ISSN 2707-1898 (print)

Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
https://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2021.03.099
Article received 11.05.2021 p.
Article accepted 01.06.2021 p.
UDK 004.421:519.15:621.372

Correspondence author
V. V. Riznyk
rvv@polynet.lviv.ua

В. В. Різник, Д. Ю. Скрибайло-Леськів, В. М. Бадзь, С. І. Глод, Ю.-М. Кулик, В. В. Лях, Н. Б. Романюк, К. І. Ткачук, В. В. Українець

Національний університет "Львівська політехніка", м. Львів, Україна

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ МОНОЛІТНОГО ТА ЦИКЛІЧНОГО ЗАВАДОСТІЙКИХ КОДІВ

Здійснено порівняльний аналіз ефективності монолітного та циклічного завадостійких кодів, побудованих на "ідеальних кільцевих в'язанках" (ІКВ), які становлять теоретичну основу для синтезу математичної моделі завадостійкого кодування даних, віддзеркалюючи властивості гармонійної розбудови реального простору. ІКВ – це кільцева послідовність цілих додатних чисел, які формують натуральний ряд на їх множині послідовним додаванням останніх. Модель ґрунтується на сучасній теорії комбінаторних конфігурацій, і може знайти широке наукове поле для розвитку фундаментальних і прикладних досліджень в області інформаційних та інфокомунікаційних технологій, пов'язаних з методами перетворення форми інформації, включаючи використання багатовимірних комбінаторних структур, алгоритмів синтезу кодів з урахуванням особливостей кожного з них залежно від критеріїв оптимізації та встановлених обмежень системи кодування даних. Монолітний ІКВ-код вигідно відрізняється від класичних кодів простотою виявлення та виправлення помилок завдяки формуванню дійсних кодових слів у вигляді нероздільних послідовностей однойменних символів, що дає змогу швидко розпізнавати помилкові та відновлювати правильні слова за мажоритарним принципом об'єднання усіх однойменних символів в єдиному пакті. Циклічний ІКВ-код належить до категорії завадостійких нероздільних кодів, які вигідно відрізняються від поліноміальних циклічних кодів спрощеними обчислювальними процедурами кодування-декодування, у той час як основною перевагою монолітного коду є його самокоректувальна спроможність з елементами машинного інтелекту. Обидва кластери завадостійких кодів становлять спільну математичну платформу для дослідження та формування двох різновидів систем кодування даних: 1) в мінімізованому базисі монолітних двійкових кодів у вигляді нероздільних пакетів однойменних символів з ваговими розрядами, значення яких відповідають числам ІКВ; 2) оптимізованих циклічних ІКВ-кодів. Виняткові властивості обох згаданих вище кодів є природним відображенням їх унікальності, що дає змогу вдосконалювати системи завадостійкого кодування, шифрування та швидкісного опрацювання інформації. Технічна унікальність монолітних ІКВ-кодів відкриває нові можливості для швидкого опрацювання великих масивів даних. У свою чергу, оптимізовані циклічні ІКВ-коди вигідно відрізняються від кодів БЧХ, завдяки спрощенню декодування, не поступаючись цим кодам за кількістю виявлених і виправлених помилок. Здійснено оцінювання ефективності систем кодування даних монолітним і циклічним ІКВ-кодами за завадостійкістю, потужністю методу, швидкістю пересилання даних.

Ключові слова: ідеальна кільцева в'язанка; оптимізація; коректувальна здатність; обчислювальна складність; продуктивність; векторні дані.

Вступ

Стрімкий розвиток інформаційних технологій швидко збагачується ефективними методами кодування даних, більшість з яких ґрунтуються на використанні математичних моделей синтезу та оптимізації систем кодування. У таких дослідженнях вагоме місце належить формуванню наборів вагових розрядів двійкового коду для розбудови системи кодування даних з поліпшеними технічними показниками за надійністю захисту від несанкціонованого доступу і природних завад. Одним зі способів боротьби з цим явищем є кодування даних за допомогою коректувальних кодів. Для підвищення завадостійкості збільшують довжину кодових комбінацій, що вимагає використання більшого часу та витраченої енергії на пересилання та опрацювання даних. Дослідження включають в себе застосування сучасних методів комбінаторної оптимізації, спрямованих на зменшення інформаційної надмірності для того, щоб спростити структуру системи кодування даних та зменшити довжину кодових сигналів без значного погіршення завадостійкого кодування. Варто зазначити, що поліпшення одних показників призводить до погіршення інших, тому під час оптимізації систем кодування доводиться знаходити вигідний компроміс поміж суперечливими чинниками для досягнення прийнятного рішення з урахуванням відповідних критеріїв та обмежень.

Актуальність вирішення проблеми полягає у розробленні загального підходу до здійснення порівняльного аналізу ефективності монолітного і циклічного ІКВ-кодів на спільній математичній платформі.

Постановка завдання дослідження – здійснити порівняльний аналіз монолітного і циклічного оптимізованих ІКВ-кодів за встановленими критеріями оптимізації та обмеженнями.

Об'єкт дослідження – кодові комбінації монолітного і циклічного оптимізованого ІКВ-кодів.

Предмет дослідження – метод порівняльного аналізу монолітного і циклічного оптимізованого ІКВ-кодів.

Мета роботи – розроблення методу порівняльного аналізу циклічних і монолітних коректувальних ІКВ-кодів, що дасть змогу обирати коди з відповідною характеристикою для поліпшення якісних показників системи кодування даних.

Для досягнення зазначеної мети потрібно виконати такі основні *завдання дослідження*:

- визначити показники для оцінки ефективності монолітних і циклічних оптимізованих ІКВ-кодів;
- здійснити порівняльний аналіз систем кодування даних монолітним і циклічним оптимізованим ІКВ-кодами;
- обговорити отримані результати дослідження та зробити відповідні висновки.

Наукова новизна отриманих результатів дослідження – вперше розроблено методику порівняння монолітних і циклічних ІКВ-кодів на спільній математичній платформі.

Практична значущість результатів дослідження – порівняльний аналіз монолітного і циклічного завадостійких ІКВ-кодів дає змогу обирати коди з відповідною характеристикою для поліпшення якісних показників системи кодування даних залежно від постановки задачі оптимізації за умов діяння шкідливих чинників впливу в мережах канального чи бездротового зв'язку.

Аналіз останніх досліджень та публікацій. Класична теорія завадостійких циклічних кодів обіймає широкий спектр методів подолання проблеми захисту даних від багатьох видів шкідливого впливу зовнішніх завад, що виникають під час діяння в системі зв'язку різного рівня інтенсивності електромагнітні поля, космічний шум та багато інших зовнішніх та внутрішніх завад. У зв'язку з цим актуальною проблемою постає дослідження й розроблення методів і алгоритмів підвищення надійності, живучості та достовірності інформаційних систем і процесів. Особливий інтерес представляє використання унікальних властивостей деяких типів комбінаторних конфігурацій, які в загальному випадку представляють собою комбінаторні системи інцидентності [7]. Поруч із застосовуванням класичних методів завадостійкого кодування [1], [2], [3], [10] актуальним завданням є дослідження потенційних можливостей нетрадиційних методів комбінаторної оптимізації систем завадостійкого кодування за спрощеними процедурами декодування без погіршення решти показників коду, таких як потужність, продуктивність, швидкість виявлення та виправлення помилок, рівень захисту від несанкціонованого доступу, спроможність опрацювання векторних даних тощо. Основна властивість циклічних кодів полягає в отриманні дозволених кодових комбінацій з початкового кодового слова шляхом циклічної перестановки його символів. Циклічні коди відносяться до різновиду поліноміальних кодів, які прийнято описувати за допомогою твірних поліномів, серед яких кодів особливе місце посідають коди, запропоновані Боузом, Чоудхурі і Хоквінгемом, або коди БЧХ [1]. Вони є узагальненням коду Хеммінга для випадку виправлення декількох незалежних помилок [9]. До класу БЧХ-кодів належать коди Голея [4] – для виправлення одноразових, подвійних і потрійних помилок, а також коди Файра [1], призначені для виявлення та виправлення серійних помилок. Інший підхід до оптимального кодування даних базується на використанні класичної теорії комбінаторних конфігурацій [7], таких як блок-схеми, різницеві множини, а також метод, який передбачає використання деяких властивостей розширених полів Ґалуа [14]

Окрему категорію завадостійких кодів становлять ІКВ-коди, до яких належать два основні типи кодових послідовностей – циклічні і монолітні надлишкові коди. На відміну від кодів БЧХ, завадостійкі ІКВ-коди обох типів формуються на спільній математичній платформі шляхом використання унікальних властивостей ІКВ, в структурі яких закладена ідея про зменшення природної інформаційної надмірності для того, щоб спростити систему. На рис. 1 наведено приклад кругової шкали з двома позначками, які нанесені нерівномірно з значеннями кутових відстаней за циклічним співвідношенням 1:2. Приклад ілюструє загальний принцип зменшення надмірності систем, який стосується проблеми подолання протиріччя між бажанням максимально спростити систему і прагненням поліпшення основної характеристики системи, вводячи штучно інформаційну надмірність.

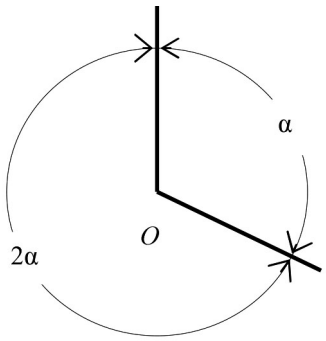

Рис. 1. Кругова шкала ідеального кутоміра з двома позначками, рознесеними на кутові відстані у співвідношенні 1:2

Відлік кутових відстаней можна продовжувати далі, здійснюючи більше одного повного обходу навколо точки *O*, обираючи початок і напрям відліку від однієї зі сторін центрального кута. Так, протягом першого повного оберту за годинниковою стрілкою схема відтворює кути α, 2α, $3\alpha = \alpha + 2\alpha$; а далі: $4\alpha = \alpha + 2\alpha + \alpha$, $5\alpha = 2\alpha + \alpha + 2\alpha$, $6\alpha = 2\alpha + \alpha + 2\alpha + \alpha$, … і т. д. Схема (рис. 1) демонструє один із способів зменшення надмірності системи шляхом розбиття кругової шкали на сумірні частини, кратні числам натурального ряду. Збільшуючи кількість нерівномірно розміщених позначок, приходимо до поняття багатозначної ідеальної кругової шкали, звідки випливає визначення ідеальної кільцевої в'язанки як базової математичної моделі синтезу оптимізованих кодів для ефективного опрацювання даних. Приклад ілюструє спосіб зменшення надмірності як загальносистемний підхід до оптимального вирішення проблеми збалансованої надмірності систем кодування даних з метою поліпшення їх основної характеристики, наприклад, завадостійкості оптимізованого циклічного ІКВ-коду, який дає змогу виявляти та виправляти помилки. При цьому досягається вигідний компроміс між суперечними вимогами до простоти та надійності.

Математичну модель ІКВ можна подати у вигляді послідовності $K_n = \{k_i, i = \overline{1,n}\}$ цілих додатних чисел, на якій всі можливі кільцеві суми вичерпують значення чисел натурального ряду від 1 до *N* всього *R* разів, де кільцевою вважається сума будь-якої кількості послідовно впорядкованих чисел ІКВ – від одного до $n-1$ [11].

Для встановлення взаємозв'язку між інформаційними параметрами ІКВ зручно подати кільцеві суми чисел на *n*-послідовності K_n у табличному вигляді (табл. 1).

Табл. 1. Кільцеві суми чисел на *n*-послідовності K_n

p_j	q_j							
	1	2	…	$l-1$	l	…	$n-1$	n
1	k_1	$\sum_{i=1}^{2} k_i$	…	$\sum_{i=1}^{l-1} k_i$	$\sum_{i=1}^{l} k_i$	…	$\sum_{i=1}^{n-1} k_i$	$\sum_{i=1}^{n} k_i$
2	S	k_2	…	$\sum_{i=2}^{l-1} k_i$	$\sum_{i=2}^{l} k_i$	…	$\sum_{i=2}^{n-1} k_i$	$\sum_{i=2}^{n} k_i$
…	…	…	…	…	…	…	…	…
$l-1$	$\sum_{i=l-1}^{n-1} k_i + k_1$	$\sum_{i=l-1}^{n} k_i + k_1 + k_2$	…	k_{l-1}	$k_{l-1} + k_1$	…	$\sum_{i=l-1}^{n-1} k_i$	$\sum_{i=l-1}^{n} k_i$
l	$\sum_{i=l}^{n-1} k_i + k_1$	$\sum_{i=l}^{n} k_i + k_1 + k_2$	…	S	k_l	…	$\sum_{i=l}^{n-1} k_i$	$\sum_{i=l}^{n} k_i$
…	…	…	…	…	…	…	…	…
$n-1$	$k_{n-1} + k_n + k_1$	$k_{n-1} + k_n + k_1 + k_2$	…	$k_{n-1} + k_n + \sum_{i=1}^{l-1} k_i$	$k_{n-1} + k_n + \sum_{i=1}^{l} k_i$	…	k_{n-1}	$k_{n-1} + k_n$
n	$k_n + k_1$	$k_n + k_1 + k_2$	…	$k_n + \sum_{i=1}^{l-1} k_i$	$k_n + \sum_{i=1}^{l} k_i$	…	S	k_n

Усі клітки таблиці за винятком тих, що розміщені зліва від діагональних, заповнені різними числами натурального ряду 1, 2, …, $S = n^2 - (n-1)$, а сума чисел, що знаходяться в діагональних клітках таблиці, дорівнює максимальному числу $S = N + 1$ цього ряду. У загальному випадку кількість однакових кільцевих сум в клітинках таблиці, окрім останнього рядка, може зустрічатися рівно *R* разів. Тоді ІКВ $(k_1, k_2, ..., k_i, ... k_n)$ буде описуватися інформаційними параметрами *S*, *n*, *R*, які взаємопов'язані математичною формулою:

$$R(S-1) = n(n-1). \qquad (1)$$

Методи синтезу математичних моделей ІКВ-кодів можна розділити за кількома категоріями стосовно обчислювальної складності. До найпростіших належать методи спрямованого перебору комбінацій на множині завчасу впорядкованих або частково-впорядкованих масивів чисел. Ці методи базуються на здійсненні логічних процедур покрокового нарощування довжини цілочислових наборів, дотримуючись правила неповторюваних сум, утворених послідовним додаванням чисел в наборі. Метод спрямованого перебору полягає в послідовному дописуванні до меншого числа збільшеного на одиницю числа з обчисленням числових значень утворених сум з двох, трьох, і т.д. наборів та перевіркою послідовностей на предмет отримання множини неповторюваних сум на кожному новому кроці нарощування їх довжини. Алгоритм закінчує побудову, коли кількість чисел в послідовності досягне встановленого значення, а загальна сума цих чисел буде рівною теоретично визначеній їх сумі. До складніших методів синтезу ІКВ належать алгоритми асиметричних розгалужень, супровідних матриць та множників, кожен з яких має свої особливості, що відрізняють їх за обчислювальною складністю і повнотою отриманих результатів [11].

Постановка завдання дослідження – порівняльний аналіз ефективності оптимізованих циклічного і монолітного ІКВ-кодів, який пов'язаний з подоланням протиріччя між потребою збільшення інформаційної надмірності зі збереженням потужності методу кодування та бажанням спростити складність процедур кодування-декодування. Для обговорення результатів дослідження необхідно висвітлити переваги та виявити слабі сторони порівнюваних кодів для визначення напрямків їх використання в інформаційно-комунікаційних системах. Комбінаторна оптимізація систем кодування даних може здійснюватися за різними критеріями залежно від конкретно поставлених вимог до якісних показників, наприклад, підвищення швидкодії, розширення діапазону кодування, зменшення енергетичних витрат тощо.

Результати дослідження та їх обговорення

1. ***Характеристика монолітних ІКВ-кодів.*** Під монолітним розуміємо код, дозволені комбінації якого складаються з двох різнойменних пакетів однойменних символів, що знаходяться один поруч одного. Конфігурація монолітних кодів може набувати вигляду ланцюга, кільця, або розгалуженого дерева. Якщо множина ваг двійкових розрядів, разом з множиною сум поруч розміщених вагових розрядів, вичерпує значення чисел натурального ряду від 1 до суми усіх двійкових ваг, це – монолітний ІКВ-код.

На відміну від традиційних двійкових кодів, монолітний код вигідно відрізняється простотою корегування кодових слів, бо поява хоча б одного символу "1" серед нулів, або "0" серед одиниць у прийнятій кодовій комбінації вказує на помилку. Помилка не виявляється тільки в тих випадках, коли хибний сигнал виникає на межі між пакетами нулів та одиниць. Решта випадків є контрольованими, що дає змогу автоматично виявляти та виправляти помилки за мажоритарним принципом "монолітності" групування однойменних символів. Завадостійкість *n*-розрядного монолітного коду можна оцінити за співвідношенням загальної кількості можливих помилкових кодових комбінацій до числа всіх дозволених комбінацій довжиною *n* бітових розрядів. Для евристичної оцінки аналізується співвідношення числа $N(n,r)$ кодових слів, які можна виявити $N_1(n,r)$, або виправити $N_2(n,r)$, до кількості усіх можливих і-розрядних кодових комбінацій, де *r* – кількість помилкових символів у кодовому слові. З урахуванням рівномірного закону розподілу ймовірностей появи випадкових символів завадостійкість монолітного коду визначається такими залежностями:

$$N_{1,2}(n,r)=\frac{1}{C_n^r}\begin{cases}C_{n-4}^r, r<n-4;\\ C_{n-8}^r, r<n-8.\end{cases} \quad (2)$$

У формулах (2) кількість сполучень із (n–4) і (n–8) по r в чисельнику зумовлено числом розрядів на межі стикування різнойменних пакетів, поза зоною яких є можливість виявити або виправити хибні символи відповідно. Ці формули встановлюють нижню границю для оцінки завадостійкості монолітного коду. Результати дослідження ефективності монолітного коду щодо виявлення $N_1(n,r)$ та виправлення $N_2(n,r)$ помилок за евристичними оцінками наведено в табл. 2, а на рис. 2 – відповідні графіки зростання завадостійкості коду за спроможністю виявлення одноразових r=1 та виправлення одно-, дво- r=2, і триразових r=3 помилок, залежно від числа n розрядів.

Табл. 2. Ефективність монолітного коду за евристичними оцінками

$r=1$	Кількість розрядів монолітного коду, n							
	5	10	15	20	25	30	40	50
C_{n-4}^1	1	6	11	16	21	26	36	46
C_{n-8}^1	-	2	7	12	17	22	32	42
N_1, %	20,0	60,0	73,3	80,0	84,0	86,6	90,0	92,0
N_2, %	-	20,0	46,7	60,0	68,0	73.3	80,0	84,0
$r=2$	Кількість розрядів монолітного коду, n							
	5	10	15	20	25	30	40	50
C_{n-4}^2	-	15	55	120	210	325	630	1035
C_{n-8}^2	-	1	21	66	136	231	496	861
N_1, %	-	33,3	52,4	63,2	70,0	74,7	80,7	84,5
N_2, %	-	2,2	20,0	34,7	45,3	53,1	63,6	70,3
$r=3$	Кількість розрядів монолітного коду, n							
	5	10	15	20	25	30	40	50
C_{n-4}^3	-	20	165	560	1330	2600	7140	15180
C_{n-8}^3	-	-	35	220	680	1540	4960	11480
N_1, %	-	16,7	36,3	49,1	57,8	64,0	72,3	77,4
N_2, %	-	-	7,7	19,3	29,6	37,9	50,2	58,6

З аналітичного розгляду графіків (рис. 2) випливає, що зі збільшенням числа n розрядів, починаючи від n=5 до 50 для виявлення $N_1(n)$ одноразових (r=1) помилок і від n=10 до 50 – для їх виправлення $N_2(n$, ефективність векторного монолітного коду зростає за експоненціальним законом.

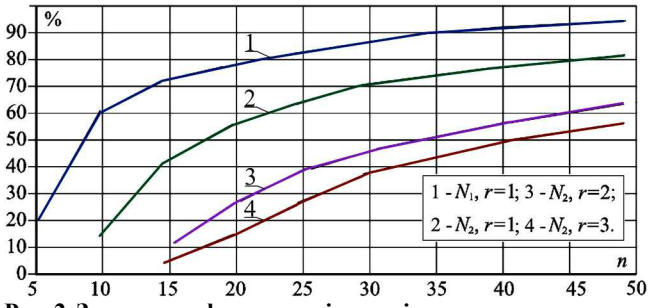

Рис. 2. Зростання ефективності монолітного коду щодо спроможності виявлення одноразових та виправлення одно-, дво-, і 3-разових помилок залежно від кількості n розрядів

Зі збільшенням розрядності коду від n=15 до 50 для виправлення дворазових (r=2), і триразових (r=3) помилок відповідно, ефективність векторного монолітного коду щодо виправлення $N_2(n$ помилок зростає дещо меншими темпами за експоненціальним законом, досягаючи при n =50 рівня 70,3% для виправлення дворазових (r=2), і 58,6% – для виправлення триразових (r=3) помилок відповідно. Обчислення кількості випадків $x(n)$ виявлення помилкових комбінацій n-розрядного кільцевого монолітного коду зручно здійснювати за числовою трапецією (табл. 3).

Табл. 3. Обчислення кількості $x(n)$ хибних символів кільцевого монолітного коду за числовою трапецією

Розрядність, n	Коефіцієнти для обчислення $x(n)$																					Сума, Σ	$x(n)=n$ Σ
4								1	+	0	+	1										2	8
5							2	+	1	+	1	+	2									6	30
6						3	+	2	+	2	+	2	+	3								12	72
7					4	+	3	+	3	+	3	+	3	+	4							20	140
8				5	+	4	+	4	+	4	+	4	+	4	+	5						30	240
9			6	+	5	+	5	+	5	+	5	+	5	+	5	+	6					42	378
10		7	+	6	+	6	+	6	+	6	+	6	+	6	+	6	+	7				56	560
11	8	+	7	+	7	+	7	+	7	+	7	+	7	+	7	+	7	+	8			72	792

У двох колонках справа наведено результати обчислення суми Σ коефіцієнтів і кількості $x(n)$ хибних символів n-розрядного кільцевого монолітного коду. Таблиця має вигляд рівносторонньої трапеції, усі клітинки якої заповнені паралельними до її сторін рядами натуральних чисел із покроковим зміщенням зверху – вниз, утворюючи струнку систему досконало впорядкованих всередині трапеції симетричних числових трикутників різних розмірів. Вона дає змогу визначити кількість хибних символів, які виявляються для n-розрядного монолітного коду шляхом додавання коефіцієнтів $x(n)$ відповідного рядка. Наприклад, для 10-розрядного ($n=10$) кільцевого монолітного коду кількість $x(n)$ хибних символів за числовою трапецією становить $10\cdot 56=560$, а його ефективність $N_1=x/n\cdot S=\ 560/10\cdot 91=60{,}8\%$, де $S=n(n-1)+2$. Цей результат добре узгоджується з евристичною оцінкою (60 %) ефективності коду з цими параметрами. У дисертаційній роботі [8] показано, що результати обчислення ефективності монолітного коду двома методами практично збігаються зі збільшенням розрядності, хоча обчислення за евристичними оцінками дають дещо нижчі показники.

Метод трапеції вигідно відрізняється від класичних систем оцінювання ефективності кодування даних можливістю здійснення аналізу ймовірнісного розподілу хибних символів залежно від місця їх появи всередині пакетів. Окрім цього, монолітний ІКВ-код дає змогу підвищити швидкість пересилання багатовимірних масивів даних шляхом кодування векторних сигналів у вигляді t-вимірних кортежів, де кодове слово може містити t-вимірний вектор даних. Прикладом двовимірної ІКВ є набір векторів ((1,0), (0,1), (0,2)), де модулем (довжиною циклу) першої складової вектора є 2, а другої – 3. Обчисливши всі кільцеві вектор-суми з урахуванням числових значень відповідних модулів, легко перевірити, що вони вичерпують множину координат двовимірної решітки 2×3: (1,0), (1,1), (1,2); (0,0), (0,1), (0,2). Кодуванню вектора ((1,0) відповідає комбінація 100, вектора (1,1) – 110, вектора (1,2) – 101, вектора (0,0) – 011, вектора (0,1) – 010, вектора (0,2) – 001. В цьому випадку двовимірний монолітний ІКВ-код дає змогу досягнути взаємно однозначної відповідності множини двовимірних векторів в алфавіті системи ко-

ординатної сітки 2×3 на поверхні тора множині двійкових кодових комбінацій. Аналогічно здійснюється синтез та дослідження монолітних ІКВ-кодів у багатовимірних просторових системах координат. До інших вагомих переваг монолітних ІКВ-кодів належить можливість кодування багатовимірних даних у вигляді імпульсних сигналів з дискретизацією за довжиною і фазою в межах одного часового періоду, пропорційного сумі чисел обраної моделі ІКВ, що дає змогу швидко здійснювати вигідне налаштування системи пересилання векторних даних за встановленими критеріями надійності, швидкодії і рівня завадостійкості.

Виправлення помилок має ймовірний характер і залежить від місця їх появи у кодовій комбінації. Якщо хибний символ з'являється на відстані двох розрядів від місця розмежування різнойменних пакетів, виправлення одиничних помилок на приймальній стороні можливе з ймовірністю 0,5. В міру віддалення від місця розмежування ця ймовірність зростає також для багаторазових помилок, які можна виявляти та виправляти за мажоритарним принципом щільності згрупованих символів у кожній групі однойменних символів.

Монолітний ІКВ-код набуває статусу оптимального за обмежень на правила формування кодових комбінацій додаванням ваг за кільцевою структурою, вичерпуючи значення чисел натурального ряду. Ця унікальна властивість дає змогу невеликою кількістю базових структурних елементів розбудовувати оптимізовані системи різного призначення, наприклад, пристроїв кодування [11], с. 104–108], запису-відтворення інформації [11], с. 117], формування команд [11], с. 118–120], перетворення інформації [11], с. 121–123], автоматичних багатоточкових регістраторів швидкості зміни параметрів [11], с. 132–135], фазорегуляторів [11], с. 135–140], антенних систем [11], с. 140–142], багатофакторних планів експерименту [11], с. 142–145], систем менеджменту інтелектуальних інформаційних технологій [13], с. 159–169], кодування та опрацювання векторних даних [12], с. 131–138]. Отже, монолітний ІКВ код дає змогу розробляти системи кодування даних з мінімізованою надмірністю за наявності обмежень на спосіб формування вагових значень дозволених кодових комбінацій для кодування даних у вигляді "пачок" однойменних символів. Даний код доцільно використовувати для забезпечення надійного зв'язку при космічних дослідженнях, супутниковій геодезії, планетарній геофізиці, проектуванні радіотелескопів, радіолокаторів та є зручним засобом конструювання та апробації радіосистем різного призначення, а також для шифрування даних [5]та в криптосистемах інформаційної безпеки [6]

2. ***Характеристика циклічних ІКВ-кодів.*** Циклічні ІКВ-коди складають великий клас нероздільних лінійних кодів, які вигідно відрізняються від поліноміальних кодів спрощеним алгоритмом обчислення під час кодування та декодування повідомлень. Класичні коди цього класу вимагають здійснення матричних обчислень під час декодування на приймальній стороні каналу зв'язку, включаючи операції ділення поліномів, якими описуються прийняті кодові слова, на твірний поліном для визначення вагових значень синдромів. При цьому часова складність декодування зростає зі збільшенням довжини коду за поліноміальним законом [1]. Циклічні ІКВ-коди вигідно відрізняються від класичних за обчислювальною складністю. Особливий інтерес становлять оптимізовані циклічні коди, які на відміну від решти ІКВ-кодів характеризуються вищою коректувальною здатністю.

У роботі [11], с. 101–104] і [12], с. 126–131] показано, що коректувальна здатність циклічного ІКВ-коду зростає зі збільшенням різниці між n і R, досягаючи максимального значення при $S = 2n$ і $R = n/2$ (якщо n – парне число), або $R = (n-1)/2$ (якщо n – непарне). Побудовані на підставі цих співвідношень параметри циклічних ІКВ-кодів дають змогу виявляти до $n-1$ або виправляти до $n/2-1$ помилок для парних і виявляти до n або виправляти до $(n-1)/2$ помилок для непарних значень n [11], с. 104]. Там же наведено приклад розрахунку коректувальної здатності ІКВ-кодів з параметрами: 1) $n = 6$, $R = 1$; 2) $n = 15$, $R = (n-1)/2 = 7$; 3) $n = 16$, $R = n/2 = 8$. У цьому переліку перший код поступається двом наступним за коректувальною спроможністю. За однакової довжини S= 31 комбінацій усіх трьох ІКВ-кодів, максимальне кількість помилок, які можна виявляти або виправляти за допомогою першого з вказаних кодів, дорівнює відповідно 9 та 4, водночас як кожен із інших двох дає змогу виявляти до 15 і виправляти до 7 помилок, тобто в 1,75 разів більше, ніж для першого коду. У табл. 4 наведено характеристику завадостійкого ІКВ-коду з оптимізованими параметрами $S = 2n-1$, $n = 2R$.

Табл. 4. Характеристика циклічного ІКВ-коду з оптимізованими параметрами $S = 2n-1$, $n = 2R$

Параметри оптимізованого ІКВ-коду				Кількість виявлених t_1 і виправлених t_2 помилок		Показники завадостійкості ІКВ-коду. Здатність:	
						виявлення помилок	виправлення помилок
S	n	R	P	t_1	t_2	(t_1/S), %	(t_2/S), %
11	6	3	22	5	2	45,4	18,2
15	8	4	30	7	3	46,7	20,0
19	10	5	28	9	4	47,3	21,1
23	12	6	46	11	5	47,8	21,7
27	14	7	54	13	6	48,1	22,2
31	16	8	62	15	7	48,4	22,6
35	17	8	70	17	8	48,6	22,9
39	20	10	78	19	9	48,7	23,1
123	62	31	246	61	30	49,6	24,4
127	64	32	254	63	31	49,6	24,4

З табл. 4 випливає, що за дотримання співвідношення $S = 2n-1$, $n = 2R$ між числовими значеннями параметрів S, n, R циклічних ІКВ-кодів спостерігається зростання їх коректувальної спроможності від 18,2 % для кодів довжиною $S = 11$ до 24,4 % – для $S = 123$ зі збільшенням довжини кодових комбінацій, наближаючись до свого максимального теоретичного значення – 50 % щодо здатності виявлення і 25 % – виправлення помилкових символів. Темпи цього зростання дещо сповільнюються зі збільшенням S. Це дає підстави говорити про недоцільність використання циклічних ІКВ-кодів високих порядків з-за швидкого збільшення структурної та інформаційної надмірності системи, що не виправдує рівня досягнутого результату, враховуючи зростання витрат на опрацювання даних. Окрім цього, циклічні коди, на відміну від монолітно-групових, не пристосовані для оптимального кодування та швидкого опрацювання наборів даних.

Обговорення результатів дослідження. Порівняльний аналіз ефективності монолітного та циклічного завадостійких кодів на спільній математичній основі дає змогу глибше зрозуміти теоретичний взаємозв'язок монолітних та циклічних кодів, які відрізняються між собою за коректувальними властивостями. Структурна особливість монолітних ІКВ-кодів полягає в тому, що всі дозволені комбінації формуються у вигляді пакетів однойменних символів з ваговими розрядами, множина лінійних сум яких вичерпує значення чисел натурального ряду фіксовану кількість разів. Це збагачує можливості їх використання для підвищення надійності пересилання даних шляхом кодування повідомлень однакового змісту кількома різними способами, зберігаючи монолітність пакетів однойменних символів. До інших переваг варто віднести можливість кодування в одному n-розрядному кодовому слові набору даних з векторними ваговими розрядами. Монолітні ІКВ-коди характеризуються не тільки високою швидкістю пересилання повідомлень, але й можливістю виправлення помилок за мажоритарним принципом збереження неподільності пакетів однойменних символів всередині дозволених кодових послідовностей. Однак ці коди потребують верифікації для визначення їх ефективності за умов діяння завад різного типу і рівня інтенсивності. На відміну від монолітних, циклічні двійкові коди з оптимізованими параметрами ІКВ набувають високої завадостійкості щодо виявлення та виправлення помилок за умов діяння зовнішніх завад, забезпечуючи виявлення та виправлення до половини і чверті помилкових символів від довжини $S= n(n–1)+1$ коду відповідно. Внаслідок порівняння технічних характеристик обох кодів можна відзначити доцільність використання монолітних кодів для формування сигналів керування системним об'єктом на множині $n(n\text{-}1)$ її фіксованих станів, зменшивши у порівнянні з традиційними методами управління кількістю керованих кодом комбінацій в n-1 разів. Натомість, циклічні коди з оптимізованими параметрами ІКВ вигідно відрізняються від монолітних вищими показниками щодо завадостійкості. зі збільшенням розрядності кодових комбінацій спроможність цих кодів виявляти помилки наближається до половини від кількості усіх символів циклічного коду, і виправляти – до чверті, наближаючись до теоретично досяжного рівня 50 і 25% відповідно від довжини кодових комбінацій. При цьому для виявлення та виправлення кожної нової помилки потрібно збільшувати довжину коду відповідно на два і чотири розряди, що призводить до зростання надмірності коду. Оптимальне рішення базується на знаходженні вигідного компромісу між потрібною завадостійкістю коду та вимушеним збільшенням його надмірності та часу декодування, що, водночас, пов'язано з виконанням додаткових процедур порівняння прийнятих кодових комбінацій, у яких можуть бути хибні символи, з правильними кодовими словами на приймальному кінці каналу зв'язку.

Підсумовуючи результати дослідження, можна бачити, що обидва коди характеризуються різними властивостями, кожен з яких має свої плюси для успішного використання в інформаційних системах кодування даних залежно від конкретних умов постановки задачі та подолання суперечності між різними чинниками впливу для досягнення вигідного компромісного рішення.

Висновки

Встановлено, що основні переваги монолітного ІКВ-коду порівняно з циклічним – вища ефективність опрацювання багатовимірних масивів даних, можливість захисту інформації від несанкціонованого доступу, швидке виправлення помилок. Код може знайти застосування в інформаційних технологіях для побудови систем кодування багатовимірних масивах даних та опрацювання великих обсягів інформації. Монолітний ІКВ-код характеризується пакетуванням однойменних символів у вигляді суцільних блоків. Останні придатні для кодування даних за кількома рівнями одночасно, що розширює можливості шифрування та захисту закодованих даних від несанкціонованого доступу. З'ясовано, що використання комбінаторних методів оптимізації монолітних і циклічних кодів, побудованих на спільній математичній моделі у вигляді ідеальної кільцевої в'язанки (ІКВ), вигідно відрізняються від класичних методів синтезу завадостійких кодів більшими можливостями опрацювання масивів даних без погіршення інших показників інформаційних систем, що дає змогу підвищити ефективність систем завадостійкого кодування, зменшивши часову складність обчислювальних процедур декодування. Опрацювання векторних даних дає змогу розробляти оптимальні інформаційні технології на підставі принципово нових систем перетворення форми інформації, у яких, на відміну від стандартних кодів, позиціям коду присвоюються відповідні значення необхідної кількості наборів ознак, поданих у вигляді впорядкованих кортежів за кількістю атрибутів. Це уможливлює кодування та пересилання однією кодовою комбінацією одночасно множини потрібної кількості ознак, яка відповідає параметрам вибраного ІКВ-коду, що відкриває перспективу створення принципово нових векторних інформаційних технологій з можливістю швидкісного опрацювання масивів даних без значного ускладнення апаратно-технічної бази та алгоритмічно-програмних засобів. Розширення сфери застосування монолітних і циклічних ІКВ-кодів розкриває нові перспективи для розвитку комбінаторних методів оптимізації інформаційно-комунікаційних систем.

References

[1] BCH code. (2020). *From Wikipedia. The Free Encyclopedia*. Retrieved from: https://en.wikipedia.org/wiki/BCH_code

[2] Blahut, R. E. (1986). Theory and Practice of Error Control Codes. Moscow: Mir, 576 p. [In Russian].

[3] Error correction code. (2021). *Wikipedia. The Free Encyclopedia*. Retrieved from: https://en.wikipedia.org/wiki/Error_correction_code

[4] Golay Code. (2021). Wolfram MathWorld the webs most extensive mathematics resource. Retrieved from: http://mathworld.wolfram.com/GolayCode.html

[5] Gryciuk, Y., & Grytsyuk, P. (2016). Implementation details for the cipher key generation Cardano permutation. Modern Problems of Radio Engineering, Telecommunications and Computer Science. Proceedings of the 13th International Conference on TCSET2016, 498–502. https://doi.org/10.1109/TCSET.2016.7452098

[6] Gryciuk, Yu., & Grytsyuk, P. (2015). Perfecting of the matrix Affine cryptosystem information security. Computer Science and Information Technologies: Proceedings of Xth International Scientific and Technical Conference (CSIT2015), 14–17 September, 2015, 67–69. https://doi.org/10.1109/stc-csit.2015.7325433

[7] Hall, M. Jr. (1986). Combinatorial Theory. John Wiley & Sons, 464 p. [In Russian].
[8] Kis, Y. P. (1997). Modeling and synthesis of protective codes by ideal ring bundles. *The thesis for Ph.D. degree*. State University "Lvivska Politechnika". Lviv, 16 p. [In Ukrainian].
[9] Macleod, M. D. (1993). Coding. In *Telecommunications Engineers Reference Book*. Cyclic Code. Retrieved from: https://www.sciencedirect.com/topics/engineering/cyclic-code
[10] Peterson, W. Wesley, & Weldon, E. J. (1972). Error-correcting codes, The MIT Press; secondedition, 560 p.
[11] Riznyk, V. V. (1989). *Synthesis of optimal combinatorial systems*. Lviv: Vyshcha shkola, 168 p. [In Ukrainian].
[12] Riznyk, V. V. (2019). Combinatorial optimization of multidimensional systems. *Models of multidimensional intelligent systems*. Lviv: Publishing Lvivskoji Politekhniky, 168 p. [In Ukrainian].
[13] Riznyk, V. V. (2021). Models of intelligent information management technologies. In the book: *Theories, Concepts, Implementation* (*Eds. Marian Duczmac, Tetyana Nestorenko*) *Monograph*. Opole: The Academy of Management and Administration in Opole, 2021.394, 159–169.
[14] Rotman, J. (1998). Galois Extensions. Universitext, 79–82. https://doi.org/10.1007/978-1-4612-0617-0._15

V. V. Riznyk, D. Y. Skrybajlo-Leskiv, V. M. Badz, C. I. Hlod, V. V. Liakh, Y.-M. Kulyk, N. B. Romanjuk, K. I. Tkachuk, V. V. Ukrajinets

Lviv Polytechnic National University, Lviv, Ukraine

COMPARATIVE ANALYSIS OF MONOLITHIC AND CYCLIC NOISE-PROTECTIVE CODES EFFECTIVENESS

Comparative analysis of the effectiveness of monolithic and cyclic noise protective codes built on "Ideal Ring Bundles" (IRBs) as the common theoretical basis for synthesis, researches and application of the codes for improving technical indexes of coding systems with respect to performance, reliability, transformation speed, and security has been realized. IRBs are cyclic sequences of positive integers, which form perfect partitions of a finite interval of integers. Sums of connected IRB elements enumerate the natural integers set exactly *R*-times. The IRB-codes both monolithic and cyclic ones forming on the underlying combinatorial constructions can be used for finding optimal solutions for configure of an applicable coding systems based on the common mathematical platform. The mathematical model of noise-protective data coding systems presents remarkable properties of harmonious developing real space. These properties allow configure codes with useful possibilities. First of them belong to the self-correcting codes due to monolithic arranged both symbols "1" and of course "0" of each allowed codeword. This allows you to automatically detect and correct errors by the monolithic structure of the encoded words. IRB codes of the second type provide improving noise protection of the codes by choosing the optimal ratio of information parameters. As a result of comparative analysis of cyclic IRB-codes based with optimized parameters and monolithic IRB-codes, it was found that optimized cyclic IRB codes have an advantage over monolithic in relation to a clearly fixed number of detected and corrected codes, while monolithic codes favorably differ in the speed of message decoding due to their inherent properties of self-correction and encryption. Monolithic code characterized by packing of the same name characters in the form of solid blocks. The latter are capable of encoding data on several levels at the same time, which expands the ability to encrypt and protect encoded data from unauthorized access. Evaluation of the effectiveness of coding optimization methods by speed of formation of coding systems, method power, and error correcting has been made. The model based on the combinatorial configurations contemporary theory, which can find a wide scientific field for the development of fundamental and applied researches into information technolodies, including application multidimensional models, as well as algorithms for synthesis of the underlying models.

***Keywords**:* Ideal Ring Bundle; optimization; corrective ability; computational complexity; performance; vector data.

Інформація про авторів:

Різник Володимир Васильович, д-р техн. наук, професор, кафедра автоматизованих систем управління. **Email:** rvv@polynet.lviv.ua; https://orcid.org/0000-0002-3880-4595
Скрибайло-Леськів Даніель Юрійович, здобувач, асистент, кафедра автоматизованих систем управління. **Email:** skrybajlo.d.yu@gmail.com
Бадзь Вікторія Мирославівна, студентка, кафедра автоматизованих систем управління. **Email:** rvv@polynet.lviv.ua
Глод Сергій Ігорович, студент, кафедра автоматизованих систем управління. **Email:** rvv@polynet.lviv.ua
Лях Вікторія Валеріївна, студентка, кафедра автоматизованих систем управління. **Email:** rvv@polynet.lviv.ua
Кулик Юрій-Марко Романович, студент, кафедра автоматизованих систем управління. **Email:** rvv@polynet.lviv.ua
Романюк Наталія Богданівна, студентка, кафедра автоматизованих систем управління. **Email:** rvv@polynet.lviv.ua
Ткачук Катерина Ігорівна, студентка, кафедра автоматизованих систем управління. **Email:** rvv@polynet.lviv.ua
Українець Василь Васильович, студент, кафедра автоматизованих систем управління. **Email:** rvv@polynet.lviv.ua

Цитування за ДСТУ: Різник В. В., Скрибайло-Леськів Д. Ю., Бадзь В. М., Глод С. І., Кулик Ю.-М., Лях В. В., Романюк Н. Б., Ткачук К. І., Українець В. В. Порівняльний аналіз ефективності монолітного та циклічного завадостійких кодів. Український журнал інформаційних технологій. 2021, т. 3, № 1. С. 99–105.

Citation APA: Riznyk, V. V., Skrybajlo-Leskiv, D. Y., Badz, B. M., Hlod, C. I., Liakh, V. V., Kulyk, Y.-M., Romanjuk, N. B., Tkachuk, K. I., & Ukrajinets, V. V. (2021). Comparative analysis of monolithic and cyclic noise-protective codes effectiveness. *Ukrainian Journal of Information Technology*, *3*(1), 99–105. https://doi.org/10.23939/ujit2021.03.099