improved hardware architecture for the area and provided a faster processing speed. The proposed method presented an area of (8n) ΔFA a processing speed of (2n+2)DFA. The architecture of the proposed work uses simple adders and Carry Propagate Adders (CPAs) which presents the simple architecture and fewer hardware resources. The scheme proposed has a faster processing speed and computing time than the other schemes used in this study for different values of n. When n it becomes large in all schemes, the proposed scheme tends to be simpler and has less delay than the other schemes. The resulting outputs are shown in Fig. 2 and 3 respectively.

Figure 3 and 4 show the performance comparison of the area and delay schemes of the proposed scheme with other known schemes. Figure 3 presents the area of the hardware architecture for the proposed scheme and other known methods used for comparison. With an increasing value of n in all schemes, the proposed scheme gets better hardware size. In Fig. 4, the delay of both the proposed and similar known schemes are compared. It can be realized that our proposed method

requires less memory in detecting and correcting multiple bits' errors. The other known schemes used in this study present high memory that reduces the computational or processing speed for implementation.

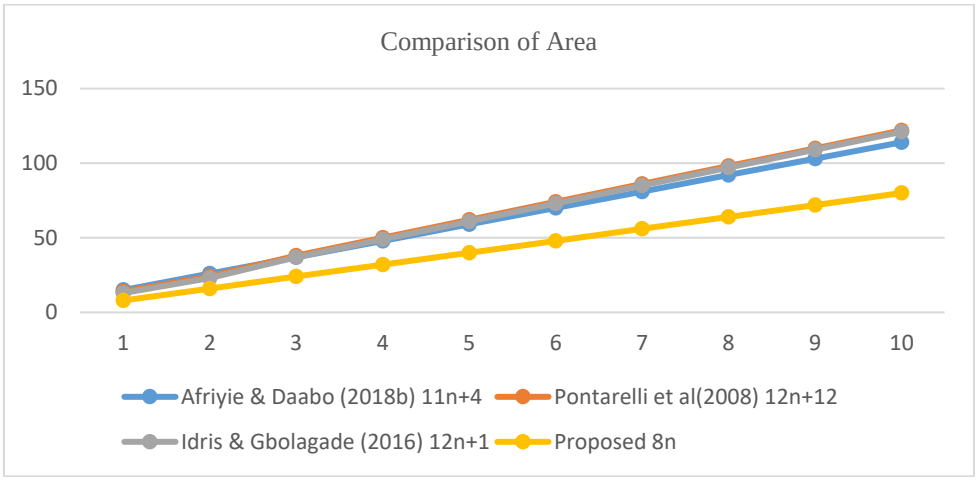

Fig. 3: Graph of proposed area with other existing works

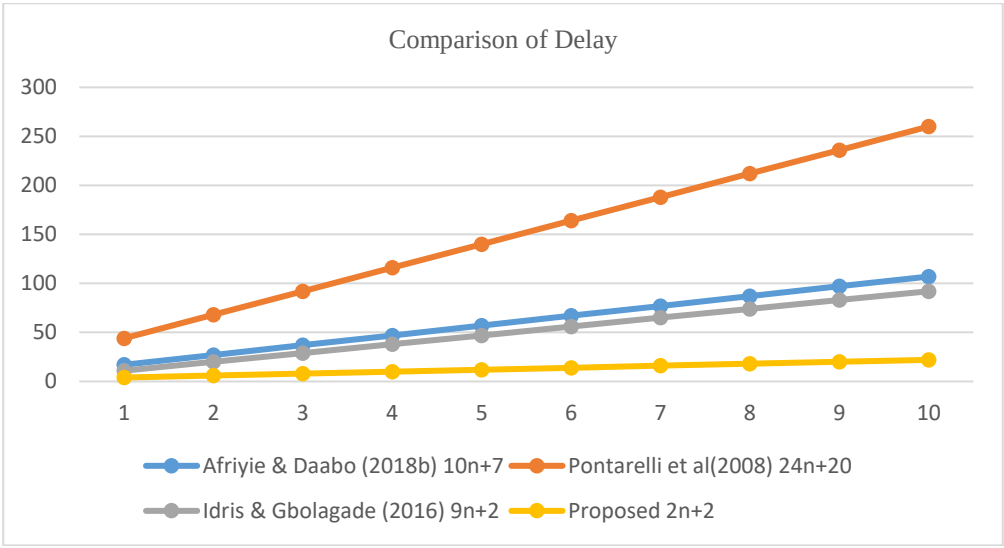

Fig. 4: Graph of proposed delay with other existing works

Table 1: The residue vectors and hamming distances for residue digits' error correction

i	$\bar{y}$	r_i	y	$d(r_i, y)$
1	221	2,1,1,4,0,0	2,3,1,4,11,11	3
2	401	2,1,1,2,11,10	2,3,1,4,11,11	3
3	557	2,1,2,4,11,13	2,3,1,4,11,11	3
4	11	2,3,1,4,11,11	2,3,1,4,11,11	0*
5	1441	1,1,1,6,11,13	2,3,1,4,11,11	3
6	41	2,1,1,6,2,7	2,3,1,4,11,11	4
7	1061	2,1,1,4,8,7	2,3,1,4,11,11	3
8	275	2,3,0,2,2,3	2,3,1,4,11,11	4
9	1061	2,1,1,4,8,7	2,3,1,4,11,11	3
10	245	2,1,0,0,11,7	2,3,1,4,11,11	4

Table 2: Comparison of various techniques and algorithm

Technique	Number of detectable and correctable errors	Schemes error detection	Error location	Fixed latency	Memory	Generalized moduli set	Output domain	Iteration
Amusa and Nwoye (2012)	Multiple	MRC	Modulus projection	Yes	Yes	No	Integer	High
Tay and Chang (2015)	Multiple	Syndrome	Syndrome check	Yes	Yes	No	Residue	High
Olabanji *et al.* (2016)	Multiple	CRT	Double consistent check	Yes	No	No	Residue	High
Aremu and Gbolagade (2017)	Multiple	CRT	Syndrome	Yes	Yes	Yes	Residue	High
Proposed Scheme	Multiple	CRT	HD	Yes	Yes	Yes	Residue	Low

Table 3: Area and delay comparison

Schemes	Area (Δ_{FA})	Delay (D_{FA})
Afriyie and Daabo (2018b)	11n +4	10n +7
Pontarelli *et al.* (2008)	12n +12	24n +20
Aremu and Gbolagade (2017)	12n +1	9n +2
Proposed	8n	2n +2

Conclusion

In conclusion, this study has presented a novel and simple algorithm that has the capability in detecting and correcting multiple bit errors in RRNS architecture. The proposed method was compared to other existing literature in RRNS for the detection and correction of errors in digital channels. The existing schemes compared in this study provide complex and time-consuming algorithms. The realization was that, the proposed method considerably performs better and requires fewer bits than the other schemes used for comparison in this study. The proposed algorithm provides fewer iterations in the decoding and encoding process that reduces the cost of redundant moduli and high-speed elementary RNS operations. The proposed scheme incorporated the traditional CRT and the HD as a joint technique that simplified the hardware design and improved the processing speed as compared with other similar known schemes in RRNS. For the proposed algorithm, detecting and correcting multiple bit errors are only possible, however, overflow and sign detections seem to be more difficult. Some prior studies have shown that the use of AFT also known as the dynamic reservation technique in residues presents high reliability in CS than the PFT technique.

For future work, the concentration of detection and correction of errors will be premised on optimization techniques to reduce the iteration steps to enhance the speed of the algorithm. Besides, a simple algorithm premised on the new CRT II for some special moduli set will be considered for both forward and reverse conversions to enhance the computational speed for detecting and correcting errors in RNS.

Acknowledgment

The author would like to especially thank anonymous reviewers who took the time to make some necessary inputs.

Ethics

This is to declare that there is no known competing financial interests or personal relationships that could have appeared to influence the work reported in this study.

References

Afriyie, Y., & Daabo, M. I. (2018a, August). A Novel Approach for the Detection and Correction of Single Bit Error in RRNS Architecture. *In 2018 IEEE 7th International Conference on Adaptive Science & Technology* (ICAST) (pp. 1-4). IEEE. doi.org/10.1109/ICASTECH.2018.8507081

Afriyie, Y., & Daabo, M. I. (2018b). Multiple Bits Error Detection and Correction in RRNS Architecture using the MRC and HD Techniques. doi.org/10.5120/ijca2018917030

Amusa, K. A., & Nwoye, E. O. (2012). Novel algorithm for decoding Redundant Residue Number Systems (RRNS) codes. *International Journal of Research and Revies in Applied Sciences* (IJRRAS), 12(1), 158-163.

Andraos, S., & Ahmad, H. (1988). A new efficient memoryless residue to binary converter. *IEEE Transactions on Circuits and Systems*, 35(11), 1441-1444. doi.org/10.1109/31.14470

Aremu, I. A., & Gbolagade, K. A. (2017). Redundant Residue Number System Based Multiple Error Detection and Correction Using Chinese Remainder Theorem (CRT). *Soft. Eng*, 5, 72-80. doi.org/10.11648/j.se.20170505.12

Ashur, A. S., Ibrahim, M. K., & Aggoun, A. (1995). Novel RNS structures for the moduli set (2n− 1, 2n, 2n+ 1) and their app, JM, ication to digital filter implementation. *Signal Processing*, 46(3), 331-343. doi.org/10.1016/0165-1684(95)00092-2

Beame, P. W., Cook, S. A., & Hoover, H. J. (1986). Log depth circuits for division and related problems. *SIAM Journal on Computing*, 15(4), 994-1003. doi.org/10.1137/0215070

Begli, M., Derakhshan, F., & Karimipour, H. (2019, August). A layered intrusion detection system for critical infrastructure using machine learning. *In 2019 IEEE 7th International Conference on Smart Energy Grid Engineering* (SEGE) (pp. 120-124). IEEE. doi.org/10.1109/SEGE.2019.8859950

Bhardwaj, M., Premkumar, A. B., & Srikanthan, T. (1998). Breaking the 2n-bit carry propagation barrier in residue to binary conversion for the [2/sup n/-1, 2/sup n/, 2/sup n/+1] modula set. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 45(9), 998-1002. https://doi.org/10.1109/81.721268

Conway, R., & Nelson, J. (1999). Fast converter for 3 moduli RNS using new property of CRT. *IEEE Transactions on Computers*, 48(8), 852-860. https://doi.org/10.1109/12.795127

Daabo, M. I., & Gbolagade, K. A. (2014). An Overflow Detection Scheme with a Reverse Converter for the Moduli set ${{2^{n}}-1 {2^{n}}{2^{n}}+ 1} $. *Journal of Emerging Trends in Computing and Information Sciences*, 5(12), 931-935. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.680.903&rep=rep1&type=pdf

Goh, V. T., & Siddiqi, M. U. (2008). Multiple error detection and correction based on redundant residue number systems. *IEEE Transactions on Communications*, 56(3), 325-330. doi.org/10.1109/TCOMM.2008.050401

Ibrahim, K. M., & Saloum, S. N. (1988). An efficient residue to binary converter design. *IEEE Transactions on Circuits and Systems*, 35(9), 1156-1158. doi.org/10.1109/31.7576

James, J., & Pe, A. (2015, August). A novel method for error correction using Redundant Residue Number System in digital communication systems. *In 2015 International Conference on Advances in Computing, Communications and Informatics* (ICACCI) (pp. 1793-1798). IEEE. doi.org/10.1109/ICACCI.2015.7275875

Jenkins, W. (1978). Techniques for residue-to-analog conversion for residue-encoded digital filters. *IEEE Transactions on Circuits and Systems*, 25(7), 555-562. doi.org/10.1109/TCS.1978.1084495

Jonsson, E. (1996). A quantitative approach to computer security from a dependability perspective. *Chalmers University of Technology*.

Krasnobaev, V., Koshman, S., Kononchenko, A., Kuznetsova, K., & Kuznetsova, T. (2019, December). The Formulation and Solution of the Task of the optimum reservation in the system of residual classes. *In 2019 IEEE International Conference on Advanced Trends in Information Theory* (ATIT) (pp. 1-4). IEEE. https://ieeexplore.ieee.org/abstract/document/9030483

Leighton, F. T. (1992). Parallel Algorithms and Architectures: Arrays-Trees-Hypercubes. Morgan-Kauffman, Los Altos, CA.

Olabanji, O. T., Gbolagade, K. A., & Yunus, A. (2016). Redundant Residue Number System Based Fault Tolerant Architecture over Wireless. In *Proceedings of Ibadan ACM, Computing Research and Innovation (CoRI'16)*, 212-216.).

Phalakarn, K., & Surarerks, A. (2018, April). Alternative Redundant Residue Number System Construction with Redundant Residue Representations. *In 2018 3rd International Conference on Computer and Communication Systems* (ICCCS) (pp. 457-461). IEEE. doi.org/10.1109/CCOMS.2018.8463305

Piestrak, S. J. (1995). A high-speed realization of a residue to binary number system converter. IEEE Transactions on Circuits and Systems II*: Analog and Digital Signal Processing*, 42(10), 661-663. doi.org/10.1109/82.471401

Pontarelli, S., Cardarilli, G. C., Re, M., & Salsano, A. (2008, October). A novel error detection and correction technique for RNS based FIR filters. *In 2008 IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems* (pp. 436-444). IEEE. doi.org/10.1109/DFT.2008.32

Soderstrand, M. A., Jenkins, W. K., Jullien, G. A., & Taylor, F. J. (Eds.). (1986). Residue number system arithmetic: Modern applications in digital signal processing. *IEEE Press*. https://dl.acm.org/doi/abs/10.5555/24966

Sun, J. D., & Krishna, H. (1992). A coding theory approach to error control in redundant residue number systems. ii. Multiple error detection and correction. IEEE Transactions on Circuits and Systems II: *Analog and Digital Signal Processing*, 39(1), 18-34. doi.org/10.1109/82.204107

Tay, T. F., & Chang, C. H. (2015). A non-iterative multiple residue digit error detection and correction algorithm in RRNS. *IEEE Transactions on Computers*, 65(2), 396-408. doi.org/10.1109/TC.2015.2435773

Tay, T. F., & Chang, C. H. (2017). Fault-tolerant computing in redundant residue number system. *In Embedded Systems Design with Special Arithmetic and Number Systems* (pp. 65-88). Springer, Cham. doi.org/10.1007/978-3-319-49742-6_4

Taylor, F. J. (1984). Residue arithmetic a tutorial with examples. *Computer*, (5), 50-62. doi.org/10.1109/MC.1984.1659138

Taylor, F., & Ramnarayan, A. (1981). An efficient residue-to-decimal converter. *IEEE Transactions on Circuits and Systems*, 28(12), 1164-1169. doi.org/10.1109/TCS.1981.1084942

Ushakov, I. A. 2013. Optimal Resource Allocation with practical statistical applications and theory, Hoboken, NJ: J. *Wiley* & *Sons*, ISBN-10: 9781118400708. doi.org/10.1002/9781118400715

Vinnakota, B., & Rao, V. B. (1994). Fast conversion techniques for binary-residue number systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 41(12), 927-929. doi.org/10.1109/81.340862

Wang, Y. (1998, November). New Chinese remainder theorems. *In Conference Record of Thirty-Second Asilomar Conference on Signals, Systems and Computers (Cat. No. 98CH36284)* (Vol. 1, pp. 165-171). IEEE. https://ieeexplore.ieee.org/abstract/document/750847/

Wang, Y. (2000). Residue-to-binary converters based on new Chinese remainder theorems. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 47(3), 197-205. doi.org/10.1109/82.826745

Yatskiv, V., & Tsavolyk, T. (2017, May). Improvement of data transmission reliability in wireless sensor networks on the basis of residue number system correcting codes using the special module system. *In 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering* (UKRCON) (pp. 890-893). IEEE. doi.org/10.1109/UKRCON.2017.8100376

Yau, S. S., & Liu, Y. C. (1973). Error correction in redundant residue number systems. *IEEE Transactions on Computers*, 100(1), 5-11. doi.org/10.1109/T-C.1973.223594