

**Communication**

# Redundant Residue Number System Based Multiple Error Detection and Correction Using Chinese Remainder Theorem (CRT)

**Idris Abiodun Aremu<sup>1</sup>, Kazeem Alagbe Gbolagade<sup>2</sup>**<sup>1</sup>Computer Science Department, School of Technology, Lagos State Polytechnics, Ikorodu, Lagos<sup>2</sup>Department of Computer Science, College of Information Communication Technology, Kwara State University, Ilorin, Kwara**Email address:**

Aremu.i@mylaspotech.edu.ng (I. A. Aremu), kazeem.gbolagade@kwasu.edu.ng (K. A. Gbolagade)

**To cite this article:**Idris Abiodun Aremu, Kazeem Alagbe Gbolagade. Redundant Residue Number System Based Multiple Error Detection and Correction Using Chinese Remainder Theorem (CRT). *Software Engineering*. Vol. 5, No. 5, 2017, pp. 72-80. doi: 10.11648/j.se.20170505.12**Received:** November 16, 2017; **Accepted:** November 30, 2017; **Published:** January 10, 2018

---

**Abstract:** During the last decade information security and reliable communication is unavoidable in information processing. Residue Number Systems (RNS) are still attracting considerable attention from the research community in digital signal processing. In this paper a new low cost method for multiple error detection and correction based on the Redundant Residue Number System (RRNS) was exhibited. RRNS is obtained by adding some redundant residues which brings in error detection and error correction competence. The proposed multiple error correction scheme exploit the Chinese Remainder Theorem (CRT) together with a novel algorithm that significantly simplifies the error correcting process for integers. The result is slightly different from the current state of the art whereby the error value is estimated using optimization algorithm such as integer programming and the proposed multiple error correction schemes does not require complex iterations in order to correct the errors.

**Keywords:** Chinese Remainder Theorem (CRT), Digital Signal Processing, Residue Number System (RNS), Redundant Residue Number System (RRNS)

---

## 1. Introduction

Over the centuries, information security has become a major issue [1]. Also Reliable communication and information security has been more important during the last one decade. Because of the carry free propagation of addition between digit in residue number system which can be used in high speed propagation such as addition, subtraction and multiplication. Reliability of these operations can be improved by adding a number of redundant moduli in the original number of the residue system also known as redundant residue number system denoted by  $(r_1, r_2, \dots, r_k, r_{k+1}, r_{k+2}, \dots, r_m)$  where  $(r_1, r_2, \dots, r_k)$  are the information number and  $(r_{k+1}, r_{k+2}, \dots, r_m)$  are the redundant residue number use to determine error position and to correct error in redundant residue number system. There are several works on error detection and correction using redundant residue number system which varies from single to multiple

error detection and correction system. Among the earlier reported work are the work of Yau and Lin [2] presented two error-correcting algorithms for redundant residue number systems, one for single residue-error correction and the other for burst residue-error correction. The two algorithm does not requires table lookup, but their implementation require memory space which is much smaller than that required by existing methods [2], [3] Watson and Hasting also proposed residue arithmetic which was use for general-purpose digital computers to detect and correct their own arithmetic and data-transmission errors. This approach was based on special properties inherent in a suitably chosen redundant residue number system (RRNS). [4] A coding theory approach to error control in redundant residue number systems (RRNSs) was also presented. It uses the concepts of Hamming weight, minimum distance, weight distribution, and error detection and correction capabilities in redundant residue number systems Ramachandran, Etzel and Jenkins, [5] to detect and

correct single error in a communication channel using redundant residue number system. Recently [6] Kati presented a residue arithmetic error correction scheme that was based on common factor using a moduli set. The work of [7] Mandelbaum was not left out in the area of error detection and correction using redundant residue number system, he also proposed a code to support other work in that area. The code theory approach of error detection and correction in RRNS was also proposed by (Sun and H. Kirshan) [8]. [9] Beckmann and Musicus design fault-tolerant convolution algorithm that is an extension of residue-number-system, the schemes applied to polynomial rings was described. The algorithm is suitable for implementation on multiprocessor systems and is able to concurrently mask processor failures. A fast algorithm based on long division for detecting and correcting multiple processor failures is presented in his work, a single fault detection and correction is studied. The coding scheme is capable of protecting over 90% of the computation involved in convolution. Goh and Siddiqi design a multiple error correction and detection using redundant residue number system [10], [11] Tay and Chang design a new algorithm for the correction of single residue digit error in Redundant Residue Number System. The location and magnitude of error can be extracted directly from a minimum size lookup table a single error correction and detection using redundant residue number system. [12] Pham, D. M., Premkumar, A. B., & Madhukumar, A. S also design a novel number theoretic transform called Inverse Gray Robust Symmetrical Number System (IGRSNS) for error control coding. IGRSNS is obtained by modifying Robust Symmetrical Number System (RSNS) that was proposed earlier, using Inverse Gray code property. Due to ambiguities present in each residue, RSNS has a short dynamic range (DR) compared to that in other number systems. The short DR of RSNS enables it to be effectively used for error detection without the addition of any redundant modulus as in Redundant Residue Number System. Although RSNS has a large redundant range, its detection ability is not optimal due to the Gray code property associated with it. In an attempt to overcome this limitation, we have proposed Inverse Gray coding to be combined with RSNS in increasing its effectiveness in error detection, and the algorithm performs well under all cases of single bit errors.

In this paper, we developed a novel error detection and correction scheme that can detect and correct more than one error (multiple error detection and correction). This scheme adopts the work [13] and [14]. The scheme also uses the conventional Chinese Remainder theorem (CRT) to detect and correct error that speeds up the processes and simplifies the error detection and correction. The algorithm adopted in this scheme is easier and simple to implement which makes the scheme more efficient and less computationally prove.

The rest of this paper is organized as follows: section 2 discusses the related review of residue number system and redundant residue number system, the proposed scheme was demonstrated theoretically in section 3, in section 4 performance evaluation of the proposed scheme was discussed and the paper concludes in section 5.

## 2. Review of Related Concepts

In this section related concepts in residue number system and redundant residue number system were discussed with some examples demonstrated.

### 2.1. Residue Number Systems

Residue number system comprises a set of moduli which are independent of each other. An integer is represented by the residue of each of the modulus and arithmetic operations are based on residues individually  $\{m_0, m_1, m_{n-1}\}$  [15]. The useful computational range  $M$  of such a number system, which is called the legitimate range, is defined by the product of all moduli in the moduli set, i.e.  $M = \prod_{i=0}^{n-1} m_i$ . A residue number system with legitimate range  $M$  is able to uniquely represent unsigned numbers in the range of  $[0, M-1]$ , or signed numbers in the range of  $[-M/2, M/2-1]$  for odd  $M$ , and  $[-M/2, M/2-1]$  if  $M$  is even. These ranges are known as the dynamic ranges. A number  $X$  within the dynamic range can be represented by the list of its residues with respect to the moduli defined in the moduli set.

### 2.2. Redundant Residue Number System

The RRNS is obtained by appending an additional  $r = (n-k)$  moduli, called redundant moduli  $m_{k+1}, m_{k+2}, \dots, m_n$  to the original moduli set of RNS. Thus  $m_1, m_2, \dots, m_k, m_{k+1}, m_{k+2}, \dots, m_n$  is a pair wise relatively prime number set forming the moduli set in RRNS. The integer  $X$  in the legitimate range  $[0, M]$  is represented by an  $n$ -tuple residue vector  $x = (x_1, x_2, \dots, x_n)$  with respect to the moduli set  $m_1, m_2, \dots, m_n$  as  $X \Leftrightarrow (x_1, x_2, \dots, x_n)$  which is referred to as an RRNS code word or RRNS code vector. The moduli  $(m_1, m_2, \dots, m_k)$  is the non redundant moduli while the remaining  $r$  moduli  $m_{k+1}, m_{k+2}, \dots, m_n$  are the redundant moduli that allow error detection and correction capability. RRNS can be used for error detection and error correction, self checking in digital computers [16]. The residue vector  $x$  can be divided into two parts: the first  $k$  residues corresponding to the  $k$  non redundant moduli are the information residues and the remaining  $r$  residues corresponding to the  $r$  redundant moduli called the parity residues. Let  $MR$  be the product of redundant moduli, that is  $MR = \prod_{i=k+1}^n m_i$ . The total DR of RRNS is  $[0, MMR]$  is divided into two adjacent ranges. The interval  $[0, M]$  is the legitimate range (DR), and the interval  $[M, MMR]$  is the illegitimate range (RR). An RRNS  $(n, k)$  code can detect up to  $(n-k)$  residue errors, or correct up to  $\lfloor (n-k)/2 \rfloor$  residue errors where  $\lfloor x \rfloor$  represents the largest integer not exceeding  $x$ . Alternatively, an RRNS  $(n, k)$  code can correct up to  $\lfloor r/2 \rfloor$  residue errors, and simultaneously detect up to  $r - \lfloor r/2 \rfloor$  residue errors, provided that  $r \geq n - k$  [17].

Example The RRNS code word for certain integer  $X$ , with moduli set  $(3, 5, 7, 11, 13, 16)$  as given as  $(r_1, r_2, \dots, r_k)$  where  $k = 6$  in Table 1. Here the information moduli set  $(3, 5, 7)$  and the redundant moduli set  $(11, 13, 16)$ . The dynamic range is 105.

**Table 1.** RRNS code word for integer  $X$  with the moduli set  $(3, 5, 7, 11, 13, 16)$ .

Integer	Non Redundant Residue			Redundant Residue		
X	$r_1$	$r_2$	$r_3$	$r_4$	$r_5$	$r_6$
2	2	2	2	2	2	2
5	3	0	2	1	3	0
10	1	0	3	10	10	10
15	0	0	1	4	2	15
21	0	1	0	10	8	5
50	2	0	1	6	11	2
100	1	0	2	1	9	4

### 2.3. Choice of Moduli

Data conversion and moduli selection are one of the greatest challenges for any RNS hardware design. Moduli choices determine the speed, dynamic range and hardware complexity of any RNS architecture. Hence, efficient moduli sets must be chosen with a sufficient dynamic range [17]. Moduli selection should satisfy the following conditions.

- N binary bit, the moduli should represent  $2^n$  distinct residue
- Computation operation of the moduli should be straight forward using binary adder

$$X = a_1 + a_2m_1 + a_2m_1m_2 + a_3m_1m_2m_3 + \dots + a_nm_1m_2m_3m_{n-1} \quad (2)$$

Where the mixed radix digit  $a_{i,i} = 1, k$  can be computed as follows

$$a_1 = x_1 \quad (3)$$

$$a_2 = |(x_2 - a_1)m_1^{-1}|_{m_2} \quad (4)$$

$$a_3 = |(x_3 - a_1)m_1^{-1}|_{m_3} - a_2|_{m_3} \quad (5)$$

$$a_n = |(((x_k - a_1)m_1^{-1}|_{m_k} - a_2)|_{m_k} - a_{k-1})|_{m_k} \quad (6)$$

For the Mixed Radix digits  $0 \leq a_i < m_i$ , using any positive number in the interval  $[0, \prod_{i=1}^n m_i]$  can be represented [17]

### 2.6. The New Chinese Remainder Theorem

Given a moduli set  $\{m_1, m_2, m_3, m_4\}$ , its equivalent weighted number  $X$  can be converted from it residue representation  $(x_1, x_2, x_3, x_4)$  as follows:

$$X = x_1 + m_1[k_1(x_2 - x_1) + k_2m_2(x_3 - x_2) + \dots + k_nm_2m_3 \dots m_n(x_n - x_{n-1})]_{m_2m_3 \dots m_n} \quad \text{such that} \quad k_1 = |m_1^{-1}|_{m_2m_3 \dots m_n}$$

$$|k_1m_1|_{m_2m_3 \dots m_n} = 1 \quad (7)$$

$$|k_2m_1m_2|_{m_3m_4 \dots m_n} = 1 \quad (8)$$

$$|k_nm_1m_2m_3 \dots m_{n-1}|_{m_n} = 1 \quad (9)$$

$$x_1 = 1, x_2 = 0, x_3 = 4, m_1 = 3, m_2 = 4, m_3 = 5, k_1 = 7 \text{ and } k_2 = 3 \quad (10)$$

$$X = 1 + 3|7(0 - 1) + 3.4(4 - 0)|_{4.5} = 1 + 3|7.19 + 12.4|_{20} = 1 + 3|133 + 48|_{20} = X = 1 + 3|133 + 48|_{20} = 1 + 3(1) = 4.$$

### 2.4. Chinese Remainder Theorem

Residue number system is a set of pair wise relatively prime moduli  $(m_1, m_2, \dots, m_n)$  and the residue representation  $(x_1, x_2, \dots, x_n)$  that is  $x_1 = [X]$  thus RNS is define in term of relatively prime moduli set  $\{m_i\}_{i=1,n}$  such that  $\gcd(m_i, m_j) = 1$  for  $i \neq j$ , while  $M = \prod_{i=1}^n m_i$  is the dynamic range. The residue of a decimal number  $X$  can be derived as  $x_i = |X|_{m_i}$

Given a moduli set  $\{(m_1, m_2, \dots, m_n)\}$ , the residue  $(x_1, x_2, \dots, x_n)$  can be converted into the corresponding decimal value  $X$  using the Chinese remainder theorem, Mixed radix conversion and New Chinese remainder theorem respectively as follows

$$X = |\sum_{i=1}^n m_i |m_i^{-1}|_{m_i} x_i|_M \quad (1)$$

Such that

$$M = \prod_{i=1}^n m_i \quad M_i = \frac{M}{m_i} \quad (2)$$

$M_i^{-1}$  is the multiplicative inverse  $m_i$

### 2.5. Mixed Radix Conversion

Mixed Radix Conversion is an alternative method which does not involve the large modulo- $M$  calculations. Given an RNS number  $(x_1; x_2; x_3 \dots \dots x_k)$  for the moduli set  $\{m_1; m_2; m_3; \dots \dots m_k\}$ .

### 3. Proposed Improved Scheme

This section discuss the propose scheme of the multiple error detection and correction method using redundant residue number system

Theorem 1.

A code based on a redundant residue number system has the minimum non zero hamming weight  $wt_{\min} \geq r + 1$  and minimum distance  $d_{\min} \geq r + 1$  (Ding, pei 1996) where  $r$  is the information moduli length

Theorem 2.

A code based on redundant residue number system can correct up to  $t$  errors and  $t \leq \left\lfloor \frac{r}{2} \right\rfloor$

A set of  $n$  pairwise relatively prime positive integer  $(m_1, m_2, \dots, m_n)$  called moduli set. Such that greatest common divisor  $\gcd(m_i, m_j) = 1$  for  $i$  and  $j$  where  $i \neq j$  and  $(m_1 < m_2 < m_n < m_{n+1} < m_{n+2}, \dots < m_n)$  from these set of  $m$  moduli, the first  $n$  moduli is non redundant moduli while the last  $n=m-k$  moduli form, a set of redundant moduli (Krishna, lin and sun, 1992)

Definition of information/Non redundant moduli set

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

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

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

Such that  $m_n$  is the dynamic range of the information moduli (i.e. legitimate range) and  $m_m$

Is the dynamic range of the redundant moduli (i.e.

illegitimate range) while  $M$  is the entire dynamic range which include both the legitimate and the illegitimate range

For multiple error detection and correction scheme we first consider a redundant residue code with a set of moduli  $m_i$ , an integer  $X$  is selected from the range  $[0, M_n]$  and the residue digits is  $x_i = (x_1, x_2, \dots, x_m)$   $m$  and  $n$  are chosen such that the theorem 2 prove that old, this allowing this code to correct up to  $t$  error such that  $t = \left\lfloor \frac{n}{2} \right\rfloor$

Let the range  $[0, M_n]$  be term as the legitimate range, while the range  $[M_n, M_m]$  be term as the illegitimate suppose  $t$  errors have been introduced into the residue digit  $Y$  when it passes through the transmission therefore  $y$  becomes  $y = x + e$  such that

$$(y_1, y_2, \dots, y_m) + (e_1, e_2, \dots, e_m) \quad (11)$$

Where  $0 \leq e_{pj} < m_{pj}$  for  $1 \leq j \leq t$  the error values are  $(e_{p1}, e_{p2}, \dots, e_{pt})$  and subscripts  $(p_1, p_2, \dots, p_m)$  are the positive of errors within  $y$ .

Receiving the vector  $y$ , error detection is first performing by determining whether  $y$  is a valid vector. This can be accomplished by computing the corresponding integer  $Y$  using the proposed generalised scheme formular as follows.

As new moduli set let us first prove that the moduli set  $\{2^{2n} - 1, 2^{2n}, 2^{2n} + 1, 2^{2n-1} - 1, 2^{2n+1} - 1\}$  is pair wise relatively prime. It is already proved that the moduli of  $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1\}$  are relatively prime for even values of  $n$  (cao, srikanthan and chang, 2005) therefore relatively  $\{2^{2n} - 1, 2^{2n}, 2^{2n} + 1, 2^{2n+1} - 1\}$  are also relatively prime for even values of  $n$  because the  $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1\}$  is a factor of  $\{2^{2n} - 1, 2^{2n}, 2^{2n} + 1, 2^{2n-1} - 1, 2^{2n+1} - 1\}$  Also we have to that  $2^{2n} - 1, 2^{2n}, 2^{2n-1} + 1, 2^{2n-1} - 1, 2^{2n+1} - 1\}$  are relatively prime to the last modulus  $2^{2n-1} - 1$

Eclulidean Theorem

$$\gcd(a, b) = \gcd(b, |a|_b) = 1 \quad (12)$$

$$\gcd(|2^{2n} - 1|, 2^{2n-1} - 1) = 1 \quad (13)$$

$$\gcd(2^{2n}, 2^{2n-1} - 1) = \gcd(|2^{2n}|_{2^{2n-1}}, 2^{2n-1} - 1) = 1$$

$$\gcd(2^{2n+1} - 1, 2^{2n-1} - 1) = \gcd(|2^{2n+1} - 1|_{2^{2n-1}-1}, 2^{2n-1} - 1) = 1 \quad (14)$$

since the greatest common divisor is equal to 1, then we say that all the modulus in the set are relatively prime to each others.

Reverse converter for  $2^{2n} - 1, 2^{2n}, 2^{2n} + 1, 2^{2n-1} - 1, 2^{2n+1} - 1$  moduli set.

The moduli set  $2^{2n} - 1, 2^{2n}, 2^{2n} + 1, 2^{2n-1} - 1, 2^{2n+1} - 1\}$  are valid and exist only for the even values of  $n$

$$M = (2^{2n} - 1)(2^{2n})(2^{2n-1} + 1)(2^{2n-1} - 1)(2^{2n+1} - 1)$$

$$\text{Such that } m_n = (2^{2n} - 1)(2^{2n}) \text{ and } m_m = (2^{2n} + 1)(2^{2n-1} - 1)(2^{2n+1} - 1)$$

Basically this superset is an extension of the three high moduli converter as proposed below speed moduli set converter proposed by [12] to design a four

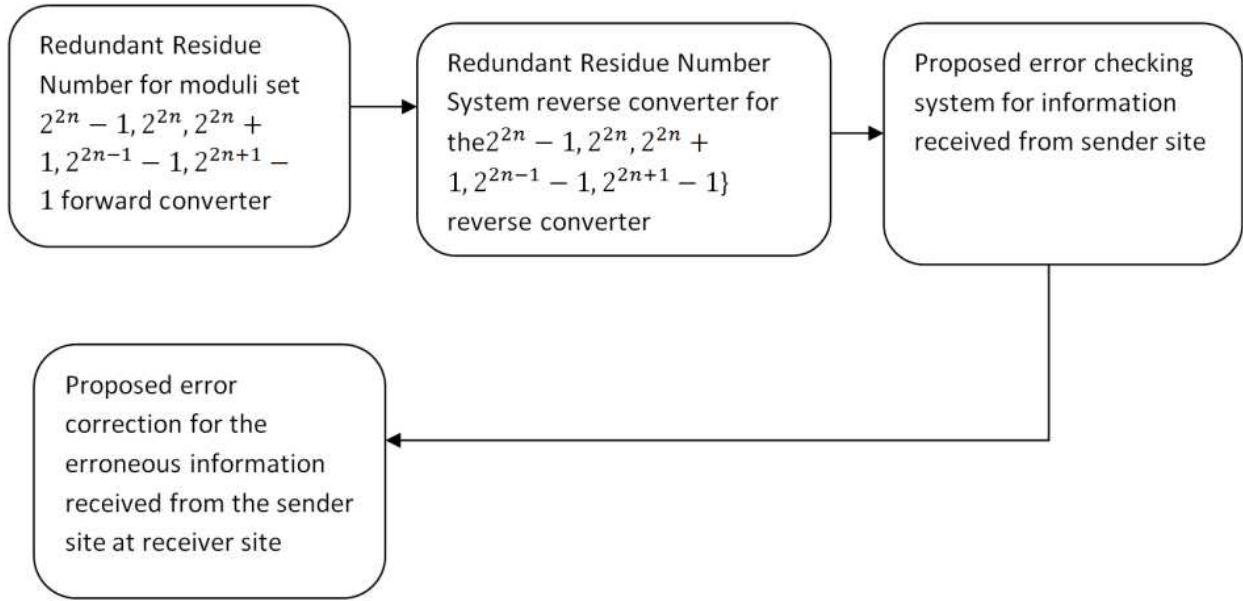


Figure 1. The Data flow diagram of the proposed multiple error detection and correction.

Algorithms for the proposed scheme

Step 1. Input parameter

The input the moduli set of the proposed scheme  $\{2^{2n} - 1, 2^{2n}, 2^{2n} + 1, 2^{2n-1} - 1, 2^{2n+1} - 1\}$  such that  $m_1 = 2^{2n-1} - 1, m_2 = 2^{2n} - 1, m_3 = 2^{2n}, m_4 = 2^{2n} + 1, m_5 = 2^{2n+1} - 1$  then input the information X

Step 2. To generate the residue digit

For (i=1, i ≤ 5, i++)

$$x_i = X \bmod m_i = |X|_{m_i} \quad (15)$$

Step 3. To determine the dynamic range of the entire system, that is the legitimate range and the illegitimate range using the following

$$M = \prod_{i=1}^n m_i = m_1 * m_2 * m_3 * m_4 * m_5$$

To determine  $m_n = \prod_{i=1}^2 m_1 * m_2$  and

To determine  $m_m = \prod_{i=3}^5 m_3 * m_4 * m_5$

Step 4: stop

Module 2 Algorithms

Step 1: start

Step 2: receiving information from the sender site as  $(y_1, y_2, \dots, y_m)$  and with respect to

$$\{(m_1, m_2, \dots, m_n)\}$$

Step 3: Compute the equivalent decimal of the information using the below CRT formular

$$Y = \left| \sum_{i=1}^n m_i |m_i^{-1}|_{m_i} x_i \right|_M \quad \text{Such that } M = \prod_{i=1}^n m_i \quad M_i = \frac{M}{m_i}$$

$M_i^{-1}$  is the multiplicative inverse  $m_i$

Step 4: Determine if the information is within legitimate or illegitimate range to decide whether there is an error in the information such that Y is valid if  $0 \leq Y < M_n$  otherwise there is an error in the information received

Step 5: stop

Algorithm for module 3

Step 1: start

Step 2: Receiving the erroneous information with respect to the moduli set such that

$$m_1 = 2^{2n-1} - 1, m_2 = 2^{2n} - 1, m_3 = 2^{2n}, m_4 = 2^{2n} + 1, m_5 = 2^{2n+1} - 1$$

Step 3: To perform consistency checking for the error position by arranging the moduli set into length three and convert the information to decimal respectively as follows

$$1. (y_1, y_2, y_3)_{RNS_{m_1 m_2 m_3}}$$

$$2. (y_1, y_3, y_4)_{RNS_{m_1 m_3 m_4}}$$

$$3. (y_1, y_4, y_5)_{RNS_{m_1 m_4 m_5}}$$

$$4. (y_2, y_3, y_4)_{RNS_{m_2 m_3 m_4}}$$

$$5. (y_2, y_4, y_5)_{RNS_{m_2 m_4 m_5}}$$

$$6. (y_3, y_4, y_5)_{RNS_{m_3 m_4 m_5}}$$

Using the above CRT

Step 4: To determine the position of the error from the output of above

Step 5: stop

Module 4: Algorithm

Step 1: start

Step 2: To restore the faulty channels with the corrected information we have  $y_i + e = y_i$

Step 3: stop

Consider a redundant residue number system with moduli set  $\{2^{2n} - 1, 2^{2n}, 2^{2n} + 1, 2^{2n-1} - 1, 2^{2n+1} - 1\}$  for even number  $n$  such that

$$m_1 = 2^{2n-1} - 1, m_2 = 2^{2n} - 1, m_3 = 2^{2n}, m_4 = 2^{2n} + 1, m_5 = 2^{2n+1} - 1$$

Where  $n=2$  and  $m=5$  from theorem 2, this can correct up to  $t=2$  errors. The legitimate range is  $[0, M_n]$  while the illegitimate range is  $[M_n, M_m]$ . Now let  $n = 2$

$$m_1 = 7, m_2 = 15, m_3 = 16, m_4 = 17, m_5 = 31$$

Taken  $X = 95$  and the equivalent residue digits is

$$x_1 = 4, x_2 = 5, x_3 = 15, x_4 = 10, x_5 = 2$$

Assuming there two errors ( $t=2$ ) have propagated into the information received during transmission at position 2 and 5 respectively, then the information received in vector  $y$  becomes  $(4, 2, 15, 10, 7)$ . Thus the following holds

$X$  become  $(4, 5, 15, 10, 2)$  and  $y$  becomes  $(4, 2, 15, 10, 7)$

From  $y$ , then the computed integer  $Y$  is follows below using the CRT we have

$$Y = \left| \sum_{i=1}^n m_i |m_i^{-1}|_{m_i} y_i \right|_M \text{ Such that } M = \prod_{i=1}^n m_i, M_i = \frac{M}{m_i}$$

$M_i^{-1}$  is the multiplicative inverse  $m_i$

Where  $M = 885360$

$$m_1 = 126480, m_2 = 59043, m_3 = 55335, m_4 = 52080, m_5 = 28560$$

$$m_1 = 7, m_2 = 15, m_3 = 16, m_4 = 17, m_5 = 31$$

And

$$x_1 = 4, x_2 = 3, x_3 = 5, x_4 = 10, x_5 = 2 \text{ and the respective } |m_i^{-1}|_{m_i} = (2, 8, 7, 4, 7)$$

$$\text{Therefore } Y = \left| m_1 |m_1^{-1}|_{m_1} x_1 + m_2 |m_2^{-1}|_{m_2} x_2 + m_3 |m_3^{-1}|_{m_3} x_3 + m_4 |m_4^{-1}|_{m_4} x_4 + m_5 |m_5^{-1}|_{m_5} x_5 \right|_M$$

$$Y = |126480 * 2 * 4 + 59042 * 8 * 2 + 55335 * 7 * 15 + 52080 * 4 * 10 + 28560 * 7 * 7|_{885360}$$

$$Y = |1011840 + 944672 + 581017 + 2083200 + 1399440|_{885360}$$

$$Y = |21249327|_{885360}$$

$$Y = 687$$

Since the computed  $Y$  is within the illegitimate range that is  $Y > 105$  it can be concluded that there are errors. Hence we perform module 3 algorithm iteratively. Therefore we have

Iteration 1

$$(y_1, y_2, y_3)_{RNS(7/15/16)}$$

$$(4, 2, 15)_{RNS(7/15/16)}$$

with error in Position channel 4 and 5, to compute the decimal equivalent by using the CRT we have

$$Y_{123} = \left| m_1 |m_1^{-1}|_{m_1} x_1 + m_2 |m_2^{-1}|_{m_2} x_2 + m_3 |m_3^{-1}|_{m_3} x_3 \right|_M$$

$$Y_{123} = |240 * 4 * 4 + 112 * 13 * 2 + 105 * 9 * 15|_{1680}$$

$$Y_{123} = |20927|_{1680} = 767$$

Iteration 2

$$(y_1, y_3, y_4)_{RNS(7/16/17)}$$

$$(4, 15, 10)_{RNS(7/16/17)}$$

with error in Position channel 2 and 5, to compute the decimal equivalent by using the CRT we have

$$Y_{134} = \left| m_1 |m_1^{-1}|_{m_1} x_1 + m_3 |m_3^{-1}|_{m_3} x_3 + m_4 |m_4^{-1}|_{m_4} x_4 \right|_M$$

$$Y_{123} = |272 * 6 * 4 + 119 * 7 * 15 + 112 * 12 * 10|_{1904}$$

$$Y_{123} = |32463|_{1904} = 95$$

Iteration 3

$$(y_1, y_3, y_5)_{RNS(7/17/31)}$$

$$(4, 15, 7)_{RNS(7/17/31)}$$

with error in Position channel 2 and 4, to compute the decimal equivalent by using the CRT we have

$$Y_{135} = |m_1|m_1^{-1}|_{m_1}x_1 + m_3|m_3^{-1}|_{m_3}x_3 + m_5|m_5^{-1}|_{m_5}x_5|_M$$

$$Y_{135} = |527 * 4 * 4 + 217 * 4 * 13 + 119 * 6 * 7|_{3689}$$

$$Y_{135} = |26450|_{3689} = 627$$

Iteration 4

$$(y_1, y_2, y_4)_{RNS(7/15/16)}$$

$$(4, 2, 10)_{RNS(7/15/17)}$$

with error in Position channel 3 and 5, to compute the decimal equivalent by using the CRT we have

$$Y_{124} = |m_1|m_1^{-1}|_{m_1}x_1 + m_2|m_2^{-1}|_{m_2}x_2 + m_4|m_4^{-1}|_{m_4}x_4|_M$$

$$Y_{124} = |255 * 5 * 4 + 119 * 14 * 2 + 105 * 6 * 10|_{1785}$$

$$Y_{124} = |14732|_{1785} = 452$$

Iteration 5

$$(y_1, y_2, y_5)_{RNS(7/15/31)}$$

$$(4, 2, 7)_{RNS(7/15/31)}$$

with error in Position channel 3 and 4, to compute the decimal equivalent by using the CRT we have

$$Y_{125} = |m_1|m_1^{-1}|_{m_1}x_1 + m_2|m_2^{-1}|_{m_2}x_2 + m_5|m_5^{-1}|_{m_5}x_5|_M$$

$$Y_{125} = |465 * 5 * 4 + 217 * 13 * 2 + 105 * 13 * 7|_{3255}$$

$$Y_{125} = |20927|_{3255} = 1712$$

Iteration 6

$$(y_2, y_3, y_4)_{RNS(15/16/17)}$$

$$(4, 2, 15)_{RNS(15/16/17)}$$

with error in Position channel 1 and 5, to compute the decimal equivalent by using the CRT we have

$$Y_{234} = |m_2|m_2^{-1}|_{m_2}x_2 + m_3|m_3^{-1}|_{m_3}x_3 + m_4|m_4^{-1}|_{m_4}x_4|_M$$

$$Y_{234} = |272 * 8 * 2 + 255 * 15 * 15 + 105 * 9 * 10|_{4080}$$

$$Y_{234} = |83327|_{4080} = 1727$$

Iteration 7

$$(y_2, y_3, y_5)_{RNS(15/16/17)}$$

$$(4, 2, 15)_{RNS(15/16/31)}$$

with error in Position channel 1 and 4, to compute the decimal equivalent by using the CRT we have

$$Y_{235} = |m_2|m_2^{-1}|_{m_2}x_2 + m_3|m_3^{-1}|_{m_3}x_3 + m_5|m_5^{-1}|_{m_5}x_5|_M$$

$$Y_{235}=|496 * 1 * 2 + 465 * 1 * 10 + 240 * 27 * 7|_{7440}$$

$$Y_{235}=|51002|_{7440}=6362$$

Iteration 8

$$(y_3, y_4, y_5)_{RNS(16/17/3)}$$

$$(4, 2, 15)_{RNS(16/17/3)}$$

With error in Position channel 1 and 2, to compute the decimal equivalent by using the CRT we have

$$Y_{345} = |m_3|m_3^{-1}|_{m_3}x_3 + m_4|m_4^{-1}|_{m_4}x_4 + m_5|m_5^{-1}|_{m_5}x_5|_M$$

$$Y_{345}=|527 * 15 * 15 + 496 * 6 * 10 + 272 * 22 * 7|_{4080}$$

$$Y_{345}=|190223|_{8432}=4719$$

Result of proposed multiple error correction and detection algorithm with i=8 iteration

From the result generated above only  $Y_{134} = 95$  is within the legitimate range which is our valid information.

**Table 2.** Below shows the summary of our result.

i	Y	Error position	Dynamic range	X
1	687	4	5	1680
2	687	2	5	1904
3	687	2	4	3689
4	687	3	5	1785
5	687	3	4	3255
6	687	1	5	4080
7	687	1	4	7440
8	687	1	2	8432

The process of recovering the original integer Y is calculated using CRT from the set of received residues from there recovering the original integer only entails the moduli operation over several iterations. The proposed scheme is slightly different from the current state of art whereby the error value is estimated using optimization algorithm such as integer programming and combined fraction

## 4. Performance Evaluation

In this section we present the performance evaluation for new algorithm and compare it with previous related algorithms. Table 1 shows the comparison between proposed method and previous ones [9].

**Table 3.** Evaluation Analysis.

Authors	Lookup Tables	Memory Space	Iteration	Generalised
Yau and Lin	No	Yes	High	No
Mohammed Sidiq	No	No	High	No
Tay and Chang	Yes	Yes	High	No
Proposed scheme	No	No	Low	Yes

## 5. Conclusion

This paper discusses about multiple error detection and error correction algorithm using RRNS set of law. The implementation of algorithm is explained by giving representative examples. RRNS techniques help in the development of a general purpose computer that has the properties like self checking, error detection and error correction. This algorithm is quite simple and easy to implement. The proposed algorithm can correct more than one errors than the other existing schemes at the expense of marginal increase in computation, reduces in number of iteration, elimination of look up table and it is compared with state of the art multiple error correction and detection in term of complexity, speed and iteration it is found to be slightly better.

## References

- [1] Aremu I. A. and Gbolagade K. A "Information encoding and decoding using Residue Number System for  $\{2^{2n}-1, 2^{2n}, 2^{2n}+1\}$  moduli sets" *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 6, Issue 8, August 2017, ISSN: 2278-1323*.
- [2] S.-S. Yau, Y.-c. Liu, Error correction in redundant residue number systems, *IEEE Trans. Computer. C-22 (1) (1973) 511*. <http://dx.doi.org/10.1109/T-C.1973.223594>.
- [3] R. W. Watson and C. W. Hastings, "Self-Checked Com-putation Using Residue Arithmetic," *Proceedings of the IEEE*, Vol. 54, No. 12, 1966, pp. 1920-1931.
- [4] S. S. S. Yau and Y. C. Liu, "Error Correction in Redundant Residue Number Systems," *IEEE Transactions on Computers*, Vol. C-22, No. 1, 1973, pp. 5-11.



- [5] D. Mandelbaum, "Error Correction in Residue Arithmetic-tic," *IEEE Transactions on Computers*, Vol. C-21, No. 6, 1972, pp. 538-545.
- [6] M. H. Etzel and W. K. Jenkins, "Redundant Residue Number Systems for Error Detection and Correction in Digital Filters," *IEEE Transactions on Acoustics Speech and Signal Processing*, Vol. 28, No. 10, 1980, pp. 588-544.
- [7] R. W. Watson, "Error Detection and Correction and Other Residue-Interacting Operations in a Redundant Residue Number System," University of California, Berkeley.
- [8] V. Ramachandran, "Single Residue Error Correction in Residue Number Systems," *IEEE Transactions on Computers*, Vol. C-32, No. 5, 1983, pp. 504-507.
- [9] Beckmann, P. E., & Musicus, B. R. (1993). Fast fault-tolerant digital convolution using a polynomial residue number system. *IEEE transactions on Signal Processing*, 41 (7), 2300-2313.
- [10] Katti, R. S. (1996). A new residue arithmetic error correction scheme. *IEEE transactions on computers*, 45 (1), 13-19.
- [11] Goh, V. T., & Siddiqi, M. U. (2008). Multiple error detection and correction based on redundant residue number systems. *IEEE Transactions on Communications*, 56 (3).
- [12] Pham, D. M., Premkumar, A. B., & Madhukumar, A. S. (2011). Error detection and correction in communication channels using inverse gray RSNS codes. *IEEE Transactions on communications*, 59 (4), 975-986.
- [13] Bankas, E. K., Gbolagade, K. A., & Cotozana, S. D. (2013, June). An effective New CRT based reverse converter for a novel moduli set  $\{2^{2n+1}-1, 2^{2n+1}, 2^{2n-1}\}$ . In *2013 IEEE 24th International Conference on Application-Specific Systems, Architectures and Processors* (pp. 142-146). IEEE.
- [14] Gbolagade, K. A. (2010). *Effective reverse conversion in residue number system processors*. Doctoral dissertation, TU Delft, Delft University of Technology, Netherland.
- [15] Aremu I. A. and Gbolagade K. A "Information encoding and decoding using Residue Number System for  $\{2^{2n}-1, 2^{2n}, 2^{2n+1}\}$  moduli sets" *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 6, Issue 8, August 2017, ISSN: 2278-1323*.
- [16] Aremu I. A. and Gbolagade K. A 'Generalized Information Security and Fault Tolerant Based On Redundant Residue Number System' *International Journal of Computer Applications (0975 – 8887) Volume 167-No .13, June 2017*.
- [17] Younes, D., & Steffan, P. (2012). A comparative study on different moduli sets in residue number system. In *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on* (pp. 1-6). IEEE.
- [18] Tay, T. F., & Chang, C. H. (2014, June). A new algorithm for single residue digit error correction in Redundant Residue Number System. In *Circuits and Systems (ISCAS), 2014 IEEE International Symposium on* (pp. 1748-1751). IEEE.
- [19] Hadjicostis, C. N. (2003). Non concurrent error detection and correction in fault-tolerant discrete-time LTI dynamic systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 50 (1), 45-55.
- [20] Beckmann, P. E., & Musicus, B. R. (1993). Fast fault-tolerant digital convolution using a polynomial residue number system. *IEEE transactions on Signal Processing*, 41 (7), 2300-2313.
- [21] T. F. Tay, C. H. Chang, A non-iterative multiple residue digit error detection and correction algorithm in RRNS. *IEEE Trans. Comput.* 65 (2), 396-408 (2016).