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

Блокові згорткові коди в задачах контролю цілісності

Для задач контролю цілісності інформаційних об'єктів в умовах природних впливів запропоновано блоковий згортковий код з використанням алгоритмів кодування–декодування, що є притаманними класичному завадостійкому корегувальному згортковому коду, який був би спроможний забезпечити виявлення та виправлення подвійних викривлень.

Ключові слова: *базове кодове слово, викривлення, згортковий код, інформаційний обмін.*

Вступ

Відомо [1–3], що канали, якими передається інформація, практично ніколи не бувають ідеальними (каналами без завад). У них завжди присутні завади, і мова може йти лише про рівні завад (співвідношення сигнал/завада) та їхній спектральний склад. Завади в каналах утворюються з різних причин, але результат їхньої дії на передану інформацію завжди один — порушується цілісність інформаційних об'єктів, інформація спотворюється (втрачається).

Для запобігання втратам інформації в каналі застосовуються різноманітні завадостійкі надмірні коди (коди з надмірністю). Перевага завадостійкого коду полягає у тому, що при прийомі його із викривленнями (кількість викривлених символів залежить від ступеня надмірності й структури коду) інформація може бути відновлена. Для різних завад у каналі існують різні за своєю структурою та надмірністю коди. Звичайно надмірність кодів знаходиться в межах 10 … 60 % або трохи більше, залежно від умов та мети їхнього застосування. Наприклад, надмірність 25 % застосовується при записі інформації на лазерні диски і в системах цифрового супутникового телебачення [3].

Відоме велике число завадостійких кодів, які класифікуються за різними ознаками. Виходячи зі змісту статті, відмітимо лише, що відомі завадостійкі згорткові коди відносяться до роздільних, безперервних, які характеризуються тим,

що операції кодування й декодування здійснюються над безперервною послідовністю символів без розбиття її на блоки.

Серед безперервних найбільш застосовні згорткові коди. У цих кодах кожні n символів складаються, як і в інших кодах, із m інформаційних і k перевірочних. Ці коди можуть мати різну надлишковість, але найбільш просто вони реалізуються при $m = k$, тобто коли $n = 2m = 2k$, а надмірність $R_k = m/n = 0{,}5$. Тоді відносну швидкість передачі R можна записати у вигляді:

$$R = 1 - R_k = m/n = m/2m = 0{,}5.$$

У цьому коді алгоритмами формування перевірочних та контрольних символів створюються послідовно пов'язані ланцюги, що й відображено в одній із назв коду «ланцюговий».

Безперечною перевагою згорткових кодів є можливість виявляти й виправляти групові викривлення, а певним недоліком — звуження області застосування лише потоковими кодами, що при передачі, наприклад, коротких повідомлень в умовах зашумленого каналу, створює певні труднощі. Ці труднощі полягають у неможливості формування відомими методами контрольних та перевірочних символів для символів, які розташовані на початку та в кінці інформаційних блоків.

У статті показана можливість побудови блокового згорткового коду з використанням алгоритмів кодування–декодування, які є притаманними для класичного згорткового коду, і не має зазначених вад.

Побудова блокового згорткового коду

При блоковому кодуванні послідовність елементарних повідомлень джерела розбивається на відрізки, і кожному відрізку ставиться у відповідність певна послідовність (блок) кодових символів, звана звично кодовою комбінацією чи базовим кодовим словом. Саме безліч усіх кодових комбінацій, можливих при даному способі блокового кодування, і є блоковим кодом.

Для побудови згаданого блокового згорткового коду як блок чи як базове кодове слово будемо розглядати фрагмент одного з незалежних ланцюгів неперервного коду, в якому кількість інформаційних символів обмежимо величиною m.

У цьому коді, як і в рекурентному, ланцюговому коді, формується $k = m$ перевірочних символів. Як у відомого ланцюгового коду кожен із них формується шляхом додавання за модулем 2 двох суміжних інформаційних так, що будь-який інформаційний символ використовуються для формування двох перевірочних. Перевірочні символи розташовуються між інформаційними після другого з інформаційних, який використовувався для його формування.

Для формування першого та останнього перевірочних символів пропонується додавати за модулем 2 останній (m-й) та перший інформаційні символи даного базового кодового слова. Цей перевірочний символ пропонується розташувати після першого інформаційного. Таким чином, на погляд авторів, усувається зазначена у вступі вада.

Основні операції алгоритму кодування–декодування утвореного блокового коду пропонується здійснювати як і у відомого ланцюгового. Зокрема, на боці

приймача з інформаційних символів ($a^{/}$) за тими ж правилами, що й перевірочні, на боці передавача, формуються контрольні. Контрольні символи порівнюються із перевірочними і, в разі їхнього неспівпадання, формується висновок про наявність викривлення.

Передавання	Приймання
$a_1 \oplus a_2 = П_{1,2}$, $a_2 \oplus a_3 = П_{2,3}$	$a_1^{/} \oplus a_2^{/} = K_{1,2}$, $a_2^{/} \oplus a_3^{/} = K_{2,3}$
…	…
$a_{m-1} \oplus a_m = П_{m-1,m}$, $a_m \oplus a_1 = П_{m,1}$	$a_{m-1}^{/} \oplus a_m^{/} = K_{m-1,m}$, $a_m^{/} \oplus a_1^{/} = K_{m,1}$

Кожен контрольний символ порівнюється із відповідним перевірочним:

$$S_{i,i+1} = K_{i,i+1} \oplus П_{i,i+1}^{/},\ S_{i+1,i+2} = K_{i+1,i+2} \oplus П_{i+1,i+2}^{/} \text{ і т.д.}$$

Ознакою відсутності викривлень є те, що всі суми дорівнюють нулю:

$$S_{i,i+1} = \ S_{i+1,i+2} = \ldots = 0.$$

Зрозуміло, що викривленим може бути як інформаційний, так і перевірочний символ. На викривлення перевірочного символу покаже те, що лише одна із сум дорівнює одиниці. Наприклад, при викривленні $П_{i,i+1}^{/}$ отримаємо $S_{i,i+1} = 1$, оскільки $K_{i,i+1}$ не співпадає з $П_{i,i+1}^{/}$. Якщо подальша передача цієї послідовності не здійснюється (ретрансляція відсутня), то ніяких виправлень здійснювати не слід.

Наявність же двох сум, які дорівнюють одиниці свідчить про викривлення двох перевірочних символів, або одного інформаційного, в разі, коли номери позиції у цій парі сум є спільними.

Для ілюстрації розглянемо приклад застосування блокового згорткового коду за умови, що перевірочні символи прийнято без викривлень. Нехай з викривленням прийнято один інформаційний символ. Формування перевірочних і контрольних символів показано на рис. 1.

Порівняємо контрольні елементи із перевірочними, які є прийнятими:

$$S_{3,4} = K_{3,4} \oplus П_{3,4}^{/} = 1 \oplus 0 = 1,$$

$$S_{4,5} = K_{4,5} \oplus П_{4,5}^{/} = 1 \oplus 0 = 1.$$

Видно, що створилися дві пари сум, які дорівнюють одиниці: $S_{3,4}$ і $S_{4,5}$.

Звідси робимо висновок, що викривлено той інформаційний символ, номер позиції якого є спільним у кожній парі сум, тобто a_4. Значення цього символу необхідно виправити на протилежне: прийнято 0 — повинна бути 1, і навпаки. Таким чином, викривлення виправлено.

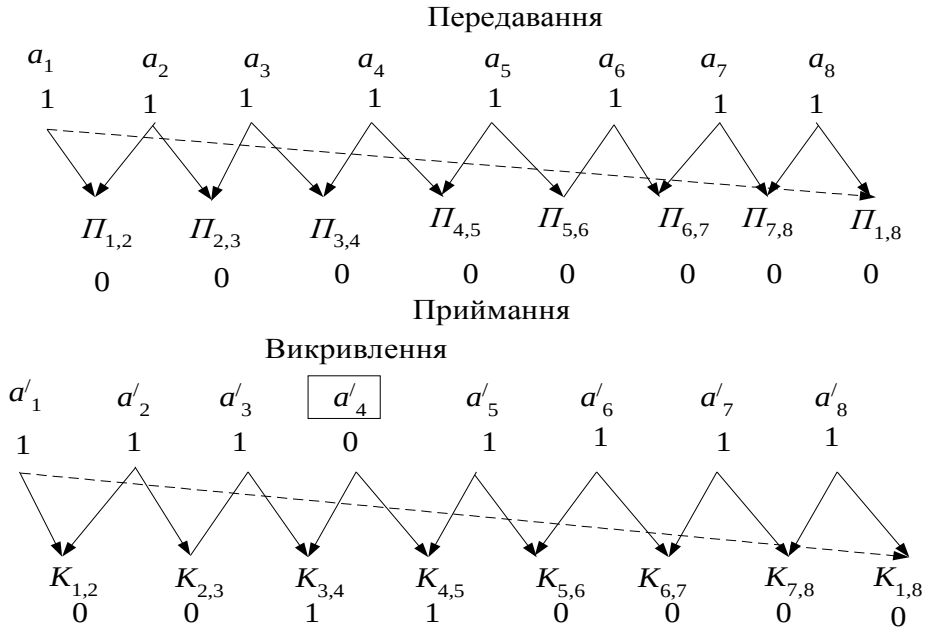

Рис. 1. Формування перевірочних і контрольних символів за наявності викривлення в символі з номером 4

Приклад 2. Значення інформаційних і перевірочних символів при передаванні — такі ж як і в попередньому прикладі (див. рис. 1). Перевірочні символи прийнято без викривлень, із викривленнями прийнято інформаційні символи a'_1, a'_4, a'_7 (рис. 2). Звернемо увагу на те, що такі викривлення перевищують можливість коду з їхнього виявлення та виправлення.

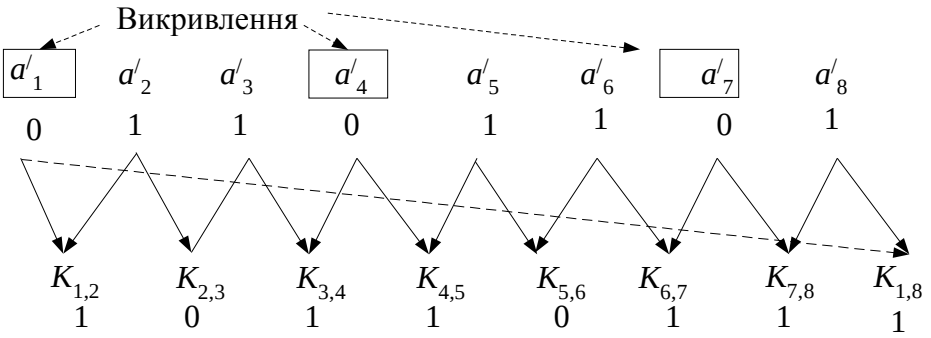

Рис. 2. Формування перевірочних і контрольних символів за наявності викривлення в символах з номерами 1, 4, 7

Результатами порівнянь перевірочних і контрольних символів є:

$$S_{1,2} = K_{1,2} \oplus П'_{1,2} = 1 \oplus 0 = 1, \quad S_{1,8} = K_{1,8} \oplus П'_{1,8} = 1 \oplus 0 = 1,$$

$$S_{3,4} = K_{3,4} \oplus П'_{3,4} = 1 \oplus 0 = 1, \quad S_{4,5} = K_{4,5} \oplus П'_{4,5} = 1 \oplus 0 = 1,$$

$$S_{6,7} = K_{6,7} \oplus П'_{6,7} = 1 \oplus 0 = 1, \quad S_{7,8} = K_{7,8} \oplus П'_{7,8} = 1 \oplus 1 = 0.$$

Ці результати порівняння свідчать про наявність викривлень в інформаційних символах з номерами 1 і 4 ($S_{1,2} = S_{1,8} = 1$, $S_{3,4} = S_{4,5} = 1$), що є вірним, і відсутність викривлень у решті символів, що є невірним, оскільки викривлення в символі з номером 7 є невиявленим. Звернемо увагу на те, що в даному випадку невірно визначена відсутність викривлень у символі, в якого до або після розташовано лише один не викривлений символ (символ з номером 8).

Приклад 3. Значення інформаційних і перевірочних символів при передаванні такі ж як і в попередньому прикладі (див. рис. 1). Перевірочні символи прийнято без викривлень, із викривленнями прийнято інформаційні символи a'_1, a'_4, a'_6 (рис. 3). Ці викривлення також перевищують можливість коду з їхнього виявлення та виправлення.

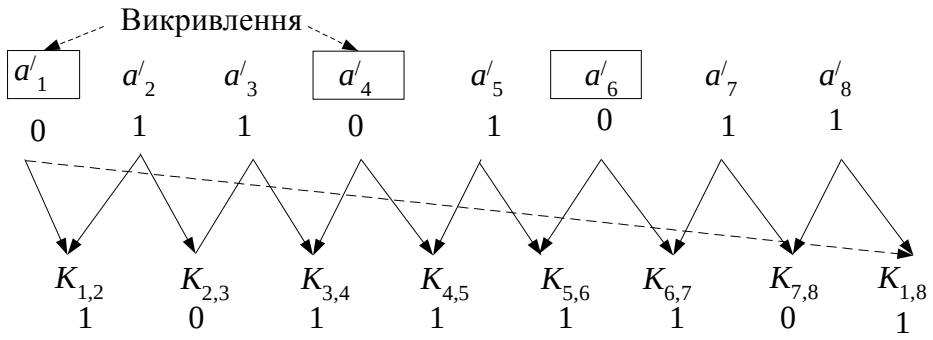

Рис. 3. Формування перевірочних і контрольних символів за наявності викривлення в символах з номерами 1, 4, 6

Результатами порівнянь перевірочних і контрольних символів є:

$$S_{1,2} = K_{1,2} \oplus П'_{1,2} = 1 \oplus 0 = 1, \quad S_{1,8} = K_{1,8} \oplus П'_{1,8} = 1 \oplus 0 = 1,$$

$$S_{3,4} = K_{3,4} \oplus П'_{3,4} = 1 \oplus 0 = 1, \quad S_{4,5} = K_{4,5} \oplus П'_{4,5} = 1 \oplus 0 = 1,$$

$$S_{5,6} = K_{5,6} \oplus П'_{5,6} = 1 \oplus 0 = 1, \; S_{6,7} = K_{6,7} \oplus П'_{6,7} = 1 \oplus 0 = 1,$$

$$S_{7,8} = K_{7,8} \oplus П'_{7,8} = 0 \oplus 0 = 0.$$

Ці результати порівняння свідчать про наявність викривлень в інформаційних символах з номерами 1, 4, 6 ($S_{1,2} = S_{1,8} = 1$; $S_{3,4} = S_{4,5} = 1$; $S_{5,6} = S_{6,7} = 1$), що є вірним, і наявність викривлень у символі з номером 5 ($S_{4,5} = S_{5,6} = 1$), що є невірним.

Звернемо увагу на те, що в даному випадку невірно визначено наявність викривлень у символі із номером 5, з обох боків якого розташовані викривлені символи.

Розглянувши три приклади з різною кількістю викривлених інформаційних символів, можна зробити висновок, що блоковий згортковий код виправляє групове викривлення в одному з інформаційних символів (див. перший та третій приклади), якщо праворуч та ліворуч від викривлення є два не викривлених символи.

Із викладеного раніше зрозуміло також, що інформаційні та перевірочні символи повинні чергуватися. Для визначеності будемо вважати, що інформаційні символи мають непарні номери, а перевірочні — парні.

Місце розташування перевірочних символів визначається двома обставинами: по-перше, групове (в даному випадку, подвійне) викривлення не повинно одночасно охоплювати інформаційний і відповідний перевірочний символи; по-друге, не повинно бути неправильного виправлення інформаційних символів, тобто не повинні бути одночасно викривлені ті перевірочні символи, номери позиції яких є спільними щодо відповідного інформаційного.

Із цих міркувань витікає, що перевірочні символи повинні розташовуватися мінімум через три інформаційних символи від найближчих із своїх інформаційних. Тоді, перевірочний символ $П_{i,i+1}$, створений з інформаційних a_i та a_{i+1}, повинен займати позицію після (i + 4) інформаційного. Наприклад, перевірочний символ $П_{1,2}$, створений з інформаційних a_1 та a_2, повинен займати позицію після 5-го інформаційного. Відповідно, перевірочний символ $П_{n,1}$, створений з інформаційних a_1 та a_n, повинен займати позицію після 4-го інформаційного, і т.д.

Неважко упевнитися в тому, що з урахуванням останніх вимог блок такого коду мінімально можливої довжини має вигляд, як показаного на рис. 4, і має складатися з n = 16 символів, коли $m = k = 8$.

Останнє може бути проілюстрованим наступним прикладом.

Приклад 4. Значення інформаційних і перевірочних символів при передаванні — такі ж як і в попередніх прикладах (див. рис. 1). Із викривленнями прийнято (рис. 4) інформаційний символ $a_2^{/}$ та перевірочний $n_6^{/}$ (на рис. 4 показані значення переданих та контрольних символів, а значення прийнятих, у тому числі викривлених символів, не показані), що відповідає можливостям коду.

Результатами порівнянь перевірочних і контрольних символів є:

$$S_{1,2} = K_{1,2} \oplus П_{1,2}^{/} = 1 \oplus 0 = 1,$$

$$S_{2,3} = K_{2,3} \oplus П_{2,3}^{/} = 1 \oplus 0 = 1,$$

$$S_{6,7} = K_{6,7} \oplus П_{6,7}^{/} = 0 \oplus 1 = 1.$$

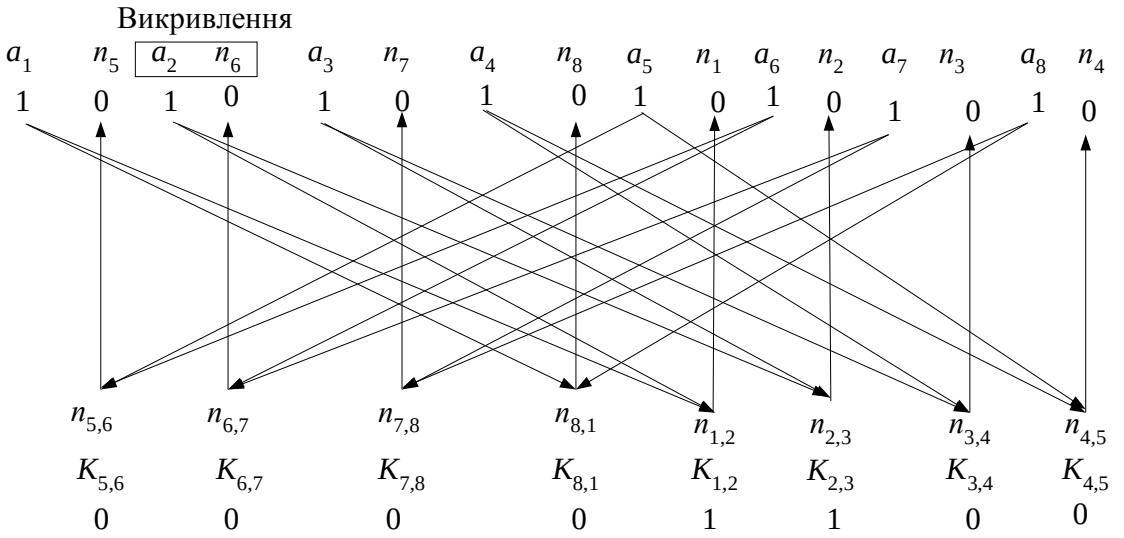

Рис. 4. Мінімально допустима структура блокового згорткового коду

Ці результати порівняння свідчать про наявність викривлень в інформаційному символі з номером 2, ($S_{1,2} = S_{2,3} = 1$), що є вірним, і наявність викривлень у перевірочному символі з номером 6 ($S_{6,7} = 1$), що також є вірним.

Отже, при такій структурі блокового згорткового коду в послідовності з шістнадцяти символів забезпечується безумовне виявлення й виправлення викривлень одного з інформаційних й одного з перевірочних символів, що розташовані послідовно. Іншими словами, код з такими параметрами забезпечує виявлення і виправлення групових (парних, розташованих послідовно) викривлень кратності 2 при досить високому значенні ймовірності викривлення символу $P_в \approx 2/16 = 0{,}125$.

Не важко помітити також, що кожне збільшення довжини коду на один інформаційний і один перевірочний символи дозволяє потенційно збільшити на одиницю кількість пар викривлених символів. Але з урахуванням наведених вище обмежень їхнє розташування не є довільним. Не важко зрозуміти, що мінімально допустима відстань m між груповими викривленнями розглянутого коду (рис. 5) дорівнює 5. Оскільки ймовірність появи в базовому кодовому слові декількох групових викривлень з такою відстанню між ними розрахувати складно, але виходячи із природи таких викривлень (можна припустити її досить низьке значення), то більш надійним є припущення, що блоковий згортковий код дозволяє в кожному базовому кодовому слові виправляти один викривлений інформаційний символ, що є притаманним і для решти двійкових блокових кодів. Але, точніше, блоковий згортковий код дозволяє виправляти пару послідовно розташованих символів, з яких один інформаційний, а другий — перевірочний, що перевищує можливості інших двійкових блокових кодів і є притаманним узагальненим [4] блоковим кодам.

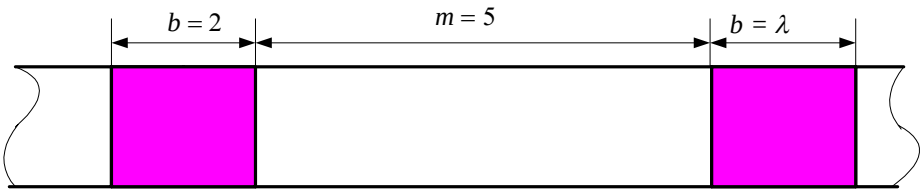

Рис. 5. Мінімально допустима відстань між груповими викривленнями

У разі ж необхідності забезпечити виявлення та виправлення чи то більшого пакета викривлень, чи то більшої кількості двократних викривлень, слід застосовувати загальновідомий механізм перемежування.

Таким чином, у статті запропоновано варіант побудови та використання згорткового завадостійкого корегувального коду та відповідні алгоритми кодування–декодування для застосування в задачах контролю, чи контролю та поновлення цілісності інформаційних об'єктів в умовах пакетних викривлень. Здійснено їхній аналіз, показані переваги та вади.

1. *Матов А.Я.* Основы теории передачи дискретной информации: Учеб. пособ. — К.: КВИРТУ ПВО, 1977. — 242 с., ил.

2. *Кунегин С.В.* Системы передачи информации. Курс лекций. — М.: в/ч 33965, 1997. — 317 с., ил.

3. *Норенков И.П., Трудоношин В.А.* Телекоммуникационные технологии и сети. — М.: МГТУ им. Н.Э.Баумана, 1999. — 432 с., ил.

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

Надійшла до редакції 19.02.2007