computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

DATA ERRORS CONTROL IN THE MODULAR NUMBER SYSTEM BASED ON THE NULLIFICATION PROCEDURE

Victor Krasnobayev [1], Sergey Koshman [1], Sergey Moroz [2], Vyacheslav Kalashnikov [3], Vitaliy Kalashnikov [3]

[1] V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine, v.a.krasnobaev@gmail.com, s.koshman@karazin.ua
[2] Kharkiv Petro Vasylenko National Technical University of Agriculture, 19 Rizdviana st., Kharkiv, 61052, Ukraine, frost9i@ukr.net
[3] Tecnológico de Monterrey, Eugenio Garza Sada av. 2501, 64849 Monterrey, Nuevo León, México, kalash@itesm.mx

Paper history:
Received 15 November 2018
Received in revised form 15 September 2019
Accepted 17 February 2020
Available online 14 May 2020

Keywords:
computer system and components;
modular number system;
information control;
modular arithmetic operations;
zeroing procedure.

Abstract: A method for error control in the modular number system (MNS) based on the use of the zeroing procedure is proposed. Error control in the MNS is a non-positional operation and requires the development of special methods, designed to increase the efficiency of this procedure. This method is designed to verify the correct implementation of the computing process of computer systems and components. It is assumed that the error in one module remainder does not affect the residual values corresponding to other modules (bases) of the MNS. The essence of the method of error control is to use the procedure of pair number zeroing with the preliminary fetching of digits. This makes it possible to increase the efficiency of information control, presented in the modular number system. The practical significance of the results obtained is that, in comparison with the existing methods of error control in MNS, the error detection time is more than halved.

1. INTRODUCTION

The main direction of modern science and technology is the development and use of new advanced information technologies based on the extensive use of computer systems and components (CSC). Information technologies are increasingly invading our lives, penetrating into all processes (social, economic, political). Scales and complexity of the tasks solved by modern computer systems impose qualitatively new requirements for their main characteristics: productivity, reliability and efficiency of systems that leads to the need to improve existing and create new means of information processing [1].

In connection with the constant complication of scientific and technical problems of processing integer data, the trend of development of CSC is aimed at increasing the speed (productivity) and reliability of the implementation of integer arithmetic operations [1, 2]. The results of researches of various groups of scientists and engineers in recent years in the field of information technology, in particular methods for increasing the productivity, reliability, survivability and also reliability of calculations of computer systems have shown that it is practically impossible to achieve this within the limits of the positional number systems (PNS).

This is due to the main disadvantage of modern CSC, functioning in the PNS: the presence of inter-digit relations between the processed numbers. These relations negatively affect the architecture of the CSC and the methods of implementing arithmetic operations, complicate the equipment, they limit the speed and reliability of performing arithmetic operations. In this regard, in the PNS, the increase in the performance of the CSC is achieved by increasing the clock frequency, as well as through the use of methods and tools for parallel data processing, and also by use of different types of reservation [3].

Application of the basic methods of increasing

the productivity of the CSC, based on the parallelization of computations, by using some properties of solvable tasks and algorithms cannot increase the productivity of CSC in each and every case. The scope of their application is limited to a class of tasks to be solved. In addition, the process of artificial dismemberment of the algorithm itself, the determination and allocation of independent computing branches and related operations requires large labor costs, and it is not always possible to parallelize arbitrary algorithms in general. It should be noted that all existing methods of increasing productivity in PNS have a general disadvantage: the impossibility of parsing the maximum algorithms that are solved at the level of elementary operations.

However, this approach does not always solve the problem of extremely large increase in speed and reliability of performing arithmetic operations in the PNS.

To date, there has been a gap between the increasing requirements for improving the performance of real-time computer systems, on the one hand, and the impossibility of satisfying these requests based on the use of existing PNS, on the other hand.

This fact led to the need to find ways to increase productivity, for example, based on the use of new structural solutions to the creation of CSC.

Scientific researches were conducted in recent years, identify promising ways to improve the performance of computer systems, which are based on the use of the modular number system (MNS) [4-6]. However, in existing researches little attention is paid to issues devoted to the implementation of positional operations in the MNS [5-7]. This article focuses on solving this problem.

2. RESEARCH METHODOLOGY AND ANALYSIS OF RESULTS

2.1 SEARCH OF WAYS OF INCREASE IN RELIABILITY

Currently, intensive searches are underway to improve the efficiency of arithmetic operations through the development and implementation of reliable and fast real-time CSC.

The results of the studies devoted to the improvement of the characteristics of CSC showed that one really practical direction is the approach based on the use of MNS codes [2-4]. Ascending from the known Chinese remainder theorem (the task of restoring the original number A_k by aggregating its remainders (deductions) $\{a_i\}$ by dividing it into a series of natural numbers $m_1, m_2, ..., m_n$ (modules) of MNS) , which was previously interpreted as a structural theorem of abstract algebra, guaranteed the specified parallelism in the calculations over integers, under the conditions that the result of ring operations belongs to the range of integers, defined by modules product of MNS [8-9]. Based on the classical works of Euler, Gauss and Chebyshev on the theory of comparisons, MNS introduced new ideas in the development of methods of highly-productive and ultra reliable CSC [10-11].

At present the attention is paid again to the use of MNS as a tool for increase in productivity, reliability, survivability and also reliability of calculations of computer systems. It is caused primarily by the following circumstances:

– the emergence of the numerous scientific and theoretical publications devoted to the theory and practice of the computer systems and components created in MNS [12];

– wide distribution of mobile processors that require high speed data processing at low energy consumption; the lack of inter-bits transfers during arithmetic operations of addition and multiplication of numbers in MNS allows us to reduce energy consumption;

– strong interest in MNS is being shown by the banking structures, where it is necessary in real time to handle large amount of data safely and reliably, i.e. they require highly-productive means for highly reliable computing with errors in self-correction, that is typical of the MNS codes;

– the elements density increasing on a single chip doesn't always allow us to perform a complete and qualitative testing; in this case there is an increasing importance of providing failover operation of CSC;

– the need for the use of the specialized CSC to perform a large number of operations on vectors, which require high-speed performance of integer addition and multiplication operations (matrix multiplication problems, the problems of the scalar product of vectors, Fourier transformation, etc.) [13-15];

– the widespread introduction of microelectronics into all spheres of human activity significantly increased relevance and importance of previously rare, and now so massive scientific and practical problems, as a digital signal and image processing, image recognition, cryptography, multi-bit data processing and storage, etc.; this circumstance requires enormous computing resources being in excess of the existing possibilities [16];

– the current level of microelectronics development is coming to its limits from the point of view of productive provision and reliability of existing and future computer systems and components of large data sets processing in real time;

– the modern development of integrated circuit

technology allows having a fresh look at the principles of devices construction with modular arithmetic employment and provides wide opportunities to use new design techniques (such as the methodology of systems design on a chip-SoC) both in the development of individual computing units, and computer systems in general; integral technology enables more flexible design of computer systems and components and allows us to implement MNS -based devices as effectively as on the basis of the binary system; furthermore at present in order to improve the effectiveness of computer devices development, automated design systems (ADS) are widely used; in this respect, the design of computer systems and components based on MNS does not differ from working with the help of ADS data of binary data-blocks in PNS [17];

– unfortunately, Ukraine today, technologically is behind the microelectronics of some leading foreign countries in contrast with the theoretical development; in this case, it is advisable to use the existing theoretical achievements and practical experience in the creation of effective computer systems and components in MNS [18-20].

One of the disadvantages of MNS is that there are no simple signs of the output of the result of operations outside the operating range [0, *M*), where:

$$M = \prod_{i=1}^{n} m_i ,$$

where M – operating range; m_i – i-th MNS base; n – number of operating bases of MNS. This requires additional time to implement the error correction process. This circumstance reduces the effectiveness of the use of MNS in the CSC.

The majority of control methods of data are based on the analysis of information that is on comparison of data. Therefore, research and development of mathematical models, methods and algorithms of comparison of numbers in MNS is an important and relevant task. Now it is possible to allocate three groups of methods of comparison of numbers in MNS [23-25].

The first group includes methods of direct comparison, based on the conversion of numbers A_{MNS} and B_{MNS} from a code MNS at PNS

$$A_{PNS} = \overline{\alpha_{\rho-1}\alpha_{\rho-2}...\alpha_0}$$

and

$$B_{PNS} = \overline{\beta_{\rho-1}\beta_{\rho-2}...\beta_0},$$

where (ρ – digits number (number length) A_{MNS} and B_{MNS}) and their further comparison on the basis of use of binary position adders.

The second group of methods includes methods based on the principle of zeroing. The procedure for the zeroing process involves transition from initial number

$$A_{MNS} = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1,}..., a_n)$$

presented to MNS to the number of species

$$A_{MNS}^{(z)} = (0, 0, ..., 0, \gamma_n^{(A)}).$$

Then, on value $\gamma_n^{(A)}$ the interval $[jm_i, (j+1)m_i)$ of hit of number is defined A_{MNS}. The number zeroing is performed in the same way

$$B_{MNS} = (b_1, b_2, ..., b_{i-1}, b_i, b_{i+1,}..., b_n)$$

from where we receive values $\gamma_n^{(B)}$. Position comparison of the received values $\gamma_n^{(A)}$ and $\gamma_n^{(B)}$ defines result of comparison of numbers A_{MNS} and B_{MNS} [24-26].

To the third group of methods, we will assign the methods based on the definition (allocation) or the formation of special features, the so-called positional features of the non-positional code [27].

To detect errors in MCC, the most commonly used procedure is zeroing. The essence of the procedure is the successive subtraction from the initial number

$$A = (a_1, a_2, \ldots, a_n, a_{n+1})$$

of certain minimum numbers $ZC^{(i)}$ – zeroing constants such that the number A is successively transformed into a number of type

$$A^{(n)} = (0, 0, \ldots, 0, \gamma_{n+1})$$

in n cycles. If the obtained value of the remainder on the control basis $\gamma_{n+1} \neq 0$, then it is assumed that the number A is erroneous. In this case, the zeroing constants must be chosen in such a way that in the subtractions such as $A - ZC^{(i)}$ the output of the number outside the operating [0, *M*) range [28-30] would not take place. A significant disadvantage of methods of error detection in MNS is the need for significant time and hardware costs in the implementation, which causes significant unproductive computing costs [31-32].

The purpose of this article is the development and research of the error control method in MNS based on the application of the zeroing procedure.

2.2 METHOD OF ERRORS CONTROL

In general, the essence of the procedure of the process of zeroing (*H*1) is the sequence of the following operations [33].

Stage 1. Initial checked number

$$A = A^{(0)} = (a_1^{(0)}, a_2^{(0)}, ...a_i^{(0)}, a_{i+1}^{(0)}, ...a_n^{(0)}, a_{n+1}^{(0)}), \quad (1)$$

is successively reduced to the form

$$A^{(H)} = (0, 0, ..., 0, 0, \gamma_{n+1})$$

by means of a subtraction operation sequence that does not result in the output of a numerical value of the $A^{(0)}$ number outside of the operating range [0, *M*) of MNS. As noted earlier, this operation in MNS is called zeroing, and means successive subtraction (from one of the MNS bases) from the initial number $A^{(0)}$ of minimum numbers, the so-called zeroing constants ($ZC^{(i)}$) of the form:

$$ZC^{(1)} = (t_{1,1}, t_{2,1}, t_{3,1}, ..., t_{n,1}, t_{n+1,1}), t_{1,1} = \overline{1, m_1 - 1};$$
$$ZC^{(2)} = (0, t_{2,2}, t_{3,2}, ..., t_{n,2}, t_{n+1,2}), t_{2,2} = \overline{1, m_2 - 1};$$
$$ZC^{(3)} = (0, 0, t_{3,3}, ..., t_{n,3}, t_{n+1,3}), t_{3,3} = \overline{1, m_3 - 1};$$
$$\dots$$
$$ZC^{(i)} = (0, 0, ..., 0, t_{i,i}, t_{i+1,i}, ..., t_{n,i}, t_{n+1,i}), t_{i,i} = \overline{1, m_i - 1};$$
$$\dots$$
$$ZC^{(n)} = (0, 0, ..., 0, t_{n,n}, t_{n+1,n}), t_{n,n} = \overline{1, m_n - 1}. \quad (2)$$

Next, the initial checked number *A* $A = A^{(0)} = (a_1^{(0)}, a_2^{(0)}, ...a_i^{(0)}, a_{i+1}^{(0)}, ...a_n^{(0)}, a_{n+1}^{(0)})$ is successively reduced to the form $A^{(H)}$, that is,

$$A = A^{(0)} = (a_1^{(0)}, a_2^{(0)}, ...a_i^{(0)}, a_{i+1}^{(0)}, ...a_n^{(0)}, a_{n+1}^{(0)})$$
$$A^{(1)} = (0, a_2^{(1)}, a_3^{(1)}, ..., a_n^{(1)}, a_{n+1}^{(1)}),$$
$$A^{(2)} = (0, 0, a_3^{(2)}, ..., a_n^{(2)}, a_{n+1}^{(2)}),$$
$$A^{(3)} = (0, 0, 0, a_4^{(3)}, ..., a_n^{(3)}, a_{n+1}^{(3)})$$

and so on.

Repeating the subtraction *n* times we get the value $A^{(H)} = (0, 0, ..., 0, a_{n+1}^{(n)})$, or $A^{(H)} = (0, 0, ..., 0, \gamma_{n+1})$, where $\gamma_{n+1} = a_{n+1}^{(n)}$. The general scheme of subtraction $A^{(i)} = A^{(i-1)} - ZC^{(i)}$ is presented in the following form

$$A^{(i-1)} = (0, 0, ..., 0, a_i^{(i-1)}, a_{i+1}^{(i-1)}, ..., a_n^{(i-1)}, a_{n+1}^{(i-1)})$$

–

$$\frac{ZC^{(i)} = (0, 0, ..., 0, a_i^{(i-1)}, t_{i+1,i}, ..., t_{n,i}, t_{n+1,i})}{A^{(i)} = [0, ..., 0, [a_i^{(i-1)} - a_i^{(i-1)}] \bmod m_i,}$$
$$[a_{i+1}^{(i-1)} - t_{i+1,i}] \bmod m_{i+1}, ..., [a_{n+1}^{(i-1)} - t_{n+1,i}] \bmod m_{n+1}],$$

where $a_{i+1}^{(i)} = (a_{i+1}^{(i-1)} - t_{t+1,i}) \bmod m_{i+1}$.

Denoting the sampling time ZC from the corresponding zeroing block (ZB) CSC as t_1, and the subtraction time from the number $A^{(i-1)}$ of constant $ZC^{(i)}$, that is, performing operation $A^{(i)} = A^{(i-1)} - ZC^{(i)}$ – after t_2, we get the total time for performing the operation of zeroing in the form $T_{H1} = n(t_1 + t_2)$. When presenting ZB in the tabular form, we can assume that practically $t_1 = t_2 = \tau_{сл}$. In this case, the zeroing time is equal to the value $T_{H1} = 2n\tau_{sub}$, where: τ_{sub} – subtraction time from number $A^{(i-1)}$ of zeroing constant $KH^{(i)}$; *n* – number of information bases of MNS.

Stage 2. After finding the value γ_{n+1} in the first step, the second stage compares γ_{n+1} with zero. If $\gamma_{n+1} = 0$ (number *A* is in range [0, *M*)), then the conclusion is drawn that the number *A* is not distorted (correct), i.e., there are no errors. If $\gamma_{n+1} \neq 0$ (number *A* isn't in range [0, *M*)), then the conclusion is drawn that the number *A* is distorted (wrong), i.e., there is an error in one of the bases (modules) m_i of MNS. Total time T_1 of error detection is defined as $T_1 = T_{Z1} + Tc_1$, where Tc_1 – time of comparing γ_{n+1} with zero. Practically time Tc_1 comparison is performed in one clock cycle, in this case it can be assumed that $T_1 \approx T_{Z1} = 2n\tau_{sub}$.

In addition, for the implementation of the nullification procedure by the method *H*1 in the ZB, it is necessary to store the *ZC*

$$ZC_{H1} = \sum_{i=1}^{n} m_i - n.$$

In this case, the number of binary digits (N_{H1}) of the ZC, which indirectly determines the amount of ZB equipment, is determined by the expression

$$N_{H1} = \left(\sum_{i+1}^{n} m_i - 1 \right)(n - i).$$

The considered basic method $H1$ does not provide the necessary speed for the implementation of the procedure of zeroing numbers, since the operation of subtracting $A^{(i+1)} = A^{(i)} - ZC^{(i)}$ and fetching the next ZC is separated in time. This is due to the fact that until the subtraction operation is not completed, the remainder of the number by which the ZC should be selected for the next stage of the zeroing process is not known.

The essence of the method of information error detection in MNS proposed in the article is based on the implementation of the procedure of pair number zeroing with preliminary selection of digits ($H4$). This method increases the efficiency of control by reducing the time it takes to implement the procedure of zeroing numbers.

The $H4$ procedure is that the zeroing operation in the ZB is combined in time with the ZB fetching operation by digits $a_i^{(i-1)}$ and $a_{n-i+1}^{(i-1)}$ of number $A^{(i-1)}$ of the constant $ZC^{(i)}$ and creation operation on values $a_i^{(i-1)}$ and $a_{n-i+1}^{(i-1)}$ of numbers $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$. At the same time, the subtraction operation from the number $A^{(i-1)}$ of the zeroing constant $ZC^{(i)}$ (i.e., operation $A^{(i-1)} - ZC^{(i)}$) and the operation of fetching the next zeroing constant

$$ZC^{(i+1)} = (0,\ldots,0,\ t_{i+1,i+1},\ t_{i+2,i+1},\ldots \\ ...,\ t_{n-1,i+1},\ 0,\ldots 0,\ t_{n+1,i+1}).$$

According to the values of $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$ in the next stage of zeroing, on the bases of m_{i+1} and m_{n-i}, we will access the ZB for the next zeroing constant

$$ZC^{(i+1)} = (0,\ldots,0,\ t_{i+1,i+1},\ t_{i+2,i+1},\ldots \\ ...,\ t_{n-1,i+1},\ 0,\ldots 0,\ t_{n+1,i+1}).$$

Indeed, the values of Δa_{i+1} and Δa_{n-i}, which will be subtracted from $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$, respectively, in order to obtain $a_{i+1}^{(i+1)}$ and $a_{n-i-1}^{(i+1)}$, are determined only by the values of $a_i^{(i-1)}$ and $a_{n-i+1}^{(i-1)}$. The number of clock cycles that are free from addition, during which access to the ZB of CSC and the formation of the next address is equal to the value $\left[(n+1)/2\right]$, ([x] is the integer closest to x, but not exceeding it). At the same time, zeroing is carried out simultaneously on two information bases of MNS a_1, a_n; a_2, a_{n-1}, etc. After every two subtractions, one additional time step is required to form the next address and access the accumulator of zeroing constants. In this regard, for every two addition clock cycles ($\tau_{sub} = \tau_0$) there is one clock cycle that is free from addition.

Based on the foregoing, the execution time of the zeroing operation for the considered operational control method ($H2$) is determined by the following expression:

$$T_{H4} = \left[\frac{n+1}{2}\right] \cdot \tau_{sub} + \left[\frac{\frac{n+1}{2}+1}{2}\right] \cdot \tau_{fetch}.$$

The number of ZC in the implementation of the nullification procedure for the method $H4$ in the ZB is determined by the formula:

$$K_{H4} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 2).$$

The number of binary digits (N_{H4}) of the ZC is determined by the expression:

$$N_{H4} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 2) \cdot (n - 2i + 1).$$

For clarity, by the methods for the data control ($H1$ and $H4$) in Fig. 1, we present a fragment of the time diagram of the operation of the ZB.

H1	Access a_1	Σ1	Access $a_2^{(1)}$	Σ2	Access $a_3^{(2)}$	Σ3	Access $a_4^{(3)}$	Σ4	…	
H4	Access a_1, a_n	Σ1	Σ2	Access $a_3^{(2)}$, $a_{n-2}^{(2)}$	Σ3	Σ4	Access $a_5^{(4)}$, $a_{n-4}^{(4)}$	Σ5	…	
	$a_2^{(1)}$, $a_{n-1}^{(1)}$	Access $a_2^{(1)}$, $a_{n-1}^{(1)}$	$a_3^{(2)}$, $a_{n-2}^{(2)}$	$a_4^{(3)}$, $a_{n-3}^{(3)}$	Access $a_4^{(3)}$, $a_{n-3}^{(3)}$	$a_5^{(4)}$, $a_{n-4}^{(4)}$	$a_6^{(5)}$, $a_{n-5}^{(5)}$	Access $a_6^{(5)}$, $a_{n-5}^{(5)}$	…	
0		1	2	3	4	5	6	7	8	9 $T_{Hj}/\tau_{cл}$

Figure 1 – Timing diagrams of the ZB for the presented zeroing methods

Based on the foregoing, we will calculate the values for estimating the time of implementation of the numbers zeroing procedure when using the presented control methods, as well as for determining the required amount of equipment contained in the ZB. The resulting data are summarized in Table 1.

As it can be seen in Table 1, despite the increase in the amount of equipment necessary for the hardware implementation of the ZB, the implementation time of the zeroing procedure is reduced when using the H4 method.

Let us compare the effectiveness of the method of error detection in the MNS proposed in the article with the existing method based on the procedure of ordinary zeroing.

To quantify the effectiveness of the proposed method, we introduce the notion of an efficiency coefficient:

$$K_{j\,\text{ef}}^{(n)} = \frac{T_{Z1}/\tau_{add} - T_{Zj}/\tau_{add}}{T_{Z1}/\tau_{add}} \cdot 100\%, \qquad (3)$$

where j – number of the zeroing method (j=4, for pairwise number zeroing with prefetching of digits).

Expression (3) can also be represented in the form (4):

$$K_{j\,\text{ef}}^{(n)} = \frac{T_{Z1} - T_{Zj}}{T_{Z1}} \cdot 100\%. \qquad (4)$$

In accordance with the expression (4), we define the quantitative value $K_{j\,ef}^{(n)}$ for $j=4$ while $n=4$, $n=6$, $n=8$, $n=10$ and $n=16$, i.e., for l-byte machine words ($l=$ 1, 2, 3, 4, 8) of CSC.

Table 1. The calculated values

l (n)	$H1$			$H4$		
	$\frac{T_{H1}}{\tau_{сл}}$	K_{H1}	N_{H1}	$\frac{T_{H4}}{\tau_{сл}}$	K_{H4}	N_{H4}
1 (4)	8	15	31	3	37	75
2 (6)	12	41	106	4	138	340
3 (8)	16	71	217	6	259	979
4 (10)	20	119	412	7	474	1930
8 (16)	32	367	1947	12	2573	16429

The resulting calculated data will be placed in Table 2.

Table 2. The value of efficiency coefficient

$l(n)$ / K_{ef}	1(4)	2(6)	3(8)	4(10)	8(16)
$K_{ef}^{(n)}$,[%]	62	66	62	65	62

Table 2 shows the calculated data T/τ_{add} of the relative error detection time of information in the MNS for the value of the number n of bases. The number of information bases of the MNS $\overline{n=1,16}$ provides a range of representation of numbers in modern CSC, which makes it possible to use the data obtained when designing them.

Here is an example of a specific technical implementation of the error detection operation in the CSC, which functions in the MNS. Let MNS be given by the bases $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$, $m_5 = 11$ ($n = 4$), i.e. one-byte ($l = 1$) CSC is considered.

In this case, the working numerical range is

$$M = \prod_{i=1}^{4} m_i = 3 \cdot 4 \cdot 5 \cdot 7 = 420,$$

and the full range is

$$M_1 = M \cdot m_{n+1} = 420 \cdot 11 = 4620.$$

The error distribution intervals are shown in Table 3.

Suppose it is necessary to carry out a control (check the fact of presence or absence of an error) of the number:

$$A = A^{(0)} = (a_1^{(0)}, a_2^{(0)}, a_3^{(0)}, a_4^{(0)}, a_5^{(0)}) = \\ = (1,0,0,1,4),$$

represented in the MNS.

Table 3. Numerical intervals of working and full ranges

$[0, M_i)$, $i=\overline{0,10}$	γ_{n+1}	$[0, M_i)$, $i=\overline{0,10}$	γ_{n+1}
0 ÷ 419	0	2520 ÷ 2939	1
420 ÷ 839	2	2940 ÷ 3359	3
840 ÷ 1259	4	3360 ÷ 3779	5
1260 ÷ 1679	6	3780 ÷ 4199	7
1680 ÷ 2099	8	4200 ÷ 4619	9
2100 ÷ 2519	10		

To do this, from the values of the digits $a_1^{(0)} = 1$ and $a_4^{(0)} = 1$ of the number A we choose from the ZB (see Table 3) the zeroing constant in the form

$$ZC^{(1)} = \left(t_{1,1}, t_{2,1}, t_{3,1}, t_{4,1}, t_{5,1}\right),$$

where $t_{1,1} = a_1^{(0)} = 1$ and $t_{4,1} = \mathrm{a}_4^{(0)} = 1$. In this case with ZB we choose $ZC^{(1)} = (1,1,1,1,1)$, Table 4.

Further, in accordance with the proposed method of H4, we perform an operation $A^{(1)} = A^{(0)} - ZC^{(1)}$:

$$\begin{array}{r} A^{(0)} = (1,0,0,1,4) \\ - \\ ZC^{(1)} = (1,1,1,1,1) \\ \hline A^{(1)} = (0,3,4,0,3) \end{array}$$

and, simultaneously, for number

$$A^{(1)} = (0,3,4,0,3)$$

with ZB we choose

$$ZC^{(2)} = \left(0,\ t_{2,2},\ t_{3,2},\ 0,\ t_{5,2}\right),$$

of form $a_2^{(1)} = t_{2,2} = 3$ and $a_3^{(1)} = t_{3,2} = 4$. In this case (see Table 4) $ZC^{(2)}$ is defined as

$$ZC^{(2)} = (0,3,4,0,3).$$

Next, we define the difference $A^{(1)} - ZC^{(2)}$:

$$\begin{array}{r} A^{(1)} = (0,3,4,0,3) \\ - \\ ZC^{(2)} = (0,3,4,0,3) \\ \hline A^{(2)} = (0,0,0,0,0). \end{array}$$

Thus, a zeroed number is obtained

$$A^{(2)} = A^{(Z)} = (0,0,...,0,...,0,\gamma_{n+1}) = (0,0,0,0,\gamma_5),$$

where $\gamma_5 = 0$. Conclusion: the number $A^{(0)} = (1,0,0,1,4)$ has no errors (see Table 3).

Verification: the number $A^{(0)}$ in the PNS is $A^{(0)} = 400$, i.e., is within the working numerical range [0, 419).

Table 4. The value of ZC

PNS	$m_1 = 3$, $m_4 = 7$	PNS	$m_2 = 4$, $m_3 = 5$
1	1,1,1,1,1	21	0,1,1,0,10
2	2,2,2,2,2	84	0,0,4,0,7
3	0,3,3,3,3	105	0,1,0,0,6
4	1,0,4,4,4	42	0,2,2,0,9
5	2,1,0,5,5	63	0,3,3,0,8
6	0,2,1,6,6	126	0,2,1,0,5
7	1,3,2,0,7	147	0,3,2,0,4
8	2,0,3,1,8	168	0,0,3,0,3
9	0,1,4,2,9	189	0,1,4,0,2
10	1,2,0,3,10	252	0,0,2,0,10
11	2,3,1,4,0	273	0,1,3,0,9
12	0,0,2,5,1	210	0,2,0,0,1
13	1,1,3,6,0	231	0,3,1,0,0
14	2,2,4,0,3	294	0,2,4,0,8
15	0,3,0,1,4	315	0,3,0,0,7
16	1,0,1,2,5	336	0,0,1,0,6
17	2,1,2,3,6	357	0,1,2,0,5
18	0,2,3,4,7	378	0,2,3,0,4
19	1,3,4,5,8	399	0,3,4,0,3
20	2,0,0,6,9		

3. CONCLUSION

In the modern world a rapid growth of volumes of information and increase in complexity of the set of scientific and technical tasks, connected with achievement of appropriate level of quality and reliability of transmitted data is observed. Therefore, the main objective of scientists in the field is development of theoretical bases for construction of high-speed and reliable CSC [30–33].

In PNS the problem of increase in reliability and productivity can't be effectively solved without deterioration some key technical and economic indicators of CSC. At the same time, there are positive results of researches which have shown efficiency of application of MNS for increase in speed of performing integer arithmetic operations, reduction of time of error detection and as a result, an increase in the productivity and reliability of CSC [36-38]. The methodological basis for building a CSC in the MNS involves a comprehensive solution to the problem of increasing the productivity and integrity of the processing of integer data, as well as providing information security, impedance, performance and durability of the functioning of CSC. Existing data comparison method in MNS

does not provide the maximum accuracy of comparison of numbers. Thus, there is a problem of improvement of a method of the fast comparison of data based on the application of the zeroing procedure [39].

It is known that considerable time of control of data reduces overall effectiveness of application of CSC in MNS while performing integer arithmetic and other modular operations. Results of the research on control methods of the data in MNS, carried out in article have shown that the existing control methods of data in MNS based on use of application of the zeroing procedure reduce control time [35-37].

Application of this method provides obtaining reliable result of control of data in MNS. By the accuracy of the control data in the MNS, we understand the probability of obtaining the true result of the control operation data presented in the MNS [39–41].

The essence of the method of error control is to use the procedure of pair number zeroing with the preliminary fetching of digits. This makes it possible to increase the efficiency of the procedure for data zeroing in comparison with other control methods up to 30%. The practical significance of the results obtained is that, in comparison with the existing methods of error control in MNS, the error detection time is more than halved. This circumstance makes it possible to increase the overall efficiency of the use of MNS while creating CSC.

4. REFERENCES

[1] J. Wang, S. Ma, Z.-G. Yang and J. Hu, "A systemic performance evaluation method for residue number system," *Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, 2016, pp. 321-325.

[2] I.Ya. Akushskii and D.I. Yuditskii, *Machine Arithmetic in Residual Classes*, Sov. Radio, Moscow, 1968.

[3] K. Phalakarn and A. Surarerks, "Alternative redundant residue number system construction with redundant residue representations," *Proceedings of the 2018 3rd International Conference on Computer and Communication Systems (ICCCS)*, Nagoya, 2018, pp. 457-461.

[4] S. Wei and C. Jiang, "Residue signed-digit arithmetic and the conversions between residue and binary numbers for a four-moduli set," *Proceedings of the 2012 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science*, Guilin, 2012, pp. 436-440.

[5] V. Krasnobayev, A. Kuznetsov, S. Koshman, S. Moroz, "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, 05 August 2018. DOI: 10.1007/978-3-319-97885-7_31.

[6] A. Armand and S. Timarchi, "Low power design of binary signed digit residue number system adder," *Proceedings of the 2016 24th Iranian Conference on Electrical Engineering (ICEE)*, Shiraz, 2016, pp. 844-848.

[7] A. Yanko, S. Koshman, V. Krasnobayev, "Algorithms of data processing in the residual classes system," *Proceedings of the 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, 2017, pp. 117-121.

[8] S. Wei, "An RSA encryption implementation method using residue signed-digit arithmetic circuits," *Proceedings of the 2012 5th International Conference on BioMedical Engineering and Informatics*, Chongqing, 2012, pp. 1299-1303.

[9] A. Safari, J. Nugent and Y. Kong, "Novel implementation of full adder based scaling in residue number systems," *Proceedings of the 2013 IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Columbus, OH, 2013, pp. 657-660.

[10] G. Harman and I. E. Shparlinski, "Products of small integers in residue classes and additive properties of Fermat quotients," *International Mathematics Research Notices*, vol. 2016, no. 5, pp. 1424-1446, Jan. 2016.

[11] D. Younes and P. Steffan, "Efficient image processing application using residue number system," *Proceedings of the 20th International Conference Mixed Design of Integrated Circuits and Systems – MIXDES 2013*, Gdynia, 2013, pp. 468-472.

[12] V. Krasnobayev and S. Koshman, "A method for operational diagnosis of data represented in a residue number system," *Cybernetics and Systems Analysis*, vol. 54, issue 2, pp. 336-344, 2018.

[13] B. Cao, T. Srikanthan and Chip-Hong Chang, "Design of residue-to-binary converter for a new 5-moduli superset residue number system," *Proceedings of the 2004 IEEE International Symposium on Circuits and Systems (IEEE Cat. No.04CH37512)*, Vancouver, BC, 2004, pp. II-841.

[14] K. Tao, L. Peng, K. Liang and B. Zhuo, "Irregular repeat accumulate low-density parity-check codes based on residue class pair," *Proceedings of the 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, Guangzhou, 2017, pp. 127-131.

[15] A. Rahman, M. T. Naseem, I. M. Qureshi and M. Z. Muzaffar, "Reversible watermarking using residue number system," *Proceedings of the 2011 7th International Conference on Information Assurance and Security (IAS)*, Melaka, 2011, pp. 162-166.

[16] F. Barsi and P. Maestrini, "Error correcting properties of redundant residue number systems," *IEEE Transactions on Computers*, vol. C-22, no. 3, pp. 307-315, March 1973.

[17] D. K. Taleshmekaeil, A. Safari and Y. Kong, "Using one hot residue number system (OHRNS) for digital image processing," *Proceedings of the 16th CSI International Symposium on Artificial Intelligence and Signal Processing (AISP 2012)*, Shiraz, Fars, 2012, pp. 064-067.

[18] A. Kuznetsov, I. Kolovanova and T. Kuznetsova, "Periodic characteristics of output feedback encryption mode," *Proceedings of the 2017 4th International Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 193-198.

[19] M. Labafniya and M. Eshghi, "An efficient adder/subtracter circuit for one-hot residue number system," *Proceedings of the 2010 International Conference on Electronic Devices, Systems and Applications*, Kuala Lumpur, 2010, pp. 121-124.

[20] Yu.V. Stasev, A.A. Kuznetsov "Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes," *Cybernetics and System Analysis*, no. 3, pp. 47-57, May-June 2005.

[21] D. J. Guan and Y. Cheng, "Parity detection for some three-modulus residue number system," *Proceedings of the 2014 Ninth Asia Joint Conference on Information Security*, Wuhan, 2014, pp. 76-81.

[22] V. Krasnobayev, S. Koshman and A. Yanko, "The method of error detection and correction in the system of residual classes," *Computer Science and Cybersecurity*, Issue 1(1), pp. 58–66, 2016.

[23] A. Mirshekari and M. Mosleh, "Hardware implementation of a fast FIR filter with residue number system," *Proceedings of the 2010 2nd International Conference on Industrial Mechatronics and Automation*, Wuhan, 2010, pp. 312-315.

[24] S. Wei, "Fast signed-digit arithmetic circuits for residue number systems," *Proceedings of the 2015 IEEE International Conference on Electronics, Circuits, and Systems (ICECS)*, Cairo, 2015, pp. 344-347.

[25] E. B. Olsen, "RNS hardware matrix multiplier for high precision neural network acceleration: 'RNS TPU'," *Proceedings of the 2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, Florence, 2018, pp. 1-5. doi: 10.1109/ISCAS.2018.8351352

[26] A. Hariri, K. Navi and R. Rastegar, "A simplified modulo (2^n-1) squaring scheme for residue number system," *Proceedings of the International Conference on "Computer as a Tool" EUROCON 2005*, Belgrade, 2005, pp. 615-618.

[27] C. Fan and G. Ge, "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, Feb. 2014.

[28] S. Jayashri and P. Saranya, "Reconfigurable FIR filter using distributed arithmetic residue number system algorithm based on thermometer coding," *Proceedings of the 2014 International Conference on Communication and Signal Processing*, Melmaruvathur, 2014, pp. 1991-1995.

[29] I. Gorbenko, A. Kuznetsov, M. Lutsenko and D. Ivanenko, "The research of modern stream ciphers," *Proceedings of the 2017 4th International Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 207-210. DOI: 10.1109/INFOCOMMST.2017.8246381

[30] S. Akhter, G. Raturi and S. Khan, "Analysis and design of residue number system based building blocks," *Proceedings of the 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, 2018, pp. 441-445.

[31] K. Runovski, & H.-J. Schmeisser, "On the convergence of Fourier means and interpolation means," *Journal of Computational Analysis and Applications*, vol. 6, issue 3, pp. 211-227, 2004.

[32] S. Bondarenko, L. Bodenchuk, O. Krynytska and I. Gayvoronska, "Modelling instruments in risk management," *International Journal of Civil Engineering and Technology*, vol. 10, issue 1, pp. 1561-1568, 2019.

[33] V. Krasnobayev, S. Koshman and A. Yanko, "The method for real-time data control within the system of residue classes based on the consecutive nullification principle" *Radioelectronic and Computer Systems*, no. 1(81), pp. 57-68, 2017.

[34] A. Molahosseini, F. Teymouri and K. Navi, "A new four-modulus RNS to binary converter," *Proceedings of 2010 IEEE International Symposium on Circuits and Systems*, Paris, 2010, pp. 4161-4164 DOI: 10.1109/iscas. 2010.5537592.

[35] T. Singh, "Residue number system for fault detection in communication networks," *Proceedings of the 2014 International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom)*, Greater Noida, 2014, pp. 157-161.

[36] L. Sousa, "Efficient method for magnitude comparison in RNS based on two pairs of conjugate moduli," *Proceedings of the 18th IEEE Symposium on Computer Arithmetic (ARITH'07)*, 2007, pp. 240-250. DOI: 10.1109/arith.2007.16.

[37] R. Chornei, V. M. Hans Daduna, & P. Knopov, "Controlled Markov fields with finite state space on graphs," *Stochastic Models*, vol. 21, issue 4, pp. 847-874, 2005. doi: 10.1080/15326340500294520

[38] H. K Bello and K.A Gbolagade, "A MRC based RNS to binary converter using the moduli set $\{2^{2n+1}-1, 2^{n-1}, 2^{2n}-1\}$," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 6, issue 7, July 2017.

[39] A. H. Navin, A. S. Khashandarag, A. R. Oskuei and M. Mirnia, "A novel approach cryptography by using residue number system," *Proceedings of the 2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, Seogwipo, 2011, pp. 636-639.

[40] V. S. Veeravalli, "Modified residue codes based on residue number system as a fault tolerance scheme," *Proceedings of the IEEE Southeastcon 2009*, Atlanta, GA, 2009, pp. 383-387.

[41] B. P. Tkach, & L. B. Urmancheva, "Numerical-analytic method for finding solutions of systems with distributed parameters and integral condition," *Nonlinear Oscillations*, vol. 12, issue 1, pp. 113-122, 2009. doi:10.1007/s11072-009-0064-6

[42] J. Bajard, L. Didier and P. Kornerup, "An RNS Montgomery modular multiplication algorithm," *IEEE Transactions on Computers*, vol. 47, no. 7, pp. 766-776, 1998. DOI: 10.1109/12.709376.

Victor Krasnobayev, *Doctor of Sciences (Engineering), Full Professor, a Professor of the Department of Electronics and Control Systems of V. N. Karazin Kharkiv National University.*

Areas of scientific interests: the theory and practice of creating computer systems and components in a residue numeral system.

Sergey Koshman, *Candidate of Sciences (Engineering), an Associate Professor of the Department of Information Systems and Technologies Security of V. N. Karazin Kharkiv National University.*

Areas of scientific interests: theory and practice of noise combating data coding in a residue numeral system.

Sergey Moroz, *Candidate of Sciences (Engineering), an Associate Professor of the Department of Automation and computer-integrated technologies of Kharkiv Petro Vasylenko National Technical University of Agriculture.*

Areas of scientific interests: the methods for fast and reliable data processing in telecommunication systems and networks.

Vyacheslav Kalashnikov, *Doctor of Sciences (Physics and Mathematics), Full Professor, Department of Systems and Industrial Engineering, Tecnológico de Monterrey, Monterrey, Nuevo León, México.*

Areas of scientific interests: information theory and coding.

Vitaliy Kalashnikov, *Ph.D., an Associate Professor at the Department of Systems and Industrial Engineering, Tecnológico de Monterrey, Monterrey, Nuevo León, México. Areas of scientific interests: information theory and coding, security information systems and technologies.*