УДК 681.5.09 **doi: 10.26906/SUNZ.2024.4.169**

А. С. Янко, А. Д. Глушко, О. І. Крук, А. Ю. Прокудін

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОЦЕСУ КОРЕКЦІЇ ДАНИХ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Анотація. У статті розглядаються вплив коригувальних здібностей непозиційних кодових структур (НКС), які представлені взаємно не простими основами системи залишкових класів (СЗК). На даний час такі НКС досліджені достатньо поверхнево та описуються скоріше якісно, ніж кількісно. До теперішнього часу практично не проводилось ґрунтовних досліджень коригувальних властивостей НКС СЗК, що мають основи, які не являються взаємно простими числами. Аналогічна система також має значні коригувальні можливості, що обумовлює необхідність оцінки можливості та доцільності застосування НКС, представлених у вигляді взаємно не простих основ для підвищення достовірності обчислень комп'ютерних систем (КС). З метою подальшого дослідження та розвитку даних НКС розглянемо ряд наукових тверджень, використання результатів яких дозволить більш повно дослідити коригувальні властивості НКС з взаємно не простими основами. Розроблено алгоритми процесів корекції та контролю даних у СЗК з взаємно попарно не простими основами. Використання цих алгоритмів спрощує процес виявлення і виправлення одиничних помилок. Зазначимо, що за простотою конструкції схем декодувальних пристроїв розглянутих НКС, не мають аналогів у позиційних системах числення. Це досягається за рахунок обмеження класу можливих коригованих помилок шляхом введення додаткової апаратурної надлишковості представлення НКС в СЗК.

Ключові слова: взаємно не прості основи; виправлення помилок; комп'ютерна систем; корекція даних; коригувальні властивості; система залишкових класів.

Вступ

Відомо, що в непозиційній системі числення в залишкових класах широке розповсюдження отримали коригувальні коди, тобто непозиційні кодові структури (НКС), що представлені набором взаємно простих основ даної системи залишкових класів (СЗК) [1]. Це обумовлено простотою формування структури цих НКС, високою ефективністю їх коригувальних властивостей, а також відносною легкістю побудови для мінімальної кодової відстані, яка буде задана [2]. У рамках даного дослідження розглянуті коригувальні НКС з взаємно не простими основами. Відсутність ґрунтовних досліджень використання коригувальних можливостей даних НКС значно обмежує ефективність та сферу використання СЗК. Дана обставина обумовлює необхідність оцінки можливості та доцільності застосування НКС, основи яких є взаємно не простими числами для підвищення достовірності обчислень комп'ютерних систем (КС).

З метою подальшого дослідження розглянемо низку наукових тверджень (НТ), використання результатів яких дозволить більш повно дослідити коригувальні властивості НКС з взаємно не простими основами СЗК. На основі доведення яких розробляється набір ефективних алгоритмів корекції даних, представлених у СЗК.

Алгоритми виявлення та виправлення помилок у СЗК

Лема 1. Для будь-якого НКС $E=(e_1\,\|\,e_2\,\|\,...\,\|\,e_m)$ в СЗК з основами k_g $(g=\overline{1,m})$ і для будь-якої пари основ k_g и k_i повинна виконуватись умова $(e_g-e_i)\equiv 0(\bmod x_{gi})$, де $x_{gi}(k_g,k_i)$ найбільший спільний дільник основ (модулів) k_g та k_i, а $g,i=\overline{1,m}$; $g\neq i$ [3]. Отже, за результатами леми 1, для визначення необхідних і достатніх умов для виявлення одиничних помилок за допомогою НКС з взаємно не простими основами СЗК сформулюємо і доведемо наступне НТ.

НТ 1. Для виявлення помилок у залишку за довільною основою k_g $(g=\overline{1,m})$ НКС $E=(e_1\,\|\,e_2\,\|\,...\,\|\,e_m)$, заданої основами $k_1,...,k_m$, необхідно, щоб основа k_g мала принаймні один, відмінний від одиниці, спільний дільник з іншими основами k_g $(g\neq i)$ [4].

Доведення. Нехай найбільший спільний дільник $x_{gi}(k_g,k_i)$ визначений для довільних основ СЗК $(g\neq i)$, і помилка сталася за основою k_g, тобто $e_g=e_g+\triangle e_g$.

Покажемо, що вираз $(e_g-e_i)\bmod x_{gi}$ еквівалентний $\triangle e_g(\bmod x_{gi})$. Згідно з лемою 1, виконується таке рівність $(e_g-e_i)=0(\bmod x_{gi})$. Запишемо вираз $e_g+\triangle e_g=e_g(\bmod k_g)$ у вигляді $e_g+\triangle e_g=k\cdot k_g+e_i$, де k – ціле число. Для визначення спотвореного залишку використаємо останній вираз $e_i=e_i+\triangle e_i-k\cdot k_i$. Тоді можемо записати, що $e_g-e_i=\left[(e_g-e_i)+(-khx_{gi})+\triangle e_g\right]$.

Так, як $(e_g-e_i)\equiv 0(\bmod x_{gi})$ та $-khx_{gi}\equiv 0(\bmod x_{gi})$, де $k_g=hx_{gi}$, а h – натуральне число, яке виконує таке порівняння $(e_g-e_i)\equiv\triangle e_g(\bmod x_{gi})$. Безумовно, що при відсутності спільних дільників, якщо $x_{gi}=1$, маємо, що $\Delta e_g\equiv(\bmod x_{gi})$, що доводить необхідну умову НТ 1, якщо помилка не кратна дільнику x_{gi}. Дійсно, $(kx_{gi}+e_{gi})\neq 0(\bmod x_{gi})$, для $0<e_{gi}<x_{gi}$.

НТ 1 можна сформулювати таким чином. Для виявлення одиничної помилки (у залишку за довільною основою k_g) НКС $E=(e_1\|e_2\|...\|e_m)$ необхідно і достатньо, щоб помилка була не кратна дільникам x_{gi} та x_g, де x_g – найменше спільне кратне дільників $x_g=(x_{g1}, x_{g2}, ..., x_{gm})$.

На основі результатів НТ 1 сформуємо алгоритм (порядок) визначення одиничної помилки.

1. Здійснюємо перевірку залишку за основою k_g. З цією метою визначаємо сукупність значень: $e_1-e_2=e_{12}(\mathrm{mod}\,x_{12})$, $e_1-e_3=e_{13}(\mathrm{mod}\,x_{13})$, …, $e_1-e_m=e_{1m}(\mathrm{mod}\,x_{1m})$. Якщо $e_{1g}=(\mathrm{mod}\,x_{1g})$, тоді здійснюється перевірка другого залишку і т. д.

2. З метою визначення значень e_{gi} $(g\neq i)$ необхідно утворити матрицю такого виду:

$$A=\begin{vmatrix} e_{12} & e_{13} \dots & e_{1m} \\ e_{21} & e_{23} \dots & e_{23} \\ & \dots & \\ e_{m1} & e_{m2} \dots & e_{mm-1} \end{vmatrix}$$

Під час складання матриці A не обов'язково вказувати справжнє числове значення e_{gi}, достатньо представити й використовувати його відмінну ознаку:

$$e_{gi}=\begin{cases} 0, \textit{ якщо } e_g-e_i=0(\mathrm{mod}\,x_{gi}), \\ 1, \textit{ яякщо } e_g-e_i\neq 0(\mathrm{mod}\,x_{gi}). \end{cases}$$

3. Якщо визначник матриці $|A|=0$, то НКС $E=(e_1\|e_2\|...\|e_m)$ – правильна, а якщо $|A|\neq 0$, то E – неправильна.

Розглянемо деякі теоретичні основи, що дають можливість спростити наведений вище алгоритм.

Враховуючи, що

$$e_g-e_i\equiv[x_{gi}-(e_g-e_i)](\mathrm{mod}\,x_{gi}),$$

визначник $|A|$ можна не знаходити. У цьому випадку достатнім є визначення діагональних елементів матриці A та додавання одного додаткового значення. e_{m1}, а саме $e_{12}, e_{23}, e_{34}, ..., e_{m-1\,m}, e_{m1}$.

Достатньо легко підтвердити, що за таких значень e_{gi}, можна виявити не тільки сам факт викривлення НКС, але й визначити локалізацію (номер) спотвореного залишку.

Для встановлення необхідних умов для проведення процедури виправлення одиничних помилок за допомогою НКС з взаємно не простими основами СЗК сформулюємо і доведемо наступне НТ.

НТ 2. Для виправлення помилки в залишку з довільною основою числа $E=(e_1, e_2, ..., e_m)$, заданої в СЗК з основами $k_1, k_2, ..., k_m$, необхідно, щоб виконувалась умова:

$$(x_{gh}-1)(x_{gi}-1)\geq k_g-1-(L_{x_{g\,h}}+L_{x_{gi}}-L_{[x_{g\,h},x_{gi}]}), \quad (1)$$

де $x_{gh}=(k_g, k_h)$, $x_{gi}=(k_g, k_i)$; $L_{x_{g\,h}}$ – кількість дільників, кратних x_{gh}; $L_{x_{gi}}$ – кількість дільників, кратних x_{gi}; $L_{[x_{gh},x_{gi}]}$ – кількість дільників, кратних найменшому спільному кратному $[x_{gh}, x_{gi}]$ дільників x_{gh} та x_{gi}, $g\neq i$.

Доведення. Обчислимо значення e_{gi}, e_{gh}, e_{ih}. Якщо помилка сталася за основою k_g, то $e_{gh}=0$, а $e_{gi}\neq 0$ та $e_{gh}\neq 0$. Кількість різних комбінацій e_{gi}, e_{gh} рівно $(x_{gi}-1)\cdot(x_{gh}-1)$, де $(x_{gi}-1)$ – число можливих значень величини e_{gi} ($e_{gi}\neq 0$), $(x_{gh}-1)$ – число можливих значень e_{gh} ($e_{gh}=0$), а число можливих помилок за основою k_g рівно k_g-1 $(\triangle e_g\neq 0)$ з урахуванням кількості невиявлених помилок. Кількість невиявлених помилок складається з кількості помилок, кратних дільнику $x_{gh}-L_{x_{gh}}$.

Таким чином, кількість можливих значень виявлених помилок дорівнює значенню $k_g-1-(L_{x_{gh}}+L_{x_{gi}}-L_{[x_{gh},x_{gi}]})$.

З метою забезпечення відповідності потенційним значенням помилок за основою k_g необхідно виконання нерівності (1), що було потрібно довести.

Необхідна умова НТ 2 є достатньою, якщо різним значенням помилок $\triangle e_g$ відповідають різні значення добутку $e_{gh}\cdot e_{gi}$, і навпаки. В цьому контексті існує однозначна відповідність між можливими значеннями та значеннями добутку $e_{gh}\cdot e_{gi}$, що дозволяє точно визначити величину помилки. Враховуючи НТ 2, складемо алгоритм корекції помилок за довільною основою k_g:

1. Встановимо номер спотвореного залишку. З цією метою розрахуємо значення:

$$e_1-e_2=e_{12}(\mathrm{mod}\,x_{12}),$$
$$e_2-e_3=e_{23}(\mathrm{mod}\,x_{23}),$$
$$\dots,$$
$$e_{m-1}-e_m=e_{m-1m}(\mathrm{mod}\,X_{m-1m}),$$
$$e_m-e_1=e_{m2}(\mathrm{mod}\,x_{m1}).$$

Якщо всі залишки $e_{gi}=0(\mathrm{mod}\,x_{gi})$, то НКС E правильна. Якщо помилка сталася за основою k_g, то $x_{gi}\neq 0$ та $e_{gh}\neq 0$ таким чином, перевірочна НКС $E=(e_1\|e_2\|...\|\tilde{e}_g\|...\|e_m)$ є неправильною.

2. За значенням e_{gi} та e_{gh} звертаємось до блоку констант помилок, де обираємо відповідне значення $\triangle e_g$.

3. Виконуємо корекцію числа E у залишку e_g, і отримуємо правильне число $E=E-\triangle E$, тобто $E=(e_1\|e_2\|...\|e_g\|...\|e_m)$.

Якщо в СЗК через виключення основи, що призвела до помилки, є можливість однозначно представити НКС E, то замість визначення величини помилки $\triangle e_g$ за значеннями e_{gi} та e_{gh}, можемо безпосередньо обчислити значення коректного залишку e_g. Далі розглянемо алгоритм (порядок) корекції помилок.

1. Розрахуємо значення залишків $e_{12}, e_{23}, ..., e_{m1}$.

2. З'ясуємо номер спотвореного залишку. Вважаємо, що помилка сталася за основою k_g. Відповідно цю основу необхідно виключити, а НКС E слід представити за основами $k_1, k_2, ..., k_m$, тобто:

$$E = (e_1 \| e_2 \| ... \| e_{g-1} \| e_{g+1} \| ... \| e_m).$$

3. Виконаємо згортання НКС E в позиційний код.

4. Визначимо справжнє значення спотвореного залишку за відомою формулою:

$$e_g = E - \left[E / k_g \right] k_g,$$

де $[y]$ – ціла частина y, що не перевищує y. Виправлена НКС:

$$E_{вип} = (e_1 \| e_2 \| ... \| e_g \| ... \| e_m).$$

Визначимо умови, які дозволяють виключити деякі основи з СЗК. З цією метою основи вихідної СЗК представимо у канонічній формі

$$k_1 = \varphi_{11}^{e_{11}} \varphi_{12}^{e_{12}} \ldots \varphi_{1j_1}^{e_{1j_1}},$$

$$k_2 = \varphi_{21}^{e_{21}} \varphi_{22}^{e_{22}} \ldots \varphi_{2j_2}^{e_{2j_2}},$$

$$\cdots$$

$$k_m = \varphi_{m1}^{e_{m1}} \varphi_{m2}^{e_{m2}} \ldots \varphi_{mj_m}^{e_{mj_m}},$$

$$K = \varphi_1^{e_1} \varphi_2^{e_2} \ldots \varphi_h^{e_h}.$$

Для однозначного визначення НКС E в СЗК з основами $k_1, k_2, ..., k_m$, що знаходиться у діапазоні $[0, K)$, слід виключити лише основи, для яких $\varphi_k = \varphi_{gj_g}$, ($k = \overline{1, h}$, $g = \overline{1, m}$). При цьому необхідно, щоб $e_k \geq e_{gj_g}$.

Таким чином, встановлено необхідні та достатні умови для корекції помилок шляхом виключення спотвореної основи.

Ці умови передбачають одночасне виконання специфічної рівності та нерівності:

$$\varphi_k = \varphi_{g\, j_g}, \quad e_k \geq e_{g\, j_g}. \qquad (2)$$

Розглянемо СЗК представлену основами $k_1 = 4$, $k_2 = 6$, $k_3 = 12$, $k_4 = 18$. При цьому $K = [4, 6, 12, 18] = 36$. Відповідно до умови (2), що визначає можливість корекції помилок, визначимо основи СЗК, які підлягають виключенню. Основи СЗК представимо у канонічній формі: $k_1 = 2^2$, $k_2 = 2 \cdot 3$, $k_3 = 2^2 \cdot 3$, $k_4 = 2 \cdot 3^2$ та $K = 2^2 \cdot 3^2$.

Очевидно, що шукані основи будуть такі $k_1, k_2 \bar{a}\, k_3$. Виконаємо перевірку, для чого складемо часткові значення найменших спільних кратних:

$$K_1 = [6, 12, 18] = 36,$$

$$K_2 = [4, 12, 18] = 36,$$

$$K_3 = [4, 6, 18] = 36;$$

$$K_4 = [4, 6, 12] = 12.$$

Часткове значення найменшого спільного кратного $K_4 < 36$, що підтверджує правильність визначення виключених основ СЗК.

Вище було представлено алгоритм виявлення та виправлення помилок у СЗК за допомогою НКС з взаємно не простими основами. Вважаємо, що при обчисленні значень $(e_h - e_{h+1}) \bmod x_{hh+1}$ встановлено, що $e_{g-1\,g} \neq 0$, $e_{g\,g+1} \neq 0$, а всі інші значення дорівнюють $e_{h\,h+1} = (e_h - e_{h+1}) \bmod x_{hh+1} = 0$. Тоді стверджується, що НКС E неправильна, а помилка присутня у залишку за основою k_g, тобто $E = (e_1 \| e_2 \| ... \| \tilde{e}_g \| ... \| e_m)$.

Звертаючись до значень $e_{g-1\,g}$ і $e_{g\,g+1}$ у блоці констант помилок, обчислимо значення помилки $\triangle e_g$, після чого визначимо правильне значення залишку $e_{g\,вип} = \tilde{e}_g - \triangle e_g$. Виправлене число буде презентоване у вигляді $E_{вип} = (e_1 \| e_2 \| ... \| e_{g\,вип} \| ... \| e_m)$. Для успішного виправлення помилки з використанням розробленого методу корекції слід, щоб помилка $\triangle e_g$ не була кратною одночасно двом дільникам $x_{g-1\,g}$ та $x_{g\,g+1}$, що обмежує клас коригованих помилок.

Метод корекції одиничних помилок, який дозволяє виправляти помилки, які є кратними одному з дільників $x_{g-1\,g}$ чи $x_{g\,g+1}$, складається з наступного. Якщо СЗК задана з взаємно не простими основами, тобто найбільший спільний дільник визначається наступним чином $(k_1, k_2, ..., k_m) \geq 2$. Визначимо всі значення $e_{h\,h+1}$, тобто $e_{12}, e_{23}, e_{34}, ..., e_{m-1\,m}, e_{m\,1}$. Не порушуючи загальності міркувань, будемо вважати, що $e_{g\,g+1} \neq 0$, а всі інші значення $e_{h\,h+1} \neq 0$. Так як $e_{g\,g+1} = (e_g - e_{g+1}) \bmod x_{g\,g+1} \neq 0$, помилка може бути виявлена лише в залишках за основами k_g або k_{g+1}.

У цьому контексті можна сформулювати дві гіпотези: перша – помилка присутня у залишку e_g, друга – помилка присутня у залишку e_{g+1}. До того як перейти до розгляду процесу корекції помилок за допомогою запропонованим методом, сформулюємо та доведемо наступну теорему НТ 3. Результати цього доведення будуть застосовані для визначення процесу збіжності сукупності НКС вигляду $E^{(h_g)} = (e_1 \| ... \| e_{g-1} \| e_{g h_g} \| e_{g+1} \| ... \| e_m)$ до правильної

НКС $E^{(\omega)} = (e_1 \| ... \| e_{g-1} \| e_{g\omega} \| e_{g+1} \| ... \| e_m)$. Попередньо розглянемо наступну лему.

Лема 2. Різниця, сума та добуток будь-яких НКС з взаємно не простими основами є кодовим словом [5].

НУ 3. Нехай у впорядкованій ($k_{g-1} < k_g$; $g = \overline{1, m}$) СЗК з основами $k_1, k_2, ..., k_m$ задано неправильне (спотворене в одному залишку) число $E = (e_1 \| e_2 \| ... e_{g-1} \| \tilde{e}_g \| e_{g+1} \| ... \| e_m)$ і нехай $\Delta k_g = \tilde{k}_g - k_g = h_h x_{g-1\,g}$. Тоді в сукупності значень $e_{gh_g} = (e_g - h_g x_{g-1\,g}) \bmod k_g$ існує таке єдине значення $e_{g\omega}$, при якому НКС $E^{(\omega)} = (e_1 \| e_2 \| e_{g\omega} \| ... \| e_m)$ є правильною, де $x_{g-1\,g}(k_{g-1}, k_g)$, а h_g може приймати значення $h_g = 1, 2, ..., k_g / x_{g-1\,g} - 1$.

Доведення. Покажемо, що існує таке значення $e_{g\omega_1}$, при якому НКС $E^{(\omega_1)} = (e_1 \| e_2 \| e_{g\omega} \| ... \| e_m)$ є не спотвореною (правильною). За умовою теореми помилка Δe_g кратна дільнику $x_{g-1\,g}$, вираз $h_g x_{g-1\,g}$ містить всі можливі числа, кратні $x_{g-1\,g}$.

Таким чином, знайдеться принаймні одне значення $h_g = \omega_1$, при якому $\Delta e_{g\omega_1} = \omega_1 x_{g-1\,g}$ та $e_{1\omega_1} = \tilde{e}_g - \Delta e_{g\omega_1}$. Покажемо, що $E^{(\omega_1)}$ єдине правильна НКС з сукупності НКС виду $E^{(h_g)}$. Вважатимемо, що існує значення $e_{1\omega_2} = \tilde{e}_g - \omega_2 x_{g-1\,g}$, для якого НКС $E^{(\omega_2)}$ також є правильною. У такому випадку, відповідно до леми 2 НКС $E^{(\omega_1)} - E^{(\omega_2)} = (0 \| ... \| e_{g\,\omega_1} - e_{g\,\omega_2} \| ... \| 0)$ є неспотвореною (правильною). Якщо число $E^{(\omega_1)} - E^{(\omega_2)}$ є правильним, то у відповідності до леми 1 отримаємо:

$$(\omega_2 - \omega_1) x_{g-1\,g} \equiv 0 (\bmod x_{1-i}),$$

$$(\omega_2 - \omega_1) x_{g-1\,g} \equiv 0 (\bmod x_{2-g}),$$

$$\dots$$

$$(\omega_2 - \omega_1) x_{g-1\,g} \equiv 0 (\bmod x_{m-g}).$$

Якщо $g \neq m$, то єдине правильна НКС $E^{(\omega_1)} - E^{(\omega_2)}$ буде нульове кодове слово. Такий результат зумовлений тим, що $x_{g-1\,g} \neq 0$ та $x_{g-1\,g}$ не дорівнює найменшому спільному кратному дільників $x_{1g}, x_{2g}, ..., x_{mg}$.

При цьому нерівність $x_{g-1\,g} \neq [x_{1g}, x_{2g}, ..., x_{mg}]$ спростовує умову довільного вибору основ $k_1, k_2, ..., k_m$. Отже, виконується наступне рівняння $E^{(\omega_1)} - E^{(\omega_2)} = (0 \| 0 \| ... \| 0 \| ... \| 0)$. Відповідно, $\omega_1 = \omega_2$, що є об'єктивним твердженням єдиності існування ω_1, за якого

$$E^{(\omega_1)} = (e_1 \| e_2 \| ... \| e_{g\omega_1} \| ... \| e_m)$$

є правильним значенням, що було потрібно довести.

Сформулюємо алгоритм корекції помилок, який базується на висновках, отриманих у теоремі НТ 3. Почнемо з аналізу першої гіпотези. Так як $e_{g-1\,g} = 0$, помилка є кратною дільнику $x_{g-1\,g}$. Отже, помилка за основою може набувати значень $\Delta e_g = h x_{g-1\,g}$, для $h_g = 1, 2, ..., k_g / x_{g-1\,g} - 1$. Обчислимо сукупність значень $e_{gh_1} = (e_g - h_g x_{g-1\,g}) \bmod k_g$. Якщо в цій сукупності знайдеться таке значення e_{gk}, при якому НКС $E^{(k)} = (e_1 \| e_2 \| ... \| e_{g\,k} \| ... \| e_m)$ є неспотвореною, то перша гіпотеза є вірною, тобто помилка присутня у залишку за основою k_g. У цьому випадку виправлена НКС $E_{вип} = E^{(k)}$, де $e_{gk} = (e_g - k x_{g-1\,g}) \bmod k_g$. Якщо при всіх значеннях e_{gh_g} НКС $E^{(h_g)}$ неправильна, то значення e_g є істинним, помилка відбулася в залишку за основою k_{g+1}. Так як $e_{g+1\,g+2} = 0$, то помилка за основою k_{g+1} кратна дільнику $x_{g+1\,g+2}$ тобто $\Delta e_{g+1} = h_{g+1} x_{g+1\,g+2}$, де $h_{g+1} = 1, 2, ..., k_{g+1} / x_{g+1\,g+2} - 1$. Далі визначимо сукупність таких значень $e_{g+1\,h_{g+1}} = (e_{g+1} - h_{g+1} x_{g+1\,g+2}) \bmod k_{g+1}$. На основі отриманих результатів НТ 3 слідує, що в цій сукупності обов'язково знайдеться таке єдине значення $e_{g+1\,P}$, при якому НКС $E^{(P)} = (e_1 \| e_2 \| ... \| e_{g+1\,P} \| ... \| e_m)$ є неспотвореною. Зазначимо, що черговість перевірки гіпотез є довільною і не впливає на ймовірність корекції помилок. Втім для підвищення швидкості визначення номера спотвореного залишку, першочергово необхідно перевірити ту гіпотезу, для якої значення $k_h / x_{h-1\,h}$ ($h = g, g+1$) є найменшим.

Наведемо приклад реалізації запропонованого алгоритму (порядку) корекції помилок за допомогою НКС з взаємно не простими основами СЗК.

Розглянемо СЗК, що представлена наступними основами $k_1 = 4$, $k_2 = 6$, $k_3 = 12$, $k_4 = 18$. При цьому $K = 36$, $x_{12} = 2$, $x_{23} = 6$, $x_{34} = 6$, $x_{41} = 2$. Обсяг НКС наведено в табл. 1.

Потрібно встановити правильність НКС $E = (3 \| 5 \| 7 \| 7)$, та за наявності факту спотворення даної НКС відредагувати неправильний залишок.

1. Необхідно обчислити значення $e_{12} = 0$, $e_{23} = 2$, $e_{34} = 0$, $e_{41} = 0$. Так як $e_{23} \neq 0$, то НКС E є неправильною, і другий чи третій залишок містить помилку.

2. Так як $k_2 / x_{12} > k_3 / x_{34}$, то перша гіпотеза полягає в тому, що помилка припускається у залишку за основою k_3.

3. Визначимо значення $e_{3h_3} = e_3 - h_3 x_{23}$ для значення $h_3 = 1$. Отримаємо $e_{3h_3} = e_3 - h_3 x_{23} = 7 - 1 \cdot 6 = 1$, при якому отримана $E^{(1)} = (3 \| 5 \| 1 \| 7)$ не являється кодовим словом (табл. 1). Відповідно перша гіпотеза буде невірною і саме в залишку за основою k_2 ста-

лася помилка.

4. Виправимо число E. Для цього розрахуємо шукане значення $e_{2h_2} = e_2 - h_2 x_{21}$ за значенням $h_3 = 1, 2$:

$$h_2 = 1,\ e_{2h_2} = e_2 - h_2 x_{21} = 5 - 1 \cdot 2 = 3,$$

$$h_2 = 3,\ e_{2h_2} = e_2 - h_2 x_{21} = 5 - 2 \cdot 2 = 2.$$

Таким чином, отримаємо два кодових слова: $E^{(1)} = (3 \,\|\, 3 \,\|\, 7 \,\|\, 7)$ та $E^{(2)} = (3 \,\|\, 1 \,\|\, 7 \,\|\, 7)$. Згідно з табл. 1, значення $E^{(2)}$ є єдиним правильним кодовим словом, тобто $E_{вип} = E^{(2)} = (3 \,\|\, 1 \,\|\, 7 \,\|\, 7)$.

Таблиця 1 – **Відповідність НСК кодовим словам СЗК [4]**

E	Кодові слова в СЗК				E	Кодові слова в СЗК			
	k_1	k_2	k_3	k_4		k_1	k_2	k_3	k_4
0	0	0	0	0	15	3	3	3	15
1	1	1	1	1	16	0	4	4	16
2	2	2	2	2	17	1	5	5	17
3	3	3	3	3	18	2	0	6	0
4	0	4	4	4	19	3	1	7	1
5	1	5	5	5	20	0	2	8	2
6	2	0	6	6	21	1	3	9	3
7	3	1	7	7	22	2	4	10	4
8	0	2	8	8	23	3	5	11	5
9	1	3	9	9	24	0	0	0	6
10	2	4	10	10	25	1	1	1	7
11	3	5	11	11	26	2	2	2	8
12	0	0	0	12	27	3	3	3	9
13	1	1	1	13	28	0	4	4	10
14	2	2	2	14					

E_g	Кодові слова в СЗК		
	k_1	k_2	k_3
0000	00	000	0000
0001	01	001	0001
0010	10	010	0010
0011	11	011	0011
0100	00	100	0100
0101	01	101	0101
0110	10	000	0110
0111	11	001	0111
1000	00	010	1000
1001	01	011	1001
1010	10	100	1010
0101	11	101	1011

Отже, запропонований метод корекції помилок у СЗК сприяє розширенню класу коригованих помилок, що суттєво розширює коригуючи можливості НКС з взаємно не простими основами СЗК.

Очевидно, що процес виявлення помилок в апаратно-часовому аспекті реалізується винятково просто. Час виявлення помилок для СЗК, заданої будь-якими взаємно не простими основами, завжди дорівнює трьом умовним часовим тактам і не залежить від кількості інформаційних основ.

Розглянемо деякі доведення, які дозволять спростити вищеописане пристрій для виявлення помилок. Спочатку доведемо співвідношення $(e_1 + \overline{e_g}) = (\overline{e_1} + e_g) \bmod x_{1g}$, на основі якого складаємо алгоритм корекції помилок. Нехай в НКС $E = (e_1 \,\|\, e_2 \,\|\, ... \,\|\, e_m)$ спотворено залишок k_i, тобто $\tilde{e}_i = (e_i + \triangle e_i) \bmod k_i$. Запишемо систему рівностей:

$$h_1 = e_g - \tilde{e}_i = e_g + (k_i - \tilde{e}_i) = (e_g - e_i + k_i - \triangle e_i) \bmod k_i,$$

$$h_2 = \tilde{e}_i - e_g = e_i + \triangle e_i - e_g = (e_i - e_g + e_i) = \bmod k_i.$$

Складемо рівності та отримаємо $h_1 + h_2 = k_i (\bmod k_i)$ або $h_1 + h_2 = 0 (\bmod x_{gi})$.

Таким чином, показано, що виконується рівняння $(e_1 + \overline{e_g}) = (\overline{e_1} + e_g) \bmod x_{1g}$, тобто в пристрої для виявлення помилок замість $m-1$ суматорів за модулем k_g достатньо мати лише один суматор за модулем k_1.

Розроблений алгоритм реалізації процесу виявлення помилок визначається наступними співвідношеннями: $e_2 + k_1 - e_1 = (e_2 + \overline{e_1}) \bmod x_{12}$ і $e_3 + k_1 - e_1 = (e_3 + \overline{e_1}) \bmod x_{13}$.

Вище розглянуті варіанти пристроїв для визначення помилок у СЗК дозволяють гарантовано виявити факт спотворення НКС E, однак при цьому не визначається номер основи, за якою сталося спотворення залишку.

Діагностика спотворення НКС E основується на наступній процедурі. Дослідимо процедуру визначення номера залишку, за яким сталося спотворення E.

Розглянемо СЗК, що представлена наступними основами $k_1 = 4$, $k_2 = 6$, $k_3 = 12$, $k_4 = 18$. При цьому $B = K = [4, 6, 12, 18] = 36$, $x_{12} = 2$, $x_{23} = 6$, $x_{34} = 6$, $x_{41} = 2$, $E = (0 \,\|\, 2 \,\|\, 8 \,\|\, 2)$.

Розглянемо випадок, що НКС E спотворена за основою k_4, тобто $e_4 = (e_4 - \triangle e_4) \bmod k_4$, та припустимо, що $\triangle e_4 = 5$. У цьому випадку на виході суматора за модулем k_2 отримаємо значення $\overline{e_2} = k_2 - e_2 = 4$; по модулю k_3 отримаємо – $\overline{e_3} = k_3 - e_3 = 4$, на виході суматора за модулем – $k_4 - \overline{e_4} = k_4 - e_4 = 11$. На виході суматора за модулем x_{12} отримаємо число, що відповідає значенню $(e_1 + \overline{e_2}) = 0 (\bmod x_{12})$, на виході суматора модулю x_{23} отримаємо число $(e_1 + \overline{e_3}) = 0 (\bmod x_{23})$, на виході суматора по модулю x_{34} отримаємо число

$(e_3 + \overline{e_4}) = 0(\mathrm{mod}\, x_{34})$, на виході суматора по модулю x_{41} отримаємо число $(e_4 + \overline{e_1}) = 1(\mathrm{mod}\, x_{41})$. На входах суматорів по модулю x_{34} та x_{41} присутній ненульовий результат операції $(e_k + \overline{e_i}) \bmod x_i$, тому відкритий четвертий елемент I, тобто на четвертій вихідній шині присутній сигнал. Звідси випливає, що помилка сталася у четвертому залишку e_4 (табл. 2).

На основі доведеного НТ 3 необхідною умовою виявлення помилки у залишку за модулем k_g СЗК є умова 1. Ця умова є і достатньою, якщо помилка $\triangle e_g = \tilde{e}_g - e_g$ не кратна одночасно дільникам $x_{g-1\ g}$ та x_{gi+1}, тобто наступним двом дільникам $x_{\triangle e_g}^{(g-1)} = (x_{g-1\ g}, \triangle e_g) = 1$ та $x_{\triangle e_g}^{(g+1)} = (x_{gi+1}, \triangle e_g) = 1$.

Таблиця 2 – **Відповідність НСК кодовим словам СЗК [4]**

E	Кодові слова в СЗК				E	Кодові слова в СЗК			
	k_1	k_2	k_3	k_4		k_1	k_2	k_3	k_4
0	0	0	0	0	18	2	0	6	0
1	1	1	1	1	19	3	1	7	1
2	2	2	2	2	20	0	2	8	2
3	3	3	3	3	21	1	3	9	3
4	0	4	4	4	22	2	4	10	4
5	1	5	5	5	23	3	5	11	5
6	2	0	6	6	24	0	0	0	6
7	3	1	7	7	25	1	1	1	7
8	0	2	8	8	26	2	2	2	8
9	1	3	9	9	27	3	3	3	9
10	2	4	10	10	28	0	4	4	10
11	3	5	11	11	29	1	5	5	11
12	0	0	0	12	30	2	0	6	12
13	1	1	1	13	31	3	1	7	13
14	2	2	2	14	32	0	2	8	14
15	3	3	3	15	33	1	3	9	15
16	0	4	4	16	34	2	4	10	16
17	1	5	5	17	35	3	5	11	17

Згідно з результатами НТ 3 побудуємо алгоритм корекції помилок за довільним основою k_g:

1. Визначимо всі можливі значення типу $(e_g - e_{g+1}) = e_{g\ g+1}(\mathrm{mod}\, x_{g\ g+1})$,

$$\begin{cases} e_1 - e_2 = e_{12}(\mathrm{mod}\, x_{12}), \\ e_2 - e_3 = e_{23}(\mathrm{mod}\, x_{23}), \\ \quad \dots \\ e_{m-1} - e_m = e_{m-1\ m}(\mathrm{mod}\, x_{m-1\ m}), \\ e_m - e_1 = e_{m1}(\mathrm{mod}\, x_{m1}) \end{cases} \qquad (3)$$

2. Якщо всі значення (3) дорівнюють нулю, то або помилки немає, або вона кратна кожному з дільників x_{g-1}, $x_{g\ g+1}$, (припускається однократна помилка).

3. Якщо $e_{g-1\ g} \neq 0$, $e_{g\ g+1} \neq 0$, а всі інші значення $e_{gi} = 0$, то помилка сталася за модулем k_g, тобто $\tilde{e}_g = e_g + \triangle e_g \ \ (1 \le \triangle e_g \le k_g - 1)$.

Згідно з доведеною НТ 3 необхідною умовою для виправлення помилки у залишку є умова записана в загальному вигляді:

$$(x_{gh} - 1)(x_{gi} - 1) \ge \gamma(\triangle e_g), \qquad (4)$$

де $\gamma(\triangle e_g) = k_g - 1 - (L_{x_{g\,h}} + L_{x_{gi}} - L_{[x_{g\,h},\, x_{gi}]})$. При цьому маємо наступні позначення $L_{x_{g\,h}}$ – число можливих дільників помилок $\triangle e_g$ за основою k_g (число можливих дільників числа $k_g - 1$), кратних значенню $x_{g\,h}$; $L_{x_{g\,hi}}$ – число можливих дільників помилок $\triangle e_g$ за основою k_g, кратних значенню x_{gi}; $L_{[x_{g\,h},\, x_{gi}]}$ – число можливих дільників помилок $\triangle e_g$ за основою k_g, кратних значенню найменшого спільного кратного чисел $x_{g\,h}$ та x_{gi}.

Зазначимо, що умова (4) є достатньою, якщо різним можливим значенням помилок $\gamma(\triangle e_g)$ за основою k_g $(g = \overline{1, m})$ відповідають різні пари величин $e_{g\,h}$ та e_{gi}.

Розглянемо приклад конкретного виконання операції корекції помилок у СЗК, заданій основами $k_1 = 4$, $k_2 = 6$, $k_3 = 12$. У цьому випадку таблиця кодових слів $B = [4, 6, 12] = 12$ подається у вигляді табл. 2. Зазначимо, що $x_{12} = (4, 6) = 2$, $x_{23} = (6, 12) = 6$, $x_{31} = (4, 12) = 4$; $\gamma(\triangle e_1) = 2$ (табл. 3), $\gamma(\triangle e_2) = 3$ (табл. 3), $\gamma(\triangle e_3) = 8$ (табл. 4), де:

$$\gamma(\triangle e_1) = k_1 - 1 - (L_{x_{12}} + L_{x_{31}} - L_{[x_{12},\, x_{31}]}),$$

$$\gamma(\triangle e_2) = k_2 - 1 - (L_{x_{12}} + L_{x_{23}} - L_{[x_{12},\, x_{23}]}),$$

$$\gamma(\triangle e_3) = k_3 - 1 - (L_{x_{23}} + L_{x_{31}} - L_{[x_{23},\, x_{31}]}).$$

Таблиця 3 – **Таблиця рішень**

e_{31}	$e_{12} = 1$	e_{23}	$e_{12} = 1$
1	$\triangle\overline{e_1} = 1$	1	$\triangle\overline{e_2} = 5$
2	–	3	$\triangle\overline{e_2} = 3$
3	$\triangle\overline{e_1} = 3$	5	$\triangle\overline{e_2} = 1$

Таблиця 4 – **Таблиця рішень**

e_{31}	e_{23}				
	1	2	3	4	5
1	$\triangle\overline{e_3} = 7$	–	$\triangle\overline{e_3} = 3$	–	$\triangle\overline{e_3} = 11$
2	–	$\triangle\overline{e_3} = 2$	–	$\triangle\overline{e_3} = 10$	–
3	$\triangle\overline{e_3} = 1$	–	$\triangle\overline{e_3} = 9$	–	$\triangle\overline{e_3} = 5$

Необхідно визначити правильність НКС $E=(11\|100\|0111)$. У перший і другий вхідні регістри заноситься вихідне число E. Перший суматор першої групи визначає значення $\overline{e_1}=k_1-e_1=01$, другий суматор визначає значення $\overline{e_2}=k_2-e_2=010$, а третій суматор визначає значення $\overline{e_3}=k_3-e_3=0101$. Перший суматор по модулю x_{gi} визначає значення $e_{12}=(e_1+\overline{e_2})\bmod_{12}$, другий суматор $e_{23}=(e_2+\overline{e_3})\bmod_{23}$, третій суматор $e_{31}=(e_3+\overline{e_1})\bmod_{13}$. Таким чином, з виходів відповідних дешифраторів тільки на другий комутатор надходять значення $e_{12}=1$, $e_{13}=3$, відповідно до яких (див. табл. 6) він визначає значення інвертованої за модулем k_2 помилки, тобто $\triangle\overline{e_2}=3$, які через другий дешифратор у двійковому коді надходить на перший вхід другого суматора, на другий вхід якого надходить значення $e_2=e_2+\triangle e_2=100$. Суматор другої групи визначає значення результату операції $(\triangle\overline{e_2}+e_2)\bmod k_2=\ =(k_2-\triangle e_2+e_2+\triangle e_2)\bmod k_2=001$. На вихід пристрою надходить виправлена НКС $E=(11\|100\|0111)$ (табл. 2).

Висновки

У статті уточнено деякі аспекти теорії коригувальних НКС, представлених набором взаємно не простих основ СЗК.

Розроблено алгоритми контролю та корекції помилок в СЗК з взаємно простими основами. Використання цих алгоритмів дозволяє відносно просто реалізувати процедуру виявлення та виправлення одноразових помилок.

Запропоновані в статті процедури контролю, виявлення і корекції одноразових помилок дозволяють локалізувати помилкову основу і виправити помилку в одному залишку всього за п’ять умовних тактів для будь-якої кількості основ СЗК. Основні переваги НКС з взаємно не простими основами СЗК полягають у технічній та часовій простоті процедури контролю та виявлення помилок.

Варто зазначити, що за простотою конструкції схем декодувальних пристроїв розглянутих НКС з взаємно не простими основами СЗК не мають аналогів у позиційних системах числення.

Це досягається за рахунок обмеження класу можливих коректованих помилок шляхом введення додаткової апаратурної надмірності представлення кодових слів.

СПИСОК ЛІТЕРАТУРИ

1. Krasnobayev V., Kuznetsov A., Yanko A., Koshman S., Zamula A. and Kuznetsova T. Data processing in the system of residual classes. Monograph. ASC Academic Publishing, 2019, 208 p. (Ebook).
2. Onyshchenko S., Yanko A., Hlushko A., Sabelnikova P. Assessment of information protection level against unauthorized access. ScienceRise, 2, Tallinn, Estonia, 2023, pp. 36–44. http://doi.org/10.21303/2313-8416.2023.003211
3. Mohan P. V. A. Residue Number Systems: Theory and Applications. Birkhäuser Basel, Switzerland, 2016, 351 p.
4. Krasnobaev V., Kuznetsov A., Yanko A., Kuznetsova K. Correction Codes in the System of Residual Classes. Proceedings of 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 2019, pp. 488-492. https://doi.org/10.1109/PICST47496.2019.9061253.
5. Янко А.С., Сабельнікова П.С. Метод виявлення та виправлення помилок на основі часових числових перерізів. Матеріали міжнародної науково-технічної конференції Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління, Баку-Харків-Жиліна, 2024, Т. 2, С. 14. https://doi.org/10.32620/ICT.24.t2.

Received (Надійшла) 24.09.2024
Accepted for publication (Прийнята до друку) 13.11.2024

Improving the efficiency of the data correction process in the system of residual classes

Alina Yanko, Alina Hlushko, Oleg Kruk, Andrii Prokudin

Abstract. The article examines the influence of the corrective abilities of non-positional code structures, which are represented by mutually non-prime bases of the system of residual classes (SRC). Currently, non-positional code structures, which are represented by a set of mutually non-prime bases of SRC, have been researched rather superficially and are described qualitatively rather than quantitatively. The fact is that until now, almost no one has been engaged in a deep research of the corrective properties of non-positional code structures of SRC, the bases of which are mutually non-prime numbers. Such a system also has significant corrective capabilities, which makes it necessary to assess the possibility and expediency of using non-positional code structures presented in the form of mutually non-prime bases for increasing the reliability of computer system calculations. For the purpose of further research and development of these non-positional code structures, we will consider a number of scientific statements, the use of the results of which will allow us to more fully investigate the corrective properties of non-positional code structures with mutually non-prime bases. Algorithms for control and correction of data in SRC with mutually pairwise non-prime bases have been developed. The use of these algorithms makes it relatively simple to implement the procedure for detecting and correcting single errors. The process of detecting errors in the considered non-positional code structures in the hardware-time aspect is implemented extremely simply. The error detection time for the SRC given by any mutually non-prime bases is always equal to three conventional time cycles and does not depend on the number of information bases. Note that due to the simplicity of the design of decoding device schemes, the considered non-positional code structures have no analogues in positional counting systems. This is achieved by limiting the class of possible corrected errors by introducing additional hardware redundancy in the representation of non-positional code structures in the SRC.

Keywords: mutually non-prime bases; error correction; computer systems; data correction; corrective properties; system of residual classes.