УДК 004.056.2

О. Я. Матов[1], В. С. Василенко[2]
[1]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна
[2]Національний авіаційний університет
вул. Космонавта Комарова, 1, 03058 Київ, Україна

Вибір величини контрольної основи для коду умовних лишків

Розглянуто вимоги щодо величини контрольної основи в задачах захисту цілісності інформаційних об'єктів телекомунікаційних мереж в умовах застосування узагальненого коду умовних лишків.

Ключові слова: *викривлення, завадостійке кодування, код умовних лишків, основи системи числення.*

Вступ

При використанні в завадостійкому кодуванні системи лишкових класів (СЛК) в класичному вигляді чи у вигляді коду умовних лишків (ЛУ-коді) [1] постає традиційна для задач цього класу проблема розрізняння не викривлених (правильних) кодових комбінацій (чисел, базових кодових слів) від викривлених (неправильних). Нагадаємо, що в цих системах кодова комбінація (базове кодове слово) розглядається як деяке (реальне в СЛК чи умовне в ЛУ-коді) число. В зазначених умовах не викривленими вважаються такі числа, величина яких не перевищує визначеного наперед діапазону представлення не викривлених чисел (робочого діапазону) $P = \prod_{i=1}^{n} p_i$, де $p_i (i = 1, 2, \ldots, n)$ — основи системи числення, обрані для даної системи представлення. В цих кодах для завадостійкого кодування, як і в інших кодах, вводиться надлишковість у вигляді реального чи умовного лишку від розподілу вихідного числа A на контрольну основу p_k (чи q). Її введення призводить до розширення діапазону представлення до величини $R = P \cdot p_k = P \cdot q$. При цьому природно вважається, що викривлені (неправильні) числа $\widetilde{A}$, на відміну від не викривлених, зосереджені за межами робочого діапазону, тобто $\widetilde{A} > P$. При виборі чи визначенні елементів системи числення в системі лишкових класів важливою задачею є вибір таких основ цієї системи, які б забезпечили просте та надійне виявлення факту викривлення, а в корегуючих кодах

також — як місця, так і величин можливих викривлень в базових кодових словах. Що стосується вибору основ, які створюють робочий діапазон, то вимога до них одна — ці основи повинні бути взаємно простими числами.

Вибір величин контрольної основи в задачах контролю цілісності

Оскільки за визначенням викривлені числа задовольняють умові $\widetilde{A} > P$, то звідсіля для задач контролю наявності викривлень неважко визначити вимогу до величини контрольної основи цієї системи, а отже, здійснити в подальшому її вибір. Тобто, для виявлення наявності викривлень досить визначити, в якому з діапазонів (робочому чи контрольному) знаходиться число, правильність якого перевіряється. Для цього слід вимагати, щоби викривлення лишку (символу початкового числа A) по будь-якій основі, наприклад, по основі p_i збільшувало би початкове не викривлене число $A < P$

$$A = \alpha_1, \alpha_2, \alpha_3, ..., \alpha_i, ..., \alpha_n, \alpha_k$$

на величину, яка забезпечує вихід викривленого числа в контрольний діапазон, тобто на величину

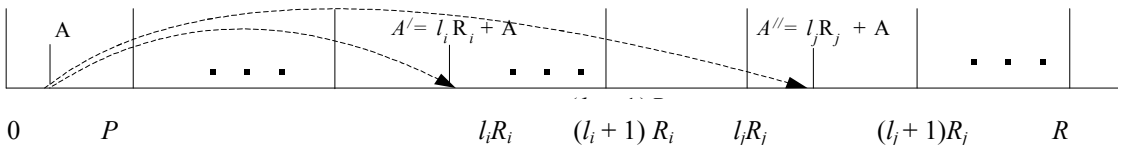
$$\Delta A = l_i \cdot R_i = 0, 0, 0, ..., \Delta\alpha_i, ..., 0, 0 > P .$$

Тоді за рахунок цього викривлене число

$$\widetilde{A} = A^{/} = A + l_i \cdot R_i = \alpha_1, \alpha_2, \alpha_3, ..., \widetilde{\alpha}_i, ..., \alpha_n, \alpha_k$$

перейде з початкового діапазону [0, P) до контрольного діапазону (див. рисунок), наприклад, до діапазону [$l_i \cdot R_i$, $(l_i + 1) \cdot R_i$) величиною $R_i = P \cdot q / p_i$. Таким чином, буде забезпечена умова

$$l_i \cdot R_i = l_i \cdot P \cdot q / p_i > P = P \cdot q / q .$$



До виходу викривленого числа за межі робочого діапазону

Звідси витікає:

$$l_i / p_i > 1 / q ,$$

а отже, при найменшому значенні $l_i = 1$

$$q > p_i,$$

тобто умовою однозначного визначення наявності викривлень є перевищення величиною контрольної основи величини будь-якої з інших основ. В останніх виразах: ΔA — величина викривлення; α_i — значення не викривленого символу (лишку по основі з номером *i*); l_i — номер інтервалу, в який потрапляє число, викривлене по основі із номером *i*; $R_i = P \cdot q / p_i$ — величина даного інтервалу; $\tilde{\alpha}_i = (\alpha_i + \Delta\alpha_i) \bmod p_i$ — значення викривленого символу; $\Delta\alpha_i$ — величина викривлення *i*-го символу.

Вибір величин контрольної основи в задачах контролю та поновлення цілісності

У задачах контролю та поновлення цілісності недостатньо лише встановити факт наявності порушення цілісності інформаційного об'єкта, а потрібно визначити місце викривлення та його величину. Зрозуміло, що для вирішення задач виявлення місця та, особливо, величин викривлень, необхідно забезпечити ідентифікацію викривленого числа (чи величини викривлення) з номером основи (для нашого прикладу — *i* чи *j*), по якій таке викривлення має місце, та визначення (в подальшому) величини цього викривлення (відповідно $\Delta\alpha_i$ чи $\Delta\alpha_j$). Для цього можна використати той факт, що аналогічне викривлення по основі p_j переводить викривлене число (див. рисунок)

$$\tilde{A} = A'' = A + l_j \cdot R_j = \alpha_1, \alpha_2, \alpha_3, ..., \tilde{\alpha}_j, ..., \alpha_n, \alpha_k,$$

до діапазону $[l_j \cdot R_j,\ (l_j + 1) \cdot R_j)$ величиною R_j.

Із наведеного витікає, що механізми визначення наявності, місця виникнення та величини викривлення повинні ґрунтуватися на виявленні тим чи іншим шляхом хоча б однієї з таких взаємно пов'язаних величин як *i*, p_i, та, відповідно, $\Delta\alpha_i$, l_i, R_i, ΔA. Також із наведеного робимо висновок, що для ідентифікації викривленого числа (чи величини викривлення) з номером основи *i* слід забезпечити попадання викривлених по різним основам чисел до різних діапазонів, що, в свою чергу, є можливим за умови, що відстань між двома довільними діапазонами, в які можуть потрапити викривлені числа, перевищувала б максимальне значення не викривленого числа (*P*). Наприклад, при $l_i \cdot R_i > l_j \cdot R_j$ (при зворотному співвідношенні результат не зміниться):

$$l_i \cdot R_i > l_j \cdot R_j + P, \text{ чи } l_i \cdot R_i - l_j \cdot R_j > P. \qquad (1)$$

У загальному випадку цей вираз із урахуванням того, що в СЛК операції в діапазоні [0, *R*) здійснюються за модулем *R*, набуде вигляду:

$$(l_i \cdot R_i - l_j \cdot R_j) \bmod R > P.$$

Звідси неважко перейти до визначення загальних вимог щодо величини контрольної основи q:

$$l_i \cdot P \cdot q / p_i - l_j \cdot P \cdot q / p_j > P \qquad (2)$$

за умови $l_i \cdot P \cdot q / p_i > l_j \cdot P \cdot q / p_j$,
чи

$$R + l_i \cdot P \cdot q / p_i - l_j \cdot P \cdot q / p_j - [(R + l_i \cdot P \cdot q / p_i - l_j \cdot P \cdot q / p_j)/R] \cdot R > P \qquad (3)$$

за умови $l_i \cdot P \cdot q / p_i < l_j \cdot P \cdot q / p_j$. В останньому виразі квадратні дужки означають обчислення цілої частини від відповідного дробового числа.

При визначенні вимог щодо величини контрольної основи q, виходячи з виразу (2), після скорочення на P одержимо:

$$l_i \cdot q / p_i - l_j \cdot q / p_j > 1,$$
$$q(l_i / p_i - l_j / p_j) > 1,$$

а, отже, в результаті вимога до контрольної основи приймає вигляд нерівності

$$q > 1/(l_i / p_i - l_j / p_j) = p_i \cdot p_j / (l_i \cdot p_j - l_j \cdot p_i). \qquad (4)$$

Звернемо увагу на те, що права частина нерівності (4) в загальному випадку може бути дробовим, а не цілим числом, яким повинна бути контрольна основа. До того ж шукане значення контрольної основи повинно бути цілим. Для розв'язання цієї нерівності спочатку слід визначити максимальне значення чисельника та мінімальне значення знаменника. Зрозуміло, що максимальне значення чисельника в цьому виразі дорівнює добутку двох найбільших із основ системи числення $p_n \cdot p_{n-1}$, а мінімальне значення знаменника (це цілочисленна величина!)

$$l_i \cdot p_j - l_j \cdot p_i = 1,$$

оскільки дорівнювати нулю знаменник може лише тоді, коли

$$l_i \cdot p_j = l_j \cdot p_i.$$

Останнє, в свою чергу, є досяжним лише при $l_i = p_i$, а $l_j = p_j$, що є неможливим (нагадаємо, що основи системи числення, наразі це величини p_i та p_j, є взаємно простими числами).

Оскільки мінімальне значення знаменника дорівнює одиниці, то граничне значення виразу (4) є цілою величиною. Причому, в разі визначення як величини,

так і місця викривлення за фактом попадання викривленого числа до інтервалу l_i чи l_j, вимога до величини контрольної основи може бути записаною у вигляді

$$q > p_n \cdot p_{n-1}. \tag{5}$$

При визначенні вимог щодо величини контрольної основи q, виходячи із виразу (3), після скорочень на P та q одержимо:

$$q + l_i \cdot q / p_i - l_j \cdot q / p_j - [1 + l_i / p_i - l_j / p_j] \cdot q > 1,$$
$$q \cdot (1 + l_i / p_i - l_j / p_j - [1 + l_i / p_i - l_j / p_j]) > 1,$$

а, отже, в результаті вимога до контрольної основи приймає вигляд нерівності

$$q > 1/(1 + l_i / p_i - l_j / p_j - [1 + l_i / p_i - l_j / p_j]). \tag{6}$$

Звернемо увагу на те, що вираз у знаменнику є дробовим число, звідси величина контрольної основи є більшою за чисельник, отже більшою за одиницю. Для уточнення цієї величини приведемо вирази у знаменнику до спільного знаменника, яким є величина $p_i \cdot p_j$, та перенесемо останню у чисельник. Тоді нерівність (6) перетвориться на вимогу

$$q > p_i \cdot p_j / (p_i \cdot p_j + l_i \cdot p_j - l_j \cdot p_i - p_i \cdot p_j \cdot [(p_i \cdot p_j + l_i \cdot p_j - l_j \cdot p_i) / (p_i \cdot p_j)]).$$

Оскільки знаменник, як і у виразі (6), є меншим одиниці, а величина контрольної основи q повинна бути цілим, взаємно простим числом з усіма іншими основами з усієї їхньої множини, то слід зробити висновок, що вимога щодо величини q перетворюються на вимогу вигляду

$$q > c \cdot p_i \cdot p_j, \tag{7}$$

де величина c з урахуванням уже визначеної вимоги (5) може прийняти таке значення $c > 1$, яке є цілим та взаємно простим числом з усіма основами використовуваної системи числення. З іншого боку, слід враховувати, що від величини q залежить можлива надлишковість коду, яку бажано мати найменшою. Виходячи з цього, слід зробити висновок, що сформульованим обмеженням задовольняє вимога, яку з урахуванням викладеного вище можна розглядати як єдину можливу:

$$q > 2 \cdot p_i \cdot p_j. \tag{8}$$

Таким чином, при дотриманні умови (8), можливо забезпечити однозначний результат виявлення та виправлення всіх можливих викривлень в одному з узагальнених символів представлення інформаційних об'єктів при їхній циркуляції в

сучасних телекомунікаційних мережах. Можливості щодо такого застосування коду умовних лишків уже розглянуті в роботах [1–3].

1. *Василенко В.С.* Использование ВУ-кодов для повышения верности информации в радіоканалах / В.С. Василенко // Матеріали 28 НТС Асоціації зв'язку України. — К.: КВІРТУ ППО. — 1991. — С. 23.

2. *Акушский И.Я.* Машинная арифметика в остаточных класах / И.Я. Акушский, Д.И. Юдицкий. — М.: Сов. радио, 1966. — 421 с.

3. *Василенко В.С.* Узагальнені завадостійкі коди в задачах забезпечення цілісності інформаційних об'єктів. Код умовних лишків / В.С. Василенко, О.Я. Матов // Реєстрація, зберігання і оброб. даних. — 2006. — Т. 6, № 4. — С. 82–93.

Надійшла до редакції 02.03.2010