Applied problems of information systems operation

UDC 681.142 doi: 10.20998/2522-9052.2020.2.22

V. Krasnobayev[1], A. Yanko[2], S. Tur[2]

[1] V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
[2] National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

METHOD FOR THE CONTROL VERIFICATION OF DIGITAL INFORMATION, REPRESENTED IN A RESIDUE NUMBER SYSTEM

Abstract. The subject of the research in the article is the control methods for the data presented in the residue number system. **The object** of research is the process of monitoring data presented in the residue number system. **The purpose** of the work is to develop a method for increasing the reliability of control of data presented in the residue number system. The following **tasks** are solved in the article: research of data control methods presented in the residue number system; development of a method for increasing the reliability of data control; consideration of examples of application of the developed method for a specific residue number system; demonstration of examples of calculation and comparative analysis of the reliability of data control presented in the residue number system. The following research **methods** are used: the basics of system analysis and the basics of machine arithmetic in the residue number system. The following **results** were obtained: A method for increasing the reliability of data control was developed; examples of application of the developed method for a specific residue number system are presented; examples of calculation and comparative analysis of the reliability of data control presented in the residue number system are given. **Conclusions:** This article presents the theoretical foundations of the process of increasing the reliability of control of data presented in the residue number system, based on the use of the procedure of zeroing numbers. A method for increasing the reliability of data control has been directly developed and presented. Examples of application of the developed method for a specific residue number system are given and examples of calculating the reliability of control of data presented in the residue number system are given. A method has been developed to increase the reliability of data control; it is a definite contribution to the theory of noise-resistant coding in a residue number system. Examples of calculation and comparative analysis of the reliability of data control confirm the practical significance of the results of this article.

Keywords: control system of information; data transmission and processing system; nulevization of number; residue number system.

Introduction

Scales and complexity of the tasks solved by modern computer systems impose qualitatively new requirements to their main characteristics: productivity, reliability and efficiency of systems that causes need of improvement existing, creations of new means of information processing.

The trend of development of computer systems and components is aimed at increasing the speed (productivity) and reliability of the implementation of integer arithmetic operations [1].

Scientific researches were conducted in recent years, identify promising ways to improve the reliability of data processing, control, diagnostics and correction of data errors of computer systems, which are based on the use of the residue number system (RNS).

Error control in the RNS is a non-positional operation and requires the development of special methods, designed to increase the efficiency of this procedure. This article focuses on finding ways for increasing the reliability of digital information control for data transmission and processing systems (DTPS) that function in a RNS are described.

Analysis of recent studies and publications

The results of studies of methods for increasing the reliability and control of calculations of computer systems and data processing tools, which have been carried out over the past decades, have shown that it is practically impossible to achieve this within the limits of the positional systems of the calculus [2].

This fact led to the need to find ways to increase reliability, for example, based on the use of new structural solutions in the creation of computer systems, through the use of non-positional machine arithmetic. In particular, on the basis of the use of a non-positional numerical system in residual classes.

The results of research in the field of the creation of high-speed and high-control computer systems of processing data of well-known authors (Valakh M., Svoboda A., Sabo N., Aksushskyi I.Y., Yuditskyi D.I., Glushkov V.M., Torgashov V.A., Amberbaev V.M., Kolyada A.A., Shimbo A., Paulier P., Thornton M.A., Dreschler R., Miller D.M., and others) shown that the use of RNS as a system for increasing the reliability of digital information control for DTPS allows developing methods based on which it increases the reliability of data control several times.

Highlighting previously unsolved parts of a common problem. The goal of the work

Currently, there are many methods for data error control in a RNS. Results of a research of control methods of the data in RNS which are carried out in this scientific field have shown that the existing control methods of data in RNS based on use of application of the zeroing procedure reduce control time [2].

This article will present the theoretical foundations of the process of increasing the reliability of the control of data presented in the system of residual classes based on the use of the nullification process of numbers.

On this considered a method for error control in the RNS based on the use of the zeroing procedure is proposed. The control verification of digital information in the RNS is a non-positional operation and requires the development of special ways, designed to increase the efficiency of this procedure. Therefore, the main task is to find effective ways for increasing the reliability of digital information control for DTPS that function in a RNS are described.

The main goal of the work is to directly develop a method for increasing the reliability of data control, give examples of the application of the developed method for a specific RNS and examples of calculating the reliability of data control presented in the system of residual classes.

Materials and methods

Considerable time spent on data control leads to a decrease in the overall efficiency of application of non-positional code structures (NCSs) in a RNS in implementing integer arithmetic and other modular operations [3]. On-line data verification methods that are recently developed in DTPSs and function in RNSs allow one to appreciably reduce verification time but, at the same time, the problem of increasing the reliability of this verification arises [4].

The objective of this article is the development of a method for increasing the reliability of data verification in DTPSs functioning in RNSs.

The well-known method of on-line data verification in RNSs is based on the obtaining and use of the so-called position indicator of a non-positional code (PINC) [5, 6]. This PINC is one of characteristics of a special code (SC) obtained from the initial NCS (being verified) $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ of data represented in an RNS by bases $\{m_i\}$ $(i=\overline{1,n+1})$ with one check residue of a_{n+1} to the check base (modulus) m_{n+1} and, in this case,

$$M=\prod_{i=1}^{n} m_i\ ;\ M_0=\prod_{i=1}^{n+1} m_i\ .$$

Let us consider a procedure for obtaining a PINC from the NCS $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ being verified. In the general form, an SC:

$$K_N^{(n_A)}=\left\{Z_{N-1}^{(A)}\ Z_{N-1}^{(A)} \dots Z_1^{(A)}\ Z_0^{(A)}\right\}, \qquad (1)$$

is a sequence of bits $Z_K^{(A)}$ $(K=\overline{0,N-1})$ consisting of ones and one zero at the n_A-th place (from right to left from the $Z_0^{(A)}$-th bit to the $Z_{N-1}^{(A)}$ bit). The parameter n_A is the PINC of the non-positional code structure $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ of data [7].

Proceeding from mathematical considerations, n_A is a natural number referring to the location of the zero bit $Z_{n_A}^{(A)}=0$ in the notation of the SC $K_N^{(n_A)}$. It determines the number j_i of the numerical interval $[j_i \cdot m_i,\ (j_i+1)\cdot m_i)$ containing the number *A*, i.e., the value of n_A with a definite accuracy *W* that depends on the magnitude of the value of the RNS modulus m_i and determines the location of the number $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ on the numerical axis $0 \div M_0$. We first consider a procedure that forms the SC $K_N^{(n_A)}$. For the chosen RNS base m_i (the rules for selecting an RNS base m_i will be described below), a constant of the form $KH_{m_i}^{(A)}=\left(a_1^{'},..., a_{i-1}^{'}, a_i, a_{i+1}^{'}, ..., a_{n+1}^{'}\right)$ is determined from the value of the residue a_i of the number $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ in the DTPS nulevization constant block (NCB). Next, using the chosen nulevization constant $KH_{m_i}^{(A)}$, the following subtraction operation is executed:

$$\begin{aligned}A_{m_i}=A-KH_{m_i}^{(A)}&=\left(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1}\right)-\\&-\left(a_1^{'}, a_2^{'}, ..., a_{i-1}^{'}, a_i, a_{i+1}^{'}, ..., a_n^{'}, a_{n+1}^{'}\right)=\\&=\left[a_1^{(1)}, a_2^{(1)}, ..., a_{i-1}^{(1)}, 0, a_{i+1}^{(1)}, ..., a_n^{(1)}, a_{n+1}^{(1)}\right].\end{aligned}$$

This operation corresponds to the shift of the number $A=(a_1, ..., a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ being verified to the left end of the interval $[j_i \cdot m_i,\ (j_i+1)\cdot m_i)$ of its initial location. In this case, we have $A_{m_i}=j_i \cdot m_i$, i.e., the number A_{m_i} is a multiple of the value of the RNS modulus m_i.

As is well known, the correctness of the number *A* in the RNS is determined by its presence or absence in the numerical information interval [0, *M*). If the number *A* is out of this interval $\left(A \ge M\right)$, then it is considered to be distorted (incorrect) [8]. In this case, using the value of n_A, it is necessary to verify the correctness or incorrectness of the initial number *A* by determining the fact of the presence or absence of the initial number *A* in the interval [0, *M*). To determine the fact of the presence of the number in the information numerical interval [0, *M*), it is necessary to execute a collection of operations of the form:

$$A_{m_i}-K_A \cdot m_i=Z_{K_A}^{(A)}. \qquad (2)$$

Operations (2) are executed in parallel (simultaneously in time) by means of a collection of *N* constants $K_A \cdot m_i$ $\left(K_A=\overline{0,N-1}\right)$ of the form:

$$\begin{cases}A_{m_i}-0\cdot m_i=Z_0^{(A)},\\A_{m_i}-1\cdot m_i=Z_1^{(A)},\\\dots\\A_{m_i}-(N_i-1)\cdot m_i=Z_{N-1}^{(A)},\end{cases} \qquad . \qquad (3)$$

where $N_i = \prod_{K=1;\, K \neq i}^{n+1} m_K$. In this case, the SC will be represented in the form (1), and the method of formation of the PINC n_A in the RNS can be described as follows [9].

1. Choose some information $\{m_i\}$, $i = \overline{1, n}$, and check $m_k = m_{n+1}$ ($m_i < m_{i+1}$) bases to represent the data $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ in the RNS; GCD $(m_i, m_j) = 1$, $i \neq j$.

2. Choose of a base $m_i \in \{m_j\}$, $(j = \overline{1, n+1})$ from which the number j_i of the numerical interval $[j_i \cdot m_i, (j_i + 1) \cdot m_i)$ is determined that contains the number $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$.

3. Determine a nulevization constant of the form $KH_{m_i}^{(A)} = \left(a_1', a_2' ..., a_{i-1}', a_i, a_{i+1}', ..., a_{n+1}'\right)$ from the value of the residue a_i of the number $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$.

4. Determine the value of

$$j_i \cdot m_i = A_{m_i} = A - KH_{m_i}^{(A)} =$$
$$= (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1}) -$$
$$-\left(a_1', a_2', ..., a_{i-1}', a_i, a_{i+1}', ..., a_n, a_{n+1}\right) =$$
$$= \left[a_1^{(1)}, a_2^{(1)}, ..., a_{i-1}^{(1)}, 0, a_{i+1}^{(1)}, ..., a_n^{(1)}, a_{n+1}^{(1)}\right].$$

5. Determine an SC $K_N^{(n_A)} = \left\{Z_{N-1}^{(A)}\, Z_{N-2}^{(A)} ... Z_0^{(A)}\right\}$ in the form $K_{N_i}^{(n_A)} = \left\{Z_{N_i-1}^{(A)}\, Z_{N_i-2}^{(A)} ... Z_0^{(A)}\right\}$. $N = \prod_{K=1;\, K \neq i}^{n+1} m_K$, $N_i =]M / m_i[$, $M = \prod_{i=1}^{n} m_i$. $A_{m_i} - K_A \cdot m_i = Z_{K_A}^{(A)}$.

6. Determine the PINC of the number $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ namely, find the numerical value of n_A for which $Z_{K_A}^{(A)} = Z_{n_A}^{(A)} = 0$, i.e. $A_{m_i} - n_A \cdot m_i = 0$; at the same time, $Z_l^{(A)} = 1$, $(A_{m_i} - l \cdot m_i \neq 0;\ l \neq n_A)$.

Analytical relationships (3) provide a unique value of from collection (2) for which $Z_{K_A}^{(A)} = Z_{n_A}^{(A)} = 0$ $(K_A = n_A)$, i.e. $A_{m_i} - n_A \cdot m_i = 0$. The other values of collection (2) equal $Z_l^{(A)} = 1$ $(A_{m_i} - l \cdot m_i \neq 0;\ l \neq n_A)$. In the general case, the number of bits in the notation of the SC $K_N^{(n_A)}$ equals the value of N. But we note that, to determine only the fact of distortion of the number A, there is no need to have and analyze the entire sequence of the collection of N values $Z_{K_A}^{(A)}$ of the SC $K_N^{(n_A)}$. To this end, it suffices to have an SC $K_N^{(n_A)}$ whose length equals only $N_i =]M / m_i[$ bits (a quantity $]M / m_i[$ denotes an integer larger than and closest to the number M / m_i, i.e., the number M / m_i is rounded up to the nearest larger integer).

This fact can be explained as follows. In performing the verification procedure to establish the fact of correctness of the number This $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, there is no need to analyze all numerical intervals $[j_i \cdot m_i, (j_i + 1) \cdot m_i)$ in which a distorted number is located outside of the information interval [0, M). In this case, to establish only the fact of correctness of the number A, the determination of numbers and analysis of locations of these intervals $[j_i \cdot m_i, (j_i + 1) \cdot m_i)$ are inessential. To verify the NCS A in the RNS, it suffices to know the location of zero in SC notation (1) (to know the numerical value of n_A) only in numerical intervals $[j_i \cdot m_i, (j_i + 1) \cdot m_i)$ belonging to the information numerical interval $0 \div M_0$, i.e., belonging to the first interval located on the segment $0 \div M_0$ after the value of M. In this case, to verify the data $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, it suffices to have an SC $K_{N_i}^{(n_A)}$ whose length is only $N_i =]M / m_i[$ bits. Thus, the method for data verification in such an RNS is as follows.

1. Determine the SC $K_{N_i}^{(n_A)}$ for the number $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$.

2. Determine the PINC n_A: $A_{m_i} - n_A \cdot m_i = 0$, $Z_{n_A}^{(A)} = 0$; $Z_l^{(A)} = 1$, $A_{m_i} - l \cdot m_i = 1$; $l \neq n_A$.

3. Perform the data verification procedure over $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ in the RNS. If $n_A > N_i$, then the number $\tilde{A}$ is incorrect (distorted). If $n_A \leq N_i$, then the number A is correct (undistorted).

For the NCS A being verified that is represented in an RNS, its PINC n_A is determined by forming an SC $K_{N_i}^{(n_A)} = \left\{Z_{N_i-1}^{(A)}\, Z_{N_i-2}^{(A)} ... Z_1^{(A)}\, Z_0^{(A)}\right\}$ in the form of a sequence of N_i bits. An RNS base m_i is chosen in a special way according to definite criteria [10].

Proceeding from the value of the residue a_i of the number $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ some nulevization constant of the form $KH_{m_i}^{(A)} = \left(a_1', a_2', ..., a_{i-1}', a_i, a_{i+1}', ..., a_n', a_{n+1}'\right)$ is chosen. Then the operation $A_{m_i} = A - KH_{m_i}^{(A)}$ is performed. Using N_i constants $K_A \cdot m_i$ $\left(K_A = \overline{0, N_i - 1}\right)$, subtraction operations $A_{m_i} - K_A \cdot m_i$ are simultaneously performed and, as a result, values of bits of $Z_{K_A}^{(A)}$ is obtained, i.e., the SC $K_{N_i}^{(n_A)}$ is formed. The value of the PINC n_A is determined from the equality $A_{m_i} - n_A \cdot m_i = 0$.

The verification procedure for the number A is as follows. If $n_A > N_i$, then the number A is considered to be incorrect. Otherwise ($n_A \le N_i$), the number A is correct.

Let us consider examples of implementation of the verification method for a concrete RNS specified by the bases $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ and $m_k = = m_{n+1} = m_5 = 11$. This RNS provides data processing in a DTPS with single-byte words ($l = 1$). In this case, $M = \prod_{i=1}^{4} m_i = 420$, $M_0 = M \cdot m_{n+1} = . = 4620$. Moreover, we consider that $m_i = 11$. In this case, $N_i = = N_{n+1} =]M / m_i[=]M / m_{n+1}[=]420/11[=]38,18[= 39$.

Table 1 presents the NCB data of the DTPS with respect to the base $m_K = m_{n+1} = 11$.

Table 1 – **Nulevization Constants** $KH_{m_{n+1}}^{(A)}$

Value of the residue $a_K = a_{n+1}$ of the number A	Constants of nulevization with respect to *m* for the value of a'				
	$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$	$m_k = = m_5 = 11$
	a'_1	a'_2	a'_3	a'_4	a'_5
0000	00	00	000	000	0000
0001	01	01	001	001	0001
0010	10	10	010	010	0010
0011	00	11	011	011	0011
0100	01	00	100	100	0100
0101	10	01	000	101	0101
0110	00	10	001	110	0110
0111	01	11	010	000	0111
1000	10	00	011	001	1000
1001	00	01	100	010	1001
1010	01	10	000	011	1010

Example 1. Verify the data represented in the form $A = (01, 00, 000, 010, 0001)$ with $m_k = m_{n+1} = = m_5 = 11$. Using the value of the residue $a_K = a_{n+1} = a_5 = 0001$ of the number A in the NCB (Table 1), choose the nulevization constant $KH_{m_{n+1}}^{(A)} = (01, 01, 001, 001, 0001)$. Then determine $A_{m_{n+1}} = A - KH_{m_{n+1}}^{(A)} = (00, 11, 100, 001, 0000)$.

By realizing relationship (3), create an SC of the form $K_{N_i}^{(n_A)} = K_{39}^{(9)} = \{11...110111111111\}$. Proceeding from the form of the SC and using the expression $A_{m_{n+1}} - n_A \cdot m_{n+1} = 0$, we obtain $n_A = 9$ ($A_{m_{n+1}} - n_A \cdot m_{n+1} = 99 - 9 \cdot 11 = 0$), i.e., $Z_{n_A}^{(A)} = Z_9^{(A)}$. We have $N_i = 39 > n_A$ and $n_A = 9$. Hence, a data error is absent.

Verification: $A = 100 < M$ and $M = 420$ (the number A is correct).

Example 2. Verify the data $A = (00, 01, 000, 010, 1010)$. Using the value of $a_5 = 1010$, choose the constant of the form $KH_{m_{n+1}}^{(A)} = (01, 10, 000, 011, 1010)$ from the NCB (Table 1). We obtain $A_{m_{n+1}} = A - KH_{m_{n+1}}^{(A)} = (10, 00, 000, 110, 0000)$. Since $A_{m_{n+1}} - n_A \cdot m_{n+1} = 440 - 44 \cdot 11 = 0$, the SC is of the form $K_{N_i}^{(n_A)} = K_{39}^{(40)} = \{11...11...11\}$ and $n_A = 40$. Here, $N_i = 39 < n_A$ and $n_A = 40$. Hence, there is an error in these data.

Verification: $A = 450 > M$ and $M = 420$ (the number A is incorrect).

Example 3. Verify the data $A = (01, 11, 010, 000, 1001)$. Using the value of $a_5 = 1001$, choose the constant $KH_{m_{n+1}}^{(A)} = (00, 01, 100, 010, 1001)$ from the NCB (Table 1). Determine $A_{m_{n+1}} = A - KH_{m_{n+1}}^{(A)} = = (01, 10, 011, 101, 0000)$. Since $A_{m_{n+1}} - n_A \cdot m_{n+1} = = 418 - 38 \cdot 11 = 0$, the obtained SC is of the form $K_{N_i}^{(n_A)} = K_{39}^{(38)} = \{011...11...11\}$ adn $n_A = 38$. Since $n_A = 38 < N_i$ and $N_i = 39$, the following conclusion is drawn: the number A is correct (is not distorted). However, the verification shows that $A = 427 > M$ and $M = 420$, i.e., the number A is incorrect. In this case, an error has been made in verifying data [10].

As is obvious from Example 3, the use of the considered method for on-line data verification in are RNSs not always provides reliable verification results. In fact, there is a collection of $(j_{n+1} + 1) \cdot m_{n+1} - M$ incorrect values of $\tilde{A}$ that are recognized as correct by the DTPS verification system (VS), which stipulates a low reliability of verification. For Example 3, the totality of such numbers can exceed 80%. In the numerical range [418, 429), there are two correct numbers A, namely, 418 and 419. At the same time, the collection of incorrect numbers $\tilde{A}$ that are determined by the DTPS VS as correct is as follows: 420, 421, 422, 423, 424, 425, 426, 427 and 428.

Thus, it is obvious that the developed method of on-line data verification in RNS and the device that implements it have a very low reliability of verification [11]. This low reliability of data verification is a result of the presence of the following nonzero residue value a:

$$\alpha = M / m_{n+1} - [M / m_{n+1}], \tag{4}$$

In turn, the presence of a nonzero residue $\alpha \ne 0$ is determined by the fact of the non-multiplicity of the value of M to the RNS check modulus m_{n+1} that determines the range of some numerical interval $[j_{n+1} \cdot m_{n+1}, (j_{n+1} + 1) \cdot m_{n+1})$ of the possible location of the number A. In this case, the verification of data $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ is performed on the basis of the use of the RNS check base m_{n+1} by forming the following SC:

$$K_{N_{n+1}}^{(n_A)} = \left\{ Z_{N_{n+1}-1}^{(A)} \, Z_{N_{n+1}-2}^{(A)} \dots Z_0^{(A)} \right\}, \tag{5}$$

This geometrically low reliability of data verification can be explained as follows [12]. The numerical information interval $[0,\ M=\prod_{i=1}^{n} m_i)$ does not hold an integer number of segments whose length equals to the value of $m_i = m_{n+1}$. In this case, the numerical axis $0 \div M_0$ includes a numerical interval $[j_{n+1}\cdot m_{n+1},\ (j_{n+1}+1)\cdot m_{n+1})$ or a numerical interval $[(N_{n+1}-1)\cdot m_{n+1},\ N_{n+1}\cdot m_{n+1})$ that contains a number *M*. Therefore, this interval simultaneously includes a collection $((j_{n+1}+1)\cdot m_{n+1})-M$ or $[N_{n+1}\cdot m_{n+1})-M]$ of incorrect numbers and a collection $M-\ j_{n+1}\cdot m_{n+1}$ (or $M-\ (N_{n+1}-1)\cdot m_{n+1}$) of correct numbers. In the course of verification of data *A*, in performing the nulevization procedure, all incorrect $((j_{n+1}+1)\cdot m_{n+1})-M$ and correct $M-j_{n+1}\cdot m_{n+1}$ numbers are shifted to the left end (to one correct number $j_{n+1}\cdot m_{n+1}$) of the interval $[j_{n+1}\cdot m_{n+1},\ (j_{n+1}+1)\cdot m_{n+1})$. In this case, the DTPS VS will recognize incorrect numbers $[N_{n+1}\cdot m_{n+1})-M]$ as correct [13]. By the reliability of data verification in a residue class we understand the probability of obtaining the true result of the operation of verification of data represented in an RNS [14]. The following ratio can be used as the quantitative index of the reliability of an estimate for data verification in RNSs:

$$P_{vr} = V_{cw} / V_{tw}, \qquad (6)$$

where, in the general case, $V_{cw} = M$ is the number (from 0 to $M \div 1$) of correct ($A < M$) code words in the operating numerical range $[0, M_0)$ for a given RNS; $V_{tw} = (V_{cw} + V_{iw})$ is the total amount of code words that are considered as correct after performed data verification; $V_{iw} = (N_i \cdot m_i - M)$ is the number of incorrect code words ($A \ge M$) that are considered as correct after performed data verification (note that $N_i =]M / m_i[= j_i + 1$).

With allowance for the aforesaid, verification reliability index (6) is specified by the relationship:

$$P_{vr} = M/(M + N_i \cdot m_i - M) = M/(N_i \cdot m_i), \qquad (7)$$

When $m_i = m_{n+1}$, we have $V_{iw} = (N_{n+1}\cdot m_{n+1} - M)$. In this case, expression (7) assumes the form:

$$P_{vr} = \frac{M}{M + N_{n+1}\cdot m_{n+1} - M} = \frac{M}{N_{n+1}\cdot m_{n+1}}, \qquad (8)$$

If we take an RNS information base, for example, $m_i = m_1$, in the capacity of the base m_i determining ranges of numerical intervals $j_i \cdot m_i \div (j_i+1)\cdot m_i$ then $N_i =]M / m_i[= N_1 =]M / m_1[$ and $N_1 = \prod_{i=2}^{n} m_i$. In this case, expression (7) assumes the form:

$$P_{vr} = M/(M + N_1 \cdot m_1 - M) = M/(N_1 \cdot m_1) = 1, \qquad (9)$$

In this case (see expression (4)), we always have $P_{vr} = 1$, i.e., when $m_i = m_1$ is chosen, the DTPS VS always provides a reliable result of data verification in an RNS [15].

The results of the of the developed method

The proposed method for increasing the reliability of verification is based on the well-known method of on-line information verification in RNSs and includes procedures of obtaining and using PINCs [10]. This feature is one of characteristics of the SC formed from the initial NCS *A* of data represented in an RNS by bases $\{m_i\}$, $i = \overline{1,\ n+1}$, with one check base number m_{n+1}.

The essence of the proposed method of increasing the reliability of data verification in RNSs consists of ensuring the maximum reliability of data verification $P_{vr} = 1$ by providing the fulfillment of the condition $\alpha = 0$ (see expression (4)). In this case, to compute the value of $N_i =]M / m_i[$, the modulus m_i that determines the number j_i of the numerical interval $[j_i \cdot m_i,\ (j_i+1)\cdot m_i)$ containing the number $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ is chosen only from the collection of *n* RNS information bases that, naturally, are multiples of the value of *M*. In this case, $\alpha = M - [M / m_i]\cdot m_i = 0$, which provides the maximum value of the verification reliability index $P_{vr} = 1$ (see relationship (7)). Let us consider an example of using the developed method for increasing the reliability of data verification in RNSs [16].

Example 4. In the RNS considered above, we choose, for example, the information base $m_i = m_1 = 3$. We obtain $N_i = N_1 = M / m_1 = 4\cdot 5\cdot 7 = 140$. In this case, the operating numerical range $[0, M_0)$ of the RNS is divided into intervals $[j_i \cdot m_i,\ (j_i+1)\cdot m_i)$. For the value of $m_1 = 3$, the information numerical interval [0, *M*) is divided exactly into $N_1 = M / m_1 = 140$ segments of length 111 each. From Table 1, we choose the NCB content concerning the base $m_1 = 3$. It is necessary to verify the number $A = (01, 11, 010, 000, 1001)$. With the help of the value of $a_1 = 01$, we choose the nulevization constant of the form $KH_{m_1}^{(A)} = (01, 01, 001, 001, 0001)$ from the NCB. Next, we determine $A_{m_1} = A - KH_{m_1}^{(A)} = (00, 10, 001, 110, 1000)$. If $A_{m_1} - n_A \cdot m_1 = 426 - 142\cdot 3 = 0$, then the SC is of the form $K_{N_i}^{(n_A)} = K_{140}^{(142)} = \{Z_{139}^{(A)}\ Z_{138}^{(A)} ... Z_1^{(A)}\ Z_0^{(A)}\} = \{11...11...11\}$. Since $N_i = 140 < n_A$ and $n_A = 142$, the number *A* contains an error.

Verification: $A = 427 > M$ and $M = 420$. The number $A > M$, i.e. it is incorrect (distorted).

By way of example. Table 2 (Fig. 1) presents the results of computation of the data verification reliability p_{rv} for six different values (11, 13, 17, 19, 23, and 29) of check bases m_{n+1} in the RNS specified by the information bases $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, and $m_4 = 7$.

Since it is known that $N_{n+1}\cdot m_{n+1} > M$ (see expression (4)), we always have $P_{vr} < 1$.

Table 2 – **Results of computation of data verification reliability values**

Values of check bases m_{n+1}	Results of computing reliability verification values in the RNS for the parameters				
	M	$\frac{M}{m_{n+1}}$	$\left]\frac{M}{m_{n+1}}\right[$	$N_{n+1} = \left]\frac{M}{m_{n+1}}\right[\cdot m_{n+1}$	P_{vr}
11	420	38,2	39	429	0,979
13	420	32,3	33	429	0,979
17	420	24,7	25	425	0,988
19	420	22,1	23	437	0,961
23	420	18,2	19	437	0,961
29	420	14,4	15	435	0,965

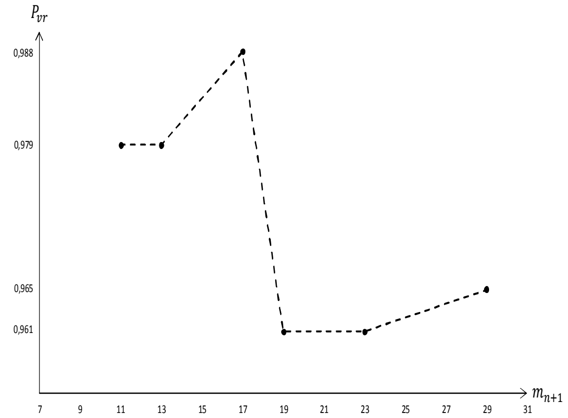

Fig. 1. The data verification reliability values

In addition to the efficiency of data verification [10], an important characteristic of a DTPS is the amount of equipment in a verification system. Note that, in an RNS, the amount of equipment of an VS depends mainly on the number of summators implementing operations of the form (3). Thus, the amount of equipment of an VS depends on the value of the quantity $N_1 = \prod_{i=2}^{n} m_i$ $(i = \overline{1,\ n})$. In this case, with allowance made for $\alpha = 0$ and the requirement of the avoidance of the decrease in the efficiency of verification, to minimize the amount of equipment of the VS in an RNS, an information base of maximum should be chosen. For an ordered RNS $(m_i < m_{i+1})$, such a base is m_n.

A preliminary estimate for the amount of equipment for DTPS with machine words consisting of l bytes can be obtained through the value of the efficiency factor:

$$K_{\text{ef}}^{(l)} = N_1 / N_n = \left(M / m_1\right) / \left(M / m_n\right) = m_n / m_1 . \quad (10)$$

Let us consider an example of data verification in an RNS for the value of $m_i = m_n$.

Example 5. The maximum information base for the above-mentioned RNS is $m_n = m_4 = 7$. In this case, $N_i = N_4 = M / m_4 = 3 \cdot 4 \cdot 5 = 60$. The operating numerical range $[0, M_0)$ is divided into intervals $[j_4 \cdot m_4, (j_4 + 1) \cdot m_4)$, i.e., into $M_0 / m_4 = 4620 / 7 = 660$ segments. For the value of $m_4 = 7$, the information interval [0, M) is divided into $N_4 = M / m_4 = 60$ numerical segments each of which has the length equal to seven ones. From Table 1, the NCB content with respect to the base $m_4 = 7$ is determined.

Assume that the number $A = (01, 11, 010, 000, 1001)$ should be verified. Using the value of $a_4 = 000$, choose the constant $KH_{m_n}^{(A)} = KH_7^{(A)} = (00,00,000,000,0000)$ from the NCB (Table 1). Then determine the value of $A_{m_n} = A_7 = A - KH_7^{(A)} = (01,11,010,000,1001)$.

As a result of execution of operations (2), we obtain the sought-for SC in the form $K_{N_4}^{(n_A)} = K_{60}^{(61)} = \left\{Z_{59}^{(A)}\, Z_{58}^{(A)} \ldots Z_1^{(A)}\, Z_0^{(A)}\right\} = \{11...11...11\}$. Proceeding from the form of the SC and using the expression $A_{m_n} - n_A \cdot m_n = 0$, we determine $n_A = 61$ $(A_{m_n} - n_A \cdot m_n = 427 - 61 \cdot 7 = 0)$. Since $N_4 = 60 < n_A$ and $n_A = 61$ the data A contain an error.

Verification: $A = 427 > M = 420$.

Table 3 (Fig. 2) presents design data on the conditional amount of equipment of a DTPS verification system functioning in an RNS and data on the comparative analysis of the decrease in the amount of the VS equipment when $m_i = m_n$.

Table 3 – **Comparative data on the amount of equipment of a DTPS verification system**

Word size of an l-byte DTPS (ρ, n, k)	RNS information bases m_i $(i = \overline{1, n})$	RNS check base m_{n+1}	RNS information base		$K_{ef}^{(l)}$
			minimum, m_1	maximum, m_n	
$l = 1$ ($\rho = 8$, $n = 4$, $k = 3$)	$m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$	$m_5 = 11$	$m_1 = 3$	$m_4 = 7$	2,3
$l = 3$ ($\rho = 24$, $n = 8$, $k = 5$)	$m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$, $m_5 = 11$, $m_6 = 13$, $m_7 = 17$, $m_8 = 19$	$m_9 = 23$	$m_1 = 3$	$m_8 = 19$	6,3
$l = 4$ ($\rho = 32$, $n = 10$, $k = 5$)	$m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $m_4 = 7$, $m_5 = 11$, $m_6 = 13$, $m_7 = 17$, $m_8 = 19$, $m_9 = 23$, $m_{10} = 29$	$m_3 = 5$	$m_1 = 2$	$m_{10} = 29$	14,5
$l = 8$ ($\rho = 64$, $n = 16$, $k = 6$)	$m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$, $m_5 = 11$, $m_6 = 13$, $m_7 = 17$, $m_8 = 19$, $m_9 = 23$, $m_{10} = 29$, $m_{11} = 31$, $m_{12} = 37$, $m_{13} = 41$, $m_{14} = 43$, $m_{15} = 47$, $m_{16} = 53$	$m_{17} = 59$	$m_1 = 3$	$m_{16} = 53$	17,6

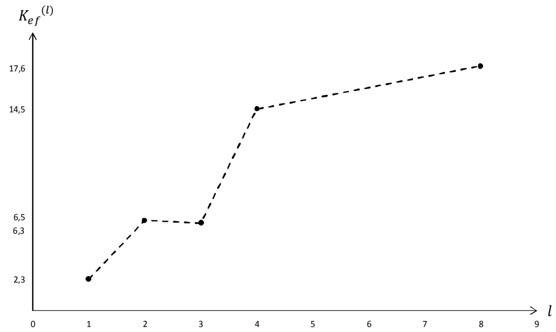

Fig. 2. The data on the amount of equipment of a DTPS verification system

The ways for increasing the reliability of digital information control for data transmission and processing systems that function in a residue number system are described [17]. The developed method increases the reliability of data control in a RNS to 3.5 percent, depending on the value of the control basis. Based on the use of this method, operational data monitoring systems can be synthesized.

Conclusions

Thus, this article describes a method developed for increasing the reliability of verification of data represented in an RNS. This method is based on the use of a PINC n_A that is one of SC characteristics. In this case, a modulus m_i that determines the number of the numerical interval containing an NCS is chosen from a collection of n possible information bases of the corresponding RNS [18]. The use of this method provides the obtaining of a reliable result of data verification in the RNS. The design data and a comparative analysis of reliability of their verification and the amount of equipment of a verification system have shown that the efficiency of non-positional data coding in RNSs considerably increases with increasing the word size of a DTPS.

References

1. Shu, S., Wang, Y. and Wang, Y. (2016), "A research of architecture-based reliability with fault propagation for software-intensive systems", *2016 Annual Reliability and Maintainability Symposium (RAMS)*, Tucson, AZ, pp. 1-6.
2. Ponochovniy, Y., Bulba, E., Yanko, A., Hozbenko, E. (2018), "Influence of diagnostics errors on safety: Indicators and requirements. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. DOI: https://doi.org/10.1109/dessert.2018.8409098
3. Akushskiy, I. Ya., Yuditskiy, D. I. (1968), *Machine arithmetic in residual classes*, M., Radio i svyaz, 444 p.
4. Torgashev, V. A. (1973), *System of residual classes and reliability of digital computers*, M., Sov. radio, 118 p.
5. Amerbaev, V. M. (1976), *Theoretical Foundations of Machine Arithmetic*, Alma-Ata, Nauka, 324 p.
6. Krasnobayev, V., Kuznetsov, A., Koshman, S. and Moroz, S. (2018), "Improved Method of Determining the Alternative Set of Numbers in Residue Number System", In: Chertov O., Mylovanov T., Kondratenko Y., Kacprzyk J., Kreinovich V., Stefanuk V. (eds) Recent Developments in Data Science and Intelligent Analysis of Information. *ICDSIAI 2018. Advances in Intelligent Systems and Computing*, vol 836. Springer, Cham, pp. 319-328. DOI: https://doi.org/10.1007/978-3-319-97885-7_31
7. Krasnobayev, V.A., Yanko, A.S. and Koshman, S.A. (2016), "A Method for arithmetic comparison of data represented in a residue number system" *Cybernetics and Systems Analysis*, vol. 52, issue 1, pp. 145-150. DOI: https://doi.org/10.1007/s10559-016-9809-2
8. Krasnobayev, V., Koshman, S. and Mavrina, M. (2013), "Method for correcting one-time data errors represented by a deduction class code", *Elektronnoe modelirovanie*, vol. 75, issue 5, pp. 43-56.
9. Fan, C. and Ge, G. (2014) "A Unified Approach to Whiteman's and Ding-Helleseth's Generalized Cyclotomy Over Residue Class Rings,", *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1326-1336, DOI: https://doi.org/10.1109/TIT.2013.2290694
10. Krasnobayev, V.A., Koshman, S.A. and Mavrina, M.A. (2014), "A Method for Increasing the Reliability of Verification of Data Represented in a Residue Number System", *Cybernetics and Systems Analysis*, vol. 50, issue 6, pp. 969–976.
11. Yanko, A., Koshman, S. and Krasnobayev, V. (2017), "Algorithms of data processing in the residual classes system", *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, pp. 117-121, DOI: https://doi.org/10.1109/infocommst.2017.8246363
12. Krasnobaev, V. A. (1990), *Methods to improve the reliability of specialized computer systems and communications*, Kharkiv, HVVKIU RV, 172 p.
13. Krasnobayev, V., Koshman, S., Yanko, A. and Martynenko, A. (2018), "Method of Error Control of the Information Presented in the Modular Number System", *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). IEEE (2018)*, DOI: https://doi.org/10.1109/infocommst.2018.863204
14. Krasnobayev, V., Kuznetsov, A., Kononchenko, A. and Kuznetsova, T. (2019), "Method of data control in the residue classes", *Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019)*. Zaporizhzhia, Ukraine, pp. 241–252.
15. (2017) *Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem.* Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov: ASC Academic Publishing, Minden, Nevada, USA, 198 p.
16. Kasianchuk, M., Yakymenko, I., Pazdriy, I. and Zastavnyy, O. (2015), "Algorithms of findings of perfect shape modules of remaining classes system", *The Experience of Designing and Application of CAD Systems in Microelectronics.*
17. Krasnobaev, V. A., Koshman, S. A., Moroz, S. A., Kurchanov, V. N. and Yanko, A. S. (2017), *Models and methods of data processing in the system of residual classes*, Monografiya, Harkov, OOO "V dele", 197 c.
18. (2017) *ISCI'2017: Information Security in Critical Infrastructures.* Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov: LAP Lambert Academic Publishing, OmniScriptum GmbH & Co. KG, Germany, 216 p.

Received (надійшла) 10.03.2020
Accepted for publication (прийнята до друку) 13.05.2020

ABOUT THE AUTHORS / ВІДОМОСТІ ПРО АВТОРІВ

Краснобаєв Віктор Анатолійович – доктор технічних наук, професор, професор кафедри електроніки і управляючих систем, Харківський національний університет імені В.Н. Каразіна, Харків, Україна;
Victor Krasnobayev – Doctor of Technical Sciences, Professor, Professor of the Department of Electronics and Control Systems, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine;
e-mail: v.a.krasnobaev@gmail.com; ORCID ID: https://orcid.org/0000-0001-5192-9918.

Янко Аліна Сергіївна – кандидат технічних наук, доцент кафедри комп'ютерних та інформаційних технологій і систем, Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна;
Alina Yanko – Candidate of Technical Sciences, Associate Professor of the Department of Computer and Information Technologies and Systems, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine;
e-mail: al9_yanko@ukr.net; ORCID ID: http://orcid.org/0000-0003-2876-9316.

Тур Сергій Геннадійович – студент спеціальності «Телекомунікації та радіотехніка» кафедри автоматики, електроніки та телекомунікацій, Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна;
Serhii Tur – student majoring in "Telecommunications and Radio Engineering" of the Department of Automation, Electronics and Telecommunications, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine;
e-mail: sergiotur30@gmail.com; ORCID ID: https://orcid.org/0000-0003-0670-1206.

Метод контрольної перевірки цифрової інформації, представленої в системі залишкових класів

В. А. Краснобаєв, А. С. Янко, С. Г. Тур

Анотація. Предметом дослідження в статті є методи контролю даних, представлених в системі залишкових класів. **Об'єкт** досліджень - процес контролю даних, представлених в системі залишкових класів. **Мета** роботи - розробка методу підвищення достовірності контролю даних, представлених в системі залишкових класів. У статті вирішуються наступні **завдання**: дослідження методів контролю даних, представлених в системі залишкових класів; розробка методу підвищення достовірності контролю даних; розгляд прикладів застосування розробленого методу для конкретної системи залишкових класів; демонстрація прикладів розрахунку і порівняльного аналізу достовірності контролю даних, представлених в системі залишкових класів. Використовуються такі **методи** дослідження: основи системного аналізу та основи машинної арифметики в системі залишкових класів. Отримані наступні **результати**: Розроблено метод підвищення достовірності контролю даних; представлені приклади застосування розробленого методу для конкретної системи залишкових класів; наведені приклади розрахунку і порівняльного аналізу достовірності контролю даних, представлених в системі залишкових класів. **Висновки:** В даній статті представлені теоретичні основи процесу підвищення достовірності контролю даних, представлених в системі залишкових класів, на основі використання процедури нулевізації чисел. Безпосередньо розроблений і представлений метод підвищення достовірності контролю даних. Наведені приклади застосування розробленого методу для конкретної системи залишкових класів і наведені приклади розрахунку достовірності контролю даних, представлених в системі залишкових класів. Розроблено метод підвищення достовірності контролю даних, є певним внеском в теорію завадостійкого кодування в системі залишкових класів. Приклади розрахунку і порівняльного аналізу достовірності контролю даних підтверджують практичну значимість результатів даної статті.

Ключові слова: обнуління числа; система передачі та обробки даних; система управління інформацією; система числення.

Метод контрольной проверки цифровой информации, представленной в системе остаточных классов

В. А. Краснобаев, А.С. Янко, С. Г. Тур

Аннотация. Предметом исследования в статье являются методы контроля данных, представленных в системе остаточных классов. **Объект** исследований - процесс контроля данных, представленных в системе остаточных классов. **Цель** работы - разработка метода повышения достоверности контроля данных, представленных в системе остаточных классов. В статье решаются следующие **задачи**: исследование методов контроля данных, представленных в системе остаточных классов; разработка метода повышения достоверности контроля данных; рассмотрение примеров применения разработанного метода для конкретной системы остаточных классов; демонстрация примеров расчета и сравнительного анализа достоверности контроля данных, представленных в системе остаточных классов. Используются следующие **методы** исследования: основы системного анализа и основы машинной арифметики в системе остаточных классов. Получены следующие **результаты**: Разработан метод повышения достоверности контроля данных; представлены примеры применения разработанного метода для конкретной системы остаточных классов; приведены примеры расчета и сравнительного анализа достоверности контроля данных, представленных в системе остаточных классов. **Выводы:** В данной статье представлены теоретические основы процесса повышения достоверности контроля данных, представленных в системе остаточных классов, на основе использования процедуры нулевизации чисел. Непосредственно разработан и представлен метод повышения достоверности контроля данных. Приведены примеры применения разработанного метода для конкретной системы остаточных классов и приведены примеры расчета достоверности контроля данных, представленных в системе остаточных классов. Разработан метод повышения достоверности контроля данных, является определенным вкладом в теорию помехоустойчивого кодирования в системе остаточных классов. Примеры расчета и сравнительного анализа достоверности контроля данных подтверждают практическую значимость результатов данной статьи.

Ключевые слова: обнуление числа; система передачи и обработки данных; система управления информацией; система счисления.