Method of Diagnostic of Non-Positional Code Structures in the System of Residue Classes Basing on the Usage of an Alternative Number Set Informativeness

Victor Krasnobayev^a, Alexander Kuznetsov^{a,b}, Anna Kononchenko^a, and Tetiana Kuznetsova^a

^a V. N. Karazin Kharkiv National University, 4 Svobody sq., Kharkiv, 61022, Ukraine

b JSC "Institute of Information Technologies," 12 Bakulin str., Kharkiv, 61166, Ukraine

Abstract

A method of diagnosis of data represented in the system of residue classes (SRC) is suggested in the article. It is shown, that the main disadvantage of existing methods of diagnosis data in SRC is a significant time of data diagnosis while the necessity of entering heavy informational redundancy to non-positional code structure (NCS) in SRC. The considered in the article method of diagnosis data in SRC allows increasing operability of a diagnosis procedure while entering minimal informational redundancy. The time of data diagnostic, compared to known methods, is decreasing firstly due to excluding the procedure of transforming numbers in SRC to positional notation as in known methods, i. e. eliminating a positional operation of numbers comparing. Secondly, the time of data diagnostic is decreased by reducing the quantity of SRC bases, which are giving the possibility of mistakes. Thirdly, the time of data diagnostic is decreased due to the usage of tabular sample value of an alternative set (AS) of numbers in SRC in one beat. The quantity of additionally entered informational redundancy is decrease by effective usage of inner informational redundancy existing in NCS. A specific example of the usage of the suggested method of diagnosis data in SRC is given. Therefore, the suggested method allows reducing the time of diagnosis of data errors in NCS, represented in SRC, which is increasing the diagnostic operability while entering minimal informational redundancy.

Keywords

Non-positional code structures, system of residue classes, alternative number set informativeness.

1. Introduction

 \overline{a}

 \odot $\mathsf{L}^\infty_\text{rec}$

A foundation of some modern specialized informational and telecommunication systems is based on computer systems (CS) of handling integer data, represented in non-positional notation in residue classes (SRC) [1–4]. In this case, one of the main ways of achieving high effectiveness of functioning of telecommunication systems while handling integer data in real-time is an improvement, firstly, such features of CS in SRC as reliability and performance of data handling [5–8].

It is known, that usage of such features of SRC as independence, rights equality, and low-discharge of residues $\{a_i\}$ defining non-positional code structure (NCS) of data 1 2 1 1 (|| ||...|| || || ||...|| ||...||) *A a a a a a a a SRC i i i n n k*

provides high user performance of implementing in CS calculation algorithms, which consist of a set of integer arithmetical operations [9–12]. The largest effectiveness of SRC usage can be achieved in case if implemented algorithms consist of a set of such arithmetical operations as addition, multiplication, and subtraction [8, 13, 14].

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine

EMAIL: v.a.krasnobaev@gmail.com (A.1); kuznetsov@karazin.ua (A.2); akononpro@gmail.com (A.3); kuznetsova.tatiana17@gmail.com (A.4)

ORCID: 0000-0001-5192-9918 (A.1)[; 0000-0003-2331-6326](https://www.scopus.com/redirect.uri?url=http://www.orcid.org/0000-0003-2331-6326&authorId=55428957200&origin=AuthorProfile&orcId=0000-0003-2331-6326&category=orcidLink) (A.2); 0000-0002-8101-6500 (A.3); 0000-0001-6154-7139 (A.4)

 \bigcirc ©️ 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings (CEUR-WS.org)

On the other hand, a necessity of providing fault-tolerant functioning of CS in SRC requires the development and deployment of methods of quick control, diagnostic, and data error correction, which are different from methods, used in regular binary positional notations (PN) [15–17].

Thus, researches, devoted to the development and improvement of quick (operative) methods of diagnostic of errors of data in CS, functioning in SRC, are important and relevant.

The aim of the article is the development of the method of quick diagnostic of data in SRC while entering minimal informational redundancy.

In the general case, the diagnosis of data in SRC is being understood as a process of defining distorted residues in NCS as as
 $A_{SRC} = (a_1 || a_2 || ... || a_{i-1} || a_i || a_{i+1} || ... || a_n || ... || a_{n+k})$

$$
A_{\textit{SRC}} = (a_{\textit{i}} \, || \, a_{\textit{i}} \, || \, ... || \, a_{\textit{i}-1} \, || \, a_{\textit{i}} \, || \, a_{\textit{i}+1} \, || \, ... || \, a_{\textit{n}} \, || \, ... || \, a_{\textit{n+k}}),
$$

where n and k are quantity of informational and control bases m_i ($i = 1, n + k$) in ordered ($m_i < m_{i+1}$) SRC, correspondingly.

The diagnostic of NCS is being performed after the data control for further probable error correction. In the article, the method of data diagnostic in the case of entering minimal $(k = 1)$ informational redundancy is considered. The minimal code distance equals two. The method is based on the concept of an alternative number set and the usage of features of NCS in SRC [10,14]. Due to those the procedure of increasing informativeness of AS in SRC is developed.

2. The Method of Diagnostic of Non-Positional Code Structures in the System of Residue Classes

Consider the method of NCS diagnostic, based on obtaining additional information about probably distorted residues of incorrect number *A* . This information is contained in all possible AS of number *A*.

Let SRC is specified by ordered $(m_i < m_{i+1})$ bases $m_1, ..., m_{n+1}$. And let an incorrect number A is defined in the process of calculations.

For increasing informativeness about placement and error measures, it is suggested to additionally define AS of number as $W_{k_{\rho_i}}\left(\tilde{A}\right) = \left\{m_{k_1}, m_{k_2}, \dots, m_{k_{\rho_i}}\right\},\$

i.e. set AS:

$$
W_{1_{\rho_1}}(\tilde{A}) = \{m_{11}, m_{12}, \dots, m_{1_{\rho_1}}\};
$$

\n
$$
W_{2_{\rho_2}}(\tilde{A}) = \{m_{21}, m_{22}, \dots, m_{2_{\rho_2}}\};
$$

\n
$$
\vdots
$$

\n
$$
W_{n+1_{\rho_{n+1}}}(\tilde{A}) = \{m_{n+1}, m_{n+2}, \dots, m_{n+1_{\rho_{n+1}}}\}.
$$

\n(1)

Tentatively calculate the value of the interval $(j+1)$ of the number A occurrence in order to define the set of values (1)

$$
j_k = \overline{m}_k \cdot \gamma_k \left(\bmod m_k \right),\tag{2}
$$

for $k = 1, n + 1$.

Also, due to value $k = n + 1$ the $W_{n+1_{\rho_{n+1}}} (A)$ equals

$$
W_{n+1_{\rho_{n+1}}}\left(\tilde{A}\right) = W\left(\tilde{A}\right).
$$

According to (2) the formation of k tables is performed, where values γ_k are matched against Δa_i . After defining AS $W_{k_{\rho_i}}(A)$, which called primary ASs, the secondary ASs are defined as vectors, components of which are possible values of errors Δa_i as:

$$
W_1^{(1)}\left(\tilde{A}\right) = \left\{\Delta a_1^{(1)}, \Delta a_2^{(1)}, ..., \Delta a_{n+1}^{(1)}\right\},\,
$$

$$
W_1^{(\psi_1)}(\tilde{A}) = \left\{ \Delta a_1^{(\psi_1)}, \Delta a_2^{(\psi_1)}, ..., \Delta a_{n+1}^{(\psi_1)} \right\};
$$

$$
W_2^{(2)}(\tilde{A}) = \left\{ \Delta a_1^{(2)}, \Delta a_2^{(2)}, ..., \Delta a_{n+1}^{(2)} \right\},
$$

$$
W_2^{(\psi_2)}(\tilde{A}) = \left\{ \Delta a_1^{(\psi_2)}, \Delta a_2^{(\psi_2)}, ..., \Delta a_{n+1}^{(\psi_2)} \right\};
$$

and so on to the value of vectors in the form of:

$$
W_n^{(\psi_n)}\left(\tilde A\right) = \left\{\Delta a_1^{(\psi_n)},\Delta a_2^{(\psi_n)},...,\Delta a_{n+1}^{(\psi_n)}\right\},\,
$$

and completely to value of vector as:

$$
W_{n+1}(\tilde{A})=\{\Delta a_1,\,\Delta a_2,\,\ldots,\,\Delta a_{n+1}\}.
$$

Components of the vector $W_{n+1}(\tilde{A})$ are compared to according components of all vectors $W_i^{(\psi_i)}(\tilde{A})$ for $i = 1, n$. The matching the measure components of vectors are chosen and the bases of SRC are defined, and their set defines resulted AS in the form of

$$
W'\left(\tilde{A}\right) = \left\{m_{z_1}, m_{z_2}, \ldots, m_{z_\rho}\right\}.
$$

Indeed, among AS $W_{k_{\rho}}(A)$ there is always a basis m_i , which gives an error Δa_i , and that basis can be only among bases, which are common for the set (1)

$$
W(\tilde{A}) \ge W'(\tilde{A}).
$$
\n(3)

When an Δa_i has such value, that number A starts to belong to the interval, then an equation is fulfilled

$$
W(\tilde{A}) = W'(\tilde{A})
$$
\n(4)

where

1 *n* $\prod_{i=1}^{\mathbf{r}}$ $M = \prod m$ $=\prod_{i=1}$

and

$$
M_1 = M \cdot m_{n+1}
$$

.

Thus, the idea of the suggested method lays in the following: all possible ASs are defined on each of the intervals of number *A* occurrence. After this, the common for these intervals bases

$$
m_{z_1},\,\ldots\,,m_{z_\rho}\,,
$$

which possibly give errors, are defined.

That set of bases define sought AS. The reduction of the number of bases in AS increases the informativeness of AS $W(A)$ about place and measure of error. It decreases the time of reducing AS to an incorrect basis (the amount of steps of tentatively AS defining is decreasing) and increases operability of diagnostic of data in SRC.

The structure scheme of the process of AS reduction is presented in Fig. 1.

Figure 1: Scheme of choice of bases in the alternative set of numbers in SRC

3. Geometrical Model of the Procedure of the Increasing AS Informativeness

The geometrical model of the suggested method should be considered. The defining of the number $(j+1)$ of the interval of distorted number A occurrence, which is influenced by error Δa_i , is equivalent to the shift of this number in the interval $j^{\frac{m_i}{2}}$, $(j+1)^{\frac{m_1}{2}}$ 1 $\frac{i}{j}$, $(j+1)$ *i* $j\frac{M_i}{(j+1)}$ m_i ['], $($ $)$ ⁻ $+$ </sub> $)$ _{*m*} $[M_{i} \left(\ldots \right) M_{i}]$ $j^{\frac{m_i}{m}}(j+1)^{\frac{m_1}{m}}$ $\begin{bmatrix} m_i & m_1 \end{bmatrix}$ to the left to value $j^{\frac{M_1}{M_2}}$ 1 $\frac{M}{\gamma}$ *m* . Decompose numerical sequence to corresponding intervals with length: $\frac{m_1}{m_2}$ 1 *M m* $, \frac{m_1}{\sqrt{m_1}}$ 2 *M m* $,...,\frac{m_1}{\cdots}$ *n*+1 *M* m_{n+} . Define the numbers of intervals $(j+1)$, in which there is an operand \overline{A} on each of the numerical segments as

$$
T_{j_1} = \left[j_1 \frac{M_1}{m_1}, (j_1 + 1) \frac{M_1}{m_1} \right],
$$

\n
$$
T_{j_{n+1}} = \left[j_{n+1} \frac{M_1}{m_{n+1}}, (j_{n+1} + 1) \frac{M_1}{m_{n+1}} \right].
$$
 (5)

Defining the primary ASs (1) corresponds to defining the intervals numbers (5). Defining the secondary AS $W'(A)$ geometrically correspond to defining the interval $[z_1, z_2]$, where

$$
z_1 = \max \in j_i \frac{M_1}{m_i};
$$

$$
z_2 = \min \in (j_i + 1) \frac{M_1}{m_i},
$$

i.e. sought interval is being defined as intersecting of intervals sets (5)
 $T_{w'(\tilde{A})} = T_{\tilde{A}} \wedge T_{\tilde{A}} \wedge \dots \wedge T_{\tilde{J}_{n+1}}.$

$$
T_{W'(\tilde{A})} = T_{j_1} \wedge T_{j_2} \wedge \dots \wedge T_{j_{n+1}}.
$$

It is obvious, that

$$
z_2 - z_1 = \frac{M_1}{M_{n+1}}.
$$
\n(6)

Condition (6) is equivalent to condition (3). If error moves operand *A* to the interval $\left[\left(m_{n+1}-1\right), M, \mathbf{M}_1\right]$, then

$$
z_2 - z_1 = \frac{M_1}{m_{n+1}} = M \tag{7}
$$

Condition (7) is equivalent to condition (4).

The suggested geometrical model confirms the correctness of the method's mathematical description, and also more clearly demonstrates the idea of the procedure of informativeness AS increasing or the reduction of the numerical interval of distorted number *A* occurrence.

Consider an example of defining AS of number *A* according to the developed method. There is SRC with bases $m_1 = 2$, $m_2 = 3$, $m_3 = 5$. The code words of this SRC are presented in Table 1.

Thus,

Table 1.

$$
M = 2 \cdot 3 = 6
$$
, $M_1 = M \cdot 5 = 30$, $m_{n+1} = m_3 = 5$, $A = (0, 2, 2)$, $\Delta A = (0, 2, 0)$.

Assume, that after the influence of a single error

$$
\Delta A = (0, 0, \dots, \Delta a_i, \dots, 0)
$$

by i^{th} basis ($\Delta a_2 = 2$) there is a number

$$
\tilde{A} = A + \Delta A = (0, 2, 2).
$$

In order to define the set of primary ASs it is needed to tentatively define values j_k .

For this, the nuvelization of a number *A* accordingly to the tables of nuvelization constants (Tables 2–4) is performed.

After this there are

$$
\gamma_1 = 1 \, , \, \gamma_2 = 1 \, , \, \gamma_3 = 2 \, .
$$

The set of primary ASs is defined as

$$
W_{1\rho_1}(\tilde{A}) = \{m_2, m_3\},
$$

\n
$$
W_{2\rho_2}(\tilde{A}) = \{m_1, m_3\},
$$

\n
$$
W_{3\rho_3}(\tilde{A}) = W(\tilde{A})^{-} \{m_1, m_2, m_3\}.
$$

Table 2

The set of secondary ASs is defined by Tables 5–7, which are formed by values j_n :

• for $\gamma_3 = 2$,

• for $\gamma_2 = 1$,

$$
W_2^{(1)}\left(\tilde{A}\right) = \{1,0,2\};
$$

$$
W_2^{(2)}\left(\tilde{A}\right) = \{0,0,3\};
$$

 $W_3(\tilde{A}) = \{1,1,2\};$

• for $\gamma_1 = 1$,

Table 5

Table 6

Implementation of choice of common SRC bases is suitable in the form of tables (Tables 8–11), where sign "+" means match of the components of secondary ASs, and sign "–" means mismatch. Those tables show, that vectors components match in the bases m_1 , m_3 , i.e. the sought AS is as $W_3(\tilde{A}) = \{m_1, m_3\}$ (table 8). Therefore, $W(\tilde{A}) > W'(\tilde{A})$. Thus, the increase of the informativeness about error placement in the distorted number *A* is guaranteed by the described method.

The geometrical interpretation example for the given SRC is represented in the following way (Fig. 2). The segment [0,30) is decomposed according to numerical intervals [15,30) , [10,15) and [12,18)

. Define numbers of intervals, in which an operand $A = (1,2,2)$ placed.

$$
T_{j_1} = [15, 30), T_{j_2} = [10, 20), T_{j_3} = [12, 18).
$$

Figure 2: Scheme of defining a sought interval

A sought interval is defined by the expression

$$
T_{W'(\tilde{A})} = [15, 18).
$$

It is obvious, that interval $T_{w'(\tilde{A})}$ is being reduced, compared to T_{j_3} , by three units (by 50%), and that leads to a decrease of the number of options of possible errors.

Geometrical interpretation confirms the effectiveness of the considered method of data in SRC diagnostic.

4. Conclusion

Thus, the suggested method allows decreasing the time of diagnostic of errors of data, represented in SRC, which increases diagnostic operability. A reduction of the number of bases in AS increases informativeness AS about error placement and measure. It decreases the time of AS reduction to incorrect bases (the number of steps of tentatively AS defining is decreasing). The usage of the suggested method of operative diagnostic of data increases the total effectiveness and feasibility of using non-positional code structures in SRC in computing systems.

The time of data diagnostic, compared to known methods, is decreasing firstly due to excluding the procedure of transforming numbers in SRC to positional notation as in known methods, i. e. eliminating a positional operation of numbers comparing. Secondly, the time of data diagnostic is decreased by reducing the quantity of SRC bases, which are giving the possibility of mistakes. Thirdly, the time of data diagnostic is decreased due to the usage of tabular sample value of an alternative set (AS) of numbers in SRC in one beat.

Therefore, the suggested method allows reducing the time of diagnosis of data errors in NCS, represented in SRC, which is increasing the diagnostic operability while entering minimal informational redundancy. The geometric model of the procedure of AS informativeness increasing and specific examples of usage of the suggested method of diagnostic of data in SRC confirms its practical feasibility.

The most effective way of the method used is in the computational chain, which does not allow perform all planned procedures to AS reduction to the incorrect basis, i.e. in a quite long chain of calculations of CS.

5. Acknowledgments

This work was supported in part by the National Research Foundation of Ukraine under Grant 2020.01/0351.

6. References

[1] P. V. A. Mohan, Residue Number Systems, Springer International Publishing, Cham, 2016. doi:10.1007/978-3-319-41385-3.

[2] I. Koren, The residue number system, in: Computer Arithmetic Algorithms, A K Peters/CRC Press, 2002. doi:10.1201/9781315275567-18.

[3] T.-C. Huang, Self-Checking Residue Number System for Low-Power Reliable Neural Network, in: IEEE 28th Asian Test Symposium (ATS), 2019, pp. 37–375. doi:10.1109/ATS47505.2019.000-3.

[4] P. V. A. Mohan, Specialized Residue Number Systems, in: P.V.A. Mohan (Ed.), Residue Number Systems: Theory and Applications, Springer International Publishing, Cham, 2016, pp. 177– 193. doi:10.1007/978-3-319-41385-3_8.

[5] F. Barsi, P. Maestrini, Error Correcting Properties of Redundant Residue Number Systems, IEEE Transactions on Computers C–22 (1973) 307–315. doi:10.1109/T-C.1973.223711.

[6] L. Yang, L. Hanzo, Coding theory and performance of redundant residue number system codes, Ieee Trans. Inform. Theory, 1999.

[7] V. Krasnobayev, A. Kuznetsov, A. Yanko, K. Kuznetsova, Correction Codes in the System of Residual Classes, in: IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S T), 2019, pp. 488–492. doi:10.1109/PICST47496.2019.9061253.

[8] V. Krasnobaev, O. Reshetniak, T. Kuznetsova, S. Florov, Y. Kotukh, Data Control Method, which Presented By Code of Non-Positioning System of Deduction Class Calculation, in: International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 2019, pp. 1–5. doi:10.1109/UkrMiCo47782.2019.9165528.

[9] M. G. Arnold, The residue logarithmic number system: theory and implementation, in: 17th IEEE Symposium on Computer Arithmetic (ARITH'05), 2005, pp. 196–205. doi:10.1109/ARITH.2005.44.

[10] V. Krasnobayev, A. Kuznetsov, A. Yanko, B. Akhmetov, T. Kuznetsova, Processing of the Residuals of Numbers in Real and Complex Numerical Domains, in: T. Radivilova, D. Ageyev, N. Kryvinska (Eds.), Data-Centric Business and Applications, Springer International Publishing, Cham, 2021, pp. 529–555. doi:10.1007/978-3-030-43070-2_24.

[11] Y. N. Kocherov, D. V. Samoylenko, A. I. Koldaev, Development of an Antinoise Method of Data Sharing Based on the Application of a Two-Step-Up System of Residual Classes, in: International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 2018, pp. 1–5. doi:10.1109/FarEastCon.2018.8602764.

[12] G. Harman, I. E. Shparlinski, Products of Small Integers in Residue Classes and Additive Properties of Fermat Quotients, International Mathematics Research Notices 5 (2016) 1424–1446. doi: 10.1093/imrn/rnv182.

[13] V. A. Krasnobayev, A. A. Kuznetsov, S. A. Koshman, K. O. Kuznetsova, A Method for Implementing the Operation of Modulo Addition of the Residues of Two Numbers in the Residue Number System, Cybernetics and Systems Analysis 56 (2020) 1029–1038. doi:10.1007/s10559-020- 00323-9.

[14] V. Krasnobaev, M. Zub, T. Kuznetsova, I. Perevozova, O. Maliy, Mathematical Model of the Process of Tabular's Implementation of the Operation Algebraic Multiplication in the Residues Class, in: International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 2019, pp. 1–6. doi:10.1109/UkrMiCo47782.2019.9165400.

[15] Y.Zhang, An FPGA implementation of redundant residue number system for low-cost fast speed fault-tolerant computations, Master's thesis, Nanyang Technological University, Singapore, 2018. doi: 10.32657/10220/47113.

[16] K. Tao, L. Peng, K. Liang, B. Zhuo, Irregular repeat accumulate low-density parity-check codes based on residue class pair, in: IEEE 9th International Conference on Communication Software and Networks (ICCSN), 2017, pp. 127–131. doi: 10.1109/ICCSN.2017.8230092.

[17] D. I. Popov, A. V. Gapochkin, Development of Algorithm for Control and Correction of Errors of Digital Signals, Represented in System of Residual Classes, in: International Russian Automation Conference (RusAutoCon), 2018, pp. 1–3. doi:10.1109/RUSAUTOCON.2018.8501826.