A new algorithm for single residue digit error correction in redundant residue number system

Chang, Chip-Hong; Tay, Thian Fatt

2014

Tay, T. F., & Chang, C.-H. (2014). A new algorithm for single residue digit error correction in redundant residue number system. 2014 IEEE International Symposium on Circuits and Systems (ISCAS), 1748-1751.

https://hdl.handle.net/10356/104943

https://doi.org/10.1109/ISCAS.2014.6865493

A New Algorithm for Single Residue Digit Error Correction in Redundant Residue Number System

Thian Fatt Tay and Chip-Hong Chang
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore.

Abstract—**This paper presents 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. This is made possible by the introduction of a new syndrome, which is proven to be unique for every different residue digit error with two criteria imposed on the choice of redundant moduli. The erroneous residue digit can be corrected by deducting the error digit retrieved from the lookup table indexed by the syndrome. Our proposed algorithm compares favorably against existing single residue digit correction algorithms, and is more amenable to hardware implementation.**

I. INTRODUCTION

The inexorable trend of device scaling presents daunting challenges to the reliability of electronic computations. Rather than being the privileged beneficiaries of nano-scale technology, high-speed low-power digital signal processors are increasingly hampered by computational uncertainties due to the high error probability of individual gates. At transistor size of few tens of nanometers and smaller, aging, noise, radiation, heat and other dynamic conditions can easily perturb a device out of specification and cause transistors operating at low supply voltage to be susceptible to single event upsets and intermittent errors. Dependability of digital systems can be significantly enhanced by incorporating fault tolerance into their design. Unfortunately, classical fault-tolerant techniques such as error correction code, self-checking logic, module replication, reconfiguration, etc. [1] are impractically expensive and non-scalable. Some of these fault diagnosis and reconfiguration approaches to counter soft errors require huge reliable memories or immense test and reconfiguration time.

Residue Number System (RNS) can potentially relax the reliability requirement of low-level circuit by virtue of its parallel and modular arithmetic operations. Due to the isolation of carry forwarding in RNS, variations in circuit power and timing or transient perturbation during computations may alter the states of many devices in proximity but the cluster errors occurred in one modulus channel will not be propagated to the others [2]. The capability of Redundant Residue Number System (RRNS) to correct cluster instead of random bit errors with lower redundancy has caught considerable attention. A six-moduli RRNS code was recently reported to provide more data storage capacity in hybrid memories than Reed-Solomon code for the same error correction capability [3]. RRNS code was also used in symbol-by-symbol adaptive multicarrier modulation to combat frequency-selective fading with better performance than the turbo-convolutional code for channel SNR above 15 dB [4]. In [5], RRNS was integrated into a multipath routing protocol to reduce the impact of data message discard in mobile ad hoc networks.

Error detection and correction algorithms in RRNS are typically performed in three steps: detection, location and correction of error [2], of which identification of error position is the most difficult. Error is normally detected by checking if the magnitude of the residue representation falls outside the legitimate computation range. Methods that use modulus projection [6]-[8], base extension [9],[10], range detection [11], etc. differ by the ways error location is identified from the received residues. These methods are either complicated, iterative, involves very large modulo operations or requires a lot of stored tables. Upon extracting the error position and magnitude, the error can be corrected by either subtracting the error digit in the residue domain or computing the magnitude of error-free residue representation.

This paper presents a new approach to single residue digit error detection and correction problem in RRNS. The algorithm distinguishes itself from others by the proposed syndrome to identify the erroneous residue and decode its error value. One important contribution is the proof of syndrome uniqueness, which makes it possible to create an error lookup table indexed by the syndrome for every possible residue digit error. The uniqueness criteria are shown to be easily fulfilled by many choices of redundant moduli from an abundant number of coprime integers. The circuit implementation of the proposed algorithm is also suggested.

II. REDUNDANT RESIDUE NUMBER SYSTEM (RRNS)

An RNS is defined by a set of positive coprime integers $\{m_1, m_2, ..., m_k\}$, where each integer m_j is called a modulus. An integer $X \in [0, M_K-1]$ can be uniquely represented by a k-tuple $(x_1, x_2, \ldots, x_k)$, where $M_K = \prod_{j=1}^{k} m_j$ and each integer x_j is called a residue digit and $x_j = |X|_{m_j}$ is the least non-negative remainder of X divided by m_j. The uniqueness of RNS representation can be proven by Chinese Remainder Theorem (CRT) [7], which states that:

$$X = \left| \sum_{j=1}^{k} M_j \left| M_j^{-1} \right|_{m_j} x_j \right|_{M_K} \qquad (1)$$

where $M_j = M_K / m_j$ and $\left| M_j^{-1} \right|_{m_j}$ is the multiplicative inverse of $\left| M_j \right|_{m_j}$.

By adding two redundant moduli, m_{k+1} and m_{k+2}, an RRNS with $n = k + 2$ coprime moduli $\{m_1, m_2, ..., m_k, m_{k+1}, m_{k+2}\}$ and a dynamic range of $M_N = M_K \times M_R$ are defined, where $M_R = m_{k+1} \times m_{k+2}$ is the product of the redundant moduli. The legitimate range $[0, M_K-1]$ represents the useful computational range of the RRNS whereas the illegitimate range $[M_K, M_N-1]$ is useful for error and overflow detection [11]. Provided that

m_{k+1}, $m_{k+2} > m_i \ \forall i \le k$ [7], the residue representation in the expanded code space is a (n, 2)-maximum distance separable code capable of detecting two and correcting one residue digit error.

III. Uniqueness of Proposed Error Syndrome

Let e_i be the error digit introduced into the modulus channel m_i for $1 \le i \le k+2$. The error magnitude E_i can be represented by an n-tuple (0, ..., e_i, ..., 0) in RRNS, where $n = k + 2$. Using CRT, E_i can be computed as [9]:

$$E_i = (M_N/m_i)\left|\left|M_i^{-1}\right|_{m_i} e_i\right|_{m_i} = a_i M_N/m_i = a_i M_K M_R/m_i \quad (2)$$

where $a_i = \left|\left|M_i^{-1}\right|_{m_i} e_i\right|_{m_i}$ is an integer in the range $[1, m_i-1]$.

The relationship between a residue representation $\tilde{X} \equiv (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n)$ that is contaminated with a residue digit error $E_i \equiv$ (0, …, e_i, …, 0) and an error-free residue representation, $X \equiv (x_1, x_2, \ldots, x_n)$ is given by

$$\begin{aligned}(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n) &\equiv (x_1, x_2, \ldots, x_n) + (0, \ldots, e_i, \ldots, 0) \\ &= (x_1, \ldots, \left|x_i + e_i\right|_{m_i}, \ldots, x_n)\end{aligned} \quad (3)$$

E_i is unique for every e_i value in m_i. If E_i can be extracted from the residue representation of $\tilde{X}$, the erroneous residue digit $\tilde{x}_i$ can be identified and corrected by $x_i = \left|\tilde{x}_i - e_i\right|_{m_i}$. As RRNS is a non-weighted number system, the error magnitude cannot be easily recovered from its residue representation. Decoding the received residue representation by CRT requires large modulo operations and is inefficient. To extract the error magnitude from an erroneous residue representation without involving large modulo operation, we define a syndrome δ as

$$\delta = \left|\left|\tilde{X}\right|_{M_K} - \left|\tilde{X}\right|_{M_R}\right|_{M_R} \quad (4)$$

where $\left|\tilde{X}\right|_{M_K} \equiv (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_k)$ and $\left|\tilde{X}\right|_{M_R} \equiv (\tilde{x}_{k+1}, \tilde{x}_{k+2})$

Theorem 1: When there is no residue error, δ is zero. If there is any error in the information (or redundant) residue, δ is modulo M_R congruent to E_i mod M_K (or M_R) with or without an offset of M_K (or M_R).

Proof: If $\tilde{X} \equiv (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n)$ is error-free, then $\left|\tilde{X}\right|_{M_K} = \left|X\right|_{M_K} = X$ and $\left|\tilde{X}\right|_{M_R} = \left|X\right|_{M_R}$.

$$\delta = \left|X - \left|X\right|_{M_R}\right|_{M_R} = \left|\lfloor X/M_R \rfloor M_R\right|_{M_R} = 0 \quad (5)$$

To use the syndrome δ to correct an residue digit error, δ must be unique for every possible error digit. The error digit can appear in either an information residue or a redundant residue. If an information residue is erroneous, then $\left|\tilde{X}\right|_{M_K} = \left|X + E_i\right|_{M_K}$ and $\left|\tilde{X}\right|_{M_R} = \left|X\right|_{M_R}$.

$$\begin{aligned}\delta &= \left|\left|X + E_i\right|_{M_K} - \left|X\right|_{M_R}\right|_{M_R} \\ &= \left|X + \left|E_i\right|_{M_K} - \alpha_K M_K - \left|X\right|_{M_R}\right|_{M_R} = \left|\left|E_i\right|_{M_K} - \alpha_K M_K\right|_{M_R}\end{aligned} \quad (6)$$

where $\alpha_K = 0$ if $X + \left|E_i\right|_{M_K} < M_K$ and $\alpha_K = 1$ otherwise.

If a redundant residue is erroneous, then $\left|\tilde{X}\right|_{M_K} = X$ and $\left|\tilde{X}\right|_{M_R} = \left|X + E_i\right|_{M_R}$.

$$\begin{aligned}\delta &= \left|X - \left|X + E_i\right|_{M_R}\right|_{M_R} \\ &= \left|X - \left(\left|X\right|_{M_R} + \left|E_i\right|_{M_R} - \alpha_R M_R\right)\right|_{M_R} = \left|-\left|E_i\right|_{M_R}\right|_{M_R}\end{aligned} \quad (7)$$

where $\alpha_R = 0$ if $\left|X\right|_{M_R} + \left|E_i\right|_{M_R} < M_R$ and $\alpha_R = 1$ otherwise.

Theorem 2: The syndrome δ is distinct for every possible error digit provided that (1) $M_R > 2\sum_{j=1}^{k}(m_j - 1) + m_{k+1} + m_{k+2} - 2$ and (2) the redundant moduli must be larger than the information moduli, i.e. $m_{k+1}, m_{k+2} > m_i \ \forall i \le k$.

Proof: The total number of possible single residue error in the information residue channels and redundant residue channels can be computed as $\sum_{j=1}^{k}(m_j - 1)$ and $(m_{k+1} - 1) + (m_{k+2} - 1)$, respectively. There are $\sum_{j=1}^{k}(m_j - 1)$ different values of e_i in the information channels. According to (6), the magnitude of any residue error can be decoded from either $\delta = \left|\left|E_i\right|_{M_K}\right|_{M_R}$ or $\delta = \left|\left|E_i\right|_{M_K} + M_K\right|_{M_R}$ depending on the value of α_K. According to (7), any of the $(m_{k+1} - 1) + (m_{k+2} - 1)$ possible error magnitudes in the redundant channels can be decoded directly from $\delta = \left|-\left|E_i\right|_{M_R}\right|_{M_R}$. Since $\delta \in [0, M_R-1]$, condition (1) in *Theorem 2* can be fulfilled by having

$$M_R > 2\sum_{j=1}^{k}(m_j - 1) + m_{k+1} + m_{k+2} - 2 \quad (8)$$

To prove the second criterion, let E_i and E_j ($E_i > E_j$) be two different error magnitudes due to the residue errors in modulus channels m_i and m_j, respectively, and m_i needs not be larger than nor different from m_j. If $m_i = m_j$, E_i and E_j are two error magnitudes due the residue errors in the same modulus channel. In any case, δ_i due to E_i must be distinguishable from δ_j due to E_j.

Case 1: E_i and E_j are due to different residue errors in any information residues (i.e., $i, j \in [0, k]$).

From (6), $\delta_i = \left|\left|E_i\right|_{M_K} - \alpha_{Ki} M_K\right|_{M_R}$ and $\delta_j = \left|\left|E_j\right|_{M_K} - \alpha_{Kj} M_K\right|_{M_R}$. For this case, $\delta_i \ne \delta_j$ if and only if $\Delta = \left|E_i\right|_{M_K} - \alpha_{Ki} M_K - \left(\left|E_j\right|_{M_K} - \alpha_{Kj} M_K\right)$ is not a multiple of M_R. Substituting $E_i = a_i M_K M_R/m_i$ from (2) into $\Delta = \left|E_i\right|_{M_K} - \alpha_{Ki} M_K - \left|E_j\right|_{M_K} + \alpha_{Kj} M_K = E_i - \beta_{Ki} M_K - \alpha_{Ki} M_K - E_j + \beta_{Kj} M_K + \alpha_{Kj} M_K$, we have

$$\Delta = \left[\frac{a_i M_K}{m_i} - \frac{a_j M_K}{m_j}\right] M_R - (\alpha_{Ki} + \beta_{Ki} - \alpha_{Kj} - \beta_{Kj}) M_K \quad (8)$$

where $\beta_{Ki} = \lfloor E_i/M_K \rfloor$ and $\beta_{Kj} = \lfloor E_j/M_K \rfloor$.

Since $a_i M_K/m_i$ and $a_j M_K/m_j$ are integers for information channel errors. The expression of (8) is not a multiple of M_R if $\alpha_{Ki}+\beta_{Ki}-\alpha_{Kj}-\beta_{Kj}$ is non-zero, i.e.,

$$\left|\alpha_{Ki}+\beta_{Ki}-\alpha_{Kj}-\beta_{Kj}\right|\geq 1 \tag{9}$$

Assume that $\alpha_{Ki}+\beta_{Ki}>\alpha_{Kj}+\beta_{Kj}$, then

$$\alpha_{Ki}+\beta_{Ki}-\alpha_{Kj}-\beta_{Kj}\geq 1$$
$$\lfloor E_i/M_K\rfloor-\lfloor E_j/M_K\rfloor+\left(\alpha_{Ki}-\alpha_{Kj}\right)\geq 1$$
$$E_i/M_K-E_j/M_K+\left(\alpha_{Ki}-\alpha_{Kj}\right)>0$$
$$\left(a_i/m_i-a_j/m_j\right)M_R>\alpha_{Kj}-\alpha_{Ki}$$
$$M_R>\frac{\left(\alpha_{Kj}-\alpha_{Ki}\right)m_im_j}{a_im_j-a_jm_i} \tag{10}$$

Since $a_i < m_i$, $a_j < m_j$ and both m_i and m_j are coprime, $\min(a_im_j - a_jm_i) = 1$. Also, $\max(\alpha_{Kj} - \alpha_{Ki}) = 1$ because $\alpha_{Ki},\alpha_{Kj}\in\{0,1\}$. Thus, the minimum value M_R must exceed is

$$M_R>\max\left(m_im_j\right) \tag{11}$$

In other words, the product of the two redundant moduli must be greater than the product of the two largest information moduli. The same conclusion can also be drawn for $\alpha_{Ki}+\beta_{Ki}<\alpha_{Kj}+\beta_{Kj}$.

Case 2: E_i and E_j are due to different errors in any redundant residues (i.e., $i, j\in\{k+1, k+2\}$).

From (7),

$$\begin{aligned}\delta_i&=\left|-\left|E_i\right|_{M_R}\right|_{M_R}=M_R-\left|E_i\right|_{M_R}=M_R-\left(E_i-\beta_{Ri}M_R\right)\\&=M_R-\left(a_iM_KM_R/m_i-\beta_{Ri}M_R\right)\\&=\left[\left(\beta_{Ri}+1\right)m_i-a_iM_K\right]\left(M_R/m_i\right)=Z_i\left(M_R/m_i\right)\end{aligned} \tag{12}$$

where $\beta_{Ri}=\lfloor E_i/M_R\rfloor$ and $Z_i=\left(\beta_{Ri}+1\right)m_i-a_iM_K$.

From (12), δ_i is an integer multiple of M_R/m_i. Since $M_R = m_{k+1}\times m_{k+2}$, δ_{k+1} and δ_{k+2} are the integer multiples of m_{k+2} and m_{k+1}, respectively. As m_{k+1} and m_{k+2} are coprime, δ_{k+1} and δ_{k+2} are always distinguishable.

For δ_i and δ_j due to different error digits in the same redundant channel (i.e., $m_i = m_j$) to be distinguishable, $Z_i \neq Z_j$. Since m_i and M_K are coprime and $a_i - a_j\in[-m_i+2, m_i-2]$,

$$\begin{gathered}\left(\beta_{Ri}-\beta_{Rj}\right)m_i\neq\left(a_i-a_j\right)M_K\\\left(\beta_{Ri}+1\right)m_i-a_iM_K\neq\left(\beta_{Rj}+1\right)m_i-a_jM_K\Rightarrow Z_i\neq Z_j\end{gathered} \tag{13}$$

From (13), the syndromes due to different error digits in the same redundant channel are unconditionally distinguishable.

Case 3: E_i and E_j are due to errors in information and redundant residues, respectively (i.e., $i\in[0, k]$ and $j\in\{k+1, k+2\}$).

From (6) and (7), $\delta_i=\left|\left|E_i\right|_{M_K}-\alpha_{Ki}M_K\right|_{M_R}$ and $\delta_j=\left|-\left|E_j\right|_{M_R}\right|_{M_R}$. For this case, $\delta_i\neq\delta_j$ if and only if $\Delta=\left|E_i\right|_{M_K}-\alpha_{Ki}M_K-\left(-\left|E_j\right|_{M_R}\right)$ is not a multiple of M_R.

$$\begin{aligned}\Delta&=E_i-\beta_{Ki}M_K-\alpha_{Ki}M_K+E_j-\beta_{Rj}M_R\\&=\left(a_iM_K/m_i-\beta_{Rj}\right)M_R-\left(\beta_{Ki}+\alpha_{Ki}-a_jM_R/m_j\right)M_K\end{aligned} \tag{14}$$

where $\beta_{Ki}=\lfloor E_i/M_K\rfloor$ and $\beta_{Rj}=\lfloor E_j/M_R\rfloor$.

Since $a_iM_K/m_i-\beta_{Rj}$ is an integer, (14) is not a multiple of M_R if and only if $\beta_{Ki}+\alpha_{Ki}-a_jM_R/m_j$ is non-zero, i.e.,

$$\left|\beta_{Ki}+\alpha_{Ki}-a_jM_R/m_j\right|\geq 1 \tag{15}$$

Assume $\beta_{Ki}+\alpha_{Ki}>a_jM_R/m_j$, then

$$\beta_{Ki}+\alpha_{Ki}-a_jM_R/m_j\geq 1$$
$$\lfloor a_iM_R/m_i\rfloor+\alpha_{Ki}-a_jM_R/m_j\geq 1$$
$$a_iM_R/m_i+\alpha_{Ki}-a_jM_R/m_j>0$$
$$M_R>\frac{-\alpha_{Ki}m_im_j}{a_im_j-a_jm_i} \tag{16}$$

When $a_im_j - a_jm_i = -1$ and $\alpha_{Ki}=1$, $M_R > \max(m_i\times m_j)$, i.e.,

$$\begin{gathered}m_{k+1}\cdot m_{k+2}>\max(m_i)\cdot\max\left(m_{k+1},m_{k+2}\right)\\\min\left(m_{k+1},m_{k+2}\right)>\max(m_i)\end{gathered} \tag{17}$$

The inequality (17) suggests that the smallest redundant modulus must be greater than the largest information modulus. The same conclusion can be drawn if $\beta_{Ki}+\alpha_{Ki}<a_jM_R/m_j$.

Combining the inequalities, (11) for Case 1 and (17) for Case 3, it can be concluded that $m_{k+1}, m_{k+2} > m_i\ \forall i\leq k$.

IV. Proposed Algorithm and Architecture for Single Residue Digit Error Correction

Based on Theorems 1 and 2, a new single residue digit error correction method is proposed as follows.

(1) Compute $\left|\tilde{X}\right|_{M_K}$ and $\left|\tilde{X}\right|_{M_R}$ by evaluating the magnitudes of $\left(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_k\right)$ and $\left(\tilde{x}_{k+1},\tilde{x}_{k+2}\right)$, respectively.

(2) Compute $\delta=\left|\left|\tilde{X}\right|_{M_K}-\left|\tilde{X}\right|_{M_R}\right|_{M_R}$.

(3) If $\delta = 0$, there is no error. Stop.

(4) Otherwise, use δ as the address to an error detection table to identify the erroneous modulus channel m_i and error digit e_i.

(5) Correct the erroneous residue digit $\tilde{x}_i$ by $x_i=\left|\tilde{x}_i-e_i\right|_{m_i}$.

Example: Consider the moduli set {7, 9, 11, 13, 17}, where 13 and 17 are the redundant moduli. Since $M_R = 13\times17 = 221 > 2(6+8+10)+12+16 = 76$ and the two redundant moduli are larger than the information moduli, conditions (1) and (2) of *Theorem 2* are fulfilled. Let $\tilde{X}\equiv 68297\equiv(5, 5, 9, 8, 8)$. $\left|\tilde{X}\right|_{M_K}=383$ and $\left|\tilde{X}\right|_{M_R}=8$ can be recovered from the residues (5, 5, 9) of RNS {7, 9, 11} and (8, 8) of RNS {13, 17}, respectively. The syndrome $\delta=\left|\left|\tilde{X}\right|_{M_K}-\left|\tilde{X}\right|_{M_R}\right|_{M_R}$ = $|383 - 8|_{221} = 154$. Since δ is non-zero, one of the residue digits is erroneous. The lookup table indexed by 154 returns $e_i = 1$ and $i = 2$ signifying $e_2 = 1$. Thus $x_2=\left|\tilde{x}_2-e_2\right|_{m_2}$ = $|5 - 1|_9 = 4$. The corrected residue representation is $(5, 4, 9, 8, 8)\equiv X = 229$.

The architecture for the syndrome computation, error detection and correction is shown in Fig. 1. The k-residue and two-residue CRTs evaluate $\left|\tilde{X}\right|_{M_K}$ and $\left|\tilde{X}\right|_{M_R}$ from

$(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_k)$ and $(\tilde{x}_{k+1}, \tilde{x}_{k+2})$, respectively. $|\tilde{X}|_{M_R}$ is then subtracted from $|\tilde{X}|_{M_K}$ by a mod M_R subtractor to produce the syndrome δ as the address to an error lookup table. The lookup table stores the corresponding $\lceil \log_2 m_{k+2} \rceil$-bit residue error digit e_i and $\lceil \log_2(k+2) \rceil$-bit erroneous modulus identifier i, which can be computed using (6) and (7). The comparator of the error correction module that compares i with a fixed integer can be implemented using simple logic gates. e_i is then gated into the i-th modular subtractor of the RRNS by the output of the i-th comparator. The outputs of the k+2 subtractors are the error-free residue digits $(x_1, x_2, \ldots, x_k, x_{k+1}, x_{k+2})$.

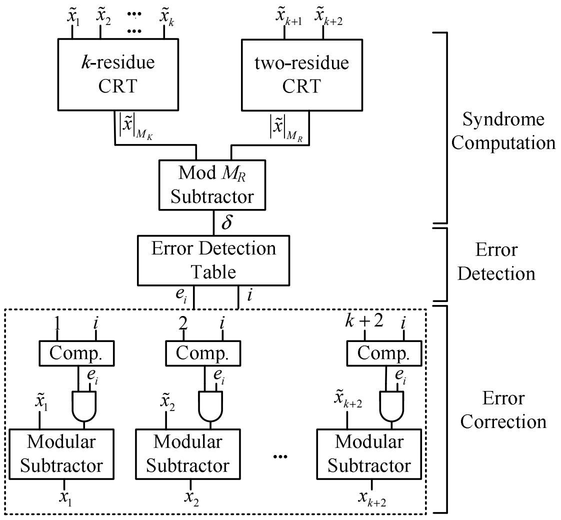

Fig. 1: Architecture for the proposed residue error correction algorithm.

V. Comparison

Table I shows the comparison of existing single residue error correction algorithms in terms of the number of redundant moduli r, the need for iterative consistency check, the output representation and the most stringent criterion on their moduli. All but [12] and [13] require redundant moduli. Redundancy is indirectly introduced into the legitimate dynamic range of [12] by scaled RNS and [13] by moduli with common factors. For comparable legitimate range, these two algorithms have larger moduli and hence slower residue arithmetic operations. No iterative consistency check is required by [6], [10]-[12] and our algorithm to detect residue error, making them more amenable to hardware implementation. Our corrected output is represented in residue domain, which is useful for correcting intermediate arithmetic processing and data transfer error within the RNS. Unlike [10], which must have an even number of moduli, there is no restriction on the number of moduli for our algorithm. The syndrome uniqueness criteria imposed on the moduli of our RRNS is easier to fulfill due to the abundant choice of coprime moduli than the condition imposed on the moduli of [11] for a practical number of information moduli.

VI. Conclusion

By selecting two redundant moduli to fulfill the uniqueness criteria for the syndrome proposed in our algorithm, any RNS computations can be endowed with a single residue error correction capability. Based on the uniqueness of the syndrome, a lookup table of all possible single residue errors of an RRNS can be constructed to enable an error digit and its position to be retrieved from the syndrome of the received residues and corrected directly by a simple modular subtractor. The proposed algorithm can be implemented using an RNS reverse converter for the information residues, a simple two-residue CRT for the redundant residues, k+3 modular subtractors, a look-up table and simple logic gates. The proposed algorithm is less restrictive in the choice and number of moduli and more suited for hardware implementation than existing single residue digit error correction algorithms.

Table I: Comparison of Single Residue Error Correction Algorithms.

Algorithm	r	Iterative?	Output domain	Most stringent moduli selection criterion
[6]	2	No	integer	$M_K \approx M_R$
[7]	2	Yes	integer	$m_{k+1}, m_{k+2} > m_i \, \forall i \le k$
[8]	≥3	Yes	integer	$M_R \ge \max(m_p m_q m_s)$, $1 \le p, q, s \le k+r$
[9]	2	Yes	residue	$M_R > 2m_i m_j - m_i - m_j$, $1 \le i, j \le k$
[10]	2	No	residue	even n; $m_{k+2} < \min(m_i \cdot m_j)$
[11]	2	No	residue	$M_R > 2m_i m_j - m_i - m_j$, $1 \le i, j \le k$
[12]	0	No	integer	$m > \max(m_i \cdot m_j)$
[13]	0	Yes	residue	$\gcd(m_i, m_j) \ne 1$
This	2	No	residue	$M_R > 2\sum_{j=1}^{k}(m_j - 1) + m_{k+1} + m_{k+2} - 2$

References

[1] V. P. Nelson, "Fault-tolerant computing: Fundamental concepts," *Computer*, vol. 23, no. 7, pp. 19–25, Jul. 1990.

[2] F. Barsi and P. Maestrini, "Error correcting properties of redundant residue number systems," *IEEE Trans. Comput.*, vol. C-22, no. 3, pp. 307-315, Mar. 1973.

[3] N. Z. Haron and S. Hamdioui, "Redundant residue number system code for fault-tolerant hybrid memories," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 7, no. 1, article 4, Jan. 2011.

[4] T. Keller, T.-H. Liew, and L. Hanzo, "Adaptive redundant residue number system coded multicarrier modulation," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 11, pp. 2292–2301, Nov. 2000.

[5] J. Alves Jr., L. F. L. Nascimento and L. C. P. Albini, "Using the redundant residue number system to increase routing dependability on mobile ad hoc networks," *Cyber Journals: J. of Selected Areas in Telecommunications*, pp. 67-73, January 2011.

[6] Y. Tang, E. Boutillon, C. Jégo and M. Jézéquel, "A new single-error correction scheme based on self-diagnosis residue number arithmetic," *Design and Architecture for Signal and Image Processing Conf.*, Edinburgh, Scotland, Oct. 2010, pp. 27-33.

[7] V. T. Goh, M. Tinauli and M. U. Siddiqi, "A novel error correction scheme based on the Chinese remainder theorem," *Ninth Int. Conf. Communications Systems*, Singapore, Sept. 2004, pp. 461-465.

[8] S. S. Wang and M. Y. Shau, "Single residue error corredtion based on *K*-term m_j-projection," *IEEE Trans. Comput.*, vol. 44, no. 1, pp. 129-131, Jan. 1995.

[9] H. Krishna, K. Lin, and J. Sun, "A coding theory approach to error control in redundant residue number systems - Part I: Theory and single error correction," *IEEE Trans. Circuits Syst. II*, vol. 39, no. 1, pp. 8–17, Jan. 1992.

[10] E. D. D. Claudio, G. Orlandi, and F. Piazza, "A systolic redundant residue arithmetic error correction circuit," *IEEE Trans. Comput.*, vol. 42, no. 4, pp. 427–432, Apr. 1993.

[11] C. C. Su and H. Y. Lo, "An algorithm for scaling and single residue error correction in residue number systems," *IEEE Trans. Comput.*, vol. 39, no. 8, pp. 1053-1064, Aug. 1990.

[12] S. Pontarelli, G. C. Cardarilli, M. Re and A. Salsano, "A novel error detection and correction technique for RNS based FIR filters," *IEEE Int. Symp. Defect and Fault Tolerance of VLSI Systems*, Boston, MA, Oct. 2008, pp. 436-444.

[13] R. S. Katti, "A new residue arithmetic error correction scheme," *IEEE Trans. Comput.*, vol. 45, no. 1, pp. 13-19, Jan. 1996.