УДК 004.056.2

О. Я. Матов[1], **В. С. Василенко**[2], **О. В. Дубчак**[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

Контрольні основи для коду умовних лишків

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

Ключові слова: *завадостійке кодування, код умовних лишків, контроль цілісності, контрольна основа, основа коду, поновлення цілісності, спотворення.*

Вступ

Спотворення інформації, тобто порушення її цілісності, можливі на будь-якому етапі її циркуляції у телекомунікаційних мережах: при зберіганні, передачі або обробці. Забезпечення цілісності інформаційних об'єктів можливе із застосуванням завадостійких корегуючих кодів, що знайшло широке застосування в протоколах передачі даних сучасних інформаційних систем. Характерною особливістю сучасних протоколів фізичного та канального рівнів є застосування багаторівневих чи багатопозиційних методів модуляції, що забезпечує потреби підвищення пропускної здатності каналів. При цьому передавання інформації здійснюється із застосуванням узагальнених символів, кожен із яких здатен переносити певну кількість двійкових інформаційних символів (біт). Але будь-яке спотворення такого узагальненого символу при застосуванні цих методів модуляції призводить до групових спотворень у відповідних інформаційних об'єктах. Отже для забезпечення потрібної цілісності інформації орієнтуються на застосування завадостійких корегуючих кодів, які були би спроможними забезпечити виявлення та виправлення пакетів спотворень значної тривалості. Як один із таких кодів пропонується узагальнений завадостійкий корегуючий код на базі теорії лишкових класів — код умовних лишків [1].

При використанні в завадостійкому кодуванні системи лишкових класів (СЛК) у класичному вигляді чи у вигляді коду умовних лишків (ЛУ-коді) [1] постає

традиційна для задач цього класу проблема розрізняння не спотворених (правильних) кодових комбінацій (чисел, базових кодових слів) від спотворених (неправильних). Нагадаємо, що у цих системах кодова комбінація (базове кодове слово) розглядається як деяке (реальне в СЛК чи умовне в ЛУ-коді) число. В зазначених умовах не спотвореними природно вважати такі числа, величина яких не перевищує визначеного наперед діапазону представлення вихідних (не спотворених) чисел (робочого діапазону) $P = \prod_{i=1}^{n} p_i$, де $p_i (i = 1, 2, \ldots, n)$ — основи системи числення, що 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. Її введення призводить до розширення діапазону представлення до величини $R = P \cdot p_k$. При цьому природно припустити, що спотворені (неправильні) числа $\tilde{A}$, на відміну від не спотворених, зосереджені за межами робочого діапазону, тобто $\tilde{A} > P$.

Постановка проблеми

Для забезпечення останнього припущення при виборі чи визначенні елементів системи числення у системі лишкових класів слід правильно вирішити важливу проблему щодо вибору таких основ цієї системи, які б забезпечили просте і надійне виявлення факту спотворення (тобто виходу спотворених чисел за межі робочого діапазону), а в корегуючих кодах також — як місця, так і величин можливих спотворень у базових кодових словах. Що стосується вибору основ, які створюють робочий діапазон, то вимога до них одна — ці основи повинні бути взаємно простими числами. Вибір основ при використанні цього коду в задачах контролю цілісності розглянуто в роботі [2]. Що ж стосується вибору основ при використанні цього коду в задачах контролю та поновлення цілісності, то в роботі [2] зроблені лише припущення щодо їхньої величини.

Отже, метою цієї роботи є визначення можливих величин контрольних основ ЛУ-коду в задачах контролю та поновлення цілісності (тобто в задачах виправлення спотворень).

Вибір величин контрольної основи в задачах контролю та поновлення цілісності

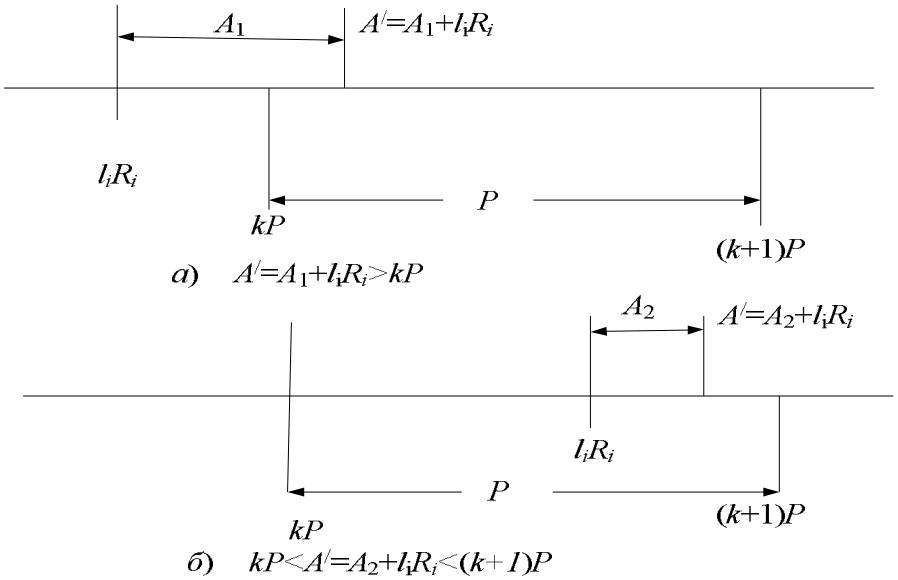
При вирішенні цієї проблеми будемо враховувати одержані в [2] підходи та результати.

Отже, для виявлення наявності спотворень досить визначити, в якому із діапазонів (робочому чи контрольному) знаходиться число, правильність якого перевіряється. Покажемо, що при правильному виборі контрольної основи цього достатньо і для визначення місця і величини такого спотворення.

Спотворене число може бути представленим як сума початкового (не спотвореного) числа A та вектора спотворень E: $\tilde{A} = A + E$, де вектор спотворення E у СЛК має лишки, що дорівнюють нулю, по усім основам, окрім тієї, де є спотворення. Надалі нагадаємо, що вектор спотворення є числом вигляду

$E = 0,0,...,\Delta A,0,0,...,0 = l_i \cdot R_i$, чи $E = 0,0,...,(l_i \cdot R_i) \bmod p_i,0,0,...,0$, оскільки тільки числа, які діляться націло на $R_i = R / p_i$ мають у своєму представленні в СЛК такий набір лишків. В останніх виразах величина $R = \prod_{i=1}^{k=n+1} p_i$ — контрольний (повний) діапазон представлення чисел у СЛК.

На числовій осі величина спотворення $E = l_i \cdot R_i$ відображається точкою в деякому піддіапазоні «контрольного» діапазону [(*P* + 1), *R*). Відповідно, процес спотворення початкового числа *A* відобразиться переміщенням точки *A* із робочого діапазону [0, *P*) до деякого піддіапазону із номером *k*. Звернемо увагу на те, що в піддіапазон із цим номером *k* спотворене число ($A' = l_i \cdot R_i + A_1$ чи $A' = l_i \cdot R_i + A_2$) може попасти (див. рисунок) залежно від величини початкового числа (A_1 чи A_2) та взаємного розташування лівих границь піддіапазонів — відповідно точок $k \cdot P$ та $l_i \cdot R_i$.



Ілюстрація розташування спотворених чисел

На рисунку (*а*) зображена ситуація, коли величина початкового числа A_1 перевищує різницю між значеннями $l_i \cdot R_i$ та $k \cdot P$, тобто коли $A_1 > (k \cdot P - l_i \cdot R_i)$. Ситуація, що зображена на рисунку (*б*) відповідає варіанту, коли величина початкового числа A_2 є меншою ніж різниця між значеннями $l_i \cdot R_i$ та $(k + 1) \cdot P$.

В обох випадках величина спотворення (чи довжина вектора спотворення) *E* відповідає умові:

$$(k - 1) \cdot P < E = l_i \cdot R_i < (k + 1) \cdot P. \quad (1)$$

Звернемо увагу на те, що цей же результат може бути одержаним залежно від величини початкового (неспотвореного) числа *A* при попаданні вектора спотво-

рення E в межі діапазону, ширину якого можна визначити із виразу (1), якщо від лівої частини цього нерівняння відняти праву:

$$\Delta E = (k+1)\cdot P - (k-1)\cdot P = 2P.$$

Отже правильний результат при декодуванні можна одержати лише у випадку, коли можливі викривлення (чи кінці вектора викривлень) є рознесеними на величину, яка є не меншою ніж $\Delta E = 2P$. Оскільки кількість піддіапазонів P в межах контрольного діапазону $R = P\cdot p_k$ визначається величиною контрольної основи (точніше, дорівнює) p_k, то і відстань між кінцями вектора викривлень залежить від величини p_k. *Цей висновок повинен бути врахованим при визначенні величини контрольної основи* p_k.

Із наведеного витікає, що механізми визначення наявності, місця виникнення та величини викривлення повинні ґрунтуватися на виявленні тим чи іншим шляхом хоча б однієї із таких взаємно пов'язаних величин як i, p_i, та, відповідно, $\Delta\alpha_i$, l_i, R_i, ΔA. Також очевидно, 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 подвійне максимальне значення не викривленого числа ($2P$). Наприклад, при $l_i \cdot R_i > l_j \cdot R_j$:

$$l_i \cdot R_i > l_j \cdot R_j + P, \text{ чи } l_i \cdot R_i - l_j \cdot R_j > 2P. \qquad (2)$$

Звідси:

$$l_i \cdot P \cdot p_k / p_i - l_j \cdot P \cdot p_k / p_j > 2P,$$
$$l_i \cdot p_k / p_i - l_j \cdot p_k / p_j > 2,$$
$$p_k \cdot (l_i / p_i - l_j / p_j) > 2,$$
$$p_k > 2/(l_i / p_i - l_j / p_j) = 2 \cdot p_i \cdot p_j /(l_i \cdot p_j - l_j \cdot p_i).$$

Оскільки шукане значення контрольної основи (мінімально можливе (граничне) значення) повинно перевищувати величину, яка визначається дробовим числом, то для пошуку максимального значення цієї дробової величини слід визначити максимальне значення чисельника та мінімальне значення знаменника. Максимальне значення чисельника у цьому виразі дорівнює подвійному добутку двох найбільших із основ системи числення $2 \cdot p_n \cdot p_{n-1}$, а мінімальне значення знаменника (це цілочисельна величина!):

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

оскільки дорівнювати нулю знаменник може лише тоді, коли

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

що, в свою чергу, є досяжним лише при $l_i = p_i$, а $l_j = p_j$, і що є неможливим (нагадаємо, що основи системи числення, наразі це величини p_i та p_j, є взаємно простими числами). Отже, в разі визначення величини та місця викривлення за фактом попадання викривленого числа до інтервалу l_i чи l_j, вимога до мінімально можливого (граничного) значення величини контрольної основи може бути записаною у вигляді:

$$p_k > 2 \cdot p_n \cdot p_{n-1}. \tag{3}$$

При зворотному співвідношенні між величинами векторів викривлення, тобто при $l_i \cdot R_i < l_j \cdot R_j$ їхня різниця є від'ємною величиною, тобто $l_i \cdot P \cdot q / p_i - l_j \cdot P \cdot q / p_j < 0$, тоді за правилами виконання модульних операцій (у цьому випадку за модулем R) умова (2) набуде вигляду:

$$l_i \cdot R_i < l_j \cdot R_j + P, \text{ чи } R + l_i \cdot R_i - l_j \cdot R_j > 2P.$$

Звідси:

$$R + l_i \cdot P \cdot p_k / p_i - l_j \cdot P \cdot p_k / p_j > 2P,$$
$$p_k + l_i \cdot p_k / p_i - l_j \cdot p_k / p_j > 2,$$
$$p_k \cdot (1 + l_i / p_i - l_j / p_j) > 2,$$
$$p_k > 2 / (1 + l_i / p_i - l_j / p_j) = 2 \cdot p_i \cdot p_j / (p_i \cdot p_j + l_i \cdot p_j - l_j \cdot p_i).$$

Як і в попередньому випадку, максимальне значення чисельника у цьому виразі дорівнює подвійному добутку двох найбільших із основ системи числення $2 \cdot p_n \cdot p_{n-1}$, а мінімальне значення знаменника (це цілочисельна величина!)

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

може бути досягнутим при мінімальному значенні другого (позитивного) доданку $l_i \cdot p_j$ та максимальному значенні третього (відмінного) $-l_j \cdot p_i$. Не важко побачити, що $\min l_i \cdot p_j = p_j$ (при $l_i = 1$), а $\max l_j \cdot p_i = (p_j - 1) \cdot p_i = p_i \cdot p_j - p_i$ (при $l_j = p_j - 1$). Тоді

$$\min (p_i \cdot p_j + l_i \cdot p_j - l_j \cdot p_i) = p_i + p_j,$$

а вираз для визначення шуканого максимального значення p_k набуває вигляду

$$p_k > 2/(1 + l_i / p_i - l_j / p_j) = 2 \cdot p_i \cdot p_j / (p_i + p_j)$$

і є меншим, ніж у виразі (3).

Отже, оскільки правильний результат декодування потрібен у будь-якій ситуації, мінімально можливі (граничні) значення величини контрольної основи слід розраховувати, виходячи із виразу (3).

Таким чином, у статті розглянуто питання визначення величин основ коду умовних лишків як для випадків його використання для контролю цілісності, так і для випадків його використання для контролю та поновлення цілісності, та запропоновано вирази для розрахунку мінімально можливих (граничних) значень величин контрольної основи.

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

2. *Василенко В.С.* Вибір величини контрольної основи для коду умовних лишків / В.С. Василенко, О.Я. Матов // Реєстрація, зберігання і оброб. даних. — 2010. — Т. 12, № 1. — С. 73–78.

Надійшла до редакції 19.05.2011