Communication

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

Idris Abiodun Aremu¹, Kazeem Alagbe Gbolagade²

¹Computer Science Department, School of Technology, Lagos State Polytechnics, Ikorodu, Lagos
²Department 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. V ol. 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 \((r_1, r_2, \ldots, r_k, r_{k+1}, r_{k+2}, \ldots, r_m)\) were \((r_1, r_2, \ldots, r_k)\) are the information number and \((r_{k+1}, r_{k+2}, \ldots, r_m)\) 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 is 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 (IGRNS) for error control coding,. IGRNS 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 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 use the conventional Chinese Remainder theorem (CRT) to detect and correct error that speed up the processes and simplify the error detection and correction. The algorithm adopted in this scheme is easier and simple to implement which make the scheme more efficient and less computationally prove

The rest of his paper is organised as follows section 2 discuss 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 discuss and the paper was conclude in section 5

2. Review of Related Concepts

In this section related concepts in residue number system and redundant residue number system was 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 \((m_0, m_1, m_{-1})\) [15]. The 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. \(M = \prod_{i=0}^{n-1} m_i \) or \(M = \prod_{i=0}^{n-1} m_i \) is able to uniquely represent unsigned numbers in the range of \([0, M − 1]\), or signed numbers in the range of \([-M −1, M + 1]\) 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 \(m_{k+1}, m_{k+2}, m_n\) to the original moduli set of RNS. Thus \(m_1, m_2, m_k, m_{k+1}, m_n\) 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 \(x=(x_1, x_2, ..., x_n)\) with respect to the moduli set \(m_1, m_2, ..., m_n\) as \(X≡(x_1, x_2, ..., x_n)\) which is referred to as an RRNS code word or RRNS code vector. The moduli \((m_1, m_2)\) is the non redundant moduli while the remaining \(r \) moduli \(m_{k+1}, m_{k+2}, m_n\) 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 \((n−k)\) residue errors where \(|x|\) represents the largest integer not exceeding \(x\). Alternatively, an RRNS \((n, k)\) code can correct up to \((n−k)\) residue errors, and simultaneously detect up to \(v\) residue errors, provided that \(v \leq n − k\) [17].

Example The RRNS code word for certain integer \(X\), with moduli set \((3, 5, 7, 11, 13, 16)\) as given as \((r_1, r_2, ..., r_k)\) 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.
2.6. The New Chinese Remainder Theorem

Forward using binary adder conditions. Moduli selection should satisfy the following
moduli sets must be chosen with a sufficient dynamic range complexity of any RNS architecture. Hence, efficient
choices determine the speed, dynamic range and hardware
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
i. N binary bit, the moduli should represent $2^n$ distinct residue
ii. Computation operation of the moduli should be straightforward using binary adder

$$X = a_1 + a_2m_1 + a_3m_1m_2 + a_3m_1m_2m_3 + \ldots + a_nm_nm_2m_3m_{n-1}$$

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

$$a_1 = x_1$$

$$a_2 = |x_2 - a_1| \mod m_2$$

$$a_3 = |x_3 - a_1| \mod m_3$$

$$a_n = |(x_k - a_{k-1})| \mod m_k$$

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]

2.4. Chinese Remainder Theorem

Residue number system is a set of pair wise relatively prime
moduli $(m_1, m_2, \ldots, m_n)$ and the residue representation
$(x_1, x_2, \ldots, x_n)$ 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 $M = \prod_{i=1}^k m_i$ is the dynamic range. The
residue of a decimal number X can be derived as $x_i = [X]_{m_i}$

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

$$X = \sum_{i=0}^n m_i \lfloor m_i^{-1} x_i \rfloor$$

Such that

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

$$M_i^{-1}$$ 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 $(x_1, x_2, x_3, \ldots, x_k)$ for the moduli set $(m_1, m_2, m_3, \ldots, m_k)$.

$$X = 2.4. Chinese Remainder Theorem$$

$$\sum_{i=0}^n m_i \lfloor m_i^{-1} x_i \rfloor$$

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

$$M_i^{-1}$$ 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 $(x_1, x_2, x_3, \ldots, x_k)$ for the moduli set $(m_1, m_2, m_3, \ldots, m_k)$.

$$X = \sum_{i=0}^n m_i \lfloor m_i^{-1} x_i \rfloor$$

Such that

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

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

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:

$$X = x_1 + m_1 |(x_2 - x_1) + k_2m_2(x_3 - x_2) + \ldots + k_nm_n(x_n - x_{n-1})|_{m_2m_3 \ldots m_n}$$

such that

$$k_1 = |m_1^{-1}|_{m_2m_3 \ldots m_n} = 1$$

$$k_2 = |m_2^{-1}|_{m_3m_4 \ldots m_n} = 1$$

$$k_n = |m_n^{-1}|_{m_1m_2 \ldots m_{n-1}} = 1$$

$$k_1 = 7 \text{ and } k_2 = 3$$

$$X = 1 + 3\lceil 7(0-1) + 3.4(4-0) \rceil_{4} = 1 + 3\lceil 7.19 + 12.4 \rceil_{20} = 1 + 3\lceil 133 + 48 \rceil_{20} = 1 + 3(1) = 4.$$
3. Proposed Improved Scheme

This section discusses the proposed scheme of the multiple error detection and correction method using redundant residue number systems.

Theorem 1.
A code based on a redundant residue number system has the minimum non zero Hamming weight \( w_{\text{min}} \geq r + 1 \) and minimum distance \( d_{\text{min}} \geq r + 1 \) (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 \( t \leq \left\lfloor \frac{n}{2} \right\rfloor \).

A set of \( n \) pairwise relatively prime positive integer \((m_1,m_2,\ldots,m_n)\) called moduli set. Such that greatest common divisor \( \gcd(m_i,m_j) = 1 \) for \( i \neq j \) and \((m_1 < m_2 < m_3 < \ldots < m_n)\) 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

\[
m_n = \prod_{i=1}^{n} m_i
\]

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

\[
M = \prod_{i=1}^{n} m_i X \prod_{i=n+1}^{m} m_i = \prod_{i=1}^{n} m_i
\]

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 \( m_1, m_2, \ldots, m_n \), an integer \( X \) is selected from the range \([0, M_n]\) and the residue digits is \( x_i = (x_{1i}, x_{2i}, \ldots, x_{mi}) \) and \( n \) are chosen such that the theorem 2 proves that old, this allowing this code to correct up to \( t \) errors 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 range, 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

\[
y' = (y_1, y_2, \ldots, y_m) + (e_1, e_2, \ldots, e_m)
\]

Where \( 0 \leq e_{pj} < m_{pj} \) for \( 1 \leq j \leq t \) the error values are \( \{e_{p1}, e_{p2}, \ldots, e_{pt}\} \) and subscripts \( \{p_1, p_2, \ldots, p_m\} \) are the set of \( p \) 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 formula as follows.

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

Euclidean Theorem

\[
gcd(a, b) = gcd(b, |a|_b) = 1
\]

\[
gcd(2^{2n-1}, 2^{2n+1} - 1) = 1
\]

\[
gcd(2^{2n}, 2^{2n+1} - 1) = gcd(2^{2n}, 2^{2n+1} - 1) = 1
\]

\[
gcd(2^{2n+1} - 1, 2^{2n+1} - 1) = gcd(2^{2n+1} - 1, 2^{2n+1} - 1) = 1
\]

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.

Reversely for \( 2^{2n-1}, 2^{2n} + 1, 2^{2n+1} - 1 \) moduli set.

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

\[
M = (2^{2n} - 1)(2^{2n+1})(2^{2n-1} + 1)(2^{2n+1} - 1)(2^{2n} - 1)
\]

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

Basically this supersets is an extension of the three high speed moduli set converter proposed by [12] to design a four
Algorithms for the proposed scheme

Step 1: Input parameter
The input the moduli set of the proposed scheme \( \{2^{2n} - 1, 2^{2n} + 1, 2^{2n-1} - 1, 2^{2n+1} - 1\}\) such that \( m_1 = 2^{2n-1} - 1, m_2 = 2^{2n} - 1, m_3 = 2^{2n}, m_4 = 2^{2n+1} - 1\)

Step 2: To generate the residue digit
For \( i = 1, \ldots, 5, i++ \)
\[
x_i = x \mod m_i = |x|_{m_i} \quad (15)
\]

Step 3: To determine the dynamic range of the entire system, that is the legitimate range and the illegitimate range using the following
\[
M = \prod_{i=1}^{5} m_i = m_1 * m_2 * m_3 * m_4 * m_5
\]
To determine \( m_n = \prod_{i=1}^{2} m_i \) and
To determine \( m_m = \prod_{i=3}^{5} m_i \) and
Step 4: stop

Module 2 Algorithms

Step 1: start
Step 2: Receiving information from the sender site as \((Q_1, Q_2, \ldots, Q_m)\) and with respect to
\[
\{(m_1, m_2, \ldots, m_n)\}
\]
Step 3: Compute the equivalent decimal of the information using the below CRT formula
\[
Y = \left[ \sum_{i=0}^{n} m_i |m_i^{-1}|m_i x_i \right]_{M}
\]
Such that \( M = \prod_{i=1}^{n} m_i \)

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 \( 0 \leq Y < M \) 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
\[
m_1 = 2^{2n-1} - 1, m_2 = 2^{2n} - 1, m_3 = 2^{2n}, m_4 = 2^{2n+1} - 1, m_5 = 2^{2n+1} - 1
\]

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. \((y_1, y_2, y_3)_{RNS_{m_1 m_2 m_4}}\)
3. \((y_1, y_2, y_3)_{RNS_{m_1 m_3 m_4}}\)
4. \((y_1, y_2, y_3)_{RNS_{m_2 m_3 m_4}}\)
5. \((y_2, y_3, y_4)_{RNS_{m_1 m_2 m_5}}\)
6. \((y_3, y_4, y_5)_{RNS_{m_1 m_3 m_5}}\)
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 \( \{2^{2n} - 1, 2^{2n}, 2^{2n+1} - 1\} \) for even number \( n \) such that

\[ m_1 = 2^{2n-1} - 1, m_2 = 2^{2n} - 1, m_3 = 2^{2n}, m_4 = 2^{2n+1} - 1 \]

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

\[ X \text{ become } (4, 5, 15, 10, 2) \text{ and } y \text{ becomes } (4, 2, 15, 10, 7) \]

From \( y \), then the computed integer \( Y \) is follows below using the CRT we have

\[ Y = \sum_{i=0}^{n-1} m_i y_i \]

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

\[ x_1 = 4, x_2 = 3, x_3 = 5, x_4 = 10, x_5 = 2 \]

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

\[ Y = 126480 \cdot 2 \cdot 4 + 59043 \cdot 8 \cdot 2 + 55335 \cdot 7 \cdot 15 + 52080 \cdot 4 \cdot 10 + 28560 \cdot 7 \cdot 7 \]

\[ Y = 1011840 + 944672 + 581017 + 2083200 + 1399440 \]

\[ Y = 21249327 \]

\[ Y = 687 \]

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

\[ (y_1, y_2, y_3)_{\text{RNS}(7/15/16)} \]

\[ (4, 2, 15)_{\text{RNS}(7/15/16)} \]

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

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

\[ Y_{123} = 240 \cdot 4 \cdot 4 + 112 \cdot 13 \cdot 2 + 105 \cdot 9 \cdot 15 \]

\[ Y_{123} = 20927 \]

\[ Y_{123} = 767 \]

Iteration 2

\[ (y_1, y_3, y_4)_{\text{RNS}(7/16/17)} \]

\[ (4, 15, 10)_{\text{RNS}(7/16/17)} \]

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

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

\[ Y_{134} = 272 \cdot 6 \cdot 4 + 119 \cdot 7 \cdot 15 + 112 \cdot 12 \cdot 10 \]

\[ Y_{134} = 1904 \]
Idris Abiodun Aremu and Kazeem Alagbe Gbolagade: Redundant Residue Number System Based Multiple Error Detection and Correction Using Chinese Remainder Theorem (CRT)

\[ Y_{123} = [32463]_{1904} = 95 \]

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

\[ Y_{135} = \left[ m_1 m_1^{-1} m_2 x_1 + m_3 m_2^{-1} m_3 x_3 + m_5 m_2^{-1} m_5 x_5 \right]_M \]
\[ Y_{135} = [527 \times 4 \times 4 + 217 \times 4 \times 13 + 119 \times 6 \times 7]_{3689} \]
\[ Y_{135} = [26450]_{3689} = 627 \]

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

\[ Y_{124} = \left[ m_1 m_1^{-1} m_2 x_1 + m_2 m_2^{-1} m_2 x_2 + m_4 m_2^{-1} m_4 x_4 \right]_M \]
\[ Y_{124} = [255 \times 5 \times 4 + 119 \times 14 \times 2 + 105 \times 6 \times 10]_{1785} \]
\[ Y_{124} = [14732]_{1785} = 452 \]

Iteration 5

\[ (y_1, y_2, y_4)_{RNS(7/15/31)} \]
\[ (4, 2, 7)_{RNS(7/15/31)} \]

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

\[ Y_{125} = \left[ m_1 m_1^{-1} m_2 x_1 + m_2 m_2^{-1} m_2 x_2 + m_5 m_2^{-1} m_5 x_5 \right]_M \]
\[ Y_{125} = [465 \times 5 \times 4 + 217 \times 13 \times 2 + 105 \times 13 \times 7]_{3255} \]
\[ Y_{125} = [20927]_{3255} = 1712 \]

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

\[ Y_{234} = \left[ m_2 m_2^{-1} m_2 x_2 + m_3 m_2^{-1} m_3 x_3 + m_4 m_2^{-1} m_4 x_4 \right]_M \]
\[ Y_{234} = [272 \times 8 \times 2 + 255 \times 15 \times 15 + 105 \times 9 \times 10]_{4080} \]
\[ Y_{234} = [83327]_{4080} = 1727 \]

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
\[
Y_{235} = |m_2| m_2^{-1} |m_2 x_2 + m_3| m_3^{-1} |m_3 x_3 + m_5| m_5^{-1} |m_5 x_5|_M
\]
\[
Y_{235} = |496 \times 1 + 2 + 465 \times 1 + 10 + 240 \times 7|_{17440} = 51002
\]
\[
Y_{235} = 6362
\]

Iteration 8

\[\left( Y_9, Y_4, Y_3 \right)_{RNS(16/17/3)} \]
\[(4, 2, 15)_{RNS(16/17/3)}\]

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

\[
Y_{345} = |m_3| m_3^{-1} |m_3 x_3 + m_4| m_4^{-1} |m_4 x_4 + m_5| m_5^{-1} |m_5 x_5|_M
\]
\[
Y_{345} = |527 \times 15 + 496 \times 6 + 10 + 272 \times 22 + 7|_{4080} = 190223
\]
\[
Y_{345} = 4719
\]

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.

| \( i \) | \( Y \) | 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].

| 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 Computation 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.
Idris Abiodun Aremu and Kazeem Alagbe Gbolagade: Redundant Residue Number System Based Multiple Error Detection and Correction Using Chinese Remainder Theorem (CRT)

[5] D. Mandelbaum, “Error Correction in Residue Arithmetic,” 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., & Cotofana, S. D. (2013, June). An effective New CRT based reverse converter for a novel moduli set \{2^n+1−1, 2 2^n+1, 2 2^n−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).