УДК 681.142:681 DOI: 10.26565/2519-2310-2019-2-04

# МЕТОД КОНТРОЛЮ ДАНИХ, ПРЕДСТАВЛЕНИХ КОДОМ НЕПОЗИЦІЙНОЇ СИСТЕМИ ЧИСЛЕННЯ КЛАСІВ ЗАЛИШКІВ

Андрій Д'яченко, Ірина Локоткова, Олеся Решетняк, Михайло Зуб, Костянтин Мисливцев

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
0andrey.090220@gmail.com, lokotosyk@ukr.net, lesyandr13@gmail.com, mishazub007@gmail.com, kostyavtx@gmail.com

**Рецензент**: Олександр Оксіюк, д.т.н., проф., Київський національний університет імені Т. Шевченка, вул. М. Ломоносова 81, Київ, 03189, Україна.
o.oksiuk@gmail.com

Надійшло: Жовтень 2019.

***Анотація:*** *Пропонується новий метод моніторингу даних, представлених у непозиційній системі класів залишків. Для коду в системі класів залишків тестові бази включаються в загальну структуру коду даних, що містить набір баз інформації. У цьому випадку баланси, які представляють операції з інформаційних та контрольних підстав одночасно та незалежно беруть участь у процесі обробки інформації. За результатами обробки інформації можна відслідковувати або поетапно, або наприкінці всіх обчислень, оскільки помилка, яка сталася в будь-якому залишку, не застосовується (не "помножується") на залишки, що залишилися. Запропонований метод контролю, заснований на принципі порівняння, в подальшому створює передумови для розробки ефективних методів діагностики і корекції помилок в класі залишків. Недоліком запропонованого методу є дещо низька оперативність контролю. Дана обставина обумовлює необхідність підвищення оперативності контролю системи обробки даних в класі залишків за рахунок зменшення часу виконання перерахованих вище операцій шляхом розробки і використання, наприклад, методів і засобів реалізації позиційних ознак непозиційних кодів у класі залишків.*

***Ключові слова:*** *метод контролю даних, клас залишків; непозиційна система.*

## 1 Вступ

Відомо, що використання властивостей непозиційної системи числення класу залишків (КЗ) забезпечує високу призначену для користувача продуктивність реалізації в системі обробки даних (СОД) обчислювальних алгоритмів, що складаються з арифметичних операцій [1-7]. Найбільша ефективність від застосування КЗ досягається в разі, коли реалізовані алгоритми складаються з сукупності таких арифметичних операцій, як додавання і віднімання множення [8-14]. Необхідність забезпечення відмовостійкого функціонування СОД вимагає розробки і впровадження в КЗ нових методів контролю і корекції помилок інформації, відмінних від методів, використовуваних в звичайних двійкових позиційних системах числення (ПСЧ) [15-21].

Відзначимо, що, по-перше, всі методи контролю та корекції даних в КЗ ґрунтуються на специфіці реалізації позиційних операцій в даній системі числення, що вимагає знання величини (можливо знаку) числа, представленого даною непозиційною кодовою структурою. По-друге, методи контролю в КЗ є подальшим розвитком контролю за модулем в ПСЧ (*арифметичні AN-коди*) [1-3, 10-14]. Дійсно, з точки зору інформаційного резервування коди є подальшим вдосконаленням відомих арифметичних багатозалишкових кодів.

Відомо, що багатозалишковий код представляється у вигляді:

$$A_k^{'} = (A_k, A_k (\mathrm{mod}\, m_1), A_k (\mathrm{mod}\, m_2), ..., A_k (\mathrm{mod}\, m_i), ...,$$
$$..., A_k (\mathrm{mod}\, m_{n-1}), A_k (\mathrm{mod}\, m_n),$$

тобто $A_k^{'} = (A_k, a_1, a_2, ..., a_n)$, де $a_i = A_k - [A_k / m_i] m_i$.

У цьому випадку, для

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

сукупність залишків $\{a_i\}$ однозначно визначає операнд $A'_к$ і чисельне значення $A_к$ стає взагалі не потрібне. Багатозалишковий код набирає вигляду непозиційного коду КЗ

$$A_к^{'} = (a_1, a_2, \ldots, a_n),$$

що дозволяє реалізувати модульні операції по окремим незалежним трактам, оперуючи тільки із залишками $\{a_i\}$. Таке кодування чисел дозволяє побудувати СОД, в якому обробка всіх залишків $a_i$ числа проводиться паралельно в часі [1, 2]. В цьому випадку узагальнена структурна схема СОД в КЗ являє собою набір окремих мікро-ЕОМ, що функціонують незалежно один від одного і паралельно в часі, причому кожна по власному певному модулю $m_i$ [12-14].

## 2 Основна частина

Процес корекції (виявлення і виправлення) помилок в інформаційній кодової структурі Ã даних складається з наступних основних етапів:

- контроль даних (*процес виявлення факту наявності помилки в числі A*);
- діагностика (*локалізація місця помилок із заданою глибиною діагностування*);
- виправлення помилок в кодовій структурі даних (*відновлення спотворених залишків*

$$\tilde{a}_j (j = \overline{1, n})$$

*числа Ã та отримання правильного числа A*).

Число

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

в КЗ представляється сукупністю

$$\{a_i\} (i = \overline{1, n})$$

залишків

$$a_i \equiv A (\mathrm{mod}\, m_i)$$

по вибраній системі інформаційних основ (*модулів*) $\{m_i\}$ в робочому (*інформаційному*) числовому інтервалі [0, M), де

$$M = \prod_{i=1}^{n} m_i$$ – загальна кількість інформаційних кодових слів.

При цьому НСД

$$(m_i, m_j) = 1,$$

при

$$i, j = \overline{1, n}\ (i \neq j).$$

Для того, щоб код КЗ володів коректуючими властивостями необхідно, щоб він містив певну інформаційну надмірність. При цьому, по-перше, необхідно визначити (виявити) і, по можливості, кількісно оцінити наявну (природну) в первісній інформаційній кодовій структурі надмірність. По-друге, при необхідності забезпечення даних додатковими коректуючими здібностями, ввести додаткову (штучну) інформаційну надмірність (застосувати методи інформаційного резервування) за рахунок введення додаткових (контрольних) підстав $\{mk\}$ КЗ. Без втрати спільності міркувань вважатимемо, що до n інформаційним підставою КЗ додано одне

$$\mathrm{m_k} = \mathrm{m_{n+1}}$$

контрольне підставу взаємно просте з будь-яким з наявних інформаційних підстав. У цьому випадку число

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

в КЗ представляється за допомогою сукупності

$$\{m_j\}\ (j = \overline{1, n+1})$$

основ у повному числовому [0, $M_0$) інтервалі, де $M_0 = M \cdot m_{n+1}$ – загальна кількість кодових слів для даного КЗ.

Відомо [1-3], що для непозиційних кодових структур в КЗ мінімальна кодова відстань визначається виразом

$$d_{\min} = K + 1,$$

тобто воно залежить як від числа до контрольних підстав, так і від величини кожного з них. Якщо для контрольних основ $m_{z_t}$ виконується умова

$$\prod_{t=1}^{k} m_{z_t} \le m_k,$$

тоді введення в систему підстав КЗ однієї контрольної

$$m_k = m_{n+1}$$

основи еквівалентно наявності К контрольних основ. З урахуванням того, що всі числа, які беруть участі в обробці даних (передача та обробка інформації), а також результат операції даними знаходиться в інтервалі [0, M), то очевидно, що якщо в результаті обробки даних отримано остаточний результат A ≥ M, то це означає, що отримане число Ã спотворене (неправильне).

Таким чином, якщо в результаті обробки даних визначено, що Ã ≥ M, то робиться висновок, що число Ã неправильне. На цьому принципі (принципі порівняння) ґрунтуються всі методи порівняння даних в КЗ. Якщо A <M, то робиться висновок, що число А правильне, а якщо A ≥ M, то число Ã неправильне. При цьому передбачаються тільки одноразові (в одному із залишків $\{a_i\}$ числа А) помилки, або пачка помилок довжиною не більше

$$k = [\log_2 (m_i - 1)] + 1$$

двійкових розрядів.

Для розгляду методу контролю (*метод прямого порівняння*) даних в КЗ на основі зазначеного вище принципу, який використовується так само при розробці методів діагностики і корекції помилок, скористаємося результатами докази відомого [1] наукового затвердження.

*Твердження*. Нехай інформаційна основа

$$\{m_i\} \; (i = \overline{1, n})$$

КЗ з однією контрольною

$$m_k = m_{n+1}$$

основою впорядковані ($m_i < m_{i+1}$), і нехай результат

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

виконання операції є правильним числом, тобто

$$A < M \; (M = \prod_{i=1}^{n} m_i).$$

Тоді стверджується, що число

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

в якому спотворений один залишок $\tilde{a}_i \neq a_i$ за основою $m_i$, є неправильним, тобто $\tilde{A} \ge M$.

Продемонструємо це.

На основі принципу порівняння правильність числа А визначається виходячи зі співвідношення.

$$A < M = M_0 / m_{n+1} \; (M_0 = \prod_{i=1}^{n+1} m_i)$$

З іншого боку, очевидно виконання умови $M_0 / m_i > M_0 / m_{n+1}$ для упорядкованого КЗ при

$$i = \overline{1, n}.$$

В цьому випадку виконується така нерівність $A < M_0 / m_i$.

Відзначимо, що залишок

$$a_i \equiv A(\mathrm{mod}\, m_i)$$

числа А по модулю $m_i$ може набувати значень

$$a_i = \overline{0, m_i - 1}.$$

У відповідності до розділу твердження, що

$$\tilde{a}_i \neq a_i,$$

і враховуючи, що інші значення залишків

$$a_j (j = \overline{1, n+1} \text{ та } i \neq j)$$

неправильного Ã числа залишаються без змін, то в інтервалі [0, $M_0/m_i$) не можуть одночасно знаходиться обидва числа А і Ã. Тоді, так як число А < $M_0/m_{n+1}$ правильне (*знаходиться в робочому [0, M ]інтервалі*), то число Ã знаходиться поза інтервалом [0, $M_0/m_i$), і тим більше знаходиться поза інтервалом [0, M).

У цьому випадку число Ã, для якого виконується умова $\tilde{A} \geq M$, є неправильним. Таким чином показано, що число

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

є спотвореним (Рис 1, 2).

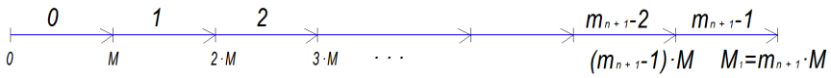


Рис. 1 - Числові інтервали для $m_k = m_{n+1}$

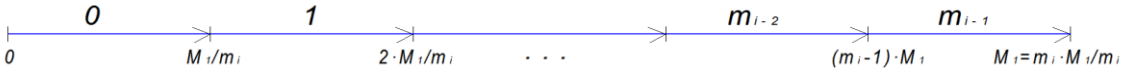


Рис. 2 - Числові інтервалі для довільного модуля *mi*

## 3 Аналіз методу контролю даних

Розглянемо метод контролю даних в КЗ, заснований на результатах і висновках розглянутого наукового затвердження.

В основі контролю лежить базова операція - порівняння результату А операції з числом

$$M = M_0/m_{n+1}.$$

Для порівняння чисел

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

та М необхідно перевести значення А в позиційну двійкову систему числення (ПСЧ). Для цього можна використовувати ортогональні базиси

$$B_i (i = \overline{1, n+1}),$$

яке представляються у вигляді [1-3]:

$$\begin{cases} B_1 = (1,0,\ldots,0,\ldots,0,0), \\ B_2 = (0,1,\ldots,0,\ldots,0,0), \\ B_i = (0,0,\ldots,1,\ldots,0,0), \\ B_n = (0,0,\ldots,0,\ldots,1,0), \\ B_{n+1} = (0,0,\ldots,0,\ldots,0,1). \end{cases} \quad (1)$$

Ортогональні базиси $B_i$ визначаються для кожного КЗ відповідно до виразу

$$B_i = \overline{m}_i \cdot M_0 / m_i \equiv 1(\mathrm{mod}\, m_i). \quad (2)$$

Значення ваги $\overline{m}_i$ ортогонального базису $B_i$ визначається як одне з рішень системи порівнянь:

$$\begin{cases} \overline{m}_i = 1, \quad 1 \cdot M_i \equiv \rho_1 (\mathrm{mod}\ m_i), \\ \overline{m}_i = 2, \quad 2 \cdot M_i \equiv \rho_2 (\mathrm{mod}\ m_i), \\ \qquad \ldots \\ \overline{m}_i = m_i - 2, \quad (m_i - 2) \cdot M_i \equiv \rho_{m-2} (\mathrm{mod}\ m_i), \\ \overline{m}_i = m_i - 1, \quad (m_i - 1) \cdot M_i \equiv \rho_{m-1} (\mathrm{mod}\ m_i). \end{cases} \tag{3}$$

Значення $\overline{m}_i$, для якого виконується умова (2), визначається шляхом підстановки можливих значень

$$\overline{m}_i = \overline{1, m_i - 1}$$

методом простого перебору. Значення А в ПСЧ визначається у співвідношенні з формулою

$$A_{ПСЧ} = (\sum_{i=1}^{n+1} a_i \cdot B_i) \bmod M_0 .$$

## 4. Приклади конкретної реалізації методу контролю даних в КЗ

Розглянемо приклади реалізації методу контролю даних для упорядкованого КЗ, заданого інформаційними $m_1 = 3, m_2 = 4, m_3 = 5, m_4 = 7$ і контрольним $m_k = m_5 = 11$ основами (рис. 3).

Даний КЗ забезпечує інформаційний інтервал [0, M) для однобайтової (l=1) СОД, де

$$M = \prod_{i=1}^{4} m_i = 420 .$$

Повний числовий інтервал уявлення числі в КЗ визначається як [0, $M_0$) (див. рис.3), де

$$M_0 = M \cdot m_{n+1} = 4620.$$

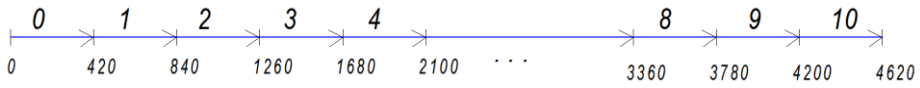


Рис. 3 - Числові інтервали для $l = 1$ ($m_k = m_{n+1} = 11$)

У таблицях 1÷5 представлені процедури визначення значень $\overline{m}_i (i = \overline{1,5})$, а в таблиці 6 розраховані значення ортогональних базисів $B_i (i = \overline{1,5})$.

Табл. 1 – Процедура визначення $\overline{m}_1$

| | |
|---|---|
| $\overline{m}_1 = 3, M_1 = 4 \cdot 5 \cdot 7 \cdot 11 = 1540$ | |
| $\overline{m}_1 = 1$ | $\overline{m}_1 \cdot M_1 = 1540 \equiv 1 (\mathrm{mod}\, m_1)$ |
| $\overline{m}_2 = 2$ | $\overline{m}_1 \cdot M_1 = 3080 \equiv 2 (\mathrm{mod}\, m_1)$ |
| $\overline{m}_1 = 1, B_1 = (1,0,0,0,0) = 1540$ | |

Табл. 2 – Процедура визначення $\overline{m}_2$

| | |
|---|---|
| $m_2 = 4, M_2 = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$ | |
| $\overline{m}_2 = 1$ | $1 \cdot M_2 = 1155 \equiv 3 (\mathrm{mod}\, m_2)$ |
| $\overline{m}_2 = 2$ | $2 \cdot M_2 = 2310 \equiv 2 (\mathrm{mod}\, m_2)$ |
| $\overline{m}_2 = 3$ | $3 \cdot M_2 = 3465 \equiv 1 (\mathrm{mod}\, m_2)$ |
| $\overline{m}_2 = 3$ | $B_2 = (0,1,0,0,0) = 3465$ |

Табл. 3 – Процедура визначення $\overline{m}_3$

| $m_3 = 5, M_3 = 3 \cdot 4 \cdot 7 \cdot 11 = 924$ | |
|---|---|
| $\overline{m}_3 = 1$ | $1 \cdot M_3 = 924 \equiv 4 (\mathrm{mod}\, m_3)$ |
| $\overline{m}_3 = 2$ | $2 \cdot M_3 = 1848 \equiv 3 (\mathrm{mod}\, m_3)$ |
| $\overline{m}_3 = 3$ | $3 \cdot M_3 = 2772 \equiv 2 (\mathrm{mod}\, m_3)$ |
| $\overline{m}_3 = 4$ | $4 \cdot M_2 = 3696 \equiv 1 (\mathrm{mod}\, m_3)$ |
| $\overline{m}_3 = 4,\ B_3 = (0,0,1,0,0) = 3696$ | |

Табл. 4 – Процедура визначення $\overline{m}_4$

| $m_4 = 7, M_4 = 3 \cdot 4 \cdot 5 \cdot 11 = 660$ | |
|---|---|
| $\overline{m}_4 = 1$ | $1 \cdot M_4 = 660 \equiv 2 (\mathrm{mod}\, m_4)$ |
| $\overline{m}_4 = 2$ | $2 \cdot M_4 = 1320 \equiv 4 (\mathrm{mod}\, m_4)$ |
| $\overline{m}_4 = 3$ | $3 \cdot M_4 = 1980 \equiv 6 (\mathrm{mod}\, m_4)$ |
| $\overline{m}_4 = 4$ | $4 \cdot M_4 = 2640 \equiv 1 (\mathrm{mod}\, m_4)$ |
| $\overline{m}_4 = 5$ | $5 \cdot M_4 = 3300 \equiv 3 (\mathrm{mod}\, m_4)$ |
| $\overline{m}_4 = 6$ | $6 \cdot M_4 = 3960 \equiv 5 (\mathrm{mod}\, m_4)$ |
| $\overline{m}_4 = 4,\ B_4 = (0,0,0,1,0) = 2640$ | |

Табл. 5 – Процедура визначення $\overline{m}_5$

| $m_5 = 11, M_5 = 3 \cdot 4 \cdot 5 \cdot 7 = 420$ | |
|---|---|
| $\overline{m}_5 = 1$ | $1 \cdot M_5 = 420 \equiv 2 (\mathrm{mod}\, m_5)$ |
| $\overline{m}_5 = 2$ | $2 \cdot M_5 = 840 \equiv 4 (\mathrm{mod}\, m_5)$ |
| $\overline{m}_5 = 3$ | $3 \cdot M_5 = 1260 \equiv 6 (\mathrm{mod}\, m_5)$ |
| $\overline{m}_5 = 4$ | $4 \cdot M_5 = 1680 \equiv 8 (\mathrm{mod}\, m_5)$ |
| $\overline{m}_5 = 5$ | $5 \cdot M_5 = 2100 \equiv 10 (\mathrm{mod}\, m_5)$ |
| $\overline{m}_5 = 6$ | $6 \cdot M_5 = 2520 \equiv 1 (\mathrm{mod}\, m_5)$ |
| $\overline{m}_5 = 7$ | $7 \cdot M_5 = 2940 \equiv 3 (\mathrm{mod}\, m_5)$ |
| $\overline{m}_5 = 8$ | $8 \cdot M_5 = 3360 \equiv 5 (\mathrm{mod}\, m_5)$ |
| $\overline{m}_5 = 9$ | $9 \cdot M_5 = 3780 \equiv 7 (\mathrm{mod}\, m_5)$ |
| $\overline{m}_5 = 10$ | $10 \cdot M_5 = 4200 \equiv 9 (\mathrm{mod}\, m_5)$ |
| $\overline{m}_5 = 6,\ B_5 = (0,0,0,0,1) = 2520$ | |

Табл. 6 – Ортогональні базиси $B_i$ КЗ

| |
|---|
| $B_1 = (1,0,0,0,0) = 1540$ |
| $B_2 = (0,1,0,0,0) = 3465$ |
| $B_3 = (0,0,1,0,0) = 3696$ |
| $B_4 = (0,0,0,1,0) = 2640$ |
| $B_5 = (0,0,0,0,1) = 2520$ |

Нехай задано правильне

$$A_{400} = (1,0,0,1,4)$$

число в КЗ.

*Приклад 1*. Визначити правильність чисел $\tilde{A} = (1,0,0,1,4)$, спотвореного по підставі

$$\mathrm{m}_1 = 3\ (\tilde{a}_1 = 0).$$

Переводимо число Ã в ПСЧ та порівнюємо його з M = 420.

$$\tilde{A} = (\sum_{i=1}^{n+1} a_i \cdot B_i) \bmod M_1 = (\sum_{i=1}^{5} a_i \cdot B_i) \bmod 4620 =$$

$$= (1540 \cdot 0 + 3465 \cdot 0 + 3696 \cdot 0 + 2640 \cdot 1 + 2520 \cdot 4) \bmod(4620) = 3480 > 420.$$

$$\bmod 4620 = 12720$$

Таким чином операнд Ã містить помилку в одному з п'яти залишків.

*Приклад 2.* Нехай число $A_{400} = (1,0,0,1,4)$ неспотворене.

В цьому випадку отримаємо

$$A = (1540 \cdot 1 + 3465 \cdot 0 + 3696 \cdot 0 + 2640 \cdot 1 + 2520 \cdot 4)$$

$$\bmod 4620 = 14260(\bmod 4620) = 400 < 420.$$

Т.ч. число А є правильне.

## 5 Висновки

1. Аналіз властивостей непозиційних кодових структур показав, що коди в КЗ є арифметичними кодами (*деякий аналог цих кодів в ПСС - арифметичні АN-коди*), придатні до використання, як для передачі, так і для обробки інформації. Для кодів КЗ контрольні основи включені в загальну кодову структуру даних, що містять сукупність інформаційних підстав. В цьому випадку залишки, якими представляються операції в КЗ з інформаційних і контрольних підстав, одночасно і незалежно беруть участь в процесі обробки інформації. Результат обробки інформації, представлений кодом КЗ, може контролюватися або поетапно, або по закінченню всіх обчислень, так як помилка, що виникла в будь-якому залишку $a_i$ числа

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

не поширюється (не "розмножується") в інші залишки

$$a_j \ (j = \overline{1, n+1} \ \text{та} \ \ i \neq j)$$

числа А (*у сусідні тракти обробки інформації СОД*). Важливе значення має факт визначення кількості і величин (за кількістю реалізованих операцій) кожного з цих етапів. Наприклад, величина кожного етапу обробки інформації (етапу обчислень) може бути визначена або по обумовленому замкненим циклом обробки алгоритму, або відповідно до можливого значення ймовірності виникнення одноразової (в одному залишку числа в КЗ) помилки.

2. Для довільної впорядкованої

$$(m_i < m_{i+1})$$

системи підстав КЗ, з одним контрольним *mk* підставою спотворення одного довільного залишку aj по модулю $m_j$ однозначно перетворює правильне (*неспотворене*) число А в неправильне Ã. В цьому випадку система контролю в КЗ достовірно визначає факт спотворення числа А.

Коригувальні здібності перешкодостійкого коду в КЗ залежить від кількості та величини контрольних $\{m_k\}$ основ. Якщо для деякої кількості r інформаційних підстав даного КЗ виконується умова

$$\prod_{i=1}^{r} m_{z_i} \leq m_k \ (m_{z_i} \in M),$$

то спотворення в одночасно декількох або навіть у всіх цих r залишках не робить правильне число А в неправильне. При цьому вважається, що СОД функціонує безвідмовно. Однак при цьому система контролю СОД не визначає номера відмовили трактів обробки даних.

3. Запропонований метод контролю, заснований на принципі порівняння, в подальшому створює відповідні передумови для розробки ефективних методів діагностики і корекції помилок в КЗ. Недоліком запропонованого методу є дещо низька оперативність контролю. Цей недолік обумовлений значними тимчасовими витратами на операції переказу числа А з КЗ в ПСЧ та порівняння чисел А і М в ПСЧ. Крім цього, якщо контролю піддається проміжний

результат обчислень, то можливо додатково буде потрібно додаткова операція перекладу числа А з ПСЧ в КЗ. Дана обставина обумовлює необхідність підвищення оперативності контролю СОД в КЗ за рахунок зменшення часу виконання перерахованих вище операцій шляхом розробки і використання, наприклад, методів і засобів реалізації позиційних ознак непозиційних коду КЗ.

4. Перспективним напрямком подальших досліджень є розробка практичних рекомендацій щодо адаптації запропонованого методу до специфіки завдань криптографії [22-30], цифрової обробки сигналів [20, 21, 31-33], та вирішення комплексу інших [34-42] обчислювальних задач.

## Посилання


[1] Akushsky I. Ya.,Yuditsky DI. Machine arithmetic in residual classes. Moscow: Soviet radio, 1968. 440 p. (In Russian)

[2] Torgashov V. A. The system of residual classes and reliability of digital computersю Moscow: Soviet radio, 1973. 118 p. (In Russian)

[3] Improved Method of Determining the Alternative Set of Numbers in Residue Number System/ Krasnobayev V., Kuznetsov A., Koshman S., Moroz S. *Recent Developments in Data Science and Intelligent Analysis of Information*. *ICDSIAI 2018*. Advances in Intelligent Systems and Computing. Springer, Cham, 2018. Vol. 836. P. 319–328.

[4] Barsi F., Maestrini P. Error Correcting Properties of Redundant Residue Number Systems. *IEEE Transactions on Computers*. 1973. Vol. C-22, № 3, P. 307–315.

[5] Krasnobayev V.A., Yanko A.S., Koshman S.A.A Method for arithmetic comparison of data represented in a residue number system. *Cybernetics and Systems Analysis*. 2016.Vol. 52, Issue 1.P. 145–150.

[6] Harman G., Shparlinski I. E. Products of Small Integers in Residue Classes and Additive Properties of Fermat Quotients. *International Mathematics Research Notices*. 2016. № 5. P. 1424–1446.

[7] Methods for comparing numbers in non-positional notation of residual classes/ V. Krasnobayev, A. Kuznetsov, M. Zub, K. Kuznetsova. *Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019)*. Zaporizhzhia, 2019. P. 581–595.

[8] Popov D. I., Gapochkin A. V. Development of Algorithm for Control and Correction of Errors of Digital Signals, Represented in System of Residual Classes. *2018 International Russian Automation Conference (RusAutoCon)*. Sochi, 2018. P. 1–3.

[9] Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes / M. Karpinski, S. Ivasiev, I. Yakymenko, M. Kasianchuk and T. Gancarczyk. *16th International Conference on Control, Automation and Systems (ICCAS)*. Gyeongju, 2016. P.1484–1486.

[10] 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.

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

[12] Method of data control in the residue classes/ V. Krasnobayev, A. Kuznetsov, A. Kononchenko, T. Kuznetsova. *Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019)*. Zaporizhzhia, 2019. P.241–252.

[13] Method of Error Control of the Information Presented in the Modular Number System/ V. Krasnobayev, S. Koshman, A. Yanko and A. Martynenko. *International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. Kharkiv, 2018. P. 39–42.

[14] Krasnobayev V. A. Method for realization of transformations in public-key cryptography. *Telecommunications and Radio Engineering*. 2007.Vol. 66, Issue 17. P. 1559–1572.

[15] Gorbenko I.D., Zamula A.A. Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems. *Telecommunications and Radio Engineering*. 2017. Vol. 76, Issue 12. P. 1079–1100.

[16] Kuznetsov A., Serhiienko R., Prokopovych-Tkachenko D. Construction of cascade codes in the frequency domain. *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. Kharkov, 2017. P.131–136.

[17] Stasev Yu.V., Kuznetsov A.A., Nosik A.M. Formation of pseudorandom sequences with improved autocorrelation properties. *Cybernetics and Systems Analysis*. 2007. Vol. 43, Issue 1. P. 1–11.

[18] Soft decoding based on ordered subsets of verification equations of turbo-productive codes/ A. Kuznetsov, A. Kiian, K. Kuznetsova, et al. *Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019)*. Zaporizhzhia, 2019. P. 873–884.

[19] Analysis and Studying of the Properties of Algebraic Geometric Codes/ A. A. Kuznetsov, I. P. Kolovanova, D. I. Prokopovych-Tkachenko, T. Y. Kuznetsova. *Telecommunications and Radio Engineering*. 2019. Vol. 78, Issue 5. P. 393–417.

[20] Puschel M., Moura J. M. F. Algebraic Signal Processing Theory: Foundation and 1-D Time. *IEEE Transactions on Signal Processing*. 2008. Vol. 56, №8. P. 3572–3585.

[21] Discrete Signals with Multi-Level Correlation Function/ O.Karpenko, A.Kuznetsov, V.Sai, Yu.Stasev. *Telecommunications and Radio Engineering*. 2012. Vol.71, Issue 1. P. 91–98.

[22] Stasev Yu.V., Kuznetsov A.A. Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes. *Kibernetika i Sistemnyi Analiz*. 2005. № 3. P. 47–57.

[23] Agarwala A., Saravanan R. A Public Key Cryptosystem based on number theory. *International Conference on Recent Advances in Computing and Software Systems*. Chennai, 2012. P. 238–241.

[24] Code-based public-key cryptosystems for the post-quantum period/ A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov. *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. Kharkov, 2017. P. 125–130.

[25] Wang B., Liu L. A flexible and energy-efficient reconfigurable architecture for symmetric cipher processing. *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*. Lisbon, 2015. P.1182–1185.

[26] Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2/ A. Kuznetsov, Y. Gorbenko, A. Andrushkevych and I. Belozersev. *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. Kharkov, 2017. P. 203–206.

[27] The research of modern stream ciphers/ I. Gorbenko, A. Kuznetsov, M. Lutsenko and D. Ivanenko. *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. Kharkov, 2017. P. 207–210.

[28] Lightweight robust cryptographic combiner for mobile devices: Crypto roulette/ M. E. Pamukov, V. Poulkov, A. Mihovska, N. R. Prasad and R. Prasad. *IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. Athens, 2014. P. 188–192.

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

[30] Thangavel M., Varalakshmi P. A novel public key cryptosystem based on Merkle-Hellman Knapsack Cryptosystem. *Eighth International Conference on Advanced Computing (ICoAC)*. Chennai, 2017. P. 117–122.

[31] Gorbenko I., Nariezhnii O., Kudryashov I. Construction method and features of one class of cryptographic discrete signals. *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. Kharkov, 2017. P.156–160.

[32] Ahmed N., Natarajan T., Rao K. R. Discrete cosine transform. *IEEE Trans. Comput.* 1974. Vol. C-23, № 1, P. 90–93.

[33] Naumenko N.I., Stasev Yu.V., Kuznetsov A.A. Methods of synthesis of signals with prescribed properties. *Cybernetics and Systems Analysis*. 2007. Vol. 43, Issue 3. P. 321–326.

[34] Accelerated Flexible Processor Architecture for Crypto Information/ Z. Dai, X. Yu, J. Su and X. Chen. *2nd International Conference on Pervasive Computing and Applications*. Birmingham, 2007. P. 399–403.

[35] Strumok keystream generator/ I. Gorbenko, O. Kuznetsov, Y. Gorbenko, A. Alekseychuk and V. Tymchenko. *IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. Kyiv, 2018. P. 294–299.

[36] Runovski, K., Schmeisser, H. On the convergence of fourier means and interpolation means. *Journal of Computational Analysis and Applications*. 2004. № 6(3). P. 211–227.

[37] Gnatyuk, V. A. Mechanism of laser damage of transparent semiconductors. *Physica B: Condensed Matter*. 2001. P. 308-310; P. 935–938.

[38] Tkach, B. P., Urmancheva, L. B. Numerical-analytic method for finding solutions of systems with distributed parameters and integral condition. *Nonlinear Oscillations*. 2009. №12(1). P.113–122.

[39] Controlled markov fields with finite state space on graphs/ Chornei, R., Hans Daduna, V. M., Knopov, P. *Stochastic Models.* 2005. Issue 21(4). P. 847–874.

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

[41] Fan C. , Ge G. A Unified Approach to Whiteman's and Ding-Helleseth's Generalized Cyclotomy Over Residue Class Rings. *IEEE Transactions on Information Theory*. 2014.Vol. 60, № 2. P.1326–1336.

[42] Rabin's modified method of encryption using various forms of system of residual classes/ M. Kasianchuk, I. Yakymenko, I. Pazdriy, A. Melnyk and S. Ivasiev. *14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*. Lviv, 2017. P. 222–224.

**Reviewer**: Oleksandr Oksiiuk, Doctor of Sciences (Engineering), Full Professor, Taras Shevchenko National University of Kiev 81 Lomonosova St., Kyiv, 03189, Ukraine. E-mail: o.oksiuk@gmail.com

Received on October 2019.

**Authors:**

Andrey Dyachenko, student, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: andrey.090220@gmail.com

Irina Lokotkova, student, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: lokotosyk@ukr.net

Olesya Reshetnyak, student, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: lesyandr13@gmail.com

Mikhail Zub, student, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: mishazub007@gmail.com

Konstantin Myslyvtsev, student, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: kostyavtx@gmail.com

**Data control method, which presented by code of non-positioning system of deduction class calculation.**

**Abstract.** The paper proposes a new method of monitoring data presented in non-positional residue class system. For code in residue class system, test bases are included in the general code structure of data containing a set of information bases. In this case, the balances that represent operations for informational and control grounds simultaneously and independently participate in the process of

information processing. The result of the information processing can be monitored either step by step or at the end of all calculations, since the error that occurred in any residue, does not apply (does not “multiply”) to the remaining residues. The control method proposed based on the principle of comparison, further creates prerequisites for developing effective methods for diagnosing and correcting errors in deduction class. The disadvantage of the proposed method is the relatively low control efficiency. This circumstance makes it necessary to increase the efficiency of data processing system control in deduction class by reducing the execution time of the above operations by developing and using, for example, methods and means for implementing the positional features of the non-positional deduction class code.

**Keywords:** Data Control Method; Residues Class; Non-Positioning System.

**Рецензент**: Александр Оксиюк, д.т.н., проф., Киевский национальный университет имени Т. Шевченко, ул. Ломоносова 81, Киев, 03189 Украина. E-mail: o.oksiuk@gmail.com

Поступила: Октябрь 2019.

**Авторы:**

Андрей Дьяченко, студент, Харьковский национальный университет им. В.Н. Каразина.
E-mail: andrey.090220@gmail.com

Ирина Локоткова, студент, Харьковский национальный университет им. В.Н. Каразина.
E-mail: lokotosyk@ukr.net

Олеся Решетняк, студент, Харьковский национальный университет им. В.Н. Каразина.
E-mail: lesyandr13@gmail.com

Михаил Зуб, студент, Харьковский национальный университет им. В.Н. Каразина.
E-mail: mishazub007@gmail.com

Константин Мисливцев, студент, Харьковский национальный университет им. В.Н. Каразина.
E-mail: kostyavtx@gmail.com

**Метод контроля данных, представленных кодом непозиционной системы счисления класса вычетов.**

**Аннотация**. В статье предлагается новый метод мониторинга данных, представленных в непозиционной системе классов вычетов. Для кода в системе классов вычетов тестовые базы включаются в общую структуру кода данных, содержащий набор баз информации. В этом случае балансы, которые представляют операции информационных и контрольных оснований одновременно и независимо участвуют в процессе обработки информации. По результатам обработки информации можно отслеживать или поэтапно, или в конце всех вычислений, поскольку ошибка, которая произошла в любом из вычетов, не применяется (не «умножается») на остатки, которые остались. Предложенный метод контроля, основанный на принципе сравнения, в дальнейшем создает предпосылки для разработки эффективных методов диагностики и коррекции ошибок в классе вычетов. Недостатком предложенного метода является относительно низкая оперативность контроля. Данное обстоятельство обусловливает необходимость повышения оперативности контроля системы обработки данных в классе вычетов за счет уменьшения времени выполнения вышеперечисленных операций путем разработки и использования, например, методов и средств реализации позиционных признаков непозиционных кодов в классе вычетов.

**Ключевые слова:** метод контроля данных; класс вычетов; непозиционная система.