UDC 681.32

F.Barsi, P.Maestrini

Italy

ERROR DETECTION IN RESIDUE NUMBER SYSTEMS WITH MAGNITUDE INDEX

1. Error control in residue number systems

Residue number systems (RNS) become first [1-2] a subject of research in computer science because they were expected to provide a mean to speed-up arithmetic processing. However, it was soon recognized that, in nonredundant RNS, the modular properties and the potential high speed of addition, subtraction and multiplication are counterbalanced by the lengthy and complicated nature of operations involving magnitude comparison, such as sign or overflow detection [3-4]. More recently, the interest has shifted toward the error detecting and correcting properties of RNS, and satisfactory results have been published both for separate codes (i.e., for the case where the redundancy takes the form of one or more redundant digits [4-5-6-7]), and for the product (AN) codes defined in RNS [8-9]. The error classes taken into consideration for detection or correction usually include single or multiple residue digit errors, although the case of single bit errors has also been considered [7-9]. This paper deals with a class of residue codes, where the redundancy takes the form of a magnitude index. As far as errors of given multiplicity are considered, the error detecting capabilities of RNS with magnitude index are the same as those of separate codes or of product codes defined in RNS. As shown in this paper, the unique feature of RNS with magnitude index consists in the fact that errors of arbitrary multiplicity are also detectable, provided the error magnitude exceeds a given threshold.

2. Residue number systems with magnitude index

Given a set of n pairwise prime, positive integers, $m_1, m_2, \ldots, m_n$,

Discrete Systems - Vol 2 - International Symposium (RIGA - settembre 30 - ottobre 4 - 1974)

called <u>moduli</u>, any integer X in the range $[0,M)$, with $M=\prod_{i=1}^{n} m_i$, is uniquely represented in the RNS of the given moduli by the n-tuple $\{x_1, x_2, \ldots, x_n\}$, where $x_i=|X|_{m_i}$, $i=1,2,\ldots,n$.

Let $\{m_{I1}, m_{I2}, \ldots, m_{Ip}\}$ be a subset of moduli, $m_I=\prod_{j=1}^{p} m_{Ij}$, $1\leq p\leq n$, and consider the equality $X=|X|_{M/m_I}+\frac{M}{m_I}\left[\frac{X}{M/m_I}\right]$: it is seen that the integer $I_X=\left[\frac{X}{M/m_I}\right]$, henceforth referred to as the <u>magnitude index</u> of X, locates X into precisely one interval of width M/m_I. The (n+1)-tuple $\{x_1, x_2, \ldots, x_n, (I_X)\}$ is a redundant representation of the number X in the given RNS and is called the <u>residue representation with magnitude index</u> of X. Note that I_X is easily derived from the residue representation of X by a mixed radix conversion procedure.

Residue representation with magnitude index is extended to relative numbers. Assuming m_I even and using a complement notation, any integer X in the range $[-M/2,M/2)$ is represented as $|X|_M$, i.e., by the (n+1)-tuple $\{x_1, x_2, \ldots, x_n, (I_X)\}$, where $x_i=|X|_{m_i}$ $(i=1,2,\ldots,n)$ and $I_X=\left[\frac{|X|_M}{M/m_I}\right]$. In this hypothesis the magnitude index I_X ranges in $[0,m_I/2)$ for positive numbers and in $[m_I/2,m_I)$ for negative numbers and the sign is detected by simple inspection of I_X.

Additive properties of the residue representation with magnitude index are straightforward. Assuming that X and Y are two numbers in the range $[-M/2,M/2)$, their residue representations are $\{x_1, x_2, \ldots, x_n, (I_X)\}$ and $\{y_1, y_2, \ldots, y_n, (I_Y)\}$. It is easily seen that $X\pm Y$ is represented as $\{|x_1\pm y_1|_{m_1}, |x_2\pm y_2|_{m_2}, \ldots, |x_n\pm y_n|_{m_n}, (|I_X\pm I_Y+i|_{m_I})\}$ where $i=1$ in the case of addition if $|X|_{M/m_I}+|Y|_{M/m_I}\geq M/m_I$, $i=-1$ in the case of subtraction if $|X|_{M/m_I}-|Y|_{M/m_I}<0$ and $i=0$ otherwise. The constant i is determined by detecting overflows and underflows of $|X|_{M/m_I}\pm|Y|_{M/m_I}$ from the range $[0,M/m_I)$; since the residue representations of $|X|_{M/m_I}$ and $|Y|_{M/m_I}$ are immediately available, this is done by the usual means [3-4].

A range overflow of the sum $|X|_M+|Y|_M$ from the range $[0,M)$ is detected if $I_X\pm I_Y+i$ comes out of $[0,m_I)$. An arithmetic overflow of $X\pm Y$ is detected, as in positional number systems, once the sign of the operands and either the sign of the result or the presence of a range overflow are known.

In the following, our consideration will be limited to the representations of relative integers, thus to nonnegative integers in the range $[0,M)$.

3. <u>Detection of errors of arbitrary multiplicity</u>

Given an RNS with magnitude index of moduli $m_1, m_2, \ldots, m_n$, where $m_{I1}, m_{I2}, \ldots, m_{Ip}$ is a subset of moduli and $m_I=\prod_{j=1}^{p}$, let $X=\{x_1, x_2, \ldots, x_n, (I_X)\}$ be either a number in the range $[0,M)$ or the sum of two arbitrary numbers in this range, thus possibly a number in overflow.

Assume that an arbitrary error ΔX affects the residue digits of X, thus yielding $X'=X+\Delta X=\{x_1', x_2', \ldots, x_n', (I_X)\}$, while I_X is unchanged. Then the magnitude index, as recomputed from X', is $I'_{X,c}=\left\lceil\frac{X+\Delta X}{M/m_I}\right\rceil$ and provides error detection for arbitrary X if and only if $|\Delta X|\geq M/m_I$ since in this hypothesis $I'_{X,c}\neq I_X$.

Conversely, suppose that an error ΔI_X affects the magnitude index itself: the wrong value is $I_X'=I_X+\Delta I_X$ and the recomputed value $I_{X,c}=I_X\neq I_X'$ allows error detection.

If X is a number in overflow and a fault alters the output of the overflow indicator, an undetectable error ensues. This situation is overcome by representing the magnitude index in the extended range $[0,M_I)$, where $M_I\geq 2m_I$. This approach allows keeping track of the magnitude of numbers in overflow and causes the overflow information to be included in the magnitude index. In absence of errors, a number $X=\{x_1, x_2, \ldots, x_n, (I_X)\}$ is recognized to be in overflow if $I_{X,c}=I_X-m_I$, where $I_{X,c}$ is the magnitude index as recomputed from the residue digits of X.

Errors affecting the magnitude index are generally detectable unless the error has magnitude $\Delta I_X=\pm m_I$, since in this case the error either is indistinguishable from, or may mask, an additive overflow. Observe also that, in the hypothesis of multiple errors affecting both the residue representation of X and the magnitude index, error detection is generally impossible because the one error may mask the other. The preceding analysis is summarized by the following:

<u>Theorem 1</u>. Consider an RNS with magnitude index of moduli $m_1, m_2, \ldots$

..., m_n where $M_I \geq 2m_I$. Then the given residue system ensures detection of any error ΔX affecting the residue representation of an arbitrary number X, either in the range $[0,M)$ or in overflow, if and only if $|\Delta X| \geq M/m_I$ or, alternatively, of any error ΔI_X affecting magnitude index I_X if and only if $\Delta I_X \neq \pm m_I$.

Example 1. In the RNS of moduli $m_1=3$, $m_2=5$, $m_3=7$, $m_4=m_I=11$, where $M=1155$, the number $X=\{120, (I_X=8)\}$ is represented as $\{2,0,3,7, (8)\}$. Suppose that the residue representation of X is altered by effect of an error $\Delta X=-107$ thus giving rise to the number $X'=\{813, (I_X=8)\}=\{0,3,1,10, (8)\}$. Since the recomputed magnitude index is $I'_{X,c}=7 \neq I_X=8$ the error is detected.

4. Detection of single residue digit errors

In the preceding Section the conditions for error detection have been stated in terms of error magnitude. More conventionally, the error detecting properties of RNS with magnitude index can also be stated by considering error classes related to error multiplicity, i.e., to the number of wrong digits in the residue representation. Our consideration will be limited to single residue digit errors: a generalization to errors of arbitrary multiplicity may follow as an immediate extension.

Given a number X, represented in an RNS with magnitude index, suppose that an error affects the i^{th} residue digit of the representation. Then a different number $X'=X+p_i\frac{M}{m_i}$ is obtained [7], where the nonzero integer p_i is called error parameter and $1 \leq i \leq n$, $-m_i < p_i < m_i$. The difference $e_i = |X'-X|_{m_i} = |p_i M/m_i|_{m_i}$, referred to as error digit, unambiguously characterizes the error, independently of the particular value of X. As X runs in $[0,M)$, the same error digit may originate from two error parameters, p_i and p'_i, with $p_i \equiv p'_i \pmod{m_i}$.

In order to determine the conditions under which the error digit e_i is detectable when affecting an arbitrary X, observe that the occurrence of the error digit e_i may determine either the error $|\Delta X| = |p_i M/m_i|$ or $|\Delta X| = |(m_i - p_i)M/m_i|$, depending on the particular X. Then, the following statement is immediately derived from Theorem 1.

Theorem 2. Given an RNS with magnitude index of moduli $m_1, m_2, \ldots, m_n$, the error digit $e_i = |p_i M/m_i|_{m_i}$, where $-m_i < p_i < m_i$, $1 \leq i \leq n$, is detectable if and only if $m_I \geq m_i / |\pm p_i|_{m_i}$.

Observe, from Theorem 2, that if error e_i is detectable, the complementary error $e_i' = |-e_i|_{m_i}$ is also detectable.

The following Corollary 1 is straightforward.

Corollary 1. Given an RNS with magnitude index, all single errors affecting the residue representation of any number X are detectable if and only if $m_I \geq \max(m_i)$, $i=1,2,\ldots,n$.

In order to keep track of additive overflows, assume that the magnitude index I_X is represented in the extended range $[0, M_I)$ with $M_I \geq 2m_I$. For consistency with the residue representation of X, it is natural to assume that I_X is given a residue representation with the moduli $m_{n+1}, m_{n+2}, \ldots, m_{n+r}$, where $M_I = \prod_{j=1}^{r} m_{n+j}$ and $r \geq 2$. In the following, the moduli $m_{n+1}, m_{n+2}, \ldots, m_{n+r}$ and the corresponding residue digits will be referred to as redundant moduli and redundant residue digits, respectively, while the moduli $m_1, m_2, \ldots, m_n$ and the corresponding residue digits will be referred to as nonredundant moduli and nonredundant residue digits, respectively.

As stated by Theorem 1, any error ΔI_X affecting the magnitude index is detectable provided $\Delta I_X \neq \pm m_I$. This limitation is automatically verified as far as single residue digit errors are assumed in the magnitude index. In fact, if an error $\Delta I_X = p_{n+i} \frac{M_I}{m_{n+i}}$ affects the $(n+i)^{th}$ residue digit and the congruence $p_{n+i} M/m_{n+i} \equiv 0 \pmod{m_I}$ is never verified, any ambiguity or masking between additive overflow and errors is removed. If $t = (m_I, M_I/m_{n+i})$ denotes the greatest common divisor of m_I and M_I/m_{n+i}, the congruence above considered becomes $p_{n+i} \frac{M_I}{t\, m_{n+i}} \equiv 0 \pmod{m_I/t}$ or, also, $p_{n+i} \equiv 0 \pmod{m_I/t}$, and is never verified if and only if $m_I/t \geq m_{n+i}$.

The preceding considerations are restated by the following:

Theorem 3. Given an RNS with magnitude index of moduli $m_1, m_2, \ldots, m_n$, assume that the magnitude index is given a residue representation with the moduli $m_{n+1}, m_{n+2}, \ldots, m_{n+r}$, where $r \geq 2$, $M_I = \prod_{j=1}^{r} m_{n+j}$. Then any error affecting a single residue digit, either redundant or nonredundant, is detectable concurrently with an additive overflow if and only if

$m_I \geq \max(m_i)$, $i=1,2,..,n$; $M_I \geq 2m_I$; $m_{n+i} \leq m_I/t$, $t=(m_I, M_I/m_{n+i})$

A simple error detection procedure is derived from the preceding discussion. Given a number $\{X, (I_X)\}$ to be tested, its magnitude index $I_{X,c}$ is recomputed from the residue representation and:

a) if $I_{X,c}=I_X$, the number is recognized to be error-free

b) if $I_{X,c} \equiv I_X \pmod{m_I}$, the number is error-free and an additive overflow is detected

c) if $I_{X,c} \not\equiv I_X \pmod{m_I}$ a single residue digit error is detected.

Example 2. In the RNS of moduli $m_1=8$, $m_2=11$, $m_3=13$, $m_4=m_I=17$, assume $M_I=35$. Observing that $M_I > 2m_I$ and assuming for the magnitude index a residue representation with the moduli $m_5=5$, $m_6=7$, the number $X=\{3471, (I_X=3)\}$ is represented as $\{7,6,0,3, (3,3)\}$. If an error affects the second residue digit, thus generating the number $X'=\{7,0,0,3, (3,3)\}=\{7007, (I_X=3)\}$, the recomputed magnitude index is $I_{X,c}=6$. Since $I_{X,c} \not\equiv I_X \pmod{m_I}$, the error is detected.

5. Detection of bit errors

In the preceding Section it has been shown that, in order to detect all single digit errors in the residue representation of any number X, the condition $m_I \geq \max(m_i)$ need to be verified. Nevertheless it follows from Theorem 2 that some error detection is also provided if $m_I < \max(m_i)$, although the percentage of error digits being detected when affecting an arbitrary number X decreases as m_I decreases.

Consider an RNS with magnitude index where $m_I < \max(m_i)$ and the magnitude index is encoded in the range $[0, M_I)$, with $M_I \geq 2m_I$. Systematic application of Theorem 2 defines, for each modulus m_i $(1 \leq i \leq n)$, the subset $E_i=\{e_{i1}, e_{i2}, \ldots, e_{ik_i}\}$ of the error digits whose detection is guaranteed, where generally $k_i < m_i$. In addition recall that any error ΔI_X affecting the magnitude index is detectable, unless $\Delta I_X = \pm m_I$. This result is of interest, provided the subsets E_i include some important subclass of single residue digit errors. As an application it will be shown how single bit errors can be made detectable through this approach.

Let x_i^j and x_i^k be two residue digits modulo m_i whose binary code-words are b_i^j and b_i^k and suppose that $D(b_i^j,b_i^k)=1$, where $D(b_i^j,b_i^k)$ is the Hamming distance between b_i^j and b_i^k. If a single bit error alters b_i^j in b_i^k, the corresponding error digit is $e_i=|x_i^k-x_i^j|_{m_i}$. If $e_i \in E_i$, single bit error detection ensues. Assuming that the subsets E_i are of sufficient cardinality, it is generally possible to determine binary codes such that, for each pair of code-words b_i^j and b_i^k whose Hamming distance is one, the corresponding residue digits x_i^j and x_i^k satisfy the condition $e_i=|x_i^k-x_i^j|_{m_i} \in E_i$ [7].

As a further application, it is possible to derive conditions under which single bit errors affecting a nonredundant digit are not masked by the simultaneous occurrence of single bit errors in the magnitude index. Consider, for the sake of simplicity, the case where a single redundant modulus, m_{n+1}, is used to encode the magnitude index and assume $m_{n+1}=M_I \geq 2m_I$.

Let E_1, $E_2, \ldots, E_n$ be the subsets of detectable errors, as determined from application of Theorem 2. If the error digit $e_{ij} \in E_i$ affects the arbitrary number $\{X, (I_X)\}$, denote by $\Delta I_X(e_{ij})$ the difference $\overline{I}_{X,c}-I_{X,c}$ where $\overline{I}_{X,c}$ and $I_{X,c}$ are the magnitude indexes as recomputed from the nonredundant residue digits of the number in error and the correct number, respectively. Then e_{ij} is masked by the simultaneous occurrence of the error digit $e_{n+1} \equiv \Delta I_X(e_{ij}) \pmod{m_{n+1}}$ or of $e_{n+1} \equiv \Delta I_X(e_{ij}) + m_I \pmod{m_{n+1}}$ if the integer X is in overflow. Moreover, the combined effect of e_{ij} and e_{n+1} simulates an overflow if $e_{n+1} \equiv \Delta I_X(e_{ij}) - m_I \pmod{m_{n+1}}$. Any other error digit e_{n+1} affecting the magnitude index concurrently with the occurrence of error e_{ij} does not prevent error detection. Denote by $e_{n+1}(e_{ij})$ the multivalued function relating to e_{ij} the error digits which, for some X, masks e_{ij} when affecting the magnitude index, and let $E_1', E_2', \ldots, E_n', E_{n+1}'$ be the subsets of error digits with $E_i' \subseteq E_i$ $(1 \leq i \leq n)$ such that the following congruences never hold for any $e_{ij} \in E_i'$ and $e_{n+1,k} \in E_{n+1}'$:

a) $e_{n+1}(e_{ij}) \equiv e_{n+1,k} \pmod{m_{n+1}}$

b) $e_{n+1}(e_{ij}) \equiv e_{n+1,k} \pm m_I \pmod{m_{n+1}}$.

TABLE I

Binary encoding for residue digits modulo $m_2=67$

0)	0000000	17)	0000110	34)	0001111	51)	0001010
1)	0010010	18)	0010111	35)	0011011	52)	0011101
2)	0110101	19)	0111001	36)	0111100	53)	1110100
3)	1111000	20)	1111110	37)	1100110	54)	1101111
4)	1101010	21)	0000001	38)	0000100	55)	0001000
5)	0001110	22)	0010110	39)	0011111	56)	0011010
6)	0110010	23)	0110111	40)	0111011	57)	0111101
7)	1110101	24)	1111001	41)	1111100	58)	1100100
8)	1101000	25)	1101110	42)	0000011	59)	0000101
9)	0001001	26)	0001100	43)	0010100	60)	0011000
10)	0011110	27)	0110110	44)	0111111	61)	0111010
11)	1110010	28)	1110111	45)	1111011	62)	1111101
12)	1100101	29)	1101001	46)	1101100	63)	0000010
13)	0000111	30)	0001011	47)	0001101	64)	0010101
14)	0011001	31)	0011100	48)	0110100	65)	0111000
15)	0111110	32)	1110110	49)	1111111	66)	1111010
16)	1100010	33)	1100111	50)	1101011		

Binary encoding for residue digits modulo $m_5=21$

0)	00000	6)	01111	11)	00001	16)	01101
1)	00011	7)	11000	12)	00010	17)	01110
2)	00101	8)	11011	13)	00111	18)	11001
3)	00110	9)	11101	14)	01000	19)	11010
4)	01001	10)	11110	15)	01011	20)	11111
5)	01010						

If the binary encoding of residue digits is such that the subsets E'_1, E'_2, ..., E'_n, E'_{n+1} include all single bit errors, any two bit errors concurrently affecting one nonredundant digit and I_X are detectable.

Example 3. Consider the RNS with magnitude index of moduli $m_1=m_I=3$, $m_2=67$, $m_3=77$, $m_4=79$ and take $m_{n+1}=m_5=M_I=21$. The following error subsets satisfy the conditions of Theorem 2 and congruences a) and b) are never verified:

$E'_1=\{1,2\}$

$E'_2=\{3,4,5,12,13,20,21,22,28,29,30,37,38,39,45,46,47,53,54,62,63,64\}$

$E'_3=\{3,4,5,12,13,14,20,21,22,29,30,31,38,39,46,47,48,55,56,57,63,64,65,72,73,74\}$

$E'_4=\{1,6,8,13,15,20,22,27,29,31,34,36,38,41,43,45,48,50,52,57,59,64,66,71,73,78\}$

$E'_5=\{6,7,8,9,10,11,12,13,14,15\}$

For each modulus m_i binary codes can be found such that, for any pair of code-words b_i^j and b_i^k whose Hamming distance is one, the corresponding residue digits x_i^j and x_i^k satisfy the relation $|x_i^k-x_i^j|_{m_i} \in E_i$. For example, Table I shows the binary encoding for m_2 and m_5.

Given the number $X=\{85631, (I_X=0)\}=\{2,5,7,74, (0)\}$ from Table I it is seen that the code-word for the residue modulo m_2 is 0001110. Assume that a single bit error alters the code-word into 0001111 (code-word for $x_2=34$) and, at same time, a single bit error alters the code-word for the redundant digit from 00000 to 01000 whose corresponding residue value is 14 (see Table I). The number in error is then $X'=\{2,34,7,74, (14)\}=\{742595, (I'_X=14)\}$. Noting that $e_2=|34-5|_{67}= 29 \in E_2$ and $e_5=|14-0|_{21}=14 \in E_5$, error detection is possible. In fact, the recomputed magnitude index is $I'_{X,c}=1$ and since $I'_{X,c} \neq I'_X$, the error is detected. •

References

[1] A.Svoboda, "The numerical system of redundant classes in mathematical machines", Proc. Int. Conference on Information Processing, UNESCO, Paris 1959, pp 419-422.

[2] H.L.Garner, "The residue number system", IRE Trans. on Electronic Computers, vol EC-8, June 1959, pp 140-147.

[3] N.S.Szabo, R.I.Tanaka, "Residue arithmetic and its applications to computer technology", New York, McGraw-Hill, 1967.

[4] I.Ya.Akuŝkiĭ, D.I.Yudickiĭ, "Maŝinnaya arifmetika v ostatočnyh klassah", Sov. Radio Eng., Moscow, 1968.

[5] R.W.Watson, "Error detection and correction and other residue interacting operations in a redundant residue number system", 1965, PhD dissertation, University of California, Berkeley.

[6] S.Sik-Song Yau, Yu-Chang Liu, "Error correction in redundant residue number systems", IEEE Trans. on Computers, vol C-22, Jan. 1973, pp 5-11.

[7] F.Barsi, P.Maestrini, "Error correcting properties of redundant residue number systems", IEEE Trans. on Computers, vol C-22, March 1973.

[8] D.Mandelbaum, "Error correction in residue arithmetic", IEEE Trans. on Computers, vol C-21, June 1972, pp 538-545.

[9] F.Barsi, P.Maestrini, "Error detection and correction by product codes in residue number systems", paper accepted for publication on IEEE Trans. on Computers.