MINIMUM-DISTANCE DECODING OF REDUNDANT RESIDUE NUMBER SYSTEM CODES

Lie-Liang Yang and Lajos Hanzo

Dept. of ECS, University of Southampton, SO17 1BJ, UK.
Tel: +44-703-593 125, Fax: +44-703-594 508
Email: lly@ecs.soton.ac.uk, lh@ecs.soton.ac.uk
, http://www-mobile.ecs.soton.ac.uk

ABSTRACT

In this contribution the conventional error-detection and error-correction algorithms used for RRNS codes are improved and unified in the context of a so-called projection-based 'minimum-distance decoding' algorithm, which can efficiently detect or correct multiple residue digit errors.

1. INTRODUCTION

The so-called residue number system (RNS) and redundant residue number system (RRNS) have drawn wide attention in high-speed parallel signal processing structures, and the RRNS has also been widely employed for self-checking, error-detection and error-correction in digital processors, arithmetic units and data transmission [1–12]. The concepts of error-correction in conjunction with RRNS codes were developed by Mandelbaum [2]. Barsi and Maestrini addressed the problems of single residue digit error correction in [3]. Krishna, Lin and Sun have discussed the correction of single or double residue digit errors, and simultaneously the detection of multiple residue digit errors in [4,5]. In this paper, we build on the contributions of [2–5], augmenting the error-correction techniques of RRNS codes and unifying them in the context of the 'minimum-distance decoding' algorithm, which can efficiently detect or correct multiple residue digit errors.

2. RESIDUE NUMBER SYSTEM AND REDUNDANT RESIDUE NUMBER SYSTEM CODES

A RNS is defined by the choice of k positive integers m_i, $(i = 1, 2, \ldots, k)$ referred to as moduli [1]. If *all the moduli are pairwise relative primes*, any integer X in the range $[0,\ M)$ - where $M = \prod_{i=1}^{k} m_i$ - can be uniquely and unambiguously represented by the so-called residue sequence:

$$X \Leftrightarrow (x_1, x_2, \ldots, x_k), \tag{1}$$

where $x_i = (X)_{m_i},\ i = 1, 2, \ldots, k$ represents the residue digits of X upon division by m_i for $i = 1, 2, \ldots, k$, while $[0,\ M)$ is the *information dynamic range*, i.e. the legitimate range of X. Given a residue sequence $(x_1, x_2, \ldots, x_k)$, the corresponding integer X in the range $[0,\ M)$ can be uniquely recovered from the k residue digits seen in Eq.(1) by the so-called *Chinese reminder theorem* (CRT) [4]. Specifically, according to the CRT, for any given k-tuple $(x_1, x_2, \ldots, x_k)$ - where $0 \leq x_i < m_i,\ i = 1, 2, \ldots, k$ - it can be shown that the numerical value of X can be found from the residue digits using [4]:

$$X = \left(\sum_{i=1}^{k} x_i T_i M_i \right)_M, \tag{2}$$

where $M_i = M/m_i$ and the integers T_i - which constitute the multiplicative inverses of M_i - are computed a *priori* by solving the so-called congruences of $T_i M_i = (\ 1\ )_{m_i}$.

In the context of error control - both error-correction and error-detection - we are concerned with RRNS [1, 4, 5]. An RRNS is obtained by appending an additional $r = (n - k)$ number of redundant moduli $m_{k+1},\ m_{k+2},\ \ldots,\ m_n$, to the previously introduced RNS, in order to form an RRNS code of n positive, pairwise relative prime moduli. Now an integer X in the range $[0,\ M)$ is represented as an n-tuple residue sequence with respect to the n moduli $(m_1, m_2, \ldots, m_n)$, expressed as:

$$X \Leftrightarrow (x_1, x_2, \ldots, x_n), \tag{3}$$

which represents an RRNS(n, k) codeword or RRNS(n, k) code vector. The moduli $m_1, m_2, \ldots, m_k$ are termed as the nonredundant moduli, while the additional r moduli m_{k+1}, $m_{k+2}, \ldots, m_n$ are the redundant moduli. Correspondingly, the residue digits $x_1, x_2, \ldots, x_k$ in Eq.(3) are the nonredundant residue digits, while $x_{k+1}, x_{k+2}, \ldots, x_n$ are the redundant residue digits. The total range $[0,\ MM_R)$ - where $M_R = \prod_{i=1}^{r} m_{k+i}$ - is the range of values that can be represented by the RRNS code. This total 'dynamic' range can be divided into the ranges defined by the nonredundant and redundant moduli. The interval $[0,\ M)$ is the legitimate range, while the interval $[M,\ MM_R)$ is the illegitimate range. By definition, any number belonging to the legitimate range will be labelled as legitimate and those belonging to the illegitimate range as illegitimate, since the latter does not represent a number or operand, directly accruing from the nonredundant information-bearing residue digits.

The necessary and sufficient conditions for a RRNS(n, k) code to achieve the maximum minimum-distance of $d =$

This work has been funded in the framework of the IST project IST-1999-12070 TRUST, which is partly funded by the European Union. The authors would like to acknowledge the contributions of their colleagues.

$n-k+1$ have been given in [10], which can be stated as follows.

Theorem 1 *Let $m_1, m_2, \ldots, m_k, m_{k+1}, \ldots, m_n$ be a group of moduli constituting the RRNS(n,k) code and $[0, M)$ - where $M = \prod_{i=1}^{k} m_i$ - be the legitimate range. Then the necessary and sufficient condition for the RRNS(n,k) code to achieve the maximum possible minimum-distance of $d = n-k+1$ is that any of the redundant moduli is larger than the largest nonredundant modulus, which is formulated as:*

$$m_{k+j} > \max\{m_1, m_2, \ldots, m_k\} \tag{4}$$

for $j = 1, 2, \ldots, n-k$.

According to Theorem 1, the RRNS(n,k) codes constitute a class of codes achieving the maximum possible minimum-distance of $d = n-k+1$, provided that the condition of Eq.(4) is satisfied. Hence, in the remainder of this paper all RRNS(n,k) codes discussed are assumed to satisfy the condition of Eq.(4), and consequently their minimum distance is $d = n-k+1$. Furthermore, we assume that the n number of moduli of the RRNS(n,k) code satisfy the relationship:

$$m_1 < m_2 < \ldots < m_k < m_{k+1} < \ldots < m_n. \tag{5}$$

3. THEORY OF PROJECTION-BASED MINIMUM-DISTANCE DECODING IN RRNS

Barsi and Maestrini [3] described a method for error detection in RRNS codes based on determining, whether a given received integer, $X \Leftrightarrow \boldsymbol{x} = (x_1, x_2, \ldots, x_k, x_{k+1} \ldots, x_n)$, $n > k$, falls within the legitimate range $[0,\ M)$ or in the illegitimate range $[M,\ MM_R)$. It was shown [3] that any single residue digit error inflicted upon a legitimate integer message X, will map to the illegitimate range of the RRNS. Barsi and Maestrini also developed a method for locating and correcting a single residue digit error for RRNS codes satisfying the condition of $n \geq k+2$ based upon the values of so-called projections computed for the RRNS(n,k) code concerned. The so-called modulus m_i-projection of X in the context of an RRNS(n,k) code is defined as [3]:

$$X_i \equiv \left(X \right)_{\frac{MM_R}{m_i}}, \tag{6}$$

i.e., the m_i-projection, X_i, can be interpreted as $X_i \Leftrightarrow \boldsymbol{x_i} = (x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$, which is the residue representation of X in a reduced RRNS with the ith residue digit x_i deleted. This m_i-projection results in the reduced RRNS$(n-1,k)$ code, where the modulus m_i is deleted from the RRNS(n,k) code. Since the RRNS is a data representation system with at least one residue digit of redundancy, the original information is retained, when the redundancy is removed.

Correspondingly, the $M_\wedge$-projection of X, denoted by $X_\wedge$, is defined by [5]:

$$X_\wedge \equiv \left(X \right)_{\frac{MM_R}{M_\wedge}}, \tag{7}$$

where $M_\wedge = \prod_{m=1}^{\lambda} m_{i_m}$, $\wedge = \{i_1, i_2, \ldots, i_\lambda\}$, and $\lambda \leq n-k$. In other words, $X_\wedge$ can also be represented as a reduced residue representation of X with the residue digits $x_{i_1}, x_{i_2}, \ldots, x_{i_\lambda}$ deleted. Hence, X can be represented by a reduced RRNS$(n-\lambda, k)$ code with the moduli $m_{i_1}, m_{i_2}, \ldots, m_{i_\lambda}$ deleted from the RRNS(n,k) code. The legitimate and illegitimate range of the reduced RRNS code are $[0,\ M')$ and $[M',\ MM_R/M_\wedge)$, respectively, where M' is the product of the first k moduli of the reduced RRNS. It follows from Eq.(7) that the $M_\wedge$-projection of any legitimate integer X of the RRNS is still a legitimate integer in $[0,\ M)$, i.e., $X_\wedge = X$, provided that a sufficiently high dynamic range is retained in the reduced RRNS, in order to unambiguously represent X.

The so-called minimum-distance decoding algorithms attempt to find a codevector $\boldsymbol{x}$ in the legitimate range, so that the received vector $\boldsymbol{y}$ lies within its error-correction decoding sphere constituted by those vectors, which are decoded to $\boldsymbol{x}$. Otherwise, if such a legitimate codevector $\boldsymbol{x}$ cannot be found, the decoder declares an uncorrectable error. A conceptually straightforward but impractical method of minimum-distance decoding is to compare the received vector $\boldsymbol{y}$ with every possible codevector of the RRNS(n,k) code. If the received vector $\boldsymbol{y}$ lies within a codevector's error-correction decoding sphere, the received vector is decoded to $\boldsymbol{x}$. Otherwise, if the received vector $\boldsymbol{y}$ does not lie within a legitimate codevector's error-correction decoding sphere, then an uncorrectable error is detected. In order to derive the associated minimum-distance decoding algorithm, a range of theorems concerning the decoding of RRNS codes are formulated below. Theorems 2 and 3 have been given in [5], therefore their proof is omitted here.

Theorem 2 *If X is a legitimate integer in the RRNS(n,k) code having a minimum distance of $d = n-k+1$, then any integer $\overline{X}$ differing from X in at least one but no more than $(d-1)$ residue digits is an illegitimate integer.*

Based on the above theorem it can be determined for the RRNS(n,k) code having a minimum distance of $d = n-k+1$ as to whether the received vector is correct or not - by checking whether the value of the received vector is in the legitimate range - provided that no more than $(n-k)$ residue digit errors were encountered. In other words, the RRNS(n,k) code can detect up to any $(n-k)$ residue digit errors by detecting the received vector's value.

Theorem 3 *[5] Let $\overline{X}$ be an illegitimate integer message in the RRNS(n,k) code. If there exists a legitimate integer message X differing from $\overline{X}$ in the i_1th, i_2th, ..., i_λth residue digits, where $\lambda \leq (n-k)$, then the $M_\wedge$-projection $\overline{X}_\wedge$ is a legitimate number, where $M_\wedge = \prod_{m=1}^{\lambda} m_{i_m}$.*

This theorem 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 integers constituting the message. This theorem also implies that an RRNS(n,k) code can be reduced to an RRNS$(n-\mu, k)$ code, where $\mu \leq n-k$, after μ number of residue digits and their related moduli are dropped. According to Theorem 1, the reduced RRNS$(n-\mu, k)$ code has a minimum distance of $d = n-k-\mu+1$ and hence - based on the associated

minimum-distance decoding algorithm such as that of Section 4 - can detect up to $(n-k-\mu)$ residue digit errors, and correct up to $\lfloor \frac{n-k-\mu}{2} \rfloor$ residue digit errors, respectively. Since the processing of each residue digit in the RRNS is independent of that of all the other residue digits, the dropped residue digits do not have to be considered in the reduced RRNS$(n-\mu,k)$ decoding. This property renders the RRNS(n,k) codes attractive for 'errors-and-erasures' decoding [8, 9].

The proof of the following Lemma has been given in [3], and therefore it is omitted here.

Lemma 1 *[3] Let X be an integer in the RRNS and $X_\wedge$ be the $M_\wedge$-projection of X, where $M_\wedge = \prod_{m=1}^{\lambda} m_{i_m}$. If $X_\wedge \neq X$, the residue representation of $X_\wedge$ in the RRNS uniquely differs from that of X in one or more of the residue digits corresponding to the moduli $m_{i_1}, m_{i_2}, \ldots, m_{i_\lambda}$.*

Theorem 4 *Assume that $\overline{X}$ is an illegitimate number in the RRNS(n,k) code exhibiting a minimum distance of $d = n-k+1$ amongst legitimate codewords. If there exists an $M_\wedge$-projection $\overline{X}_\wedge$ - where $M_\wedge = \prod_{m=1}^{\lambda} m_{i_m}$ and $1 \leq \lambda \leq \lfloor \frac{n-k}{2} \rfloor$ - which is a legitimate integer, then $\overline{X}_\wedge$ is the only legitimate integer in the RRNS(n,k) code.*

Proof: Since the legitimate integer $\overline{X}_\wedge$ is the $M_\wedge$-projection of $\overline{X}$, according to Lemma 1, the residue representation of $\overline{X}_\wedge$ uniquely differs from that of $\overline{X}$ in one or more residue digits corresponding to the moduli $m_{i_1}, m_{i_2}, \ldots, m_{i_\lambda}$. Since we have assumed that $1 \leq \lambda \leq \lfloor \frac{n-k}{2} \rfloor$, we have $d(\overline{\boldsymbol{x}}, \boldsymbol{x}_\wedge) \leq \lfloor \frac{n-k}{2} \rfloor$, where $\overline{\boldsymbol{x}}$ and $\boldsymbol{x}_\wedge$ denote the residue representations of $\overline{X}$ and $\overline{X}_\wedge$ in the RRNS(n,k) code, respectively. Since $\overline{X}_\wedge$ is a legitimate integer, $\boldsymbol{x}_\wedge$ represents a codevector of the RRNS(n,k) code.

Let us assume furthermore that there exists another $M_{\wedge'}$-projection $\overline{X}_{\wedge'} \neq \overline{X}_\wedge$, which is also a legitimate integer in the RRNS(n,k) code, where $M_{\wedge'} = \prod_{l=1}^{\beta} m_{i_l}$ and $1 \leq \beta \leq \lfloor \frac{n-k}{2} \rfloor$. Then, according to Lemma 1, we have $d(\overline{\boldsymbol{x}}, \boldsymbol{x}_{\wedge'}) \leq \lfloor \frac{n-k}{2} \rfloor$, where $\boldsymbol{x}_{\wedge'}$ denotes the residue representation of the integer $\overline{X}_{\wedge'}$ and it is a codevector of the RRNS(n,k) code corresponding to the legitimate integer $\overline{X}_{\wedge'}$. Then, according to the triangular inequality of:

$$d(\boldsymbol{x}_\wedge, \boldsymbol{x}_{\wedge'}) \leq d(\overline{\boldsymbol{x}}, \boldsymbol{x}_\wedge) + d(\overline{\boldsymbol{x}}, \boldsymbol{x}_{\wedge'}),$$

we have

$$d(\boldsymbol{x}_\wedge, \boldsymbol{x}_{\wedge'}) \leq \lfloor \frac{n-k}{2} \rfloor + \lfloor \frac{n-k}{2} \rfloor \leq n-k,$$

which means that two codevectors in the RRNS(n,k) code have a distance of less than $(n-k+1)$. This contradicts the condition of having a minimum distance of $d = n-k+1$. Hence, if there exists an $M_\wedge$-projection $\overline{X}_\wedge$ - where $M_\wedge = \prod_{m=1}^{\lambda} m_{i_m}$ and $1 \leq \lambda \leq \lfloor \frac{n-k}{2} \rfloor$ - which is a legitimate integer, then this $\overline{X}_\wedge$ is the only legitimate integer in the RRNS(n,k) code. This proves Theorem 4.

Theorem 5 *Let $\overline{X}$ be an illegitimate integer in the RRNS (n,k) code exhibiting a minimum distance of $d = n-k+1$ amongst legitimate codewords. If this received vector includes no more than $\lfloor \frac{n-k}{2} \rfloor$ residue digit errors in its residue representation $\overline{X} \Leftrightarrow \overline{\boldsymbol{x}}$, then there exists one and only one legitimate number, $\overline{X}_\wedge$, which is derived by the $M_\wedge$-projection, where $M_\wedge = \prod_{m=1}^{\lambda} m_{i_m}$ and $1 \leq \lambda \leq \lfloor \frac{n-k}{2} \rfloor$.*

Proof: Let $1 \leq \lambda \leq \lfloor \frac{n-k}{2} \rfloor$ be the number of erroneous residue digits in the residue representation $\overline{X} \Leftrightarrow \overline{\boldsymbol{x}}$. Furthermore, let the i_1th, i_2th, ..., i_λth residue digits be the erroneous ones. Then - according to Theorem 3 - the $M_\wedge$-projection $\overline{X}_\wedge$ is a legitimate number. Since $1 \leq \lambda \leq \lfloor \frac{n-k}{2} \rfloor$, therefore according to Theorem 4 $\overline{X}_\wedge$ is the only legitimate number. This proves the theorem.

Theorems 4 and 5 suggest that in an RRNS coded communication system, the received vectors can be decoded using the projection techniques proposed in [3]. Theorems 4 and 5 guarantee that the RRNS(n,k) code can correct up to $\lfloor \frac{n-k}{2} \rfloor$ number of residue digit errors and that the decoded codevector is the one that has the minimum distance from the received vector. Hence this decoding scheme is a minimum-distance decoding scheme.

4. PROJECTION-BASED MINIMUM-DISTANCE DECODING ALGORITHM

The first step of the error-correction in RRNS codes (and the only step in the error-detection procedure) is to check, whether the received residue vector $\boldsymbol{y}$ is a legitimate codevector in the RRNS. A simple technique of accomplishing this is to compute the corresponding integer Y and check, whether $0 \leq Y < M$. If $0 \leq Y < M$, then $\boldsymbol{y}$ is a codevector. Otherwise, if $M \leq Y < MM_R$, then the received residue vector $\boldsymbol{y}$ included at least one residue digit error. However, this 'range-checking' approach may require processing large-valued integers. A suitable method of avoiding this is invoking the so-called base-extension (BEX) [11] method using the mixed radix conversion (MRC) [7]. The MRC is an operation used to represent an integer $Y \Leftrightarrow \boldsymbol{y}$ in the form of [11]:

$$Y = a_1 + a_2 m_1 + a_3 m_1 m_2 + \cdots + a_n \prod_{i=1}^{n-1} m_i, \qquad (8)$$

where $0 \leq a_l < m_l$, $l = 1, 2, \ldots, n$, and we define $\prod_{i=1}^{0} m_i = 1$. For a given residue digit sequence $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ the mixed radix digits $a_1, a_2, \ldots, a_n$ are computed from the residue digits $y_1, y_2, \ldots, y_n$ as follows [11]:

$$\begin{aligned} a_1 &= y_1, \\ a_2 &= \left((y_2 - a_1) m_1^{-1} \right)_{m_2}, \\ &\cdots \\ a_n &= \Big(\big((\cdots ((y_n - a_1) m_1^{-1} - a_2) m_2^{-1} \\ &\quad - \cdots) - a_{n-1} \big) m_{(n-1)}^{-1} \Big)_{m_n}. \end{aligned} \qquad (9)$$

In an RRNS, the digits $a_1, a_2, \ldots, a_k$ are referred to as the nonredundant mixed radix digits, and $a_{k+1}, a_{k+2}, \ldots, a_n$ are termed as the redundant mixed radix digits. It can be shown that if $0 \leq Y < M$, then all the redundant mixed radix digits will be zeros [11].

Furthermore, the integer message Y corresponding to a received residue vector $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ can be computed from any k out of the n residue digits and their related moduli, according to the projection theory of [3]. This concept is augmented below.

Let $y_{i_1}, y_{i_2}, \ldots, y_{i_k}$ be k out of n residue digits from $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$, where - without loss of generality -

we assume that $i_1 < i_2 < \ldots < i_k$. Then, the integer Y can be computed from these k residue digits and their related moduli according to Eq.(8) and Eq.(9), which can be expressed with the aid of the MRC as:

$$Y = a_{i_1} + a_{i_2} m_{i_1} + a_{i_3} m_{i_1} m_{i_2} + \cdots + a_{i_k} \prod_{l=1}^{k-1} m_{i_l}. \quad (10)$$

Based on Y computed according to Eq.(10), the remaining $(n-k)$ residue digits can be recomputed using the approach proposed in [7], which is expressed as:

$$y'_j \equiv \Big(Y \Big)_{m_j} \equiv (\ldots(((a_{i_1})_{m_j} + (a_{i_2} m_{i_1})_{m_j})_{m_j} + (a_{i_3} m_{i_1} m_{i_2})_{m_j})_{m_j} + \cdots + (a_{i_k} \prod_{l=1}^{k-1} m_{i_l})_{m_j}))_{m_j} \quad (11)$$

for all $j = 1, 2, \ldots, n;\ j \notin \{i_1, i_2, \ldots, i_k\}$. The process summarized in Eq.(10) and (11) is the above-mentioned BEX. It can be shown - in contrast to the above-mentioned range-checking technique - that according to this approach no large-valued integers have to be processed. The difference between the residue digits y'_j, which were computed by the decoder according to Eq.(11) and the received residue digits y_j in $\boldsymbol{y}$ can be expressed as:

$$\Delta_j = y'_j - y_j,\ j = 1, 2, \ldots, n;\ j \notin \{i_1, i_2, \ldots, i_k\}, \quad (12)$$

where the quantities $\{\Delta_j\}$ are referred to as *syndromes* [4], and all the received residue digits of $\boldsymbol{y}$ corresponding to $\{\Delta_j,\ j = 1, 2, \ldots, n;\ j \notin \{i_1, i_2, \ldots, i_k\}\}$ are referred to as parity residue digits.

A fundamental property of the syndrome digits has been given in [12], which is re-stated in the following theorem.

Theorem 6 *[12] Under the assumption that no more than $\lfloor \frac{n-k}{2} \rfloor$ residue digit errors occur in an RRNS code having a minimum distance of $d = n - k + 1$, based on the $(n-k)$ number of syndrome digits $\Delta_{k+1}, \Delta_{k+2}, \ldots, \Delta_n$ computed from Eq.(12) the following three observations can be stated:*

Observation 1 *A received residue digit vector $\boldsymbol{y}$ is an error-free codevector if and only if all the $(n-k)$ syndrome digits are zero.*

Observation 2 *λ $(1 \leq \lambda \leq \lfloor \frac{n-k}{2} \rfloor)$ out of the $(n-k)$ parity residue digits in $\boldsymbol{y}$ are in error if and only if λ corresponding syndrome digits are non-zero.*

Observation 3 *At least one of the received information residue digits in $\boldsymbol{y}$ - which correspond to the first k residue digits of $y_1, y_2, \ldots, y_k$ - are in error if and only if more than $\lfloor \frac{n-k}{2} \rfloor$ syndrome digits are non-zero.*

Let $m_1, m_2, \ldots, m_k, m_{k+1}, \ldots, m_n$ be the moduli in an RRNS(n, k) code $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ constituting the transmitted codevector and $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ be the received vector. Then, with the aid of Theorems 2 to 5 and upon invoking the above-mentioned so-called consistency checking method of Theorem 6, the proposed minimum-distance decoding algorithm can be outlined as follows.

Minimum-distance RRNS Decoding Algorithm:

Table 1: Integer messages and their corresponding codevectors for a RRNS(4,2) code using moduli 3, 5, 7, 8.

message value	x_1	x_2	x_3	x_4
0	0	0	0	0
1	1	1	1	1
2	2	2	2	2
3	0	3	3	3
4	1	4	4	4
5	2	0	5	5
6	0	1	6	6
7	1	2	0	7
8	2	3	1	0
9	0	4	2	1
10	1	0	3	2
11	2	1	4	3
12	0	2	5	4
13	1	3	6	5
14	2	4	0	6

Step 1: Compute the syndromes Δ_{k+1}, Δ_{k+2}, $\ldots$, Δ_n from the received nonredundant residue digits $(y_1, y_2, \ldots, y_k)$ according to Eq.(12). Let the MRC of $(y_1, y_2, \ldots, y_k)$ be expressed as an $M_\wedge$-projection with $M_\wedge = 1$. If there are no more than $\lfloor \frac{n-k}{2} \rfloor$ syndromes that are non-zero, then proceed to Step 5. Otherwise, continue with Step 2.

Step 2: Compute the $M_\wedge$-projections and their corresponding syndromes Δ_{i_1}, Δ_{k+2}, Δ_{k+3}, $\ldots$, Δ_n according to Eq.(12) for the parity digits from the residue digits $(y_1, y_2, \ldots, y_{k+1})$, where $M_\wedge = m_{i_1}$, $i_1 = 1, 2, \ldots, k$. If there exists a legitimate $M_\wedge$-projection, which results in no more than $\lfloor \frac{n-k}{2} \rfloor$ corresponding non-zero syndromes, then go to Step 5. Otherwise proceed to Step 3.

Step 3: Compute the $M_\wedge$-projections and their corresponding syndromes Δ_{i_1},Δ_{i_2},Δ_{k+3},Δ_{k+4}, $\ldots$,Δ_n according to Eq.(12) for the parity digits from the residue digits $(y_1,\ y_2,\ \ldots,\ y_{k+2})$, where $M_\wedge = m_{i_1} m_{i_2}$, $(i_1,\ i_2 = 1,\ 2,\ \ldots,\ k+1,$ and $i_1 \neq i_2)$. If there exists a legitimate $M_\wedge$-projection, which results in no more than $\lfloor \frac{n-k}{2} \rfloor$ corresponding non-zero syndromes, then go to Step 5. Otherwise compute the $M_\wedge$-projections and their corresponding syndromes from the extended residue digits $(y_1, y_2, \ldots, y_{k+i})$, $i > 2$, and the above process is repeated, until the condition $i = t = \lfloor \frac{n-k}{2} \rfloor$ is met, in which case proceed to *Step 4*.

Step 4: Compute the $M_\wedge$-projections and their corresponding syndromes Δ_{i_1},$\ldots$,Δ_{i_t}, Δ_{k+t+1}, Δ_{k+t+2}, $\ldots$,Δ_n according to Eq.(12) for the parity digits from the residue digits $(y_1, y_2, \ldots, y_{k+t})$, where $t = \lfloor \frac{n-k}{2} \rfloor$, $M_\wedge = \prod_{j=1}^{t} m_{i_j}$, $(i_1, i_2, \ldots, i_t = 1, 2, \ldots, k+t-1,$ and $i_1 \neq i_2 \neq \cdots \neq i_t)$. If there exists a legitimate $M_\wedge$-projection, which results in no more than $\lfloor \frac{n-k}{2} \rfloor$ corresponding non-zero syndromes, then go to the next step. Otherwise, declare that more than $\lfloor \frac{n-k}{2} \rfloor$ residue errors were detected and hence the code's error correction capability was exceeded. Stop.

Step 5: Invoke the legitimate $M_\wedge$-projection from the above steps in order to correct the erroneous residue digits corresponding to the non-zero syndromes with the aid of Eq.(11) and express the decoded result as

$\hat{\boldsymbol{x}} = (\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_n)$. Stop.

Let us now illustrate the inner-working of the above algorithm with the aid of an example.

Example 1 *Let $m_1 = 3, m_2 = 5, m_3 = 7$ and $m_4 =$*

8 *be four moduli in the RRNS(4,2) code, where moduli 3 and 5 are the nonredundant moduli. As an example, 15 codevectors and their corresponding integer message values are shown in Table 1. Let* $X = 11 \Leftrightarrow (x_1, x_2, x_3, x_4) = (2, 1, 4, 3)$ *be the transmitted codeword. Then the possible decoding cases can be summarised as follows.*

Case 1 **(no residue digit errors)***: Let the received vector be* $(y_1, y_2, y_3, y_4) = (2, 1, 4, 3)$*, which includes no erroneous residue digits. It can be shown that the received integer message corresponding to* $(y_1, y_2) = (2, 1)$ *is* $Y = 11$ *according to Table 1*[1] *and that according to Eq.(11) and Eq.(12) we have syndromes of* $\Delta_3 = (y_3' - y_3) = (\ Y\ )_{m_3} - y_3 = (\ 11\ )_7 - 4 = 0$ *and* $\Delta_4 = (y_4' - y_4) = (\ Y\ )_{m_4} - y_4 = (\ 11\ )_8 - 3 = 0$ *from the first step of the decoding algorithm. Hence, we conclude that there are no residue errors in the received vector.*

Case 2 **(one error in the redundant part)***: Let the received vector be* $(y_1, y_2, y_3, y_4) = (2, 1, \overline{3}, 3)$*, where the residue digit with over-bar is in error. It can be shown that the received integer message corresponding to* $(y_1, y_2) = (2, 1)$ *is* $Y = 11$ *according to Table 1 and that we have* $\Delta_3 = (\ 11\ )_7 - 3 = 4 - 3 = 1$*, while* $\Delta_4 = (\ 11\ )_8 - 3 = 3 - 3 = 0$ *from Step 1 of the decoding algorithm. Since the number of non-zero syndromes is one, which is not higher than* $t = \lfloor \frac{n-k}{2} \rfloor = \frac{4-2}{2} = 1$*, hence we conclude that a residue error occurred for residue digit* y_3*. According to Theorem 6 the erroneous residue digit* y_3 *can be corrected with the aid of Eq.(11) to the residue value of* $\hat{x}_3 = (\ 11\ )_7 = 4$ *at Step 5 of the decoding algorithm.*

Case 3 **(one error in the nonredundant part)***: Let the received vector be* $(y_1, y_2, y_3, y_4) = (2, \overline{3}, 4, 3)$*. According to Step 1 of the decoding algorithm, the integer corresponding to* $(y_1, y_2) = (2, 3)$ *is* $Y = 8$ *in Table 1, which results in* $\Delta_3 = (\ 8\ )_7 - 4 = (\ -3\ )_7 \equiv 4$*,* $\Delta_4 = (\ 8\ )_8 - 3 = (\ -3\ )_7 \equiv 5$*. Hence, we conclude according to Theorem 6 that there may be a residue error, which occurred in the nonredundant information part and the decoding process must proceed to Step 2 of the algorithm. At Step 2, the* $M_\wedge$ *projections of* $M_\wedge = m_1$ *and* $M_\wedge = m_2$ *are computed from* (y_1, y_2, y_3)*. The* $M_\wedge = m_1$*-projection of* $(y_1, y_2, y_3) = (2, 3, 4)$ *can be expressed as* $Y_{\wedge_1} \Leftrightarrow (y_2, y_3) = (3, 4)$ *by simply omitting the residue digit corresponding to* m_1 *according to Eq.(6). It can be readily seen that* $Y_{\wedge_1} = 18$ *since* $(Y_{\wedge_1})_5 = (\ 18\ )_5 = 3$*,* $(Y_{\wedge_1})_7 = (\ 18\ )_7 = 4$*, which is in the corresponding legitimate range* $[0, 5 \cdot 7 = 35)$ *of the* m_1*-projection. However, since* $Y_{\wedge_1} = 18$ *is not in the legitimate nonredundant information range of [0,15) and since* $\Delta_1 = ((\ 18\ )_3 - 2)_3 = 1$*,* $\Delta_4 = ((\ 18\ )_8 - 3)_8 = (\ -1\ )_8 = 7$*, hence according to Step 2 of the algorithm the* m_1*-projection is not the desired one. Similarly, the* m_2*-projection of* $(y_1, y_2, y_3) = (2, 3, 4)$ *can be expressed as* $Y_{\wedge_2} \Leftrightarrow (y_1, y_3) = (2, 4)$ *according to Eq.(6). It can be shown that the* m_2*-projection* $Y_{\wedge_2} = 11$ *- since* $(\ 11\ )_3 = 2$ *and* $(\ 11\ )_7 = 4$ *- is in the legitimate nonredundant information range of [0,15) and has* $(\Delta_2 = (\ 11\ )_5 - 3)_5 = (\ -2\ )_5 \equiv 3$*,* $\Delta_4 = ((\ 11\ )_8 - 3)_8 = 0$*. Since the number of non-zero syndromes is one, which is not higher than* $t = \lfloor \frac{n-k}{2} \rfloor = \frac{4-2}{2} = 1$*, consequently, according to Step 2 of the algorithm we conclude that a residue error occurred for residue digit* y_2*, which can be corrected to* $\hat{x}_2 = (Y_{\wedge_2})_5 = (\ 11\ )_5 = 1$ *at Step 5 of the decoding algorithm.*

Similarly, if more than one residue errors occurred, it can be shown that the decoding algorithm will result in uncorrectable residue errors and outputs an erroneous codeword.

In summary, the minimum-distance decoding algorithm of RRNS codes has been introduced and interpreted. Our future work is focused on a range of applications of this algorithm, such as for example those in [8, 9].

[1] Note that this step is usually implemented with the aid of the BEX algorithm given by Eq.(9). Here, however, a simple table-lookup was used for the sake of conceptual simplicity.

5. REFERENCES

[1] R. W. Watson and C. W. Hastings, "Self-checked computation using residue arithmetic," *Proc. of the IEEE*, vol. 54, pp. 1920–1931, Dec. 1966.

[2] D. Mandelbaum, "Error correction in residue arithmetic," *IEEE Trans. on Comput.*, vol. 21, pp. 538–545, June 1972.

[3] F. Barsi and P. Maestrini, "Error correction properties of redundant residue number systems," *IEEE Trans. on Comput.*, vol. 22, pp. 307–315, March 1973.

[4] H. Krishna, K.-Y. Lin, and J.-D. Sun, "A coding theory approach to error control in redundant residue number systems - Part I: theory and single error correction," *IEEE Trans. Circuits Syst.*, vol. 39, pp. 8–17, January 1992.

[5] J.-D. Sun and H. Krishna, "A coding theory approach to error control in redundant residue number systems - Part II: multiple error detection and correction," *IEEE Trans. Circuits Syst.*, vol. 39, pp. 18–34, Jan. 1992.

[6] M. H. Etzel and W. K. Jenkins, "Redundant residue number systems for error detection and correction in digital filters," *IEEE Trans. on Acous., Speech, and Signal Proc.*, vol. 28, pp. 538–545, Oct. 1980.

[7] E. D. D. Claudio, G. Orlandi, and F. Piazza, "A systolic redundant residue arithmetic error correction circuit," *IEEE Trans. on Comput.*, vol. 42, pp. 427–432, Apr. 1993.

[8] L.-L. Yang and L. Hanzo, "Performance of residue number system based DS-CDMA over multipath fading channels using orthogonal sequences," *Euro. Trans. on Telecom.*, vol. 9, pp. 525–536, Nov. - Dec. 1998.

[9] L.-L. Yang and L. Hanzo, "Ratio statistic test assisted residue number system based parallel communication systems," in *Proc. of IEEE VTC'99*, (Houston, USA), pp. 894–898, May 1999.

[10] L.-L. Yang and L. Hanzo, "Coding theory and performance of redundant residue number system codes." submitted to IEEE Trans. on Inform. Theory, 1999 (www-mobile.ecs.soton.ac.uk/lly).

[11] W. K. Jenkins and E. J. Altman, "Self-checking properties of residue number error checkers based on mixed radix conversion," *IEEE Trans. on Circuit and Syst.*, vol. 35, pp. 159–167, Feb. 1988.

[12] S. S.-S. Yau and Y.-C. Liu, "Error correction in redundant residue number systems," *IEEE Trans. on Comput.*, vol. 22, pp. 5–11, Jan. 1973.