Error Correcting Properties of Redundant Residue Number Systems

FERRUCCIO BARSI AND PIERO MAESTRINI

Abstract—The error correcting properties of the redundant residue number systems (RRNS) are investigated through a more natural approach than was previously known. The necessary and sufficient condition for the correction of a given error affecting a single residue digit of any legitimate number in an RRNS is determined. The minimal redundancy allowing the correction of the whole class of the single residue digit errors is derived and an efficient procedure for error correction is given. Moreover, it is shown that a smaller redundancy and a single redundant modulus may allow the correction of certain important subclasses of single residue digit errors, e.g., the set of errors affecting a single bit in the code. Examples are given.

Index Terms—Arithmetic error codes, error detection and correction, residue arithmetic, residue codes, residue number systems.

I. INTRODUCTION

SINCE their introduction, the residue number systems (RNS) were considered a promising way to provide a very fast arithmetic. This idea was originated from the modular nature of the addition, subtraction, and multiplication in RNS, i.e., from the well-known property that the ith digit of the sum, difference, and product is exclusively dependent on the ith digits of the operands [1]. This property determines the potential high speed of the residue arithmetic, since carries and borrows are suppressed in the addition and subtraction and, furthermore, because the multiplication is executed in a single step by means of a modular hardware not dissimilar from the one implementing the addition.

However, such advantages of the residue arithmetic are neutralized by the very awkward nature of some operations, i.e., division, magnitude comparison, sign detection, additive and multiplicative overflow detection, which, conversely, are much simpler in positional systems.

Because of this, the interest has shifted toward the fault tolerance characteristics of RNS, for application in such cases where both transmission and computational errors are to be controlled.

In RNS, the error detecting and correcting capability is usually achieved by the addition of one or more redundant residue digits. The use of RNS for error detection or correction has some interesting advantages over the conventional arithmetic error codes based upon positional number systems as summarized by the following arguments.

Argument 1: In RNS, the modular nature of most arithmetic operations is naturally reflected by a modular organization of the arithmetic processor, where each digit of the representation is processed separately from the others by a dedicated module. As far as modular operations are individually tested, this fact implies that any failures localized in a single arithmetic module has a local effect; i.e., a single residue digit is altered. All errors in this class, or important subclasses thereof, are easily detected or corrected in RNS.

Argument 2: In RNS, the residue digits are not hierarchically ordered, as contrasted to positional number systems. This observation suggests that some kind of "graceful degradation" may be easily introduced in computers based upon RNS in the case of permanent faults affecting any determined number of residue digits. In fact, the faulty modules may be disconnected and the remaining modules redistributed between nonredundant and redundant digits, thus allowing an arbitrary compromise between lower precision and reduced error control capability.

Argument 3: Because of their nature, the arithmetic operations in RNS are most naturally realized by table lookup techniques, each residue digit requiring different tables. By storing such tables in appropriate memory devices (READ-MOSTLY memories or electrically alterable READ-ONLY memories), general purpose arithmetic modules are realized. This allows an easier application of the degradation techniques mentioned in Argument 2 and the introduction of a standby spare organization at low cost, since a general purpose spare module may replace any faulty module, by simply storing the appropriate tables.

The error detecting and correcting properties of RNS have been discussed to some extent in the literature [2]-[4], [6]. This paper, through a more natural approach to the problem, provides a deeper insight into the error correcting capabilities of RNS. In particular, the redundancy necessary and sufficient for single residue digit error correction is determined, and an efficient error correcting procedure is derived that directly operates on the residue representation of numbers. Mandelbaum [6] has found an equivalent condition for error correction in the case where two redundant moduli are used; however, his procedure for error correction operates on a positional (e.g., binary) representation of numbers and requires, for implementation, a separate positional processor. An alternative procedure, which also operates on the residue representation, has been presented by Watson [2]; however, it requires more redundancy than the method being presented.

Additionally, in this paper it is shown that the consideration of subsets of the set of single residue digit errors is also of interest, since certain important error classes (e.g., the errors effecting a single bit in the binary encoding of residue digits)

Manuscript received July 5, 1972; revised October 16, 1972.
The authors are with the Istituto di Elaborazione dell'Informazione, Consiglio Nazionale delle Ricerche, Pisa, Italy.

may be corrected with less redundancy and by the use of a single redundant modulus.

II. Definitions and Basic Properties

Given a set of n pairwise prime positive integers $m_1, m_2, \cdots, m_n$ called *moduli*, the nonnegative integers X in the range $[0, M)$, where $M = m_1 m_2 \cdots m_n$, are uniquely represented by the n-tuples $x_1, x_2, \cdots, x_n$ of their residues modulo m_i ($x_i = |X|_{m_i}, i = 1, 2, \cdots, n$). The set of the n-tuples and the interpretation function assigning to each n-tuple a natural number in the range $[0, M)$, and vice versa, are defined as the residue number system (RNS) of moduli $m_1, m_2, \cdots, m_n$.

Given an RNS of moduli $m_1, m_2, \cdots, m_n$ and an integer X in the range $[0, M)$, then the integer $X_i = |X|_{M/m_i}$ is defined as the *m_i-projection* of X [4]. More generally, the integer $X_P = |X|_{M/m_P}$, where $m_P = m_{i1} m_{i2} \cdots m_{ik}$, is defined as the *$m_P$-projection* of X.

The following theorem is straightforward.

Theorem 1: If $X \neq X_P$, the residue representations of X and X_P uniquely differ in one or more of the residue digits modulo $m_{i1}, m_{i2}, \cdots, m_{ik}$.

Proof: Since m_j ($m_j \neq m_{i1}, m_{i2}, \cdots, m_{ik}$) is a divisor of M/m_P and $X_P = |X|_{M/m_P}$, then $|X|_{m_j} = |X_P|_{m_j}$;[1] i.e., any pair of residue digits modulo m_j of X and X_P coincide. Moreover, assume that the remaining residue digits of X and X_P also coincide. Then, from $|X|_{m_i} = |X_P|_{m_i} (1 \leqslant i \leqslant n)$, it follows that $|X|_M = |X_P|_M$;[2] i.e., $X = X_P$. Since this contradicts the hypothesis, at least a pair of residue digits $|X|_{m_{is}}, |X_P|_{m_{is}}$ $(1 \leqslant s \leqslant k)$ are necessarily different.

This paper will be concerned with the redundant residue number systems (RRNS), representing the integers in the range $[0, M)$, where $M = \Pi_{i=1}^{n} m_i$, by the $(n + r)$-tuples of their residues modulo the $n + r$ pairwise prime moduli $m_1, m_2, \cdots, m_n, m_{n+1}, \cdots, m_{n+r}$. The moduli m_i and the residue digits x_i ($i = 1, 2, \cdots, n$) will be referred to as *nonredundant moduli* and *nonredundant digits*, respectively. The moduli m_k and the residue digits x_k ($k = n + 1, \cdots, n + r$) will be referred to as *redundant moduli* and *redundant digits*, respectively. The product of redundant moduli, $m_R = m_{n+1} m_{n+2} \cdots m_{n+r}$ is defined as the *redundant product*. The $(n + r)$-tuples representing the integers in the range $[0, M)$ are defined as *legitimate numbers*, while the $(n + r)$-tuples related to integers in the range $[M, Mm_R)$ are defined as *illegitimate numbers*. Theorem 2 immediately follows from the above definitions.

Theorem 2: The m_R-projection X_R of any number X in the range $[0, Mm_R)$ is a legitimate number.

Assume that a legitimate number X in a given RRNS is altered by an error effecting the single residue digit $x_i (1 \leqslant i \leqslant n + r)$. Then a different integer $\bar{X}$ will be generated; and, since $|X|_{m_j} = |\bar{X}|_{m_j}$ for any $m_j \neq m_i$, then also $|X|_{Mm_R/m_i} = |\bar{X}|_{Mm_R/m_i}$ [5] and the following equation holds for an appropriate integer p_i:

$$\bar{X} = X + p_i \frac{Mm_R}{m_i}.$$

The value of the residue digit in error is

$$\bar{x}_i = |\bar{X}|_{m_i} = \left| x_i + p_i \frac{Mm_R}{m_i} \right|_{m_i}.$$

The difference

$$e_i = |\bar{x}_i - x_i|_{m_i} = \left| p_i \frac{Mm_R}{m_i} \right|_{m_i}, \qquad (2\text{-}1)$$

which will be referred to as error digit, completely describes the error under consideration.

The following property [4], whose proof is omitted for the sake of brevity, will be used extensively in the following test.

Theorem 3: Let X be a legitimate number in the RRNS of moduli $m_1, m_2, \cdots, m_n, m_{n+1}, \cdots, m_{n+r}$, where $r \geqslant 1$. If $m_R > m_i$ ($i = 1, 2, \cdots, n$), then all integers $\bar{X}$ differing from X in a single residue digit $x_j (1 \leqslant j \leqslant n + r)$ are illegitimate numbers.

Incidentally, observe that Theorem 3 and the m_i-projections provide a very natural approach to deriving the well-known [2] error detecting properties of RRNS. In fact, in the hypothesis of Theorem 3, all errors effecting a single residue digit of a legitimate number X are detected by any procedure leading to the identification of illegitimate numbers. The identification may derive from the straightforward observation that a given integer X in the RRNS of moduli $m_1, m_2, \cdots, m_{n+r}$ is a legitimate number if and only if $X = X_R$; i.e., if the "consistency check" introduced by Watson [2] is verified.

III. Error Correction in RRNS

Once an integer $\bar{X}$ has been detected as being in error, other means are required to unambiguously determine the legitimate number X from which $\bar{X}$ was generated as a result of some machine failure, under the hypothesis of single residue digit errors. The basic properties leading to error location and correction are stated by the following theorems.

Theorem 4: Let $\bar{X}$ be an illegitimate number in the RRNS of moduli $m_1, m_2, \cdots, m_n, m_{n+1}, \cdots, m_{n+r}$. Then there exists a legitimate number X differing from $\bar{X}$ in the single residue digit x_i iff the m_i-projection $\bar{X}_i$ is a legitimate number.

Proof: The condition is sufficient since, by Theorem 1, $\bar{X}$ and $\bar{X}_i$ uniquely differ in the residue digit x_i. Then, the legitimate number $X = \bar{X}_i$ is a solution to the problem. In order to prove the necessity, assume that X is a legitimate number with $|X|_{m_j} = |\bar{X}|_{m_j}$ for $m_j \neq m_i$. Then $|X|_{Mm_R/m_i} = |\bar{X}|_{Mm_R/m_i}$ [5], i.e., $X_i = \bar{X}_i$. Since $X = X_i + p_i (Mm_R/m_i)$ for some nonnegative p_i, and X has been assumed legitimate, it follows that $\bar{X}_i = X_i$ is also legitimate.

Theorem 5: Under the hypothesis of Theorem 4 and if $m_R = \Pi_{j=1}^{r} m_{n+j} \geqslant m_i (1 \leqslant i \leqslant n + r)$, the legitimate number differing from $\bar{X}$ in the single residue digit x_i is unique.

Proof: Assume that X and X' are two different legitimate numbers, both differing from $\bar{X}$ in the single residue digit x_i.

[1] If a congruence holds modulo m, then it also holds modulo any divisor of m [5].

[2] If a congruence holds for several pairwise prime moduli, then it also holds for a modulus equal to their product [5].

From the hypothesis, $|X|_{Mm_R/m_i} = |X'|_{Mm_R/m_i}$; i.e., $X_i = X_i'$. Since $X = X_i + p_i(Mm_R/m_i)$ and $X' = X_i' + p_i'(Mm_R/m_i)$ for some nonnegative integers p_i and p_i', from the inequalities $0 \leqslant X < M, 0 \leqslant X' < M, 0 \leqslant X_i = X_i' < Mm_R/m_i, Mm_R/m_i \geqslant M$, it follows that $p_i = p_i' = 0$ and $X = X_i'$, thus contradicting the original assumption.

In the hypothesis of errors affecting single residue digits, from Theorems 4 and 5 it follows that any given illegitimate number $\bar{X}$ may be derived from *as many legitimate numbers as it has legitimate projections.* If the projections of $\bar{X}$ all are illegitimate, except the single m_i-projection $\bar{X}_i$ $(1 \leqslant i \leqslant n + r)$, then the wrong residue digit x_i is unambiguously determined. Once the error has been located in the residue digit x_i, error correction is immediate and unambiguous if $m_R \geqslant m_i$. In fact, the legitimate number $\bar{X}_i$ differs from $\bar{X}$ in the single residue digit x_i (Theorem 1). Then, by Theorem 5, $\bar{X}_i$ coincides with the legitimate number X, originating $\bar{X}$ by the effect of a single residue digit error.

Consider in an RRNS of moduli $m_1, m_2, \cdots, m_n, m_{n+1}, \cdots, m_{n+r}$, where $m_R \geqslant m_i$ $(1 \leqslant i \leqslant n + r)$, a legitimate number X and assume that a single error e_i $(1 \leqslant i \leqslant n + r)$ affects the residue digit x_i of X, thus originating (Theorem 3) an illegitimate number $\bar{X}$. In most cases, two or more projections of $\bar{X}$ may be legitimate, thus making the error localization impossible. As usually required, we shall restrict our consideration to the case where a given error e_i is correctable when affecting any legitimate number X. Then, in order to evaluate the error correcting capabilities of a given RRNS and to optimally define an RRNS with given error correcting capabilities, the following problems are to be solved.

Problem 1: Given an RRNS, determine, for each residue digit, the class of errors leading to illegitimate numbers $\bar{X}$ all of whose projections except one are illegitimate, when affecting any legitimate number X.

Problem 2: Given, for each residue digit, the class of errors whose correction is required, determine the smallest redundant product such that the errors of the given class originate illegitimate numbers $\bar{X}$ all of whose projections except one are illegitimate, when affecting a single residue digit of any legitimate number X.

The resolution of both problems is a consequence of the following theorem, whose proof is given in the Appendix.

Theorem 6: Assume that an error $e_i = |p_i Mm_R/m_i|_{m_i}$ $(1 \leqslant p_i \leqslant m_i - 1)$ affects the single residue digit x_i $(1 \leqslant i \leqslant n + r)$ of any legitimate number X in the RRNS of moduli $m_1, m_2, \cdots, m_n, m_{n+1}, \cdots, m_{n+r}$, where $m_R = \Pi_{s=1}^{r} m_{n+s} \geqslant m_k$ $(1 \leqslant k \leqslant n + r)$, thus originating an illegitimate number $\bar{X}$. Then, for any X, the projection $\bar{X}_j$ $(j \neq i, 1 \leqslant j \leqslant n + r)$ is illegitimate if and only if the following inequality holds:

$$m_R \geqslant \frac{m_i m_j}{|\pm p_i m_j|_{m_i}}. \tag{3-1}$$

From Theorem 6, the determination of the class of errors whose correction is possible in a given RRNS is immediate, as stated by the following corollary, whose proof is straightforward.

Corollary 1: The error $e_i = |p_i Mm_R/m_i|_{m_i}$, affecting the residue digit x_i $(1 \leqslant i \leqslant n + r)$ of any legitimate number X in the RRNS of moduli $m_1, m_2, \cdots, m_n, m_{n+1}, \cdots, m_{n+r}$, where $m_R > m_k$ $(1 \leqslant k \leqslant n + r), r \geqslant 2$, is correctable if inequality (3-1) holds for every $j \neq i$.

Note that the additional hypothesis $r \geqslant 2$ has been added to point out that inequality (3-1) cannot hold for $j = n + 1$ if $r = 1$, since in this case $m_R = m_j = m_{n+1}$.

The problem of the optimal definition of an RRNS with an assigned error correcting capability has been discussed in the literature, assuming that the class of the errors to be corrected coincides with the whole set of the single residue digit errors. A further contribution in this assumption is given in Section IV. In Sections V and VI it is assumed that the class of errors to be corrected coincides with an important subset of the set of single residue digit errors (i.e., the errors affecting a single bit of the binary encoding of the residue digits), and it is shown that, in this hypothesis, considerable error correcting capabilities may be retained with much less redundancy.

IV. An Efficient Procedure for Single Residue Digit Error Correction

The redundancy necessary and sufficient to allow the correction of the whole class of the single residue digit errors is easily derived from the following theorem.

Theorem 7: Assume that, in an RRNS of moduli $m_1, m_2, \cdots, m_n, m_{n+1} \cdots, m_{n+r}$, an arbitrary illegitimate number $\bar{X}$ is given such that the m_i-projection $\bar{X}_i$ is legitimate, where i is also arbitrary. Then the m_j-projections $(j \neq i, 1 \leqslant j \leqslant n + r)$ all are illegitimate if and only if $r \geqslant 2, m_R \geqslant \max(m_i m_j)$.

Proof: Given the illegitimate number $\bar{X}$, assume that the m_i-projection $\bar{X}_i$ $(1 \leqslant i \leqslant n + r)$ is legitimate. Then $\bar{X} = \bar{X}_i + p_i(Mm_R/m_i)$ may be assumed as originated by the single residue digit error $e_i = |p_i Mm_R/m_i|_{m_i}$ affecting the legitimate number $\bar{X}_i$. Since $\bar{X}$ is arbitrary and $\bar{X} \neq \bar{X}_i, p_i$ may be any integer in the range $[1, m_i - 1]$. As stated by Theorem 6, the m_j-projection $\bar{X}_j$ $(j \neq i, i \leqslant j \leqslant n + r)$ is illegitimate if and only if the inequality (3-1) holds. Since p_i ranges in the complete system of residues modulo m_i, except the number zero, and m_i, m_j are relatively prime, the expression $|\pm p_i m_j|_{m_i}$ also ranges in the same system of residues [5], except the number zero. Then, for appropriate p_i, the expression $|\pm p_i m_j|_{m_i}$ equals 1 and inequality (3-1) becomes

$$m_R \geqslant m_i m_j, \quad j \neq i, \quad 1 \leqslant j \leqslant n + r. \tag{4-1}$$

Since the subscripts are arbitrary, (4-1) may be restated as $m_R \geqslant \max(m_i m_j)$. The additional hypothesis $r \geqslant 2$ points out that (4-1) cannot hold for $j = n + 1$ if $r = 1$; i.e., $m_R = m_{n+1}$.

Equation (4-1) also states the minimal redundancy allowing the correction of the whole class of the single residue digit errors. In fact, if $m_R \geqslant \max(m_i m_j)$ and an arbitrary single residue digit error e_i affects any legitimate number X, an illegitimate number $\bar{X}$ is originated, whose m_i-projection $\bar{X}_i$ is legitimate and equals X (Theorems 4 and 5), while $\bar{X}_j$ is illegitimate for every $j \neq i$; thus making the error correction unambiguous.

An equivalent result, for the case where $r = 2$, has recently been derived by Mandelbaum [6]. However, the theory based upon the m_i-projections presented above also suggests an efficient procedure for error correction, which operates on the residue representation of the numbers and makes exclusive use of the modular operations provided by a residue arithmetic processor. This contrasts with Mandelbaum's procedure, which requires for implementation a separate positional (e.g., binary) processor. The procedure being presented also compares favorably with the alternative method known from the literature [2], based upon base extension and table lookup. In fact, this method generally implies the use of more redundancy than stated by theorem 7, since most values of m_R in the range $[\max(m_i m_j), 2\max(m_i m_j))$ are to be discarded.

The procedure for error correction is the following.

Phase 1: Given the number $\bar{X} = \{\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_i, \cdots, \bar{x}_{n+r}\}$ to be tested, its m_i-projection $(1 \leqslant i \leqslant n + r)$ is first determined by base extension [1]; i.e., the residue digit $\bar{x}_i^*$ is computed from the digits $\bar{x}_j$ $(j \neq i)$ such that $\bar{X}_i = \{\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_i^*, \cdots, \bar{x}_{n+r}\}$ falls in the range $[0, Mm_R/m_i)$. The base extension procedure is carried out by considering the residue digits as follows: a) the nonredundant digits, except $\bar{x}_i$ if $i \leqslant n$, in an arbitrary order (at the end of this step, the intermediate result is saved for subsequent use); 2) the redundant digits, except $\bar{x}_i$ if $i > n$, in an arbitrary order; and 3) the digit x_i. This phase of the error correction procedure requires $2(n + r) - 1$ modular operations in the worst case.

Phase 2: Phase 1 yields a mixed-radix [1] representation for $\bar{X}_i$ of the form

$$\bar{X}_i = a_0 + a_1 m_1 + a_2 m_1 m_2 + \cdots + a_{n-1} \prod_{j=1}^{n-1} \cdot m_j + \cdots + a_{n+r-1} \prod_{j=1}^{n+r-1} m_j \quad (4\text{-}2)$$

where $0 \leqslant a_k < m_k$ $(1 \leqslant k < n + r)$ and $a_{n+r-1} = 0$. The subscripts of the moduli are placed according to the ordering established in Phase 1. Two cases are to be considered.

Case a: If $i > n$, the ordering of the modules guarantees that $\bar{X}_i < M$ if and only if $a_k = 0$ for $k \geqslant n$ in (4-2). Then, in this case, the magnitude evaluation of $\bar{X}_i$ is carried out without any further arithmetic.

Case b: If $i \leqslant n$, (4-2) does not allow direct evaluation of $\bar{X}_i$ against M, since the multipliers of a_k do not include the legitimate modulus m_i for any k. Then a mixed-radix conversion procedure is resumed from the step computing a_{n-1} by utilizing, for initialization, the intermediate result saved during Phase 1. In this procedure, the recomputed digit x_i^* is considered first, and the redundant digits follow in any order. The final result is a mixed-radix representation for $\bar{X}_i$, where the multipliers of a_k are divided by M for $k \geqslant n$. Thus, $\bar{X}_i < M$ if and only if $a_k = 0$ for $k \geqslant n$. This additional phase of the error correcting procedure requires $2(r + 1)$ modular operations in the worst case.

Phase 3: Phases 1 and 2 are iterated for different i until a legitimate m_i-projection is found. If $\bar{X}_i < M$, the correct number $X = \bar{X}_i$ is unambiguously determined under the hypothesis of single residue digit errors, and the procedure stops. In fact the hypothesis that two or more m_i-projections are legitimate is excluded by Theorem 7, unless $\bar{X} = X$ is legitimate; in this case $\bar{X}_i = \bar{X} = X$ for any i, and the procedure keeps its validity. If the m_i-projections all are illegitimate, the number $\bar{X}$ is recognized as illegitimate, but it cannot originate from any single residue digit error affecting a legitimate number; thus the error correction is impossible.

Example 1: Given the RRNS of moduli $m_1 = 11$, $m_2 = 16$, $m_3 = 17$, $m_4 = 3$, $m_5 = 7$, $m_6 = 13$, where $M = m_1 m_2 m_3 = 2992$, $m_R = m_4 m_5 m_6 = 273$ (observe that $\max(m_i m_j) = m_2 m_3 = 272 < m_R$), assume that the number $\bar{X} = 359\,070 = \{8, 14, 13, 0, 5, 10\}$ is given. The m_i-projections are computed in any sequence (e.g., $i = 1, 2, 3, \cdots, 6$) until a legitimate $\bar{X}_i$ is found. Actually, $\bar{X}_1 = 62\,046 > M$; $\bar{X}_2 = 1713 < M$. Then $\bar{X}$ is illegitimate; the correct number is $X = \bar{X}_2 = 1713 = \{8, 1, 13, 0, 5, 10\}$.

V. Correction of Single-Bit Errors by the Use of Two or More Redundant Moduli

A condition under which a single residue digit error e_i is correctable, when affecting an arbitrary legitimate number X, has been given in Corollary 1. As an immediate consequence, the redundancy necessary to correct a given subclass of the class of the single residue digit errors is determined, and it is verified that such redundancy may be less than that required to achieve the error correcting capability extended to the whole class of single digit errors.

In fact, given an RRNS of moduli $m_1, m_2, \cdots, m_n, m_{n+1}, \cdots, m_{n+r}$, where $r \geqslant 2$, assume that $E_i = \{e_i^1, e_i^2, \cdots, e_i^h\}$, $(1 \leqslant i \leqslant n + r, h < m_i - 1)$, is a subset of the set of the errors that may affect the ith residue digit, and again take $e_i^k = |p_i^k Mm_R/m_i|_{m_i}$. If $|\pm p_i^k m_j|_{m_i} \neq 1$ for each e_i^k in E_i and for every $m_j \neq m_i$, then the right member of inequality (3-1) becomes

$$\frac{m_i m_j}{|\pm p_i^k m_j|_{m_i}} < m_i m_j \quad (5\text{-}1)$$

and from Corollary 1 it follows that a redundant product $m_R < m_i m_j$ is sufficient to correct the errors in E_i. If this reasoning is iterated for all m_i $(i = 1, 2, \cdots, n + r)$, it is concluded than an RRNS with $r \geqslant 2$, $m_R < \max(m_i m_j)$ may allow the correction of the single residue digit errors in the subclass $\{E_1, E_2, \cdots, E_{n+r}\}$.

If the subsets E_i are assumed nonvoid for all i, a lower bound for the redundant product allowing the correction of the errors in the above defined subclass is also found. In fact, for each $e_i = |p_i Mm_R/m_i|_{m_i}$, the pair of values yielded by the expression $|\pm p_i m_j|_{m_i}$ is complementary modulo m_i. If the smaller of such values is denoted by y, then $y \leqslant m_i/2$ and the condition of Corollary 1 becomes $m_R \geqslant 2m_j$ $(j \neq i)$; or, equivalently, since i and j are arbitrary, $m_R \geqslant 2\max(m_k)$, where $1 \leqslant k \leqslant n + r$. This proves that any RRNS allowing the correction of the errors in $\{E_1, E_2, \cdots, E_{n+r}\}$, where E_i is nonvoid for each i, also allows the detection of the whole class of single residue digit errors.

The existence of RRNS where $m_R < \max(m_i m_j)$, whose error correction capability is limited to a subclass of the set of the single residue digit errors, is of interest provided that the

TABLE I

0	0000	8	1000
1	0111	9	1111
2	1110	10	0110
3	0101	11	1101
4	1100	12	0100
5	0011	13	1011
6	1010	14	0010
7	0001	15	1001

TABLE II

0	0000	8	1100
1	0001	9	1101
2	0011	10	1111
3	0010	11	1110
4	0100	12	1000
5	0101	13	1001
6	0111	14	1011
7	0110	15	1010

TABLE III

0	0000000	23	1100000	46	0100000
1	0010000	24	1110000	47	0110000
2	0100100	25	0000100	48	1100100
3	0110100	26	0010100	49	1110100
4	1101110	27	0101110	50	0001110
5	0000001	28	1100001	51	0100001
6	0010001	29	1110001	52	0110001
7	0100101	30	0000101	53	1100101
8	0110101	31	0010101	54	1110101
9	1101100	32	0101100	55	0001100
10	0000011	33	1100011	56	0100011
11	0010011	34	1110011	57	0110011
12	0100111	35	0000111	58	1100111
13	0110111	36	0010111	59	1110111
14	1101101	37	0101101	60	0001101
15	0000010	38	1100010	61	0100010
16	0010010	39	1110010	62	0110010
17	0101011	40	0001011	63	1101011
18	0111011	41	0011011	64	1111011
19	1101111	42	0101111	65	0001111
20	0000110	43	1100110	66	0100110
21	0010110	44	1110110	67	0110110
22	0101010	45	0001010	68	1101010

correctable errors coincide or include some important class of errors. As an example, we shall consider the case when the subclass under consideration includes the set of errors affecting a single bit in the binary code of the residue digits. In fact, under a very general hypothesis, it can be assumed that these are the errors whose probability is the highest. A procedure for the optimal determination of an RRNS allowing the correction of the single-bit errors will be given later in this Section.

Let c_i^j and c_i^k be two words in the binary code of the ith residue digit, whose Hamming distance is one [this will be denoted by $D(c_i^j, c_i^k) = 1$], and x_i^j and x_i^k, respectively, the residues coded by c_i^j and c_i^k. Then, a fault altering c_i^j in c_i^k determines a single-bit error $e_i^{j,k}$ whose correction is possible if

$$e_i^{j,k} = |x_i^k - x_i^j|_{m_i} \in E_i. \tag{5-2}$$

Thus, the subsets E_i of the errors whose correction is possible include all the errors affecting a single bit in the binary code of the ith digit, provided that a code of $n_i = \ulcorner \log_2 m_i$ bits[3] may be found, by which the relation (5-2) is satisfied for all pairs c_i^j, c_i^k, such that $D(c_i^j, c_i^k) = 1$.

[3] If $n_i > \ulcorner \log_2 m_i$, the problem has a trivial solution, since a code may be selected where there exist no pairs c_i^j, c_i^k such that $D(c_i^k, c_i^k) = 1$.

The existence of binary codes with such property is dependent upon the particular subset E_i under consideration. A number of conditions under which such codes exist have been determined [7]. In particular, solutions are found under very general hypotheses if the cardinality of E_i is not smaller than $2n_i$, although a smaller cardinality is sufficient if particular moduli are considered. Examples of encodings are given in Tables I-III.

Given an RRNS of moduli $m_1, m_2, \cdots, m_n, m_{n+1}, \cdots, m_{n+r}$, where $r \geqslant 2$, $m_R < \max(m_i m_j)$, such that the errors in the subclass $\{E_1, E_2, \cdots, E_{n+r}\}$ are correctable, the error correcting procedure substantially coincides with the one given in Section IV, as summarized below.

Phase 1: Given an illegitimate member $\bar{X}$, the m_i-projections $\bar{X}_i$ $(1 \leqslant i \leqslant n + r)$ are first computed as explained in Section IV.

Phase 2: The m_i-projections are evaluated as in Section IV.

Phase 3: If the m_i-projection $\bar{X}_i$ is legitimate and the m_j-projections $\bar{X}_j$ $(j \neq i, 1 \leqslant j \leqslant n + r)$ all are illegitimate, the correct number $X = \bar{X}_i$ is immediately determined. If either no legitimate m_i-projection is found, or two or more legitimate

m_i-projections exist, the error correction is not possible.

Example 2: Assume that the RRNS of moduli $m_1 = 11, m_2 = 16$, $m_3 = 17$, $m_4 = 7$, $m_5 = 23$ is given, where $M = m_1 m_2 m_3 = 2992$, $m_R = m_4 m_5 = 161$. Observe that M is the same as in Example 1, while $m_R < \max(m_i m_j) = m_2 m_3 = 272$. The subsets of the correctable errors E_i are determined as

$$E_1 = \{3,4,5,6,7,8\}$$

$$E_2 = \{2,4,7,8,9,12,14\}$$

$$E_3 = \{2,4,5,6,7,10,11,12,13,15\}$$

$$E_4 = \{1,2,3,4,5,6\}$$

$$E_5 = \{1,6,7,8,9,11,12,14,15,16,17,22\}.$$

The binary encoding of the residue digits modulo m_2 is given in Table I. This code satisfies the previously discussed requirements for single-bit error correction. Binary codes with the same property are easily determined for the remaining moduli and are omitted for the sake of brevity.

Let us consider the legitimate number $X = 125 = \{4,13,6,6,10\}$: from Table I it is seen that the binary code for $x_2 = 13$ is 1011. Assume that a single-bit error affects the residue digit modulo 16, which then becomes 1111. The illegitimate number $\bar{X} = 120\,553 = \{4,9,6,6,10\}$ is thus obtained. The m_i-projections of $\bar{X}$ are

$$\bar{X}_1 = 32\,969;\quad \bar{X}_2 = 125;\quad \bar{X}_3 = 7209;$$

$$\bar{X}_4 = 51\,737;\quad \bar{X}_5 = 15\,833.$$

Since only $\bar{X}_2$ is legitimate, the error is correctable; $X = \bar{X}_2 = 125$ is the correct number.

Example 3: Consider again the RRNS and the binary encoding defined in Example 2. Assume that, given the legitimate number $X = 125$ (where again $x_2 = 1011$), a multiple-bit error affects the residue digit modulo 16, which becomes 0010. The illegitimate number $\bar{X} = 90\,446 = \{4,14,6,6,10\}$ is thus obtained, whose m_i-projections are

$$\bar{X}_1 = 2862;\quad \bar{X}_2 = 125;\quad \bar{X}_3 = 5438;$$

$$\bar{X}_4 = 21\,630;\quad \bar{X}_5 = 6670.$$

Since both $\bar{X}_1$ and $\bar{X}_2$ are legitimate, the error correction is not possible.

In order to optimally define an RRNS with single-bit error correcting capability, the following procedure may be used.

Step 1: Consider a set of t pairwise relatively prime moduli. This set includes both the nonredundant and redundant moduli, although the partition is still undetermined. As a first step for each modulus m_i $(1 \leqslant i \leqslant t)$ and for each integer p_i^k in the range $[1, m_i - 1]$, determine the smallest integer $m_{R,i}^k$ such that the inequality

$$m_{R,i}^k \geqslant \frac{m_i m_j}{\left| \pm p_i^k\, m_j \right|_{m_i}} \tag{3-1}$$

holds for every $m_j \neq m_i$ $(1 \leqslant j \leqslant t)$. For each modulus m_i, the integers $m_{R,i}^k$ defined above determine a partial ordering in the set of the integers p_i^k $(1 \leqslant p_i^k \leqslant m_i - 1)$, p_i^{k1} being defined as not being a successor to p_i^{k2} if $m_{R,i}^{k1} \leqslant m_{R,i}^{k2}$.

Step 2: For each m_i, the required cardinality of E_i, denoted card (E_i), is estimated [e.g., card $(E_i) = 2\lceil \log_2 m_i \rceil$ such that the existence of a binary encoding with the above discussed property is possible. Then, a subset P_i of the set of the integers p_i^k is defined such that card (P_i) = card (E_i) and such that any p_i^k in P_i is not a successor to any p_i^h not in P_i. Taking an integer $p_i^f \in P_i$ such that any $p_i^k \in P_i$ is not a successor to p_i^f, consider for subsequent use the integer $m_{R,i}^f$.

Step 3: Determine the largest of the integers $m_{R,i}^f$, denoted m_R^f $(1 \leqslant i \leqslant t)$. Then consider the subsets of the given set of moduli such that each subset contains two or more moduli, and select among them the subset S_R such that the product of the moduli in S_R, denoted by m_R, is not smaller than m_R^f and such that the product of the moduli in any other considered subset is either smaller than m_R^f or larger than m_R. The moduli in S_R are assumed to be redundant moduli; the remaining moduli are assumed to be nonredundant. The product of the nonredundant moduli is again denoted by M. An RRNS is thus completely defined.

Step 4: The error digit $e_i^k = \left| p_i^k M m_R / m_i \right|_{m_i}$ is computed; from Theorem 6 it follows that e_i is correctable in the above defined RRNS. If the computation of e_i^k is iterated for each p_i^k in P_i and for all i, a subclass $\{E_1, E_2, \cdots, E_t\}$ of correctable errors is defined.

Step 5: For each residue digit, a binary code is determined such that relation (5-2) holds for all pairs c_i^j, c_i^k in the code such that $D(c_i^j, c_i^k) = 1$. If such a code cannot be determined for some m_i, the procedure is iterated from Step 2 with a better estimate of card (E_i).

VI. Correction of Single-Bit Errors by the Use of a Single Redundant Modulus

As far as subclasses of the single residue digit errors are considered (e.g., the errors affecting a single bit in the code), Theorem 6 suggests a different procedure for error correction, by which the requirement of two or more redundant moduli is removed.

In fact, given an RRNS of $n + 1$ moduli, where $m_R = m_{n+1}$, $m_R > m_k$ $(1 \leqslant k \leqslant n)$, assume that an error $e_i = \left| p_i M m_{n+1} / m_i \right|_{m_i}$ affects a nonredundant digit x_i of an arbitrary legitimate number X. If the hypothesis of Theorem 6 is verified for $m_j \neq m_i$ ranging in the nonredundant subset of moduli $(1 \leqslant j \leqslant n)$, then the m_j-projections $\bar{X}_j$ are illegitimate, while the m_i-projection $\bar{X}_i$ is legitimate. Moreover, since, as previously observed, (3-1) cannot be satisfied for $j = n + 1$, the m_{n+1}-projection $\bar{X}_{n+1}$ is also legitimate. Since two legitimate projections are found (i.e., $\bar{X}_i$ and $\bar{X}_{n+1}$), the error localization is ambiguous, unless it can be established by a different means that the error does not affect the redundant digit.

This discrimination is again derived from Theorem 6 since any error $e_{n+1} = \left| p_{n+1} M \right|_{m_{n+1}}$ affecting the redundant residue digit, and such that (3-1) is verified for each $j \leqslant n$, originates an illegitimate number $\bar{X}$ whose m_j-projections $(j \leqslant n)$ all are illegitimate, while the single m_{n+1}-projection X_{n+1} is legitimate.

The above arguments are summarized by the following.

Corollary 2: Given an RRNS of moduli $m_1, m_2, \cdots, m_n, m_{n+1}$ where $m_R = m_{n+1} > m_k$ $(1 \leqslant k \leqslant n)$, the error $e_i = |p_i M m_R / m_i|_{m_i}$ affecting the residue digit x_i $(1 \leqslant i \leqslant n+1)$ of an arbitrary legitimate number X is correctable if the inequality

$$m_R \geqslant \frac{m_i m_j}{|\pm p_i m_j|_{m_i}}$$

holds for every $j \neq i$, $1 \leqslant j \leqslant n$.

Assume that for each modulus m_i $(1 \leqslant i \leqslant n+1)$ a subset E_i of error digits is given such that the hypothesis of Corollary 2 holds for every e_i in E_i. Thus, as far as our consideration is limited to the single residue digit error in the subclass $\{E_1, E_2, \cdots, E_{n+1}\}$, the following procedure may be used for error correction.

1) Given an illegitimate number $\bar{X}$, the m_i-projections $\bar{X}_i$ are computed.

2) The m_i-projections are evaluated.

3) If the single m_{n+1}-projection $\bar{X}_{n+1}$ is legitimate, the error is localized in the redundant digit and $X = \bar{X}_{n+1}$ is the correct number. If two legitimate projections are found, i.e., $\bar{X}_{n+1}$ and $\bar{X}_i$ $(1 \leqslant i \leqslant n)$, the error is assumed to affect the nonredundant digit x_i and $X = \bar{X}_i$ is the correct number. If three or more legitimate projections are found, the error correction is not possible in the given RRNS.

As compared with the case where two or more redundant moduli are available, this procedure may allow the same or a wider error correcting capability by the use of a smaller redundancy, because lesser constraints exist in the choice of m_R. However, if an error e_{n+1} occurs, which is not an element of E_{n+1}, an illegitimate number $\bar{X}$ having two legitimate projections, $\bar{X}_{n+1}$ and $\bar{X}_i$ $(1 \leqslant i \leqslant n)$, may be originated, and a wrong correction may follow. This is the main drawback to the above procedure; although it is not different in principle from the possibility of a wrong correction in the use of any procedure for single residue digit error correction if an error affecting multiple residue digits occurs.

The preceding procedure may again be used for the correction of the class of the errors affecting a single bit in the binary code of the residue digits. An RRNS with such error correcting capability is optimally defined by a procedure that is not dissimilar from the one derived in Section V when two or more moduli are used, as sketched below.

Step 1: Assume that the subset of the nonredundant moduli $m_1, m_2, \cdots, m_t$ is given, and denote by $M = \Pi_{i=1}^{t} m_i$ the range of the legitimate numbers. For each modulus m_i $(1 \leqslant i \leqslant t)$ a subset P_i and an integer $m_{R,i}^f$ are defined, as explained in the procedure of Section V, Steps 1 and 2.

Step 2: Define $m_R = m_{t+1}$ as the smallest positive integer, pairwise prime with any given m_i such that $m_R > \max(m_{R,i}^f)$, $(1 \leqslant i \leqslant t)$. Then, determine the subset P_R of the positive integers modulo m_R such that the hypothesis of Corollary 2 holds for each element of P_R.

Step 3: From the subsets $P_1, P_2, \cdots, P_t, P_R$, and by the use of the relation $e_i = |p_i M m_R / m_i|_{m_i}$, the subclass $\{E_1, E_2, \cdots, E_t, E_R\}$ is determined. The errors in this subclass are correctable in the RRNS of moduli $m_1, m_2, \cdots, m_t, m_R$.

Step 4: For each residue digit, a binary code is determined such that the relation (5-2) holds for all pairs c_i^j, c_i^k in the code such that $D(c_i^j, c_i^k) = 1$. If the encoding is unsuccessful for the redundant modulus, a larger m_R is selected and the procedure is resumed from Step 2. If the encoding is unsuccessful for some nonredundant m_i, a better estimate is attempted for card (E_i), and the procedure is iterated from Step 1.

Example 4: Assume that the RRNS of moduli $m_1 = 11$, $m_2 = 16$, $m_3 = 17$, $m_4 = 69$ is given, where $M = m_1 m_2 m_3 = 2992$, $m_R = m_4$. Observe that M is the same as in the previous examples, while m_R is smaller. The subsets of the correctable errors are determined as

$E_1 = \{1,2,5,6,9,10\}$

$E_2 = \{1,3,4,8,12,13,15\}$

$E_3 = \{3,4,7,8,9,10,13,14\}$

$E_4 = \{1,5,6,15,19,23,25,26,30,39,43,44,46,50,54,63,64,68\}$.

The binary encoding of the residue digits modulo m_2 and m_4 are given in Tables II and III. Such codes satisfy the requirements for single-bit error correction. Binary codes with the same property are easily determined for the remaining moduli and are omitted for the sake of brevity.

Let us consider the legitimate number $X = 125 = \{4,13,6,56\}$. From Table II it is seen that the binary code for $x_2 = 13$ is 1001. Assume that a single-bit error affects the residue digit x_2, which is altered in 1000. The illegitimate number $\bar{X} = 116\,252 = \{4,12,6,56\}$ is thus obtained.

The m_i-projections of $\bar{X}$ are

$$\bar{X}_1 = 3444; \quad \bar{X}_2 = 125; \quad \bar{X}_3 = 6956; \quad \bar{X}_4 = 2556.$$

Since two legitimate projections are found, the error is correctable; $X = \bar{X}_2 = 125$ is the correct number.

Example 5: Again consider the RRNS and the binary encodings of Example 4. Given the legitimate number $X = 125 = \{4,13,6,56\}$, from Table III it is seen that the binary code for $x_4 = 56$ is 0100011. Assume that a single-bit error affects the residue digit x_4, which is altered in 1100011. The illegitimate number $\bar{X} = 137\,757 = \{4,13,6,33\}$ is thus obtained.

The m_i-projections of $\bar{X}$ are

$$\bar{X}_1 = 6381; \quad \bar{X}_2 = 8727; \quad \bar{X}_3 = 4173; \quad \bar{X}_4 = 125.$$

Since the single m_4-projection is legitimate, the error is correctable; $X = \bar{X}_4 = 125$ is the correct number.

Appendix

Proof of Theorem 6

In order to prove that inequality (3-1) is necessary, assume that the residue digit x_i of an arbitrary legitimate number X is affected by the error e_i, thus originating (Theorem 3) the illegitimate number $\bar{X}$ whose projection $\bar{X}_j$ $(j \neq i)$ is illegitimate. Since the residue digits of $X = \bar{X}_i$ and $\bar{X}$ coincide, except for the single digit x_i, $\bar{X}_i$ and $\bar{X}$ are congruent modulo $M m_R / m_i$, i.e.,

$$\bar{X} = \bar{X}_i + p_i \frac{Mm_R}{m_i}, \qquad 1 \leqslant p_i < m_i. \tag{A-1}$$

Similarly, for the projection $\bar{X}_j$ $(1 \leqslant j \leqslant n + r, j \neq i)$ there exists an appropriate p_j such that

$$\bar{X} = \bar{X}_j + p_j \frac{Mm_R}{m_j}, \qquad 0 \leqslant p_j < m_j. \tag{A-2}$$

By the hypothesis, and observing that the existence of an illegitimate $\bar{X}_j$ implies $m_R > m_j$,

$$0 \leqslant \bar{X}_i \leqslant M - 1; \quad M \leqslant \bar{X}_j \leqslant \frac{Mm_R}{m_j} - 1 \tag{A-3}$$

and, by combination of inequalities (A-3),

$$0 < \bar{X}_j - \bar{X}_i < Mm_R/m_j. \tag{A-3$'$}$$

Replacing in (A-3′) the difference $\bar{X}_j - \bar{X}_i$ derived from (A-1) and (A-2),

$$0 < p_i \frac{Mm_R}{m_i} - p_j \frac{Mm_R}{m_j} < \frac{Mm_R}{m_j},$$

that is,

$$0 < p_i m_j - p_j m_i < m_i,$$

or, equivalently,

$$p_i m_j - p_j m_i = |p_i m_j|_{m_i}. \tag{A-4}$$

The combination of (A-1), (A-2), and (A-4) gives

$$\bar{X}_j = \bar{X}_i + p_i \frac{Mm_R}{m_i} - p_j \frac{Mm_R}{m_j} = \bar{X}_i + \frac{Mm_R}{m_i m_j} |p_i m_j|_{m_i}. \tag{A-5}$$

Substituting for $\bar{X}_j$ in the inequalities (A-3),

$$\bar{X}_i \geqslant M - \frac{Mm_R}{m_i m_j} |p_i m_j|_{m_i} \tag{A-6$'$}$$

$$\bar{X}_i \leqslant \frac{Mm_R}{m_j} - \frac{Mm_R}{m_i m_j} |p_i m_j|_{m_i} - 1. \tag{A-6$''$}$$

The inequalities (A-6′) and (A-6″) are necessarily true if $\bar{X}_i$ is legitimate and $\bar{X}_j$ is illegitimate. Since $\bar{X}_i = X$ is an arbitrary integer in the range $[0, M - 1]$, replace the appropriate extreme of this range in (A-6′) and (A-6″) as follows:

$$\frac{Mm_R}{m_i m_j} |p_i m_j|_{m_i} \geqslant M \tag{A-7$'$}$$

$$\frac{Mm_R}{m_i m_j} |p_i m_j|_{m_i} \leqslant \frac{Mm_R}{m_j} - M. \tag{A-7$''$}$$

Then for m_R the following inequalities hold:

$$m_R \geqslant \frac{m_i m_j}{|p_i m_j|_{m_i}} \tag{A-8$'$}$$

$$m_R \geqslant \frac{m_i m_j}{m_i - |p_i m_j|_{m_i}}, \tag{A-8$''$}$$

i.e., more symmetrically

$$m_R \geqslant \frac{m_i m_j}{|\pm p_i m_j|_{m_i}}.$$

This proves the necessity of the condition of Theorem 6. The sufficiency is proved by contradiction. Assume that the inequalities (A-8′) and (A-8″) hold, i.e.,

$$m_R \geqslant \frac{m_i m_j}{|\pm p_i m_j|_{m_i}}$$

and that an error affecting the single residue digit x_i $(1 \leqslant i \leqslant n + r)$ of a legitimate number X originates an illegitimate number $\bar{X}$, whose projection $\bar{X}_j$ is legitimate. As stated by Theorem 3, the projection X_i is also legitimate. From the inequalities $0 \leqslant X_i < M$, $0 \leqslant X_j < M$ and since, by the hypothesis, $m_R \geqslant m_j$, we obtain

$$-Mm_R/m_j \leqslant -M < \bar{X}_j - \bar{X}_i < M \leqslant Mm_R/m_i. \tag{A-9}$$

From the combination of (A-1) and (A-2),

$$\bar{X}_j - \bar{X}_i = p_i \frac{Mm_R}{m_i} - p_j \frac{Mm_R}{m_j}. \tag{A-10}$$

If $\bar{X}_j - \bar{X}_i > 0$, (A-4) is again derived, and, since

$$p_i \frac{Mm_R}{m_i} - \frac{Mm_R}{m_j} p_j < M,$$

the following inequality is derived:

$$m_R < \frac{m_i m_j}{|p_i m_j|_{m_i}},$$

which contradicts the original assumption.

If $\bar{X}_j - \bar{X}_i < 0$, we derive from inequality (A-9)

$$0 < \bar{X}_j - \bar{X}_i + \frac{Mm_R}{m_j} < \frac{Mm_R}{m_j},$$

and, introducing (A-10),

$$0 < p_i \frac{Mm_R}{m_i} - (p_j - 1) \frac{Mm_R}{m_j} < \frac{Mm_R}{m_j}.$$

Then,

$$0 < p_i m_j - (p_j - 1) m_i < m_i,$$

or, equivalently,

$$p_i m_j - (p_j - 1) m_i = |p_i m_j|_{m_i}.$$

Observing that

$$-(p_i m_j - p_j m_i) = m_i - |p_i m_j|_{m_i} = |-p_i m_j|_{m_i},$$

and since, combining (A-10) and (A-9),

$$-M < \bar{X}_j - \bar{X}_i = p_i M m_R / m_i - p_j M m_R / m_j < 0,$$

the following inequality is derived:

$$m_R < \frac{m_i m_j}{|-p_i m_j|_{m_i}},$$

which again contradicts the original assumption.

References

[1] N. S. Szabo and R. I. Tanaka, *Residue Arithmetic and Its Applications to Computer Technology*. New York: McGraw-Hill, 1967.

[2] R. W. Watson, "Error detection and correction and other residue interacting operations in a residue redundant number system," Ph.D. dissertation, Univ. California, Berkeley, 1965.

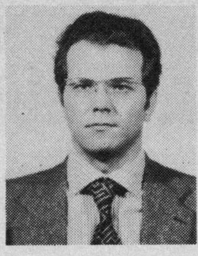
[3] R. W. Watson and C. W. Hastings, "Self-checked computation using residue arithmetic," *Proc. IEEE*, vol. 54, pp. 1920–1931, Dec. 1966.

[4] I. Ya. Akusŝkiî and D. I. Yudickiî, "Maŝinnaya arifmetika v ostatoĉnyh klassah," *Sov. Radio* (Moscow), 1968.

[5] I. M. Vinogradov, *Elements of Number Theory*. New York: Dover, 1954.

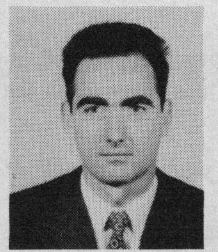
[6] D. Mandelbaum, "Error correction in residue arithmetic," *IEEE Trans. Comput.*, vol. C-21, pp. 538–545, June 1972.

[7] F. Barsi and P. Maestrini, "Correzione di classi di errori singoli nei codici residui," IEI, Pisa, Italy, Internal Rep., 1972.



Ferruccio Barsi was born in Lucca, Italy, on January 3, 1942. He received the Dr. Ing. degree in electronic engineering from the University of Pisa, Pisa, Italy, in 1969.

Since 1969 he has been with the Istituto di Elaborazione dell'Informazione, Consiglio Nazionale delle Ricerche, Pisa, Italy. He has been engaged in research on minicomputer architecture, fault diagnosis, and arithmetic codes.



Piero Maestrini was born in Colle di Val d'Elsa, Italy, on January 9, 1938. He received the Dott. Ing. degree in electronic engineering (cum laude) from the University of Pisa, Pisa, Italy, in 1962, and the Libera Docenza in switching theory and electronic computers in 1971.

Since 1962 he has been a Researcher at the Istituto di Elaborazione dell'Informazione, Consiglio Nazionale delle Ricerche, Pisa, Italy. Since 1969 he has also been an Associate Professor with the Department of Electrical and Electronic Engineering, University of Pisa. He has been engaged in research concerning digital electronics, computer architecture, microprogramming and arithmetic codes.