Method of Error Control of the Information Presented in the Modular Number System

Victor Krasnobayev, Sergey Koshman
V.N. Karazin Kharkiv National University
Kharkiv, Ukraine
v.a.krasnobaev@gmail.com, s.koshman@karazin.ua

Alina Yanko, Anatolii Martynenko
Poltava National Technical Yuri Kondratyuk
University Poltava, Ukraine
al9_yanko@ukr.net, martynenko@pntu.edu.ua

***Abstract*—A method for error control in the modular number system (MNS) based on the use of the zeroing procedure is proposed. 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 proposed method is that, when performing the procedure of zeroing in the MNS, the operation of determining is combined in time, in accordance with the corresponding digits of the number A, the zeroing constant and the calculation operation for the corresponding values of the digits of the number A. This makes it possible to increase the efficiency of monitoring information presented in the modular number system.**

Keywords—computer system and components, modular number system, information control, modular arithmetic operations

I. Introduction

A modern feature of an industrial society is the development and use of new advanced information technologies based on the extensive use of computer systems and components (CSC). 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. The results of recent years on the study of methods for increasing the performance and reliability of the calculations of CSC 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, 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. However, this approach does not always solve the problem of cardinal increase in speed and reliability of performing arithmetic operations in the PNS.

II. Research Methodology And Analysis Of Results

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 modular number system (MNS) codes [1-3]. 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: $M = \prod_{i=1}^{n} m_i$ is operating range; m_i is i-th MNS base; n is number of operating bases of MNS. This requires additional time to implement error correction process. This circumstance reduces effectiveness of use of MNS in CSC.

To detect errors in MNS, the most commonly used procedure is zeroing. The essence of the procedure consists in 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 [4-7] 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 [8-12].

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.

III. Method Of Error Control

In general, the essence of the procedure of the process of zeroing consists of the sequence of the following operations.

Stage 1. Initial checked number

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

is successively reduced to the form $A^{(H)} = (0, 0, \ldots, 0, 0, \gamma_{n+1})$ 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 consists from 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:

978-1-5386-6611-1/18/$31.00 ©2018 IEEE

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

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

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

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

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 $T_{H1} = 2n\tau_{сл}$, where: $\tau_{сл}$ – 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 on 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 $T_1 \approx T_{Z1} = 2n\tau_{add}$.

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 (PNZPSD). The PNZPSD procedure is that the zeroing operation in the ZB is combined in time with the BZC selection 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 selecting the next zeroing constant

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

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 refer to the BZC for the next zeroing constant

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

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 the reference is made to the BZC 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 ($\tau_{add} = \tau_0$) there is one clock cycle that is free from addition. Let's 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:

$$K_{j\,\text{ef}}^{(n)} = \frac{T_{Z1}/\tau_{add} - T_{Zj}/\tau_{add}}{T_{Z1}/\tau_{add}} \cdot 100\%, \qquad (1)$$

where j – number of the zeroing method (j=2, for pairwise zeroing; j=3, for pairwise zeroing with prefetching of digits; j=4, for pairwise number zeroing with prefetching of digits).

Expression (1) can also be represented in the form (2)

$$K_{j\,\text{ef}}^{(n)} = \frac{T_{Z1} - T_{Zj}}{T_{Z1}} \cdot 100\%. \qquad (2)$$

In accordance with the expression (2), we define the quantitative value $K_{j\,ef}^{(n)}$ for $j=\overline{2,4}$ 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.

The resulting calculated data will be placed in Table I.

TABLE I. CALCULATED DATA OF THE 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 I 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 II.

TABLE II. THE ERROR DISTRIBUTION INTERVALS

$[0,M_i)$, $i=\overline{0,10}$	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		

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.

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 III) 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 $t_{4,1}=a_4^{(0)}=1$. In this case with ZB we choose $ZC^{(1)}=(1,1,1,1,1)$, Table III. Further, in accordance with the proposed method of PNZPSD, we perform an operation $A^{(1)}=A^{(0)}-ZC^{(1)}$:

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

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 III) $ZC^{(2)}$ is defined as $ZC^{(2)}=(0,3,4,0,3)$.

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

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

TABLE III. THE ZEROING CONSTANT

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		

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 2).

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

IV. Conclusion

The essence of the method of error control is to use the procedure of pair number zeroing with the preliminary selection 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 in the creation of CSC.

References

[1] I.Ya. Akushskii and D.I. Yuditskii, *Arifmetika mashiny v klassah ostatkov* [*Machine Arithmetic in Residual Classes*], Sov. Radio, Moscow, 1968. (in Russian)

[2] V. Krasnobayev, A. Yanko and S. Koshman, "A Method for arithmetic comparison of data represented in a residue number system," *Cybernetics and Systems Analysis*, vol. 52, issue 1, pp. 145-150, 2016.

[3] O. Karpenko, A. Kuznetsov, V. Sai and Yu. Stasev, "Discrete Signals with Multi-Level Correlation Function," *Telecommunications and Radio Engineering*, vol. 71, issue 1, pp. 91-98, 2012.

[4] V. Krasnobayev, S. Koshman and M. Mavrina, "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, 2014.

[5] S. Kavun, A. Zamula and I. Mikheev, "Calculation of expense for local computer networks," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 146-151.

[6] 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.

[7] O. Kazymyrov, R. Oliynykov and H. Raddum, "Influence of addition modulo 2n on algebraic attacks," *Cryptography and Communications*, vol. 8, issue 2, pp. 277–289, April 2016.

[8] *The Morgan Kaufmann Series in Computer Architecture and Design by David A. Patterson*, Morgan Kaufmann; 1 edition, 2016.

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

[10] O. Kuznetsov, Yu. Gorbenko, I. Bilozertsev, A. Andrushkevych and O. Narizhnyi, "Algebraic Immunity of Non-linear Blocks of Symmetric Ciphers," *Telecommunications and Radio Engineering*, vol. 77, issue 4, pp. 309-325, 2018.

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

[12] Yu.V. Stasev, A.A. Kuznetsov, and A.M. Nosik, "Formation of pseudorandom sequences with improved autocorrelation properties", *Cybernetics and Systems Analysis*, vol. 43, issue 1, pp. 1-11, January 2007.

[13] N. Naumenko, Yu. Stasev, and A. Kuznetsov, "Methods of synthesis of signals with prescribed properties," *Cybernetics and Systems Analysis*, vol. 43, Issue 3, pp. 321-326, May 2007.

[14] V. Ruzhentsev, and R. Oliynykov, "Properties of Linear Transformations for Symmetric Block Ciphers on the basis of MDS-codes," *Proceedings of the 6th International Conference on Network Architecture and Information System Security SAR-SSI*, 2011, pp. 193-196.

[15] O. Potii, O. Illiashenko, and D. Komin, "Advanced Security Assurance Case Based on ISO/IEC 15408," *Theory and Engineering of Complex Systems and Dependability Advances in Intelligent Systems and Computing*, vol. 365, pp 391-401, 2015.

[16] Amir Sabbagh Molahosseini, Leonel Seabra de Sousa, and Chip-Hong Chang, *Embedded Systems Design with Special Arithmetic and Number Systems*, Springer International Publishing, 2017.

[17] V. Dolgov, I. Lisitska, and K. Lisitskyi, "The new concept of block symmetric ciphers design," *Telecommunications and Radio Engineering*, vol. 76, issue 2, pp. 157-184, 2017.

[18] A. Kuznetsov, A. Smirnov, D. Danilenko, and A. Berezovsky, "The statistical analysis of a network traffic for the intrusion detection and prevention systems," *Telecommunications and Radio Engineering*, vol. 74, issue 1, pp. 61-78, 2015.

[19] R. Gavrylko, and Yu. Gorbenko, "A physical quantum random number generator based on splitting a beam of photons," *Telecommunications and Radio Engineering*, vol. 75, issue 2, pp. 179-188, 2016.