NOVEL ALGORITHM FOR DECODING REDUNDANT RESIDUE NUMBER SYSTEMS (RRNS) CODES

Amusa, K. A.[1] & Nwoye E. O.[2]
[1]Electrical and Electronic Engineering Dept., Federal University of Agriculture, Abeokuta
[2]Biomedical Engineering Dept., University of Lagos, Lagos
Email: amusaakinwale@yahoo.com, nwoyeephraimo@yahoo.com

ABSTRACT
Error control is one major challenge of data transmission through modern digital systems. A number of error control schemes have been employed to address this challenge in order to facilitate efficient and reliable data transmission through digital systems. This paper however, presents an improved method for error correction usingRedundant Residue Number System (RRNS)codes. RRNS codes are maximum-minimum distance block codes with widerapplication in the area of signal processing such as self-checking in arithmetic units, error control in digital processors and data transmission. The proposed method is premised on modulus projection approach. The proposed algorithm considerably reduces the computation overhead for RRNS codesdecodingbecause it employed hybrid method in integer recovery process.

Keywords: *Error Control, Modulus projection, Data Transmission, Redundant Residue Number System Code, Computation overhead, Block Codes*

1. INTRODUCTION

A number of error-control schemes have been used to realize efficient and reliable transmission of data through modern digital systems such as filters, arithmetic units and digital signal processors. This paper however presents an improved error control scheme based on redundant residue number system. A residue number system (RNS) for integer is a method of representing weighted number system (WNS) by a set of its remainders. Error-control is realized by appending these residues with extra ones. These additional residues constitute parity digits, hence, the term redundant residue number system.Error correction codes based on RNS are attractive because of the inherent characteristics of RNS. Such features include; parallelism, modularity, fault-tolerance, carry-free operations, and lack of order significance among the residues [1]. Appreciable efforts have been expended with respect to RRNS codes by many scholars. Self-checking architectures were first introduced by Watson and Hastings[2]. In the course of investigating error correcting properties of RRNS, Barsi and Maestrini [3] developed the concept of legitimate and illegitimate range. Jenkins et al applied successfully mixed radix conversion (MRC) technique and Base Extension (BEX)operationto RRNS application in digital filters and residue number error checkers in [4] and [5]. Krishna et al in [7] and [8] proposed coding theoretic framework for RRNS. Krishna et al. [7] and [8] presented discussion on single residue digit error correction and multiple residue digits error correction respectively. Approach given by Goh and Siddiqi [10] employed Chinese Remainder Theorem (CRT) to recover the integer from received residues and came up with another method of multiple error-controlsin RRNS codes.

In this paper, a novel approach to error-control in RRNS is proposed. This scheme is based on the strategy where estimates of transmitted integer are computed from the received residues. The proposedscheme here neither requires complex optimization nor involve large modulo operation because CRT is not employed.Briefly, the proposed scheme involves conversion of received residues to its mixed radix form to detect whether it is error free or not. If all redundant mixed radix digits are zeros, then the received residues is error free and the integer is computed from mixed radix digits via BEX operation. If some or all of redundant mixed radix digits are non-zero, then the received residues are declared to be erroneous. Based on the error detecting capability of the RRNS code in question, its projection depth is determined. This is then used in performing moduli projection to obtain reduced residue. Corresponding integer is determined from reduced residue using matrix method for integer recovery from residues. Hamming distances are computed for residue representation of computed integers found lying within the legitimate rangeof the RRNS code and the received residue. Any of the integers that have Hamming distance of less or equal to the error correcting capability of the RRNS code is the transmitted integer.

2. REDUNDANT RESIDUE NUMBER SYSTEM

Yang and Hanzo [1] defined RRNSby a set of n pair-wise positive integers $m_1, m_2, m_3, \ldots, m_k, m_{k+1}, m_{k+2}, \ldots, m_n$ called moduli. Among these n moduli, the first k moduli form a set of non-redundant moduli, and their product represents the dynamic range, M, of the RNS as given by equation (1)

M =$\prod_{i=1}^{k} m_i$ (1)

The remaining $r = n - k$ moduli form the set of redundant moduli that allows error detection and correction in the RRNS.
Suppose M_R is the product of redundant moduli as given below in equation (2),

$M_R = \prod_{i=k+1}^{n} m_i$ (2)

Every integer X in the range $[M + ?)$ can be represented by a unique residue sequence x having n components $x_1, x_2, x_3, \ldots, x_n$ that is,

$$X \Leftrightarrow x_{i=1}^{n} \quad (3)$$

Where $x_i \equiv X \ (mod m_i)$ (4)

Where $A \equiv B means A is congruent to B$

The integer x_i is the ith residue digit corresponding to the ith modulus m_i and satisfies the inequality $0 \leq x_i < m_i$. From the foregoing, it follows that the residue vector x can be divided into two parts; the first k non-redundant moduli are called the information digits, and the remaining r residue digits corresponding to the r redundant moduli are called the parity digits.

Given a residue $x = [x_1, x_2, x_3, \ldots, x_n]$ the corresponding integer X can be uniquely determined by solving n congruencies in equation (4). This is simplified via the use of Chinese Remainder Theorem (CRT). According to this theorem, for any given residue vector $(x_1, x_2, x_3, \ldots, x_n)$ where $0 \leq x_i < m_i$ for $i = 1, 2, 3, \ldots, n$, there exist one and only one integer X such that $0 \leq X < M$ and $x_i \equiv X \ (mod m_i)$. This number X is calculated as follows in equations (5) to (7):

$$X \equiv x_i T'_i M'_i \ (mod\ M) \quad (5)$$

Where $M'_i = \frac{M}{m_i}$ (6)

And the integers $T'_i, i = 1, 2, 3, \ldots, n$ are determined a priori using the congruencies

$$T'_i M'_i = 1 \ (mod\ m_i) \quad (7)$$

The integers T'_i are regarded as the multiplicative inverses of M'_i.

The real-time implementation of the CRT is however, not practical as it requires modular operations involving a large integer M. In order to avoid processing of large integers, a commonly used alternative is the base extension (BEX) operation alongside with the mixed radix conversion (MRC) method [16].MRC is formulated as follows [16]: given a set of residues $(x_1, x_2, x_3, \ldots, x_n)$ defined on the corresponding set of moduli $\{m_1, m_2, m_3, \ldots, m_n\}$ and a set of mixed radix digits $\{a_1, a_2, \ldots, a_n\}$, the decimal equivalent of the residues can be determined as follows in equation (8) to (9):

$X = a_1 + a_2 m_i + a_3 m_1 m_2 + \ldots + a_n \prod_{i=1}^{n-1} m_i$ (8)

Where the mixed radix digit (MRD) are given as:

$a_1 = x_1$

$a_2 = ((x_1 - a_1) m_1^{-1})_{m_2}$

$\ldots$

$a_n = (((\ldots((x_n - a_1) m_1^{-1} - a_2) m_2^{-1} - \ldots -) a_{n-1}) m_{(n-1)}^{-1})_{m_n}$ (9)

For the mixed radix digits $0 \leq a_i < m_i$, any positive number in the range $[0, \prod_{i=1}^{n} m_{i-1}]$ can be unambiguously represented.

A variant of MRC was developed into a generalized matrix method for integer recovery from its residues by Gbolagade and Cotofona [6]. The method utilizes the periodicity property of RNS. It is formulated as follows [6]:

Given the moduli set $\{m_1, m_2, m_3, \ldots, m_n\}$, the residue set $(x_1, x_2, x_3, \ldots, x_n)$ is converted into decimal equivalent X as shown in equations (10) and (11)

$X = \sum_{i=1}^{n} P_i$ (10)
Where P_i is defined as
$P_i = A.B.C$ (11)
with $A = (m_1\ m_2\ m_3 \ldots m_{i-1})$, $B = ((m_1\ m_2\ m_3 \ldots m_{i-1})^{-1}) mod\ m_i$ and
$C = (t_{(i-1)j}) mod\ m_i$
$i > 1\ and\ (t_{(i-1)j})$ is a value to be determined based on matrix based computation.

3. ALGORITHM FORMULATION

Altman and Jenkins [5] presented algorithm for locating a single residue digit error based on the properties of modulus projection and mixed radix conversion (MRC). The modulus m_i- projection of X in an RRNS (n, k) code, given by X_i, defined in equation (14) as [8]

$$X_i \equiv \text{X (mod } \frac{\text{M}M_R}{m_i}\text{)} \qquad (12)$$

That is, X_i can be expressed as $[x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ which is the residue form of X in a reduced RRNS with the ith residue digit, x_i, deleted. The mixed radix representation of X_i is given by

$X_i = \sum_{l=1}^{n} a_l \prod_{r=1}^{l-1} m_r\ ,\ l \neq i\ , r \neq l$ (13)

The first k mixed radix digits are still regarded as the non-redundant mixed radix digits and the remaining are the redundant mixed radix digits. It is clear that if X_i is a legitimate number, all of redundant mixed radix digits are zero. Generally, the $M_\wedge$ - projection of integer X, denoted by $X_\wedge$, is given by equation (16)

$$X_\wedge \equiv \text{X (mod M}M_R/M_\wedge\text{)} \qquad (14)$$

Where $M_\wedge = \prod_{\alpha=1}^{\lambda} m_{i_\alpha}$, $\wedge = \{i_1 i_2, \ldots, i_c, \ldots, i_\lambda\}$, $i_1 < i_2 < \ldots < i_c < \ldots < i_\lambda$ and $\lambda \leq n - k = d - 1$, d is the code minimum distance.

Theorem 1 [8]: Suppose $\bar{X}$ is an illegitimate integer message in the RRNS (n, k) code. Suppose also that there exists a legitimate integer message X that differs from $\bar{X}$ in the $i_1 th, i_2 th, \ldots, i_\lambda th,$ residue digits, where $\lambda \leq$ (n-k), then the $M_\wedge$ - projection $X_\wedge$ is a legitimate number.

Theorem 1 suggests that the correct or (transmitted) integer message X can be recovered from an illegitimate (or erroneously received) integer message by dropping some of the received residue digits and their related moduli, provided that the erroneous residue digits are the dropped ones and the reduced RRNS exhibits a sufficiently high dynamic range to unambiguously represent the integer constituting the message. That is, a reduced form of RRNS is possible. Furthermore, the integer Y corresponding to this residue digits can be determined from k out of these n residue digits and their corresponding moduli , in line with the projection theory of [3].

To extend this for correction of more than one residue digit error, the idea could be extended as follows. Given an RRNS (n, k)code with $t\ (= \lfloor \frac{n-k}{2} \rfloor)$error correcting capability, if we select β $(= n - k)$error positions as projection depth such that most of the possible combinations are taken care of, a total of $h = \beta_{C_t}$ combinations of t errors are covered in a single iterationin each modulus projection operation.
This idea is better explain with the aid of numerical illustrations. Consider cases of the following RRNS (n, k) codes: (8, 4) code; (9, 5) code; (9, 3) code; (10, 4) code; (11, 3) code; (12, 4) code and (12, 3) code. The first two codes has error correcting capability of two i.e. t=2 and β=4. The next two has capacity of correcting three residue errors, t=3 and β= 6 while the last three can correct four residue digit errors with t=4 and β=8; 8and 9 respectively.

Possible error positions selections using respective projection depth β are:
RRNS (8, 4) code: (1, 2, 3, 4); (3, 4, 5, 6); (5, 6, 7, 8); (7, 8, 1, 2) i.e. 4 possibilities
RRNS (9, 4) code: (1, 2, 3, 4, 5); (3, 4, 5, 6, 7); (5, 6, 7, 8, 9); (7, 8, 9, 1, 2); (9, 1, 2, 3, 4); (2, 3, 4, 5, 6); (4, 5, 6, 7, 8); (6, 7, 8, 9, 1); (8, 9, 1, 2, 3) i.e. 9 possibilities

RRNS (9, 3) code: (1, 2, 3, 4, 5, 6); (4, 5, 6, 7, 8, 9); (7, 8, 9, 1, 2, 3) i.e. 3 possibilities
RRNS (10, 4) code: (1, 2, 3, 4, 5, 6); (4, 5, 6, 7, 8, 9); (7, 8, 9, 10, 1, 2); (10, 1, 2, 3, 4, 5); (3, 4, 5, 6, 7, 8); (6, 7, 8, 9, 10, 1); (9, 10, 1, 2, 3, 4); (2, 3, 4, 5, 6, 7); (5, 6, 7, 8, 9, 10); (8, 9, 10, 1, 2, 3) i.e. 10 possibilities
RRNS (11, 3) code: (1, 2, 3, 4, 5, 6, 7, 8); (5, 6, 7, 8, 9, 10, 11, 1); (9, 10, 11, 1, 2, 3, 4, 5); (2, 3, 4, 5, 6, 7, 8, 9); (6, 7, 8, 9, 10, 11, 1, 2); (10, 11, 1, 2, 3, 4, 5, 6); (3, 4, 5, 6, 7, 8, 9, 10); (7, 8, 9, 10, 11, 1, 2, 3); (11, 1, 2, 3, 4, 5, 6, 7); (4, 5, 6, 7, 8, 9, 10, 11); (8, 9, 10, 11, 1, 2, 3, 4) i.e. 11 possibilities
RRNS (12, 3) code: (1, 2, 3, 4, 5, 6, 7, 8, 9); (5, 6, 7, 8, 9, 10, 11, 12, 1); (9, 10, 11, 12, 1, 2, 3, 4, 5) i.e. 3 possibilities
RRNS (12, 4) code: (1, 2, 3, 4, 5, 6, 7, 8); (5, 6, 7, 8, 9, 10, 11, 12); (9, 10, 11, 12, 1, 2, 3, 4) i.e. 3 possibilities.

From the foregoing, the followings can be deduced;

a. Selection of possible error positions are guided by the error detecting capacity of the code. For instance, RRNS (10, 5) code has error detecting capacity of 5; therefore each selection is made of five residue digits;
b. Variation of a possible error position selection from other is guided by the error correcting capability of RRNS code. For instance, two possible selections in RRNS (7, 3) code are (1, 2, 3, 4) and (3, 4, 5, 6), the two differs in terms of residue digit positions by the error detecting capability of the code; which in this case equal 2;
c. The maximum number of selection for possible combinations of error positions using this approach is generally less or equal to the code length n.

Hence, the maximum number of iterations that is required to recover the original integer using this method is estimated as given in equation (15),

$$h(\mathbf{max}) = n \qquad (15)$$

Invocation of modulus projection using the projection depth as explain above will result in more than one possible solutions falling within the legitimate range. This is due to the fact that the algorithm attempt correction of residue digits error greater than the code capability. To resolve this ambiguity maximum likelihood decoding (MLD) approach is employed. Let the set of solutionsthat fall within the legitimate range obtained from a scheme set to correct β >t residue digits error in an RRNS(n, k)code be given by,

$$\boldsymbol{R} = \{R_1, R_2, R_3, \dots, R_{l+1}, \dots, R_\theta\} \qquad (16)$$

With θbeing the number of solution that falls within the legitimate range of the RNS. For each of R_l , $i = 1, 2 \dots \theta$, the corresponding residue vector r_i is obtained using equation (4). Applying MLD, the Hamming distances $d(\mathrm{y}, r_l)$, between the received residue vector y and each of the computed residue vector r_l are evaluated. Anyone that has Hamming distance less than or equal to t (the error correcting capability of the code), the corresponding integer R_i is the transmitted integer.

The proposed algorithm for decoding RRNS(n, k)code can then be described thus,
Step 1: obtain the received residue vector y and the corresponding $moduli\ m_i$
Step 2: Compute the mixed radix digits based on y and m_i. Check if all the redundant mixed radix digits are zero. If yes, declarethe received vector as error free.Compute Y = Xand stop. Otherwise, proceed to step 3.
Step 3: Determine the projection depth$\beta = n - k$, perform moduli projection of depth β on the received residue y to get reduced residue $\overline{y_c}$for c = 1 to h (the number of possible selections)
Step 4: While $c \leq h$,compute estimate $\overline{Y_c}$of the integer from $\overline{y_c}$ for each selection using matrix method. If $\overline{Y_c}$ is in the legitimate range, set $\overline{Y_c} = R_l$ and proceed to Step 5. Otherwise, increase c by 1
Step 5: Calculate the residue vector r_l from R_l and the Hamming distance $d(y, r_l)$.
Step 6: Output $X = R_l : d(y, r_l) \leq t$

4. RESULT AND DISCUSSION

Using RRNS (7, 3) code, the chosen moduli set are $\{3, 5, 7, 8, 11, 13, 17\}$, the legitimate range of the code is [0, 105) and the illegitimate range is [105, 2042040). This code has error correcting capability $t\ \left(= \lfloor \frac{n-k}{2} \rfloor\right) =$ 2Suppose the transmitted integer message X= 89, $x \equiv$ (2, 4, 5, 1, 1, 11, 4) when coded into residue vector using equation (4). Also, suppose the received vector has two errors introduced in the course of transmission at positions $u_1 = 3$ and $u_2 = 4$. Let the received vector be $y \equiv (2, 4, 6, 7, 1, 11, 4)$. Four error positions are selected in line with the

algorithm as the projection depth$\beta = 4$. The values of redundant mixed radix digits obtained using equation (9) are a_4 =7, a_5 =5, a_6 =12 and $a_7 = 13$, which are all non-zero. Thus, it can be said that there are errors in the received residue vector. Table 1 gives the result obtained when moduli projection of depth 4 was carried out on the received residue as stated in the algorithm.From Table 1, it can be seen that there are three possible solutions that fall within the legitimate range (one in duplicates). Let them be $R = (89, 91, 104)$. In line with the algorithm, the residue vectors r_l and Hamming distances are calculated. The result is presented in Table 2.As can be seen in Table 2, the only value of r_l that has a Hamming distance which is less than or equal to $t = 2$ is 89. Therefore, the algorithm has correctly recovered the transmitted integer.

Table 1: Result of Double Residue Digits Error Correction using the Proposed Algorithm

h	Error Position selections				Reduced Received Residue after Projection $\overline{y_c}$	Corresponding Moduli of Reduced Received Residue	$\overline{Y_c}$
	u_1	u_2	u_3	u_4			
1	1	2	3	4	1, 11, 4	11, 13, 17	91
2	3	4	5	6	2, 4, 4	3, 5, 17	89
3	5	6	7	1	4, 6, 7	5, 7, 8	249
4	7	1	2	3	7, 1, 11	8, 11, 13	375
5	2	3	4	5	2, 11, 4	3, 13, 17	89
6	4	5	6	7	2, 4, 6	3, 5, 7	104
7	6	7	1	2	6, 7, 1	7, 8, 11	111

Table 2: The residue vectors and Hamming distances for two Residues digits error correction

i	R	r_i	y	d (r_i ,y)
1	89	2, 4, 5,1,1, 11,4	2, 4, 6, 7, 1, 11, 4	2
2	91	1, 1, 0, 3, 3, 0, 6	2, 4, 6, 7, 1, 11, 4	7
3	104	2, 4, 6, 0, 5, 0, 2	2, 4, 6, 7, 1, 11, 4	4

5. CONCLUSION

The need to have faster and efficient decoding algorithm for RRNS code cannot be ignored going by its wider applications in the field of signal processing. This paper has been able to exploit the properties of modulus projection to develop a streamlined procedure for RRNS codes decoding. The algorithm is suitable for an arbitrary number of residue digit errors corrections, as long as the number of errors is within the error-correction capability of the RRNS code in question. All that is required is that the number of moduli-projection employed must be equal to the number of redundant moduli the RRNS code has. When compared with previous works on decoding of RRNS codes, the proposed algorithm here seem better in terms of a number of features inherent in decoding of RRNS code. This is summarized in Table 3 below.

Table 3: Comparison of various Algorithms for Multiple Residue Digits Errors Correction

Features of RRNS code	Jenkins's Algorithm [5]	Krishna et. al Algorithm [8]	Goh & Siddiqi Algorithm [10]	Proposed Algorithm
Multiple error correction	Applicable	Applicable	Applicable	Applicable
Integer recovery method	Continued fraction operation	Iterations with BEX operation	Iterations with CRT operation	Matrix method
Memory requirement	Small as CRT is not used	Small as CRT is not used	Large as CRT is involved	Small as CRT is not involved
Number of trials for recovery of integer	n_{C_t}	n_{C_t}	$\lceil n_{C_t} / (n-\mathrm{t})_{C_t} \rceil$	n_{max}

Where * is the largest integer greater than or equal to *, n is the RRNS code length, k is the number of non-redundant residue digits and t is the error correcting capability of the code.

5. REFERENCES

[1]. [1]L.-L. Yang and L. Hanzo (2001), "RRNS Based Error Correction Codes", Proc. 54th Vehicle Technol. Conf., 2001, pp. 1472-1476

[2]. R.W. Watson and C.W. Hastings (1966)," Self-checkedComputations using Residue Arithmetic": Proc. Of IEEE Vol.54,No.12, pp.1920-1931

[3]. F. Barsi and P. Maestrini (1973) "Error Correcting Properties ofRRNS": IEEE Trans. Computer, pp.307-315

[4]. W. K. Jenkins (1983), "The Design of error checkers for self-checking Residue Number Arithmetic": IEEE Trans. Computer, pp.388-396

[5]. W.K. Jenkins and E.J. Altman (1988), "Self-checking properties ofResidue Number Error Checkers Based on Mixed Radix Conversion": IEEE Trans. Circuits Syst., pp.159-167

[6]. K.A Gbolagade and S.D Cotofana (2008), "Generalized Matrix method for efficient Residue to Decimal Conversion IEEE Trans. Computer, pp. 1414 – 1417

[7]. H. Krishna, K.Y. Lin and J.D. Sun (1992), "A Coding Theory Approach to Error Control in RRNS-part 1:-Theory and single error- Correction": IEEE Trans. Circuits and Syst. II Analog & DSP, Vol. 39, pp.8-17

[8]. H. Krishna and J.D. Sun (1992), "A Coding Theory Approach toError Control in RRNS-part II: Multiple errors Detection and Correction": IEEE Trans. Circuits and Syst. II Analog and DSP, Vol. 39, pp.18-34

[9]. H. Krishna and J.D. Sun (1993), "On Theory and Fast Algorithms forError Correction in RRNS Product Codes": IEEE Trans. Computer, Vol.42, No.7, pp.840-853

[10]. V.T. Goh and M.U. Siddiqi (2008), "Multiple Error Detection andCorrection Based on RRNS": IEEE Trans. on Communications Vol.56, No.3, pp.325-330

[11]. D.M. Mandelbaum (1976), "On a class of Arithmetic Codes and aDecoding Algorithm": IEEE Trans. Inform. Theory, Vol. 22, pp.85-88

[12]. O. Goldreich, D. Ron and M. Sudan(2000)," Chinese Remaindering With Errors", IEEE Trans. Infor. Theory, Vol. 46, pp.1330-1338

[13]. R. E. Blahut (1984), Fast Algorithms for Digital Signal Processing:Reading, M.A, Addison-Wesley

[14]. L.-L. Yang and L. Hanzo (1999),"Coding Theory and Performanceof RRNS Codes": Submitted to IEEE Trans. on Information Theory,http://www-mobile.ecs.soton.ac.uk/

[15]. E. D. D. Claudio and F. Piazza (1983), "A systolic redundant Residue error correction Circuit": IEEE Trans. Computer, Vol. 42, No. 4, pp.427-432

[16]. S.S-Yau and Y.-C. Liu (1973), "Error Correction in RRNS": IEEE Trans. Computer, Vol. C-22, pp.5-11

[17]. D. M. Mandelbaum (1972), "Error–correction in ResidueArithmetic", IEEE Trans. Computer, Vol.21, No.6, pp.538-545

[18]. H.M. Yassine (1999), "Fast Arithmetic Based on RNS Architectures": IEEE ISCAS '99, pp. 2947-2950, Singapore

[19]. M.H. Etzel and W.K. Jenkins (1980), "RNS for Error Detection and Correction in Digital Filters": IEEE Trans. Acoustic Speech Signal Processing, pp.538-544