Chapter 7

THE METHOD OF ERROR DETECTION AND CORRECTION IN THE SYSTEM OF RESIDUAL CLASSES

Viktor A. Krasnobayev
V. N. Karazin Kharkiv National University,
Svobody sq.,4, Kharkov, 61022, Ukraine;
krasnobaev_va@rambler.ru

Alina S. Yanko
Poltava National Technical Yuri Kondratyuk University,
Pershotravnevyi avenue 24, Poltava, 36011, Ukraine;
al9_yanko@ukr.net

Sergey A. Koshman
Kharkov National Technical University of Agriculture named after Peter Vasylenko, Artyoma st., 44, Kharkiv, 61002, Ukraine;
s_koshman@ukr.net

Abstract

The method of correcting of single errors in the system of residual classes (SRC) were presented in this chapter. The results of the analysis of corrective capability of arithmetic code shown the high efficiency of using of nonpositional code structures in the SRC. The examples of correction of single data error witch provided by code of the SRC are given in the chapter.

Key words*: the system of residual classes, validity of data control, information redundancy, correction of data single errors.*

Introduction

In general, for the control, diagnosis and error correction data is needed to possess a specific structure of the code correction capacity. To do this, you need to enter some information redundancy, that is, to apply the method of information redundancy. This applies to nopositional code structure (NCS) of the residual classes (SRC) [1-3]. In the SRC value of redundancy $R = M_0 / M$ ($M_0 = \prod_{i=1}^{n+k} m_i$;

$M = \prod_{i=1}^{n} m_i .$) uniquely determines the corrective possibilities of error-correcting code nonpositional. Correcting codes in SRC can have any value of the minimum code distance (MCD) $d_{\min}^{(SRC)}$. This depends on the values of redundancy R. In SRC established between redundancy correcting code R, the value $d_{\min}^{(SRC)}$ of MCD and the number k of check bases. Correcting code has a value $d_{\min}^{(SRC)}$ of MCD, if the degree R of redundancy is not less than the product of any $d_{\min}^{(SRC)} - 1$ bases SRC. On the one hand we have that

$$R \geq \prod_{i=1}^{d_{\min}^{(SRC)}-1} m_{q_i} ,$$

on the other hand, on the other hand –

$$R = M_0 / M = \prod_{i=1}^{n+k} m_i / \prod_{i=1}^{n} m_i = \prod_{i=1}^{k} m_{n+i} .$$

In this case, legitimately argue that $d_{\min}^{(SRC)} - 1 = k$, or

$$d_{\min}^{(SRC)} = k + 1 . \tag{1}$$

There are two approaches to the problem of ensuring NCS in SRC necessary corrective properties.

The first approach. Knowing the requirements for correcting the NCS properties, for example, the number of errors witch detected $t_{\det.}$ or corrected $t_{cor.}$, to introduce, by controlling the amount k or magnitude $\{m_{n+k}\}$ of bases necessary redundancy information R. Information redundancy R determines the minimum code distance $d_{\min}^{(SRC)}$ NCS in SRC.

Then, in accordance with the theory of error-correcting coding (TECC) for the orderly $(m_i < m_{i+1})$ SRC have that

$$t_{\det.} \leq d_{\min}^{(SRC)} - 1 , \tag{2}$$

$$t_{\det.} \leq k ; \tag{3}$$

$$t_{cor.} \leq \left[\frac{d_{\min}^{(SRC)} - 1}{2} \right], \tag{4}$$

$$t_{cor.} \leq \left[\frac{k}{2} \right]. \tag{5}$$

The second approach. For a given type of NCS $A_{SRC} = (a_1 \,||\, a_2 \,||\, ... \,||\, a_{i-1} \,||\, a_i \,||\, a_{i+1} \,||\, ... \,||\, a_n \,||\, ... \,||\, a_{n+k})$ (for a given value of k)

correction capabilities (defined value $d_{\min}^{(SRC)}$) code in SRC determined in accordance with the expressions (3) and (5).

Note that if ordered SRC expanded by adding *k* control bases to *n* information module, that MCD $d_{\min}^{(SRC)}$ of the error-correcting code increased on the value of *k* (see the expression (1)). Zoom values $d_{\min}^{(SRC)}$ can also be due to the reduction of the number *n* of information bases, that is due to the transition to computing with less precision. It is clear that between the correction capability R of error correcting codes and precision calculations W in SRC exists an inverse relationship. The same computer can perform data processing with high precision W, but a small correction capability R. Or with less precision W, but with a higher possibility of the correction control , diagnosis and correction of data errors, as well as higher speed data (the run-time of basic operations in CSR inversely to the number *n* of information bases) [1,2].

Draw analysis of the possible correction of single data errors in SRC with a minimum of information redundancy by introducing only one ($k = 1$) the control base. In this case, in accordance with a TECC in SRC [4-7], MCD equal magnitude $d_{\min}^{(SRC)} = k + 1$. When $k = 1$ we have MCD $d_{\min}^{(SRC)} = 2$ that, in accordance with the general theory of error-correcting coding will guarantee only detect any single error (error in one of the residues a_i $(i = \overline{1, n+1})$) in the NCS. In general, the process of correcting data errors in SRC as a positional numbering system (PNS), is composed of three stages. The first stage – control data (the definition of the rightness or wrongness of the original number A_{SRC}). The second stage. Diagnosis wrong number $\tilde{A}_{SRC}$ (defining a distorted residual $\tilde{a}_i$ of the base m_i of SRC of number $\tilde{A}_{SRC}$). And finally, the third stage, the correction of an incorrect residual $\tilde{a}_i$ of the true number a_i, that is correct a wrong number $\tilde{A}_{SRC}$ (getting the right number $A_{SRC} = \tilde{A}_{cor.}$). The degree of information redundancy R (correcting capacity of code) is estimated by a size of MCD $d_{\min}^{(PNS)}$. In the SRC, as noted above, the value of MCD determined by the ratio $d_{\min}^{(SRC)} = k + 1$, where k – the base control quantity in ordered SRC.

1 Scientific findings

In this chapter we consider the NCS

$$A_{SRC}=(a_1\,||\,a_2\,||\,...\,||\,a_{i-1}\,||\,a_i\,||\,a_{i+1}\,||\,...\,||\,a_n\,||\,...\,||\,a_{n+k})$$

in SRC with minimal $(k=1)$ additional information redundancy. In this case, it is determined that $d_{\min}^{(SRC)}=2$.

In accordance with the general TECC, in the PNS with minimum code distance $d_{\min}^{(PNS)}=2$ in the code structure uniquely (reliably) is determined by a one-time mistake. In the PNS a single data error meant the distortion of one bit of information, the type of $0\rightarrow 1$ or $1\rightarrow 0$. To correct this single error in the PNS is necessary to satisfy the condition that $d_{\min}^{(PNS)}=3$.

In SRC, unlike PNS, a single error is the distortion of one residual a_i with base m_i. Since the residual a_i of the number

$$A_{SRC}=(a_1\,||\,a_2\,||\,...\,||\,a_{i-1}\,||\,a_i\,||\,a_{i+1}\,||\,...\,||\,a_n\,||\,a_{n+1})$$

with base m_i contains $z=\{[\log_2(m_i-1)]+1\}$ – binary digits, it is formally possible to assume that in SRC (at $d_{\min}^{(SRC)}=2$ $(k=1)$) within one residual a_i, can be found a stack of errors of no more than z bits. However, in the literature [4,5,8] shows that in some cases when $d_{\min}^{(SRC)}=2$ the value in the SRC is possible to correct single errors.

Taking into account the specificity properties and features representation NCS in SRC opportunity to correct errors when $d_{\min}^{(SRC)}=2$, you can try to explain as follows:

– a single error in the PNS and in the SRC refers to different concepts. This was shown above. In this regard, the MCD $d_{\min}^{(PNC)}$ for PNS and $d_{\min}^{(SRC)}$ for SRC has different meaning and quantitative assessment;

– existing (implicitly) in NCS natural (primary) information redundancy, which is available in the residual $\{a_i\}$ of the procedure due to the formation of these residual, positive (in terms of improved noise immunity and reliability of data transmission and processing) begins to appear only at presence of the artificial (secondary) information redundancy. Artificial information redundancy is introduced into the NCS due to the use (in addition to n the information base) k control bases SRC. A distinctive feature of SRC is a significant manifestation of primary information redundancy only if secondary, due to the introduction of control bases;

– in the literature [2] was shown, the correction code in the SRC with a simple pairs base is to the value MCD equal of value $d_{\min}^{(SRC)}$ only if the degree of information redundancy is not less than a product any $d_{\min}^{(SRC)}-1$ base of SRC.

The presence and interaction of primary and secondary information redundant, additional time during the procedure (use of temporal redundancy) in the error correction process, provides in some cases, able to correct single errors in SRC $d_{\min}^{(SRC)}=2$ (at $k=1$).

Really, if given the expression (3) and (5), for the orderly SRC, it can be draw a conclusion. When one ($k=1$) control based m_{n+1} of the SRC, the NCS

$$A=(a_1 \,||\, a_2 \,||\, ... \,||\, a_{i-1} \,||\, a_i \,||\, a_{i+1} \,||\, ... \,||\, a_n \,||\, a_{n+1})$$

may have different meanings $d_{\min}^{(SRC)}$. In this case, it depends on the magnitude of the control base m_{n+1}.

If, for each individual module of SRC condition $m_i < m_{n+1}$ $(i=\overline{1,n})$, then, in accordance with the expression (1), we can conclude that $d_{\min}^{(SRC)}=2$, i. e., in accordance with equation (2) we obtain that $t_{\text{det.}}=1$. If the totality of information bases $\{m_i\}$ for an arbitrary pair of modules condition $m_i \cdot m_j < m_{n+1}$ $(i,\, j=\overline{1,n}$; $i \neq j)$, in this case $d_{\min}^{(SRC)}=3$ и $t_{\text{det.}}=2$. Thus, for the NCS in the SRC with $k=1$, MCD $d_{\min}^{(SRC)}$ can be different depending on the magnitude of the control base m_{n+1} of the SRC.

Consider the ratio by which the error can be corrected in the residual $\tilde{a}_i$ [1]. Let the wrong number ($\tilde{A} \geq M$)

$$\tilde{A}=(a_1 \,||\, a_2 \,||\, ... \,||\, a_{i-1} \,||\, \tilde{a}_i \,||\, a_{i+1} \,||\, ... \,||\, a_n \,||\, a_{n+1})$$

including error $\tilde{a}_i=(a_i+\Delta a_i) \bmod m_i$ reliably contained in the residue a_i modulo m_i.

It is obvious

$$\tilde{A}=(A+\Delta A) \bmod M_0 \,. \tag{6}$$

Given that the amount of error may be represented as $\Delta A=(0 \,||\, 0 \,||\, ... \,||\, 0 \,||\, \Delta a_i \,||\, 0 \,||\, ... \,||\, 0 \,||\, 0)$, when the correct ($A<M$) number A can be determined as follows:

$$\begin{aligned}A &= (\tilde{A}-\Delta A) \bmod M_0 = \\ &= \left[(a_1 \,||\, a_2 \,||\, ... \,||\, a_{i-1} \,||\, \tilde{a}_i \,||\, a_{i+1} \,||\, ... \,||\, a_n \,||\, a_{n+1}) - \right. \\ &\left. -(0 \,||\, 0 \,||\, ... \,||\, 0 \,||\, \Delta a_i \,||\, 0 \,||...||\, 0 \,||\, 0)\right] \bmod M_0 = \\ &= [a_1 \,||\, a_2 \,||\, ... \,||\, a_{i-1} \,||\, (\tilde{a}_i-\Delta a_i) \bmod m_i \,||\, a_{i+1} \,||\, ... \,||\, a_n \,||\, a_{n+1}] \bmod M_0 \,.\end{aligned}$$

Obtain a quantitative estimate of the value of A. Since the number A is correct, i.e. stored in the numerical range [0, *M*), then the following inequality must be fulfilled

$$A = \left(\tilde{A} - \Delta A\right) \operatorname{mod} M_0 < M \ . \tag{7}$$

Given that the value ΔA of the error value is equal $\Delta A = \Delta a_i \cdot B_i$, then the inequality (7) will have the following form:

$$\begin{gathered} \tilde{A} - \Delta a_i \cdot B_i - r \cdot M_0 < M \ \text{ or} \\ \tilde{A} - \Delta a_i \cdot B_i - r \cdot M_0 < M_0 \,/\, m_{n+1} (r = 1, 2, 3, ...) \,, \\ \tilde{A} - (\tilde{a}_i - a_i) \cdot B_i - r \cdot M_0 < M_0 \,/\, m_{n+1} \,, \\ \tilde{A} - (a_i - \tilde{a}_i) \cdot B_i - r \cdot M_0 < M_0 \,/\, m_{n+1} \,, \\ (a_i - \ \tilde{a}_i) \cdot B_i < M_0 \,/\, m_{n+1} - \tilde{A} + r \cdot M_0 \,, \\ a_i - \tilde{a}_i < (M_0 \,/\, m_{n+1}) \,/\, B_i - \tilde{A} \,/\, B_i + r \cdot M_0 \,/\, B_i \,, \\ a_i < \tilde{a}_i + (M_0 \,/\, m_{n+1}) \,/\, B_i - \tilde{A} \,/\, B_i + r \cdot M_0 \,/\, B_i \,. \end{gathered} \tag{8}$$

Given that the orthogonal basis for the module m_i of the SRC is represented as $B_i = \overline{m}_i \cdot M_0 \,/\, m_i$, the expression (8) becomes:

$$a_i < \tilde{a}_i + (m_i + r \cdot m_i \cdot m_{n+1}) \,/\, (\overline{m}_i \cdot m_{n+1}) - \tilde{A} \,/\, B_i \qquad \text{or}$$

$$a_i < \tilde{a}_i + m_i \left(1 + r \cdot m_{n+1}\right) / \, (\overline{m}_i \cdot m_{n+1}) - \tilde{A} \,/\, B_i \,. \tag{9}$$

Since the value of the residual a_i is a natural number, then the value of $m_i (1 + r \cdot m_{n+1}) \,/\, (\overline{m}_i \cdot m_{n+1}) - \tilde{A} \,/\, B_i$ in the expression (9) must be an integer. Therefore, taking the whole of the last relation, we obtain a formula for the correction of an error in the residual $\tilde{a}_i$ of $\tilde{A}$ as

$$a_i = (\tilde{a}_i + [m_i \cdot \left(1 + r \cdot m_{n+1}\right) / \, (\overline{m}_i \cdot m_{n+1}) - \tilde{A} \,/\, B_i) \operatorname{mod} m_i] \,. \tag{10}$$

To confirm the results of theoretical studies, we consider examples of monitoring and correction of the data in the SRC.

Example 1. Implement control and, if necessary, to carry out a correction of the number $A_{SRC} = (0 \,||\, 0 \,||\, 0 \,||\, 0 \,||\, 5)$ which is set in the SRC with the information base $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_5 = 7$ and with the reference base $m_k = m_5 = 11$. However $M = \prod_{i=1}^{n} m_i = \prod_{i=1}^{4} m_i = 420$ and $M_0 = M \cdot m_{n+1} = 420 \cdot 11 = 4620$. Orthogonal bases $B_i \ (i = \overline{1, n+1})$ of SRC are in [6].

I. Data control $A_{SRC} = (0 \,||\, 0 \,||\, 0 \,||\, 0 \,||\, 5)$. In accordance with the control procedure [1], we define the value of

$$A_{PNS} = \left(\sum_{i=1}^{n+1} a_i \cdot B_i \right) \bmod M_0 = \left(\sum_{i=1}^{5} a_i \cdot B_i \right) \bmod M_0 =$$
$$= (a_1 \cdot B_1 + a_2 \cdot B_2 + a_3 \cdot B_3 + a_4 \cdot B_4 + a_5 \cdot B_5) \bmod M_0 =$$
$$= (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 0 \cdot 2640 + 5 \cdot 2520) \bmod 4620 =$$
$$= (5 \cdot 2520) \bmod 4620 = 12600 (\bmod 4620) = 3360 > 420 .$$

Thus, the process control is determined that $A_{SRC} = 3360 > M = 420$. In this case, the possible occurrence of only once errors, it is concluded that the number of considered $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$ is incorrect ($3360 > M = 420$). To correct the number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$, you must first make a diagnosis data, i.e. identify distorted residual $\tilde{a}_i$. Then it is necessary to determine the true value of the residual a_i to modular m_i and then spend correcting distorted residual $\tilde{a}_i$.

II. Diagnostics data $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. In accordance with the method of projections [1,2], we construct possible projections $\tilde{A}_j$ of the number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$:

$$\tilde{A}_1 = (0 \| 0 \| 0 \| 5),$$
$$\tilde{A}_2 = (0 \| 0 \| 0 \| 5),$$
$$\tilde{A}_3 = (0 \| 0 \| 0 \| 5),$$
$$\tilde{A}_4 = (0 \| 0 \| 0 \| 5)$$

and

$$\tilde{A}_5 = (0 \| 0 \| 0 \| 0).$$

The formula for calculating of the projections of values $\tilde{A}_{jPNS}$ in the PNS has the form [1]

$$\tilde{A}_{jPNS} = \left(\sum_{\substack{i=1; \\ j=\overline{1,n+1}.}}^{n} a_i \cdot B_{ij} \right) \bmod M_j = (a_1 \cdot B_{1j} + a_2 \cdot B_{2j} + \ldots + a_n \cdot B_{nj}) \bmod M_j \qquad (11)$$

.

In accordance with the formula (11) we can calculate all the values $\tilde{A}_{jPNS}$. Next, we perform $(n+1)$ a comparison of numbers $\tilde{A}_{jPNS}$ with the number $M = M_0 / m_{n+1}$. If among the projections $\tilde{A}_i$ have number no inside information $[0, M)$ numerical range (i.e. $\tilde{A}_k \geq M$), which contains *k* of the correct numbers, than it is concluded that these *k* residual of the number A are not distorted.

Erroneous may be only the remains which are among the remaining $[(n+1)-k]$ residual number $\tilde{A}_{SRC}$. Set of the partial working base for a given SRC and set of partial orthogonal bases are presented in [6-9]. So, we have that

$$\tilde{A}_{1PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i1}\right) \mathrm{mod}\, M_1 = (a_1 \cdot B_{11} + a_2 \cdot B_{21} + a_3 \cdot B_{31} + a_4 \cdot B_{41}) \,\mathrm{mod}\, M_1 =$$

$$= (0 \cdot 385 + 0 \cdot 616 + 0 \cdot 1100 + 5 \cdot 980) \,\mathrm{mod}\, 1540 = 280 < 420 .$$

We conclude that the residual a_1 of числа $\tilde{A}_1$ – it is possibly $\overline{a}_1$ distorted residual;

$$\tilde{A}_{2PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i2}\right) \mathrm{mod}\, M_2 = (a_1 \cdot B_{12} + a_2 \cdot B_{22} + a_3 \cdot B_{32} + a_4 \cdot B_{42}) \,\mathrm{mod}\, M_2 =$$

$$= (0 \cdot 385 + 0 \cdot 231 + 0 \cdot 330 + 5 \cdot 210) \,\mathrm{mod}\, 1155 = 1050 > 420 .$$

Thus, we find that a_2 accurate not distorted residual;

$$\tilde{A}_{3PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i3}\right) \mathrm{mod}\, M_3 = (a_1 \cdot B_{13} + a_2 \cdot B_{23} + a_3 \cdot B_{33} + a_4 \cdot B_{43}) \,\mathrm{mod}\, M_3 =$$

$$= (0 \cdot 616 + 0 \cdot 693 + 0 \cdot 792 + 5 \cdot 672) \,\mathrm{mod}\, 924 = 588 > 420 .$$

We find that a_3 accurate not distorted residual;

$$\tilde{A}_{4PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i4}\right) \mathrm{mod}\, M_4 = (a_1 \cdot B_{14} + a_2 \cdot B_{24} + a_3 \cdot B_{34} + a_4 \cdot B_{44}) \,\mathrm{mod}\, M_4 =$$

$$(0 \cdot 220 + 0 \cdot 165 + 0 \cdot 369 + 5 \cdot 540) \,\mathrm{mod}\, 660 = 60 < 420 .$$

Conclusion: the residual a_4 to modular m_4 of number $\tilde{A}_4$ – perhaps distorted residual $\overline{a}_4$

$$\tilde{A}_{5PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i5}\right) \mathrm{mod}\, M_5 .$$

Since $M_5 = M = 420$, that the residual $\overline{a}_5$ of the control module $m_k = m_5$ will be always a range of possible $\overline{a}_i$ distorted residual of number in the SRC.

The general conclusion. In the process of data diagnostics introduced in NCS $\tilde{A} = (0 \,||\, 0 \,||\, 0 \,||\, 0 \,||\, 5)$, decided not exactly distorted residual: $a_2 = 0$ and $a_3 = 0$. Erroneous may be the residual of the bases m_1, m_4 and m_5, i. e. residual $\overline{a}_1 = 0$, $\overline{a}_4 = 0$ and $\overline{a}_5 = 5$. In this case it is necessary to carry out the correction of residual $\overline{a}_1$, $\overline{a}_4$ and $\overline{a}_5$.

III. It is correction of data error $\tilde{A}_{3360} = (0 \,||\, 0 \,||\, 0 \,||\, 0 \,||\, 5)$. As known [1] formula

$$a_i = \left(\bar{a}_i + \left[\frac{m_i \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_i} - \frac{\tilde{A}}{B_i} \right] \right) \bmod m_i \,, \qquad (12)$$

spend correcting $\bar{a}_1$, $\bar{a}_4$ and $\bar{a}_5$ of possible distorted residuals a_1, a_4 and a_5 , where $r = 1, 2, 3, \ldots$.

So we have that

$$a_1 = \left(\bar{a}_1 + \left[\frac{m_1 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_1} - \frac{\tilde{A}}{B_1} \right] \right) \bmod m_1 = \left(0 + \left[\frac{3 \cdot (1 + r \cdot 11)}{11 \cdot 1} - \frac{3360}{1540} \right] \right) \bmod 3 = (0 +$$

$$+[3,27 - 2,18]) \bmod 3 = (0 + [1,09]) \bmod 3 = (0 + 1) \bmod 3 = 1 \,;$$

$$a_4 = \left(\bar{a}_4 + \left[\frac{m_4 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_4} - \frac{\tilde{A}}{B_4} \right] \right) \bmod m_4 = \left(0 + \left[\frac{7 \cdot 12}{11 \cdot 4} - \frac{3360}{2640} \right] \right) \bmod 7 = (0 + [1,9 -$$

$$-1,27]) \bmod 7 = (0 + [0,63]) \bmod 7 = (0 + 0) \bmod 7 = 0 \,;$$

$$a_5 = \left(\bar{a}_5 + \left[\frac{m_{n+1} \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_{n+1}} - \frac{\tilde{A}}{B_5} \right] \right) \bmod m_{n+1} = \left(5 + \left[\frac{11 \cdot (1 + 11)}{11 \cdot 6} - \frac{3360}{2520} \right] \right) \bmod 11 =$$

$$= (5 + [2 - 1,3]) \bmod 11 = (5 + [0,7]) \bmod 11 = (5 + 0) \bmod 5 = 0 \,.$$

According to the resulting residuals $a_1 = 1$, $a_4 = 0$ and $a_5 = 0$, rebuilding (correcting) the number of distorted $\tilde{A}_{3360} = (0 \,||\, 0 \,||\, 0 \,||\, 0 \,||\, 5)$, i.e. the correct number, will have the following form: $\tilde{A}_{cor.} = (1 \,||\, 0 \,||\, 0 \,||\, 0 \,||\, 5)$. To verify the data correction, by the known formula [1], we define the value of the number $\tilde{A}_{cor.} = (1 \,||\, 0 \,||\, 0 \,||\, 0 \,||\, 5)$ as follows [4]

$$\tilde{A}_{cor.PNS} = \left(\sum_{i=1}^{5} a_i \cdot B_i \right) \bmod M_0 = (a_1 \cdot B_1 + a_2 \cdot B_2 + a_3 \cdot B_3 + a_4 \cdot B_4 + a_5 \cdot B_5) \bmod M_0 =$$

$$= (1 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 0 \cdot 2640 + 5 \cdot 2520) \bmod 4620 = 14140 (\bmod 4620) =$$

$$= 280.$$

Since $280 < M = 420$, so the number $\tilde{A}_{280} = (1 \,||\, 0 \,||\, 0 \,||\, 0 \,||\, 5)$ is correct. In order to clarify the correct procedures of correction of number $\tilde{A}_{3360}$ we spend calculation and comparison of the values and the right residuals $a_2 = 0$ and $a_3 = 0$.

In this case we have $a_2 = \left(0 + \left[\frac{4 \cdot (1 + 11)}{11 \cdot 3} - \frac{3360}{3465} \right] \right) \bmod 4 = 0$ and

$$a_3 = \left(0 + \left[\frac{5 \cdot (1 + 11)}{11 \cdot 4} - \frac{3360}{3696} \right] \right) \bmod 5 = 0 \,.$$

The obtained results $a_2 = 0$ and $a_3 = 0$ of calculations of residuals by modular m_2 and m_3 of SRC, validate the correction of wrong number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. Thus, the original number $\tilde{A}_{SRC} = (0 \| 0 \| 0 \| 0 \| 5)$ is wrong $\tilde{A}_{3360}$, where the single error $\Delta a_1 = 1$ has occurred on the base m_1. This error is transferred the correct number A_{280} to not correct $\tilde{A}_{3360}$. In order to determine whether the correct number A_{280} is true we will carry out additional research of processes of distortion and correction of number A_{280} by the base $m_1 = 3$. The number N_{NW} of possible wrong (distorted) $\tilde{A}_{SRC}$ code words (only a single error) for each correct number A_{SRC} equals $N_{NW} = \sum_{i=1}^{n+1} m_i - (n+1)$.

The results showed that the distortion of the residuals a_1 by modular $m_1 = 3$ of the correct number A_{280} can lead to only two wrong numbers $\tilde{A}_{3360} = (\tilde{0} \| 0 \| 0 \| 0 \| 5)$ and $\tilde{A}_{1820} = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$. This fact indicates that the corrected number $A_{ucn.} = A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ is not only correct (which lying in the range [0, 420)) but also true. The truth of the resulting number $A_{280} = (\hat{1} \| 0 \| 0 \| 0 \| 5)$ by the fact that only a single error $\Delta a_1 = 2$ on the base $m_1 = 3$ transfer the number

$$(\tilde{A} = (A + \Delta A) \bmod M_0 = (1 \| 0 \| 0 \| 0 \| 5) + (2 \| 0 \| 0 \| 0 \| 0) =$$
$$= [(1+2) \bmod 3 \| 0 \| 0 \| 0 \| 5] = (\tilde{0} \| 0 \| 0 \| 0 \| 5))$$

to the only wrong number

$$\tilde{A}_{3360} = (\tilde{0} \| 0 \| 0 \| 0 \| 5).$$

Example 2. Assume that the correct number $A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ and let $\Delta a_1 = 1$. Then

$$\tilde{A} = (A + \Delta A) \bmod M_0 = (1 \| 0 \| 0 \| 0 \| 5) + (1 \| 0 \| 0 \| 0 \| 0) =$$
$$= \left[(1+1) \bmod 3 \| 0 \| 0 \| 0 \| 5\right] = (\tilde{2} \| 0 \| 0 \| 0 \| 5).$$

This number in SRC is corresponded to the number 1820 in the PNS, i.e. number $\tilde{A}_{1820}$ is wrong. Carry out fix number $\tilde{A}_{1820}$. Before correction of number $\tilde{A}_{1820}$ spend data diagnosis. For this we first form the projection $A_j \ (j = \overline{1, 5})$ of number $\tilde{A}_{1820} = (2 \| 0 \| 0 \| 0 \| 5)$. It will have the following code structure in SRC: $\tilde{A}_1 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_2 = (2 \| 0 \| 0 \| 5)$, $\tilde{A}_3 = (2 \| 0 \| 0 \| 5)$, $\tilde{A}_4 = (2 \| 0 \| 0 \| 5)$ and $\tilde{A}_5 = (2 \| 0 \| 0 \| 0)$.

Next, we will define all the projections values $\tilde{A}_{j\,PNS}$:

$\tilde{A}_{1PNS}=(5\cdot 980)\mod 1540=280<420=M$;

$\tilde{A}_{2PNS}=(2\cdot 385+5\cdot 231)\mod 1155=1925\big(\mod 1155\big)=770>420=M$;

$\tilde{A}_{3PNS}=(2\cdot 616+5\cdot 672)\mod 924=4592\big(\mod 924\big)=896>420=M$;

$\tilde{A}_{4PNS}=(2\cdot 220+5\cdot 540)\mod 660=3140\big(\mod 660\big)=500>420=M$;

$\tilde{A}_{5PNS}=2\cdot 280(\mod 420)=560\big(\mod 420\big)=140<420=M$.

So as $\tilde{A}_{2\Pi CC}$, $\tilde{A}_{3\Pi CC}$ and $\tilde{A}_{4\Pi CC}>420$, then it is concluded that the residuals $a_2=0$, $a_3=0$ and $a_4=0$ of number $\tilde{A}_5=(2\,||\,0\,||\,0\,||\,0\,||\,5)$ is not distorted. Distortions $\overline{a}_1=2$ and $\overline{a}_5=5$ can be only residuals a_1 and a_5. At first spend correcting of residual $\overline{a}_1=2$. We have that

$$a_1=\left(\overline{a}_1+\left[\frac{m_1\cdot(1+r\cdot m_{n+1})}{m_{n+1}\cdot\overline{m}_1}-\frac{\tilde{A}}{B_1}\right]\right)\mod m_1=\left(2+\left[\frac{3\cdot(1+11)}{11\cdot 1}-\frac{1820}{1540}\right]\right)\mod 3=$$

$$=\big(2+[3,27-1,18]\big)\mod 3=\big(2+[2,09]\big)\mod 3=(2+2)\mod 3=4(\mod 3)=1\,.$$

Thus the corrected residual by modular m_1 is equal $a_1=1$.

The similar way we obtain the value $a_5=5$. According to the resulting residual a_1 , a_5 we correct the wrong number $\tilde{A}_{1820}=(\tilde{2}\,||\,0\,||\,0\,||\,0\,||\,5)$. Eventually, in the process correcting we obtain the correct number $A_{280}=(1\,||\,0\,||\,0\,||\,0\,||\,5)$.

Example 3. Implement number control $A_{SRC}=(0\,||\,0\,||\,0\,||\,2\,||\,1)$. In the case of distortion diagnose and correct the data.

I. Data check $A_{SRC}=(0\,||\,0\,||\,0\,||\,2\,||\,1)$. In accordance with a known procedure of control determine A_{PNS} by the formula

$$A_{PNS}=\left(\sum_{i=1}^{n+1}a_i\cdot B_i\right)\mod M_0=(0\cdot 1540+0\cdot 3465+0\cdot 3696+2\cdot 2640+$$

$$+1\cdot 2520)\mod 4620=7800(\mod 4620)=3180>420\,.$$

This number is wrong $\tilde{A}_{3180}$.

II. Data diagnostic $\tilde{A}_{3180}=(0\,||\,0\,||\,0\,||\,2\,||\,1)$. We construct all possible projections $\tilde{A}_j$ of number $\tilde{A}_{3180}$: $\tilde{A}_1=(0\,||\,0\,||\,2\,||\,1)$, $\tilde{A}_2=(0\,||\,0\,||\,2\,||\,1)$, $\tilde{A}_3=(0\,||\,0\,||\,2\,||\,1)$, $\tilde{A}_4=(0\,||\,0\,||\,0\,||\,1)$ and $\tilde{A}_5=(0\,||\,0\,||\,0\,||\,2)$.

We define the values of all five projections $\tilde{A}_j$ in the PNS:

$$\tilde{A}_{1SRC} = \left(0 \,\|\, 0 \,\|\, 2 \,\|\, 1\right) = \tilde{A}_{1PNS} = \left(a_1 \cdot B_{11} + a_2 \cdot B_{21} + a_3 \cdot B_{31} + a_4 \cdot B_{41}\right) \bmod M_1 =$$

$$= (0\cdot385 + 0\cdot616 + 2\cdot1100 + 1\cdot980) \bmod 1540 = 100 < M = 420;$$

$$\tilde{A}_{2SRC} = \left(0 \,\|\, 0 \,\|\, 2 \,\|\, 1\right) = \tilde{A}_{2PNS} = (a_1 \cdot B_{12} + a_2 \cdot B_{22} + a_3 \cdot B_{32} + a_4 \cdot B_{42}) \bmod M_2 =$$

$$= (0\cdot385 + 0\cdot231 + 2\cdot330 + 1\cdot210) \bmod 1155 = 870 > M = 420;$$

$$\tilde{A}_{3SRC} = \left(0 \,\|\, 0 \,\|\, 2 \,\|\, 1\right) = \tilde{A}_{3PNS} = (a_1 \cdot B_{13} + a_2 \cdot B_{23} + a_3 \cdot B_{33} + a_4 \cdot B_{43}) \bmod M_3 =$$

$$= (0\cdot616 + 0\cdot693 + 2\cdot792 + 1\cdot672) \bmod 924 = 418 < M = 420;$$

$$\tilde{A}_{4SRC} = (0 \,\|\, 0 \,\|\, 0 \,\|\, 1) = \tilde{A}_{4PNS} = (a_1 \cdot B_{14} + a_2 \cdot B_{24} + a_3 \cdot B_{34} + a_4 \cdot B_{44}) \bmod M_4 =$$

$$= (0\cdot220 + 0\cdot165 + 2\cdot396 + 1\cdot540) \bmod 660 = 540 > M = 420;$$

$$\tilde{A}_{5SRC} = (0 \,\|\, 0 \,\|\, 0 \,\|\, 2) = \tilde{A}_{5PNS} = (a_1 \cdot B_{15} + a_2 \cdot B_{25} + a_3 \cdot B_{35} + a_4 \cdot B_{45}) \bmod M_5 =$$

$$= (0\cdot280 + 0\cdot105 + 2\cdot336 + 1\cdot120) \bmod 420 = 240 < M = 420.$$

As a result of calculations of values $\tilde{A}_{j\,PNS}$ and comparing them with the value $M = 420$ of the interval length $[0, 420)$ of processing of correct numbers A_{SRC} in SRC we obtain the following.

Set of residuals $a_2 = 0$, $a_4 = 0$ is correct (residuals are not distorted), and the residuals $\overline{a}_1 = 0$, $\overline{a}_3 = 0$ and $\overline{a}_5 = 1$ of the wrong number $\tilde{A}_{3180} = (0 \,\|\, 0 \,\|\, 0 \,\|\, 2 \,\|\, 1)$ may be distorted (may be wrong).

III. Correction is possible distorted residuals $\overline{a}_1$, $\overline{a}_3$ и $\overline{a}_5$ of the number $\tilde{A}_{3180}$.

It is necessary to be corrected, possibly distorted residuals $\overline{a}_1 = 0$, $\overline{a}_3 = 0$ and $\overline{a}_5 = 1$ by the formula $a_i = \left(\tilde{a}_i + \left[\frac{m_i \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \overline{m}_i} - \frac{\tilde{A}}{B_i}\right]\right) \bmod m_i$. Then we have that

$$a_1 = \left(\overline{a}_1 + \left[\frac{m_1 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \overline{m}_1} - \frac{\tilde{A}}{B_1}\right]\right) \bmod m_1 = \left(0 + \left[\frac{3 \cdot (1 + r \cdot 11)}{11 \cdot 1} - \frac{3180}{1540}\right]\right) \bmod 3 =$$

$$= \left(0 + \left[3{,}27 - 2{,}06\right]\right) \bmod 3 = \left(0 + \left[1{,}21\right]\right) \bmod 3 = \left(0 + 1\right) \bmod 3 = 1.$$

In this way $a_1 = 1$. For value $\overline{a}_3$ we have

$$a_3 = \left(\tilde{a}_3 + \left[\frac{m_3 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \overline{m}_3} - \frac{\tilde{A}}{B_3}\right]\right) \bmod m_3 = \left(0 + \left[\frac{5 \cdot (1 + r \cdot 11)}{11 \cdot 4} - \frac{3180}{3696}\right]\right) \bmod 5 =$$

$$=\left(0+\left[1,36-0,86\right]\right)\bmod 5=\left(0+\left[0,5\right]\right)\bmod 5=\left(0+0\right)\bmod 5=0.$$

In this way $a_3=0$. To obtain the value of the residual $\overline{a}_5$

$$a_5=\left(\tilde{a}_5+\left[\frac{m_5\cdot(1+r\cdot m_{n+1})}{m_{n+1}\cdot\overline{m}_5}-\frac{\tilde{A}}{B_5}\right]\right)\bmod m_5=\left(1+\left[\frac{11\cdot(1+r\cdot 11)}{11\cdot 6}-\frac{3180}{2520}\right]\right)\bmod 11=$$

$$=\left(1+\left[2-1,26\right]\right)\bmod 11=\left(1+\left[0,74\right]\right)\bmod 11=\left(1+0\right)\bmod 11=1.$$

We have that $a_5=1$. According to the obtained values $a_1=1$, $a_3=0$ and $a_5=1$ of the recovered residuals we correct the distorted number translit.ru to the correct number $A_{SRC}=(1\,||\,0\,||\,0\,||\,2\,||\,1)$. It is the check $100<420$.

2 Conclusions

In contrast to the code of PNS, the arithmetic codes in the SRC has additional corrective opportunities was shows in the paper.

Thus, it is available to the NCS both primary and secondary information redundancy, in some cases, may allow the correction of single errors in SRC with MCL of $d_{\min}^{(KB)}=2$. However, for correction of single error require carrying out of additional time procedures data processing i.e. use of addition to the information redundancy use of time redundancy. These examples of realization of the specific implementation of correction procedures of single error show practical feasibility of this method the error correction of error data witch present in the SRC.

References

[1] Akushskii I. Ya. Mashinnaya arifmetika v ostatochnykh klassakh / I. Ya. Akushskii, D. I. Yuditskii. – M.: Sov. radio, 1968. – 440 s. (In Russian).

[2] Torgashov V. A. Sistema ostatochnykh klassov i nadezhnost' TsVM / V. A. Torgashov. – M.: Sov. radio, 1973. – 118 s. (In Russian).

[3] Krasnobaev V. A. Nadezhnostnaya model' EVM v sisteme ostatochnykh klassov / V. A. Krasnobaev // Elektronnoe modelirovanie. – 1985. – №4. – S. 44 – 46. (In Russian).

[4] Krasnobayev V.A. A method for increasing the reliability of verification of data represented in a residue number system / V.A. Krasnobayev, S.A. Koshman, M.A. Mavrina // Cybernetics and Systems Analysis. – 2014. – Vol. 50. – Issue 6. – P. 969-976.

[5] Krasnobaev V.A. Metod ispravleniya odnokratnykh oshibok dannykh, predstavlennykh kodom klassa vychetov / V.A. Krasnobaev, S.A. Koshman, M.A. Mavrina // Elektronnoe modelirovanie. – 2013. – T. 35, № 5. – S. 43–56. (In Russian).

[6] Moroz S.A. Metody kontrolya, diagnostiki i korrektsii oshibok dannykh v informatsionno-telekommunikatsionnoi sisteme, funktsioniruyushchei v klasse vychetov / S.A. Moroz, V.A. Krasnobaev // Informatsiino-keruyuchi sistemi na zaliznichnomu transporti. – 2012. – № 2. – S. 60 – 78. (In Russian).

[7] Kuznetsov A. A. Statisticheskii analiz setevogo trafika dlya sistem obnaruzheniya i predotvrashcheniya vtorzhenii / A. A. Kuznetsov, A. A. Smirnov, D. A. Danilenko, A. Berezovskii // Radiotekhnika: Vseukr. mezhved. nauch.-tekhn. sb. – Kh.: KhNURE. – 2014. – Vyp. 176. – S. 97-110. (In Russian).

[8] Kuznetsov A. A. Modelirovanie algebraicheskoi struktury shifra AES s ispol'zovaniem apparata tsepnykh drobei / A. A. Kuznetsov, Yu. I. Gorbenko, S. V. Kostenko // Visnik KhNU imeni V. N. Karazina. Ser.: Matematichne modelyuvannya. Informatsiini tekhnologiï. Avtomatizovani sistemi upravlinnya. – 2014. – №1131. – S. 37-53. (In Russian).

[9] Gorbenko I. D. Statistichni vlastivosti blokovikh simetrichnikh shifriv vidpovidno do ISO/IEC 29192-2 / I. D. Gorbenko, O. O. Kuznetsov, A. V. Samoilova // Radiotekhnika: Vseukr. mezhved. nauch.-tekhn. sb. – Kh.: KhNURE. – 2014. – Vyp. 176. – S. 40-44. (In Russian).