UDC 681.142.01

DATA SINGLE-ERROR CORRECTION METHOD OF A RESIDUE CLASS CODE

Viktor Krasnobayev[1], Sergey Koshman[1], Alina Yanko[2], Sergey Moroz[3]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
v.a.krasnobaev@gmail.com, s_koshman@ukr.net
[2] Poltava National Technical Yuri Kondratyuk University, Pershotravnevyi avenue 24, Poltava, 36011, Ukraine
al9_yanko@ukr.net
[3] Kharkiv Petro Vasylenko National Technical University of Agriculture, Rizdviana st., 19, Kharkiv, 61052, Ukraine
frost9i@ukr.net

Reviewer: Sergii Kavun, Doctor of Sciences (Economics), Ph.D. (Engineering), Full Prof., Kharkiv Educational and Research Institute of the University of Banking , Kharkiv, Ukraine
kavserg@gmail.com

Received on November 2017

Abstract: *The method of correction of single errors in the residue class (RC) is considered in this article. The results of analysis of arithmetic code correcting possibilities showed high efficiency of the use of position-independent code structures in RC, due to the presence in the non-position code structure of primary and secondary redundancy. Examples of correction of the data single errors witch presented by the code of RC are made in the article.*

Keywords: *non-positional code structure, residue classes, positional numeral systems, minimum code distance, error-control coding, data diagnosing and correction.*

1 Introduction

In general, in order to verify, diagnose and correct errors a code structure requires a certain error-correcting capability. In this case, code is required to be introduced to data duplication, i.e. information redundancy should be implemented. All of the above fully refers to a non-positional code structure (NCS) in residue classes (RC) [1-3].

For each random RC the amount of redundancy $R = M_0 / M$ uniquely determines correction capability of a non-positional error-correcting code. Error correcting codes in RC can have any given values of minimum code distance (MCD) $d_{\min}^{(RC)}$, which depends on the value of redundancy R. The acquainted theorem [1] establishes a link between error-correcting code redundancy R, the value of MCD $d_{\min}^{(RC)}$, and the amount of RC check bases k.

Error-correcting code has MCD values $d_{\min}^{(RC)}$ in case when the degree of redundancy R is not less than the product $d_{\min}^{(RC)} - 1$ of RC bases. On the one hand we get $R \geq \prod_{i=1}^{d_{\min}^{(RC)}-1} m_{q_i}$, but 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, it's correct to state that $d_{\min}^{(RC)} - 1 = k$, or

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

There are two approaches to solve the problem of providing NCS with all required error-correcting properties in RC.

The first approach. If the requirements for error-correcting properties of NCS are known, for example, depending on amount of errors being detected $t_{\det.}$ or corrected $t_{cor.}$ required information redundancy R should be introduced, using the amount of k or the value $\{m_{n+k}\}$ of check bases. Redundancy R determines minimum code distance $d_{\min}^{(RC)}$ of NCS in RC.

Then, according to the error-control coding (ECC) theory for an ordered $(m_i < m_{i+1})$ RC we have that

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

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

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

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

The second approach. For a given NCS $A_{RC} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| ... \| a_{n+k})$ (for a given value k) its error-correcting capabilities (determined by the $d_{\min}^{(RC)}$ value) of RC code are defined by the expressions (3) and (5).

Note that, if an ordered RC is extended by adding k check bases to n information modules, then MCD $d_{\min}^{(RC)}$ of the error-correcting code is increased by the value k (see expression (1)).

The values of $d_{\min}^{(RC)}$ can be also increased by decreasing the number n of information bases, i.e. by transitioning to less accurate calculations. It's clear that in RC between error-correcting R properties of error-control codes and calculation accuracy W inverse proportion exists. The same computer can perform arithmetical calculations or any other math operations both with high W accuracy but a low error-correcting R capability and with lower W accuracy, but with a higher capability R of error detection and correction in order to verify, diagnose and correct data faults, as well as to demonstrate higher data processing performance (the time to execute basic operations is inversely proportional to n information bases in RC) [2, 4, 5].

2 The main part

Now we'll analyze the process of single-error correcting data capability in RC given the minimal information redundancy by introduction of a single ($k = 1$) check base. In this case, according to the error control coding theory in RC [1, 2], MCD is equal to the value $d_{\min}^{(RC)} = k + 1$. If $k = 1$, then MCD is $d_{\min}^{(RC)} = 2$, which, as according to the general error control coding theory, ensures any single-error detection (an error in one of the residues a_i $(i = \overline{1, n+1})$) in NCS.

In general, just as in the positional numeral system (PNS), the process of data error correction in RC consists of three stages. The first stage – data checking (correctness or incorrectness verification of the initial number A_{RC}). On the second stage diagnosing the false $\tilde{A}_{RC}$ number (detection of a single corrupted residue $\tilde{a}_i$ of the number $\tilde{A}_{RC}$ to the base m_i in RC). And, finally, on the third stage correcting the invalid residue $\tilde{a}_i$ to its true value a_i of the number, i.e. correcting false $\tilde{A}_{RC}$ number (getting the correct number $A_{RC} = \tilde{A}_{cor.}$).

The degree of information redundancy R (code error-correcting property) is estimated by the value of MCD $d_{\min}^{(PNS)}$. As previously noted, the value of MCD is defined by the ratio $d_{\min}^{(RC)} = k + 1$, where k is the amount of check bases in an ordered RC.

Let's start with the NCS $A_{RC} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| ... \| a_{n+k})$ in RC having a minimal $(k = 1)$ additional information redundancy. In this situation it's considered that $d_{\min}^{(RC)} = 2$.

According to the error control coding theory in PNS if the minimum code distance is granted to be $d_{\min}^{(PNS)} = 2$, a single error in a code structure is ensured to be detected. In PNS a single error is understood as a corruption of a single information bit, for instance $0 \to 1$ or $1 \to 0$. In order to correct this single error it's required to ensure the condition, when $d_{\min}^{(PNS)} = 3$.

Contrary to PNS, a single error in RC is understood as a corruption of a single residue a_i modulo m_i. Inasmuch as the residue a_i of the number $A_{RC} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ modulo m_i contains $z = \{[\log_2(m_i - 1)] + 1\}$ binary bits, then it's formally correct to be considered that if $d_{\min}^{(RC)} = 2$ $(k = 1)$ is within limits of a single residue a_i, an error cluster can be detected in RC, with its length not exceeding z binary bits. However in RC, as it is shown in literature [1, 2, 5], there are some cases when a single errors can be corrected while $d_{\min}^{(RC)} = 2$.

In the light of specific features and properties of NCS representation in RC an error-correcting capability given $d_{\min}^{(RC)} = 2$ can be explained in the following manner.

1. A single error in PNS and in RC are different concepts, as it was shown before. With that being said, MCD $d_{\min}^{(PNS)}$ for PNS and $d_{\min}^{(RC)}$ for RC has different meaning and measure.

2. Existing (implicitly) intrinsic (natural, primal) information redundancy in NCS, being stored in residues $\{a_i\}$ due to their forming procedure, has a positive effect (from the perspective of increasing data jam-resistance, transfer and processing reliability) that kicks in only with the presence of a subsidiary (artificial, secondary) information redundancy. An artificial information redundancy in NCS is being introduced by using (additionally to n information bases) k check bases in RC. A distinguishing feature of RC is its significant display of the intrinsic information redundancy only if the subsidiary one is also present, due to introduction of check bases.

3. As shown in [1,2,5], error control code in RC with mutually prime bases has the MCD value of $d_{\min}^{(RC)}$ only if the information redundancy level is not less than the product of any $d_{\min}^{(RC)} - 1$ bases of a given RC.

The availability and interaction of primary and secondary redundancies during the subsidiary tests (time redundancy usage) of error-correcting process, which may provide a single-error error-correcting capability in RC, while $d_{\min}^{(RC)} = 2$ (given $k = 1$).

Indeed, according to the expressions (3) and (5) for an ordered RC following conclusions can be made: with a single $(k = 1)$ check base m_{n+1} in RC, the NCS $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ can have several values of $d_{\min}^{(RC)}$. In this case, it depends on the value of check residue m_{n+1}. If, for every different RC modulus condition $m_i < m_{n+1}$ $(i = \overline{1, n})$ is met, then conclusion can be made that $d_{\min}^{(RC)} = 2$, as according to the expression (1), and $t_{\text{det.}} = 1$, according to the expression (2). If the condition $m_i \cdot m_j < m_{n+1}$ $(i, j = \overline{1, n};\ i \neq j)$ is met across the totality of $\{m_i\}$ information bases for a random modulus pair, then $d_{\min}^{(RC)} = 3$ and $t_{\text{det.}} = 2$.

Thus, for the NCS in RC given $k = 1$, the MCD $d_{\min}^{(RC)}$ can vary, depending on the value of RC check base m_{n+1}. Assume, RC is given information bases $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ and moreover $m_k = m_{n+1} = m_5 = 11$. In this case error verification of any single corrupted NCS residue can be ensured.

Assume, for example, $m_k = m_{n+1} = 61$. Ad hoc, we'll draw up a Table 1, mapping information bases to check bases. As Table 1 shows, number representation specificity in RC in some cases allows not only to detect an error, but to find a place of its occurrence with the use of a single check base, which would be impossible to do in the PNS, utilizing existing methods of detecting and correcting errors.

Let's assume, that in the corrupted ($\tilde{A} \geq M$) number $\tilde{A} = (a_1 \| a_2 \| ... \| a_{i-1} \| \tilde{a}_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$

the error $\tilde{a}_i = (a_i + \Delta a_i) \bmod m_i$ is verified to be present in the residue a_i modulo m_i.

Table 1 – Research results of error-correcting capabilities of error control codes in RC ($l = 1$)

$m_k = m_{n+1} = m_5 = 61$; $d_{\min}^{(RC)} = k + 1 = 2$, $\prod_{i=1}^{3} m_i \le m_5$.							Max. amount of detectable data errors in RC	Max. amount of correctable data errors in RC
RC information bases				$\prod_{r=1}^{k'} m_{i_r} \le m_{n+1}$	k'	$d_{\min}^{(RC)'} = k' + 1$		
$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$					
+	–	–	–	$3 < 61$	1	2	1	0
–	+	–	–	$4 < 61$	1	2	1	0
–	–	+	–	$5 < 61$	1	2	1	0
–	–	–	+	$7 < 61$	1	2	1	0
+	+	–	–	$3 \cdot 4 = 12 < 61$	2	3	2	1
+	–	+	–	$3 \cdot 5 = 15 < 61$	2	3	2	1
+	–	–	+	$3 \cdot 7 = 21 < 61$	2	3	2	1
–	+	+	–	$4 \cdot 5 = 20 < 61$	2	3	2	1
–	+	–	+	$4 \cdot 7 = 28 < 61$	2	3	2	1
–	–	+	+	$5 \cdot 7 = 35 < 61$	2	3	2	1
+	+	+	–	$3 \cdot 4 \cdot 5 = 60 < 61$	3	4	3	2

We'll take a look at the ratio, which makes it possible to correct an error in a given residue $\tilde{a}_i$ [1].

It's clear that:

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

Basing on that the error magnitude can be equated to $\Delta A = (0 \| 0 \| \ldots \| 0 \| \Delta a_i \| 0 \| \ldots \| 0 \| 0)$, then the correct ($A < M$) number A can be expressed as follows:

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

We'll quantify the value of A. Inasmuch number A is correct, i.e. is contained in numerical interval $[0, M)$, then the following inequality will be fulfilled:

$$A = (\tilde{A} - \Delta A) \bmod M_0 < M. \tag{7}$$

Basing on the value of the error ΔA is equal to $\Delta A = \Delta a_i \cdot B_i$, then the inequality (7) will be expressed as:

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

Since the orthogonal base of RC module m_i takes the form of $B_i = \overline{m}_i \cdot M_0 / m_i$, then the expression (8) shows up as:

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

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

Inasmuch as the value of the residue a_i is a natural number, then the value of $m_i (1 + r \cdot m_{n+1}) / (\bar{m}_i \cdot m_{n+1}) - \tilde{A} / B_i$, as shown in the expression (9), should be an integer. Thus, taking an integral part of the last ratio, the formula for correcting error in the residue $\tilde{a}_i$ of the number $\tilde{A}$ will be:

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

We'll have a look at the examples of error correction in RC.

Example №1. Perform data verification of the number $A_{RC} = (0 \| 0 \| 0 \| 0 \| 5)$ and correct it if required, when RC was given information $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_5 = 7$ and check $m_k = m_5 = 11$ bases. Thereby, $M = \prod_{i=1}^{n} m_i = \prod_{i=1}^{4} m_i = 420$ and $M_0 = M \cdot m_{n+1} = 420 \cdot 11 = 4620$. Orthogonal RC bases B_i $(i = \overline{1, n+1})$ are shown in Table 2.

I. Data verification of $A_{RC} = (0 \| 0 \| 0 \| 0 \| 5)$. According to the control procedure [1] the value will be defined as:

Table 2 – Orthogonal RC bases B_i $(l = 1)$

$B_1 = (1 \| 0 \| 0 \| 0 \| 0) = 1540$, $\bar{m}_1 = 1$
$B_2 = (0 \| 1 \| 0 \| 0 \| 0) = 3465$, $\bar{m}_2 = 3$
$B_3 = (0 \| 0 \| 1 \| 0 \| 0) = 3696$, $\bar{m}_3 = 4$
$B_4 = (0 \| 0 \| 0 \| 1 \| 0) = 2640$, $\bar{m}_4 = 4$
$B_5 = (0 \| 0 \| 0 \| 0 \| 1) = 2520$, $\bar{m}_5 = 6$

$$A_{PNS} = \left(\sum_{i=1}^{n+1} a_i \cdot B_i \right) \bmod M_0 = \left(\sum_{i=1}^{5} a_i \cdot B_i \right) \bmod M_0 = (a_1 \cdot B_1 + a_2 \cdot B_2 + a_3 \cdot B_3 +$$

$$a_4 \cdot B_4 + a_5 \cdot B_5) \bmod M_0 = (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 0 \cdot 2640 + 5 \cdot 2520) \bmod 4620 =$$

$$= (5 \cdot 2520) \bmod 4620 = 12600 (\bmod 4620) = 3360 > 420 .$$

Thus, in the process of data verification it was evaluated, that $A_{RC} = 3360 > M = 420$. In this case, with the possibility of only single errors appearing, conclusion is made that the number in question $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$ is incorrect ($3360 > M = 420$).

In order to correct the number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$ data is required to be verified first, i.e. corrupted residue $\tilde{a}_i$ has to be detected. Once done, the true value of the residue a_i modulo m_i needs to be defined, whereupon the corrupted residue $\tilde{a}_i$ should be corrected.

II. Data diagnosing of $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. According to the mapping method [1,2], possible projections $\tilde{A}_j$ of the number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$ are:

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

$$\tilde{A}_4 = (0 \| 0 \| 0 \| 5) \text{ and } \tilde{A}_5 = (0 \| 0 \| 0 \| 0) .$$

Computational formula for the values $\tilde{A}_{j\,PNS}$ of PNS number projections is written as [1]:

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

According to the expression (11) we'll compute all the values of $\tilde{A}_{j\,PNS}$. Once done, we will make $(n+1)$ comparison of the $\tilde{A}_{j\,PNS}$ numbers to the number $M = M_0 / m_{n+1}$. If there are any numbers not being contained in the informational numeric interval $[0, M)$, which contains k correct numbers (i.e. $\tilde{A}_k \geq M$), among $\tilde{A}_i$ projections, then conclusion is made that these k residues of the number A are not corrupted. Only the residues among the rest $[(n+1)-k]$ number $\tilde{A}_{RC}$ residues can be false.

The set of the active quotient residues for a given RC and the totality of the quotient B_{ij} orthogonal bases are shown in Table 3 and Table 4 respectively.

Table 3 – Set of the active quotient RC residues ($l = 1$)

j \ i	m_1	m_2	m_3	m_4	M_j
1	4	5	7	11	1540
2	3	5	7	11	1155
3	3	4	7	11	924
4	3	4	5	11	660
5	3	4	5	7	420

Table 4 – The totality of the quotient orthogonal RC bases B_{ij} ($l = 1$)

B_{ij} i / j	1	2	3	4
1	385	616	1100	980
2	385	231	330	210
3	616	693	792	672
4	220	165	396	540
5	280	105	336	120

Now then (Table 4):

$$\tilde{A}_{1PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i1} \right) \bmod M_1 = (a_1 \cdot B_{11} + a_2 \cdot B_{21} + a_3 \cdot B_{31} + a_4 \cdot B_{41}) \bmod M_1 =$$
$$= (0 \cdot 385 + 0 \cdot 616 + 0 \cdot 1100 + 5 \cdot 980) \bmod 1540 = 280 < 420.$$

Arriving at conclusion, that the residue a_1 of the number $\tilde{A}_1$ is possibly a corrupted residue $\bar{a}_1$;

$$\tilde{A}_{2PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i2} \right) \bmod M_2 = (a_1 \cdot B_{12} + a_2 \cdot B_{22} + a_3 \cdot B_{32} + a_4 \cdot B_{42}) \bmod M_2 =$$
$$= (0 \cdot 385 + 0 \cdot 231 + 0 \cdot 330 + 5 \cdot 210) \bmod 1155 = 1050 > 420.$$

Hence, the residue a_2 is ensured being not corrupted;

$$\tilde{A}_{3PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i3} \right) \bmod M_3 = (a_1 \cdot B_{13} + a_2 \cdot B_{23} + a_3 \cdot B_{33} + a_4 \cdot B_{43}) \bmod M_3 =$$
$$= (0 \cdot 616 + 0 \cdot 693 + 0 \cdot 792 + 5 \cdot 672) \bmod 924 = 588 > 420.$$

Deduced, the residue a_3 is ensured being not corrupted;

$$\tilde{A}_{4PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i4}\right) \bmod M_4 = (a_1 \cdot B_{14} + a_2 \cdot B_{24} + a_3 \cdot B_{34} + a_4 \cdot B_{44}) \bmod M_4 =$$
$$= (0 \cdot 220 + 0 \cdot 165 + 0 \cdot 369 + 5 \cdot 540) \bmod 660 = 60 < 420.$$

Conclusion: the residue a_4 modulo m_4 of the number $\tilde{A}_4$ is possibly a corrupted residue $\bar{a}_4$;

$$\tilde{A}_{5PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i5}\right) \bmod M_5 . \text{ Since } M_5 = M = 420,$$

the residue $\bar{a}_5$ of the check module $m_k = m_5$ will be always among the totality of possibly corrupted residues $\bar{a}_i$ of RC number.

Overall conclusion. During data diagnosing of $\tilde{A} = (0 \| 0 \| 0 \| 0 \| 5)$ in NCS, the residues $a_2 = 0$ and $a_3 = 0$ were ensured not being corrupted. The residues to the bases m_1, m_4 and m_5 might be corrupted, i.e. the residues $\bar{a}_1 = 0$, $\bar{a}_4 = 0$ and $\bar{a}_5 = 5$. In this case it's required to correct the residues $\bar{a}_1$, $\bar{a}_4$ and $\bar{a}_5$.

III. Correcting data errors $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. According to the acquainted [1] expression:

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

we will correct possibly $\bar{a}_1$, $\bar{a}_4$ and $\bar{a}_5$ corrupted residues a_1, a_4 and a_5, where $r = 1, 2, 3, \dots$.

It turns out that:

$$a_1 = \left(\bar{a}_1 + \left[\frac{m_1 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_1} - \frac{\tilde{A}}{B_1}\right]\right) \bmod m_1 = \left(0 + \left[\frac{3 \cdot (1 + r \cdot 11)}{11 \cdot 1} - \frac{3360}{1540}\right]\right) \bmod 3 =$$
$$= (0 + [3{,}27 - 2{,}18]) \bmod 3 = (0 + [1{,}09]) \bmod 3 = (0 + 1) \bmod 3 = 1;$$
$$a_4 = \left(\bar{a}_4 + \left[\frac{m_4 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_4} - \frac{\tilde{A}}{B_4}\right]\right) \bmod m_4 = \left(0 + \left[\frac{7 \cdot 12}{11 \cdot 4} - \frac{3360}{2640}\right]\right) \bmod 7 =$$
$$= (0 + [1{,}9 - 1{,}27]) \bmod 7 = (0 + [0{,}63]) \bmod 7 = (0 + 0) \bmod 7 = 0;$$
$$a_5 = \left(\bar{a}_5 + \left[\frac{m_{n+1} \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_{n+1}} - \frac{\tilde{A}}{B_5}\right]\right) \bmod m_{n+1} = \left(5 + \left[\frac{11 \cdot (1 + 11)}{11 \cdot 6} - \frac{3360}{2520}\right]\right) \bmod 11 =$$
$$= (5 + [2 - 1{,}3]) \bmod 11 = (5 + [0{,}7]) \bmod 11 = (5 + 0) \bmod 5 = 0.$$

With accordance to the computed residues $a_1 = 1$, $a_4 = 0$ and $a_5 = 0$ we are correcting (recovering) the corrupted number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$, i.e. the corrected number becomes $\tilde{A}_{cor.} = (1 \| 0 \| 0 \| 0 \| 5)$.

To validate corrected data, as according to the acquainted [1] expression, we'll define the value of the number $\tilde{A}_{cor.} = (1 \| 0 \| 0 \| 0 \| 5)$ in the following way (see Table 2):

$$\tilde{A}_{cor.PNS} = \left(\sum_{i=1}^{5} a_i \cdot B_i\right) \bmod M_0 = (a_1 \cdot B_1 + a_2 \cdot B_2 + a_3 \cdot B_3 + a_4 \cdot B_4 + a_5 \cdot B_5) \bmod M_0 =$$
$$= (1 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 0 \cdot 2640 + 5 \cdot 2520) \bmod 4620 = 14140 (\bmod 4620) = 280.$$

Thus $280 < M = 420$, the number $\tilde{A}_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ is correct.

In order to validate correctness of the number $\tilde{A}_{3360}$ we'll make a computation and comparison of the values to the correct residues $a_2 = 0$ and $a_3 = 0$. In this case they are $a_2 = \left(0 + \left[\frac{4 \cdot (1 + 11)}{11 \cdot 3} - \frac{3360}{3465}\right]\right) \bmod 4 = 0$ and $a_3 = \left(0 + \left[\frac{5 \cdot (1 + 11)}{11 \cdot 4} - \frac{3360}{3696}\right]\right) \bmod 5 = 0$. The resulted computations $a_2 = 0$ and $a_3 = 0$ of the residues modulo m_2 and m_3 in RC verified correctness of the corrupted number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. Thus, the original number $\tilde{A}_{RC} = (0 \| 0 \| 0 \| 0 \| 5)$ is corrupted $\tilde{A}_{3360}$, wherein the single error $\Delta a_1 = 1$ occurred modulo m_1. This error made the correct number A_{280} being corrupted $\tilde{A}_{3360}$.

In order to verify if the correct number A_{280} is true, subsidiary tests on the process of corruption and correction of the number A_{280} modulo $m_1 = 3$ are required. The amount of possible N_{CC} incorrect (corrupted) $\tilde{A}_{RC}$ codewords (if only a single error occurred) for each correct A_{RC} number are

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

Test results have shown that corruption of the residue a_1 modulo $m_1 = 3$ of the correct number A_{280} can produce only two incorrect numbers: $\tilde{A}_{3360} = (\tilde{0} \| 0 \| 0 \| 0 \| 5)$ and $\tilde{A}_{1820} = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$. This points to the fact that the corrected number $A_{cor.} = A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ is both correct (is contained in the interval [0, 420)) and true.

The trueness of the resulted number $A_{280} = (\hat{1} \| 0 \| 0 \| 0 \| 5)$ is confirmed by the fact that the single error $\Delta a_1 = 2$ to the base $m_1 = 3$ converts $(\tilde{A} = (A + \Delta A) \bmod M_0 = = (1 \| 0 \| 0 \| 0 \| 5) + (2 \| 0 \| 0 \| 0 \| 0) = \left[(1+2) \bmod 3 \| 0 \| 0 \| 0 \| 5\right] = (\tilde{0} \| 0 \| 0 \| 0 \| 5))$ this number to the unique incorrect number $\tilde{A}_{3360} = (\tilde{0} \| 0 \| 0 \| 0 \| 5)$.

Example №2. Assume, the correct number is $A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ and assume that $\Delta a_1 = 1$. In this case $\tilde{A} = (A + \Delta A) \bmod M_0 = (1 \| 0 \| 0 \| 0 \| 5) + (1 \| 0 \| 0 \| 0 \| 0) = = \left[(1+1) \bmod 3 \| 0 \| 0 \| 0 \| 5\right] = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$. This RC number is relevant to the number 1820 in PNS, i.e. the number $\tilde{A}_{1820}$ is incorrect. We'll correct the number $\tilde{A}_{1820}$ now.

Data diagnosing should be made ahead of correcting the number $\tilde{A}_{1820}$. To do this we'll map projections A_j $(j = \overline{1, 5})$ of the number $\tilde{A}_{1820} = (2 \| 0 \| 0 \| 0 \| 5)$ first. Resulted RC code structures are: $\tilde{A}_1 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_2 = (2 \| 0 \| 0 \| 5)$, $\tilde{A}_3 = (2 \| 0 \| 0 \| 5)$, $\tilde{A}_4 = (2 \| 0 \| 0 \| 5)$ and $\tilde{A}_5 = (2 \| 0 \| 0 \| 0)$.

All the projections of $\tilde{A}_{j\,PNS}$ are:

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

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

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

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

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

Inasmuch as $\tilde{A}_{2PNS}$, $\tilde{A}_{3PNS}$ and $\tilde{A}_{4PNS} > 420$, the conclusion is made that the residues $a_2 = 0$, $a_3 = 0$ and $a_4 = 0$ of the number $\tilde{A}_5 = (2 \| 0 \| 0 \| 0 \| 5)$ are not corrupted. Only the residues a_1 and a_5 can be corrupted $\bar{a}_1 = 2$ and $\bar{a}_5 = 5$.

We obtain, that:

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

$$= \left(2 + [3{,}27 - 1{,}18]\right) \bmod 3 = \left(2 + [2{,}09]\right) \bmod 3 = (2+2) \bmod 3 = 4 (\bmod 3) = 1.$$

Hence, the corrected residue modulo m_1 is $a_1 = 1$. In a like manner the residue $a_5 = 5$.

Applying the results a_1 and a_5 the corrupted number $\tilde{A}_{1820} = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$ is corrected. As a final result the corrected number is $A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$.

Example №3. Performing verification of the number $A_{RC} = (0 \| 0 \| 0 \| 2 \| 1)$. In case corruption was detected, data diagnosing and correction should be made.

I. Data checking of $A_{RC} = (0 \| 0 \| 0 \| 2 \| 1)$. According to the acquainted control procedure A_{PNS} will be calculated using expression:

$$A_{PNS} = \left(\sum_{i=1}^{n+1} a_i \cdot B_i \right) \mathrm{mod}\, M_0 = (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 2 \cdot 2640 + 1 \cdot 2520) \mathrm{mod}\, 4620 =$$

$$= 7800 (\mathrm{mod}\, 4620) = 3180 > 420$$. This number is incorrect $\tilde{A}_{3180}$.

II. Data diagnosing of $\tilde{A}_{3180} = (0 \| 0 \| 0 \| 2 \| 1)$. All possible projections $\tilde{A}_j$ of the number $\tilde{A}_{3180}$ are: $\tilde{A}_1 = (0 \| 0 \| 2 \| 1)$, , $\tilde{A}_3 = (0 \| 0 \| 2 \| 1)$, $\tilde{A}_4 = (0 \| 0 \| 0 \| 1)$ and $\tilde{A}_5 = (0 \| 0 \| 0 \| 2)$.

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

$$\tilde{A}_{1RC} = (0 \| 0 \| 2 \| 1) = \tilde{A}_{1PNS} = (a_1 \cdot B_{11} + a_2 \cdot B_{21} + a_3 \cdot B_{31} + a_4 \cdot B_{41}) \mathrm{mod}\, M_1 =$$
$$= (0 \cdot 385 + 0 \cdot 616 + 2 \cdot 1100 + 1 \cdot 980) \mathrm{mod}\, 1540 = 100 < M = 420;$$
$$\tilde{A}_{2RC} = (0 \| 0 \| 2 \| 1) = \tilde{A}_{2PNS} = (a_1 \cdot B_{12} + a_2 \cdot B_{22} + a_3 \cdot B_{32} + a_4 \cdot B_{42}) \mathrm{mod}\, M_2 =$$
$$= (0 \cdot 385 + 0 \cdot 231 + 2 \cdot 330 + 1 \cdot 210) \mathrm{mod}\, 1155 = 870 > M = 420;$$
$$\tilde{A}_{3RC} = (0 \| 0 \| 2 \| 1) = \tilde{A}_{3PNS} = (a_1 \cdot B_{13} + a_2 \cdot B_{23} + a_3 \cdot B_{33} + a_4 \cdot B_{43}) \mathrm{mod}\, M_3 =$$
$$= (0 \cdot 616 + 0 \cdot 693 + 2 \cdot 792 + 1 \cdot 672) \mathrm{mod}\, 924 = 418 < M = 420;$$
$$\tilde{A}_{4RC} = (0 \| 0 \| 0 \| 1) = \tilde{A}_{4PNS} = (a_1 \cdot B_{14} + a_2 \cdot B_{24} + a_3 \cdot B_{34} + a_4 \cdot B_{44}) \mathrm{mod}\, M_4 =$$
$$= (0 \cdot 220 + 0 \cdot 165 + 2 \cdot 396 + 1 \cdot 540) \mathrm{mod}\, 660 = 540 > M = 420;$$
$$\tilde{A}_{5RC} = (0 \| 0 \| 0 \| 2) = \tilde{A}_{5PNS} = (a_1 \cdot B_{15} + a_2 \cdot B_{25} + a_3 \cdot B_{35} + a_4 \cdot B_{45}) \mathrm{mod}\, M_5 =$$
$$= (0 \cdot 280 + 0 \cdot 105 + 2 \cdot 336 + 1 \cdot 120) \mathrm{mod}\, 420 = 240 < M = 420.$$

The calculations of the $\tilde{A}_{j\,PNS}$ values and comparing them to the verification interval $[0, 420)$ range of correct RC numbers A_{RC} resulted in following. The totality of the residues $a_2 = 0$ and $a_4 = 0$ is correct (residues are not being corrupted), while the residues $\bar{a}_1 = 0$, $\bar{a}_3 = 0$ and $\bar{a}_5 = 1$ of the incorrect number $\tilde{A}_{3180} = (0 \| 0 \| 0 \| 2 \| 1)$ might be incorrect (could have been corrupted).

III. Correcting possibly corrupted residues $\bar{a}_1$, $\bar{a}_3$ and $\bar{a}_5$ of the number $\tilde{A}_{3180}$.

Possibly corrupted residues $\bar{a}_1 = 0$, $\bar{a}_3 = 0$ and $\bar{a}_5 = 1$ required to be corrected using expression

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

Then:

$$a_1 = \left(\bar{a}_1 + \left[\frac{m_1 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_1} - \frac{\tilde{A}}{B_1} \right] \right) \mathrm{mod}\, m_1 = \left(0 + \left[\frac{3 \cdot (1 + r \cdot 11)}{11 \cdot 1} - \frac{3180}{1540} \right] \right) \mathrm{mod}\, 3 =$$
$$= (0 + [3,27 - 2,06]) \mathrm{mod}\, 3 = (0 + [1,21]) \mathrm{mod}\, 3 = (0 + 1) \mathrm{mod}\, 3 = 1.$$

Hence, $a_1 = 1$.

For the value $\bar{a}_3$ it is:

$$a_3 = \left(\tilde{a}_3 + \left[\frac{m_3 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_3} - \frac{\tilde{A}}{B_3} \right] \right) \mathrm{mod}\, m_3 = \left(0 + \left[\frac{5 \cdot (1 + r \cdot 11)}{11 \cdot 4} - \frac{3180}{3696} \right] \right) \mathrm{mod}\, 5 =$$
$$= (0 + [1,36 - 0,86]) \mathrm{mod}\, 5 = (0 + [0,5]) \mathrm{mod}\, 5 = (0 + 0) \mathrm{mod}\, 5 = 0.$$

In this case $a_3 = 0$.

For the residue $\bar{a}_5$ value is:

$$a_5 = \left(\tilde{a}_5 + \left[\frac{m_5 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_5} - \frac{\tilde{A}}{B_5}\right]\right) \bmod m_5 = \left(1 + \left[\frac{11 \cdot (1 + r \cdot 11)}{11 \cdot 6} - \frac{3180}{2520}\right]\right) \bmod 11 =$$
$$= \left(1 + [2 - 1,26]\right) \bmod 11 = \left(1 + [0,74]\right) \bmod 11 = (1 + 0) \bmod 11 = 1.$$

Obtaining that $a_5 = 1$.

Using the calculated values $a_1 = 1$, $a_3 = 0$ and $a_5 = 1$ of the recovered residues the corrupted number $\tilde{A}_{RC} = (0 \| 0 \| 0 \| 2 \| 1)$ can be corrected, becoming $A_{RC} = (1 \| 0 \| 0 \| 2 \| 1)$. Verified by $100 < 420$.

3 Conclusions of research

Contrary to PNS (positional numeral system), arithmetic RC (residue class) codes feature additional correcting properties. Thus, NCS (non-positional code structure) involves both intrinsic and subsidiary information redundancies, that in some cases results in allowing to correct single errors in RC, while MCD is $d_{\min}^{(RC)} = 2$. However, correcting single errors requires performing subsidiary tests of data checking, i.e. time redundancy usage, additionally to information redundancy. Examples of specific implementation of a single error correcting procedures were introduced, that prove reviewed method is possible to be implemented in order to correct data errors in RC.

References

[1] Akushskii I. Ya. Mashinnaya arifmetika v ostatochnykh klassakh / I. Ya. Akushskii, D. I. Yuditskii – M.: Sov. Radio, 1968. – 440 s.

[2] 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. – November 2014. – Volume 50, Issue 6, pp. 969-976.

[3] Modeli i metody obrabotki dannykh v sisteme ostatochnykh klassov: [monografiya] / [Krasnobaev V. A., Koshman S. A. i dr.] – Khar'kov: OOO "V dele", 2017. – 197 s.

[4] Stasev Yu.V., Kuznetsov A.A., Nosik A.M. Formation of pseudorandom sequences with improved autocorrelation properties // Cybernetics and Systems Analysis, Volume 43, Issue 1, January 2007, Pages 1 – 11.

[5] Karpenko O., Kuznetsov A., Sai V. Stasev Yu.. Discrete Signals with Multi-Level Correlation Function // Telecommunications and Radio Engineering. - Volume 71, 2012 Issue 1. pp. 91-98.

Рецензент: Сергій Кавун, доктор економічних наук, к.т.н., проф., Харківський інститут банківської справи УБС НБУ, Харків, Україна.
E-mail: kavserg@gmail.com

Надійшло: Листопад 2017.

Автори:
Віктор Краснобаєв, д.т.н., проф.., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: v.a.krasnobaev@gmail.com

Сергій Кошман, к.т.н., доцент, Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: s_koshman@ukr.net

Аліна Янко, к.т.н., Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна.
E-mail: al9_yanko@ukr.net

Сергій Мороз, к.т.н., Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна.
E-mail: frost9i@ukr.net

Метод виправлення однократних помилок даних, що представлені кодом класу лишків.

Анотація. У даній статті розглянуто метод виправлення однократних помилок у класі лишків (КЛ). Результати аналізу коригувальних можливостей арифметичного коду показали високу ефективність використання непозиційних кодових структур у КЛ, за рахунок наявності у непозиційній кодової структурі первинної та вторинної надмірності. У статті наведені приклади виправлення одноразових помилок даних, що представлені кодом КЛ.

Ключові слова: непозиційна кодова структура, клас лишків, позиційна система числення, мінімальна кодова відстань, завадостійке кодування, діагностика та корекція даних.

Рецензент: Сергей Кавун, доктор экономических наук, к.т.н., проф., Харьковский институт банковского дела УБД НБУ, пр. Победы, 55, г. Харьков, 61174, Украина.
E-mail: kavserg@gmail.com

Поступила: Ноябрь 2017.

Авторы:
Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: v.a.krasnobaev@gmail.com

Сергей Кошман, к.т.н., доцент, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: s_koshman@ukr.net

Алина Янко, к.т.н., Полтавский национальный технический университет имени Юрия Кондратюка, Полтава, Украина.
E-mail: al9_yanko@ukr.net

Сергей Мороз, к.т.н., Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, Харьков, Украина.
E-mail: frost9i@ukr.net

Метод исправления однократных ошибок данных, представленных кодом класса вычетов.

Аннотация. В данной статье рассмотрен метод исправления однократных ошибок в классе вычетов (КВ). Результаты анализа корректирующих возможностей арифметического кода показали высокую эффективность использования непозиционных кодовых структур в КВ, за счёт наличия в непозиционной кодовой структуре первичной и вторичной избыточности. В статье приведены примеры исправления однократных ошибок данных, представленных кодом КВ.

Ключевые слова: непозиционная кодовая структура, класс вычетов, позиционная система счисления, минимальное кодовое расстояние, помехоустойчивое кодирование, диагностика и коррекция данных.