ISSN 2707-1898 (print)

Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2020.02.066
Article received 18.02.2020 p.
Article accepted 25.10.2020 p.
UDK 004.421:519.15:621.[372+391]

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

В. В. Різник, Д. Ю. Скрибайло-Леськів

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

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЦИКЛІЧНИХ КОДІВ МЕТОДАМИ КОМБІНАТОРНОЇ ОПТИМІЗАЦІЇ

Розглянуто методи підвищення ефективності циклічних кодів, побудованих на підставі комбінаторних конфігурацій типу "ідеальних кільцевих в'язанок" (ІКВ) за трьома чинниками – коректувальною здатністю, потужністю методу кодування та складністю процедури декодування. В основу методики покладено принцип комбінаторної оптимізації, який ґрунтується на алгебричній теорії впорядкованих цілочислових послідовностей з кільцевою структурою, причому усі числа разом з усіма сумами поруч розміщених чисел вичерпує значення чисел натурального ряду. Запропоновано два теоретично обґрунтовані підходи до підвищення завадостійкості циклічних кодів: впровадженням оптимізованого ІКВ-коду та монолітно-групового. Оптимізований циклічний ІКВ-код вигідно відрізняється від решти кодів цього класу вищою корегувальною здатністю при тій же довжині кодових слів. Оптимізовані ІКВ-коди становлять велику групу циклічних кодів, побудованих на комбінаторній різноманітності математичних моделей з добором відповідного співвідношення між параметрами коду для досягнення його заданих технічних характеристик. Завадостійкі монолітно-групові коди належать до групи самокоректувальних кодів з кільцевою структурою та ймовірнісною оцінкою рівня завадостійкості.

Ця властивість дає змогу за мажоритарним принципом миттєво виявляти певну частину, або усі хибні символи у кодовому слові. Здійснено математичні розрахунки для обчислення оптимізованих співвідношень між параметрами циклічних ІКВ-кодів, за яких вони досягають максимальної коректувальної спроможності. Розглянуто і проаналізовано алгоритм побудови та збільшення потужності методів кодування оптимізованих завадостійких ІКВ-кодів. Наведено конкретні приклади підвищення ефективності циклічних кодів методами комбінаторної оптимізації з відповідними розрахунками і таблицями. Проведено порівняльний аналіз ІКВ-кодів з кодами Голея та Боуза-Чоудхурі-Хоквінгема (БЧХ) за коректувальною здатністю, потужністю методу кодування та обчислювальною складністю процедур декодування. З'ясовано переваги та недоліки циклічних і кільцевих монолітно-групових ІКВ-кодів порівняно з класичними аналогами. Окреслено перспективи використання результатів дослідження в задачах інформаційно-комунікаційних технологій.

Ключові слова: комбінаторна конфігурація, обчислювальна складність, коректувальний код, оптимізований циклічний код, ефективність коду, самокоректувальний монолітно-груповий код.

Вступ

Сучасний розвиток інформаційних технологій пов'язаний з дослідженням методів поліпшення систем кодування та опрацювання інформації. Вагомого значення набувають питання розроблення критеріїв оцінки їх якості, реалізації принципів оптимізації, методів якісного контролю, класифікації, кодування й забезпечення достовірності інформації. 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 [15]. Поруч із застосовуванням класичних методів завадостійкого кодування [6], [25] актуальним завданням є дослідження потенційних можливостей нетрадиційних методів комбінаторної оптимізації систем завадостійкого кодування за спрощеними процедурами декодування без погіршення решти показників циклічного коду, в т. ч. потужності цього коду, скорочення часу виявлення та виправлення помилок.

Для формування ефективних систем кодування та декодування циклічних кодів використано інциденті числові конфігурації типу ІКВ з унікальними комбінаційними властивостями [18]. Велику групу оптимальних комбінаторних кодів цього класу складають надлишкові двійкові коди, які можуть не тільки виявляти, але й виправляти теоретично будь-яку кількість помилок простим порівнянням прийнятих комбінацій з табличним списком безпомилкових кодових слів. Асимптотична оцінка часової складності процедури декодування таких кодів не перевищує $O(n^2)$, тоді як складність цих процедур для класичних циклічних кодів з еквівалентними параметрами щонайменше – $O(n^3)$.

Складність кодування-декодування класичних кодів пояснюється потребою здійснення певної послідовності матричних обчислень на приймальній стороні каналу зв'язку, в т.ч. й операції ділення поліномів, якими описуються прийняті кодові слова, на твірний поліном для визначення вагових значень синдромів [9]. Зі збільшенням довжини коду складність декодування класичних циклічних кодів зростає за поліноміальним законом. Тому декодування повідомлень, закодованих циклічним ІКВ-кодом, здійснюється швидше, ніж кодами Голея [35], Боуза-Чоудхурі-Хоквінгема [4] та іншими кодами цього класу, а темпи зростання часової складності декодування класичних кодів вищі, ніж для оптимізованих ІКВ-кодів.

Об'єкт дослідження – завадостійке кодування даних за допомогою циклічних кодів.

Предмет дослідження – комбінаторні методи і засоби підвищення ефективності циклічних кодів для завадостійкого кодування даних.

Мета роботи – підвищення ефективності циклічних кодів методами комбінаторної оптимізації, які дадуть змогу здійснити завадостійке кодування даних.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- проаналізувати останні дослідження та публікації, які стосуються методів завадостійкого кодування даних, насамперед циклічних кодів;
- охарактеризувати циклічні завадостійкі коди, визначити методи підвищення їх ефективності;
- здійснити порівняльний аналіз класичних кодів з циклічним ІКВ-кодом;
- розробити комбінаторний метод побудови оптимізованих циклічних ІКВ-кодів, які дадуть змогу здійснити завадостійке кодування даних;
- обговорити отримані результати дослідження та зробити відповідні висновки.

Наукова новизна отриманих результатів дослідження – розроблено метод підвищення ефективності циклічних кодів, побудованих на підставі комбінаторних конфігурацій типу "ідеальних кільцевих в'язанок" (ІКВ) за такими чинниками, як коректувальною здатністю, потужністю методу кодування та складністю процедури декодування. Проведено порівняльний аналіз ІКВ-кодів з кодами Голея та Боуза-Чоудхурі-Хоквінгема (БЧХ) за коректувальною здатністю, потужністю методу кодування та обчислювальною складністю процедур декодування. З'ясовано переваги та недоліки циклічних і кільцевих монолітно-групових ІКВ-кодів порівняно з класичними аналогами.

Практична значущість результатів дослідження – наведено конкретні приклади підвищення ефективності циклічних кодів методами комбінаторної оптимізації з відповідними розрахунками і таблицями, окреслено перспективи використання результатів дослідження в задачах інформаційно-комунікаційних технологій.

Аналіз останніх досліджень та публікацій. Під завадостійкими кодами розуміють коди, що дають змогу знаходити і виправляти помилки, що виникають в результаті впливу завад. Завадостійкість кодування забезпечується за рахунок введення надлишковості в кодові комбінації. Теоретичною базою ефективного використання надлишковості, що вводиться, є теорія завадостійкого кодування, яка для кожного конкретного каналу дає змогу вибрати найбільш ефективний метод виявлення та виправлення помилок.

Теорія завадостійкого кодування даних заснована на використанні глибокого апарату сучасних абстрактних розділів математики і передусім алгебри. Циклічний код – одна з найбільш яскравих ілюстрацій того, як розумне застосування результатів абстрактної математичної теорії дає можливість створити прості й ефективні технічні пристрої – кодери і декодери. В світовій літературі нараховується більше десятка монографій, присвячених теорії завадостійкого кодування. Першою і методично найбільш досконалою цього напряму є монографія У. Пітерсона "Коды, исправляющие ошибки" [26], видана в 1961 році, перекладена й видана російською мовою в 1964 році.

Питаннями розвитку теорії завадостійкого кодування займались такі зарубіжні фахівці як Р. Галлагер, У. Пітерсон, Е. Уелдон, А. Д. Вітербі, Д. К. Омура, Р. К. Боуз, Д. К. Рой-Чоудхурі, Е. Р. Берлекемп, Д. Мессі, І. С. Рід, Г. Соломон, Р. Блейхут, Д. Форні, К. Беруа, Д. Хагенауер, а також російські вчені Е. Л. Блох, В. Д. Колесник, В. О. Шварцман [31], Е. Т. Мірончиков, К. Ш. Зігангіров, В. В. Золотарев [39], Ю. П. Акулінічев [1], Е. М. Габідулін, В. В. Зяблов, А. Г. Зюко, С. Л. Портной та ін.

Наприклад, в роботах [1], [20], [26], [31], [39] систематично викладені методи і описані характеристики різних алгоритмів завадостійкого кодування. Розглянуто методи багатопорогового декодування даних для блокових і згорткових кодів, які мають технологічні переваги перед іншими алгоритмами корекції помилок і можуть знайти застосування в різних областях зв'язку, забезпечуючи при цьому високі характеристики декодування. У роботах [5], [8], [10], [19], [21] розглядаються методи захисту даних від помилок, які широко використовують в різних протоколах сучасних телекомунікаційних мереж.

У роботі [16] запропоновано підхід до забезпечення достовірності в процесі обміну інформацією в системах зв'язку і передачі даних (СЗіПД) комплексів радіомоніторингу за рахунок використання завадостійкого кодування (ЗК). Водночас, у роботах [2], [3] достатньо повно досліджено вплив навмисних завад на завадозахищеність засобів радіозв'язку із ЗК. Однак аналіз цих робіт показує, що розрахунки завадостійкості систем зв'язку (СЗ) та систем передачі інформації (СПІ) проведено тільки для сигналів з двійковою фазовою маніпуляцією. Можливості використання ЗК в СЗ та СПІ, а також критерії ефективності й шляхи підвищення ефективності СЗ та СПІ розглядаються в роботах [7], [13], [19], [20], [23], [33], [36], [37], [38]. Зокрема, у роботі [19] описано різні методи декодування блокових кодів і особливості реалізації алгебраїчних декодерів у вигляді спеціалізованих процесорів. Обговорення згорткових кодів проілюстровано результатами чисельного моделювання. Проте у них відсутні розрахунки ефективності ЗК для передач на підставі сигналів із частотною маніпуляцією (ЧМ) і ЗК.

У навчальному посібнику з теорії кодування [24] охочі до навчання можуть вивчити коригувальні коди, тобто коди, які виявляють і виправляють помилки, які виникають внаслідок дії шуму при зберіганні та передачі інформації. Основною проблемою тут є економне використання надмірності для досягнення необхідної завадостійкої передачі даних каналами з шумом або їх зберігання на деякому носії. Знання цього розділу необхідно для розробників сучасних електронних цифрових інформаційних систем. У посібнику з теорії та практики цифрового зв'язку [14], [19] окрім класичних алгоритмів декодування блокових і згорткових кодів детально розглянуто сучасні ідеї декодування з "м'яким рішенням", а також проведення ітеративного декодування даних.

У детальному довіднику [32] описані основні методи кодування даних, такі як метод Соломона-Ріда, метод Хеммінга, метод Ріда-Маллера, методи побудови завадостійких кодів, що коректують помилки, а також наведено їхні властивості. Описано принципи завадостійкого кодування, циклічні коди, принципи лінійного програмування та багато іншого.

Постановка завдання підвищення ефективності кодів пов'язана з проблемою подолання протиріччя між потребою збільшення інформаційної надмірності, необхідної для забезпечення належної коректувальної здатності циклічних кодів зі збереженням потужності методу кодування, та стремлінням зменшити поліноміальну складність процедур кодування-декодування. Виконання цього завдання вимагає пошуку компромісу між усіма складовими для досягнення прийнятного результату. Для збільшення потужності методу кодування використано можливості кодування методом інверсного перетворення дозволених комбінацій, а також залученням ізоморфних варіантів ІКВ та їхніх дзеркальних відображень відносно основних чи інверсних послідовностей [28].

Результати дослідження та їх обговорення

Характеристика циклічних завадостійких кодів. Сьогодні розроблено десятки кодів, які теоретично можуть виявляти довільну кількість помилок. За наявності такої різноманітності завадостійких кодів важко здійснити їхній чіткий розподіл на групи за ознаками, що взаємно не перекриваються. Циклічні коди складають велику групу часто використовуваних на практиці лінійних кодів [9]. Їх основна властивість, полягає в тому, що кожен вектор, що отримується з початкового кодового слова шляхом циклічної перестановки його символів, також є дозволеним кодовим вектором. Прийнято описувати циклічні коди за допомогою твірних поліномів $G(x)$ степені $r = n - k$, де r – кількість перевірних символів у кодовому слові. Циклічні коди відносяться до різновиду поліноміальних кодів. Серед циклічних кодів особливе місце займає клас кодів, запропонованих Боузом, Чоудхурі й Хоквінгемом. Ці коди є узагальненням коду Хеммінга для випадку виправлення декількох незалежних помилок [9]. Окремими випадками БЧХ-коду є коди Файра [4], призначені для виявлення та виправлення серійних помилок, код Голея [35], – для виправлення одноразових, подвійних і потрійних помилок, а також коди Ріда-Соломона [9]. До циклічних завадостійких кодів належать два основні різновиди ІКВ-кодів – оптимізовані двійкові та монолітно-групові надлишкові коди, які дають змогу виявляти та виправляти помилки. Для спрощення побудови циклічних завадостійких ІКВ-кодів використовують комбінаторні властивості "ідеальних кільцевих в'язанок" (ІКВ). Математичну модель ІКВ можна представити як послідовність $K_n = (k_1, k_2, ..., k_i, ..., k_n)$ цілих додатних чисел, на якій всі можливі кільцеві суми вичерпують значення чисел натурального ряду $1, 2, ..., S_n = n(n-1)$ рівно R разів, де кільцевою вважається сума будь-якої кількості послідовно впорядкованих чисел ІКВ – від одного до (n–1) [18]. Під час дослідження кодів використовують послідовності цілих додатних чисел, впорядкованих у вигляді замкненої кільцевої схеми, де всі числа разом зі сумами двох, трьох і т.д. поруч розміщених чисел відтворюють натуральний ряд R різними способами. Метою дослідження завадостійкості монолітно-групових і циклічних кодів, побудованих на підставі ІКВ, є підвищення ефективності методів кодування та декодування за коректувальною спроможністю, потужністю і процесуальною складністю. В основу покладено метод доповнення базового ІКВ-коду інверсними кодовими послідовностями, ізоморфними варіантами ІКВ та їхніми дзеркальними відображеннями [28]. Розроблено програму комп'ютерного моделювання оптимізованих циклічних і монолітно-групових ІКВ-кодів для верифікації результатів стосовно підвищення завадостійкості та швидкодії в розширеному робочому діапазоні кодування.

Порівняльний аналіз класичних кодів з циклічним ІКВ-кодом. До найчастіше уживаних класичних завадостійких кодів належать коди Боуза-Чоудхурі-Хоквінгема (БЧХ), Голея, Ріда-Соломона та інші. Код БЧХ – це великий клас кодів, здатних виправляти деяку кількість помилок [4], який відіграє важливу роль в теорії і практиці кодування [6], [17], [25]. Досконалий код Голея з параметрами (23,12,7) – це один із двох взаємопов'язаних кодів, який виправляє три помилки., причому розширений код Голея з параметрами (24,12,8) має більшу довжину для перевірки на парність [9]. Коди Ріда-Соломона належать до підкласу оптимізованих недвійкових кодів. Інтерес до циклічних кодів визначається добре опрацьованими методами кодування та декодування. Формальний опис методів декодування циклічних БЧХ-кодів наведено в [4], [30], який базується на використанні елементів теорії полів Ґалуа [29]. Для знаходження твірного полінома БЧХ-коду над полем $GF(q)$ з довжиною n і мінімальною відстанню dвизначають нормований поліном мінімальної степені над $GF(q)$, коренями якого є $d-1$ послідовно впорядкованих степенів елементів розширеного поля $GF(q^m)$ порядку $n = q^m - 1$ і за алгоритмом [4] обчислюють твірний поліном, як НСК мінімальних функцій від елементів обраного цикломатичного класу, які є коренями незвідного полінома над обраним $GF(q)$. Алгоритм полягає у знаходженні твірного полінома БЧХ-коду над полем $GF(q)$ з довжиною n і мінімальною відстанню d за умови $n = (q^m - 1)/s$, де m і s – цілі додатні числа. Для мінімізації кількості перевірних символів послідовно впорядковані степені елементів вибирають так, щоб сумарна довжина цикломатичних класів була мінімальною.

Коди БЧХ дають змогу виправляти більше однієї помилки. Для цього необхідно дотримати умови, за якої мінімальна кодова відстань і кількість виправлених помилок t_2 пов'язані рівнянням $d = 2t_2 + 1$, довжину n коду визначає рівняння $n = 2^h - 1$, а величиною h визначається вибір числа контрольних символів k згідно з співвідношенням [34]:

$$k \le ht_2 = [log_2(n+1)]t_2 . \quad (1)$$

Недоліком коду БЧХ є велика алгоритмічна складність, що пов'язано з необхідністю побудови твірного поліному за допомогою мінімальних многочленів, які є простими незвідними многочленами. Кількість таких многочленів рівне числу помилок, які підлягають виправленню. Тому коди БЧХ, хоча й мають переваги перед іншими кодами стосовно потужності, але поступаються за алгоритмічною складністю та інформаційною надмірністю під час виправлення багаторазових помилок. Код Голея є досконалим кодом довжиною $n = 23$ з кількістю $k = 12$ інформаційних символів. Кодова від-

стань коду Голея $d = 7$, що дає змогу виправляти до трьох помилок включно, які виникають у блоці із 23 символів. Цей код був використаний в ході програми Вояджер під час пересилання кольорових зображень Юпітера і Сатурна апаратами Вояджер-1 і Вояджер-2 [35].

Процедура декодування розширеного (24,12,8) кода-Голея реалізує алгоритм з використанням рядків і стовпців підматриці **B** перевірної матриці $H = (B, I_{12})$. Цей код може бути побудований додаванням загальної перевірки на парність до кодових слів (23,11,7) кодаГолея. Дванадцять рядків підматриці B, позначені як row_i, $1 \le i < 12$, набувають вигляду таблиці в 16-ій системі числення [35]. Процедура декодування включає в себе обчислення синдрому, визначення коректувальних векторів та покрокову перевірку відповідних умов щодо виправлення помилок. Якщо вектор містить несумісні комбінації помилок, декодування припиняється з відмовою. В алгоритмі декодування міняються місцями інформаційні і перевірні позиції кодового слова. Властивості кодів Голея описані в роботах [11], [12].

Методи побудови оптимізованих циклічних ІКВ-кодів. Відносно простий алгоритм побудови оптимізованих циклічних ІКВ-кодів довжиною S_n, який дає змогу виявляти до $0{,}5 \cdot S_n$ і корегувати до $0{,}25 \cdot S_n$ помилок передбачає виконання таких операцій:

1) обрати ІКВ $(k_1, k_2, \ldots, k_i, \ldots, k_n)$ з параметрами S_n, n, R з числовими значеннями $S_n = 2n$, або $n = 2R$;
2) заготовити і пронумерувати одновимірний масив довжиноюS_n та заповнити його комірки n інформаційними "одиницями", порядкові номери яких збігаються з числами x_j, $j = \overline{1,n}$, знайденими за формулою

$$x_j = \sum_{i=1}^{j} k_i,\ j = \overline{1,n}; \qquad (2)$$

3) заповнити порожні комірки масиву інформаційними "нулями";
4) циклічним зсувом отриманої кодової послідовності знайти решту $S_n - 1$ комбінацій;
5) результати побудови занести в таблицю кодових комбінацій ІКВ-коду з параметрами S_n, n, R, де:

$$S_n + 1 = n(n-1)/R. \qquad (3)$$

Приклад побудови кільцевого коду за допомогою ІКВ (1, 1, 2, 1, 2, 4) з параметрами $S_n = 11$, $n_1 = 6$, $R_1 = 3$ ілюструє табл. 1.

Табл. 1. Оптимізований ІКВ-код (1,1,2,1,2,4);
$S_n = 11$, $n_1 = 6$, $R_1 = 3$

№	Нумерація позицій кодових символів										
з/п	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	1	1	0	1	1	0	1	0	0	0	1
2	1	1	1	0	1	1	0	1	0	0	0
3	0	1	1	1	0	1	1	0	1	0	0
4	0	0	1	1	1	0	1	1	0	1	0
5	0	0	0	1	1	1	0	1	1	0	1
6	1	0	0	0	1	1	1	0	1	1	0
7	0	1	0	0	0	1	1	1	0	1	1
8	1	0	1	0	0	0	1	1	1	0	1
9	1	1	0	1	0	0	0	1	1	1	0
10	0	1	1	0	1	0	0	0	1	1	1
11	1	0	1	1	0	1	0	0	0	1	1

У побудованому коді кожна з $S_n(S_n - 1)/2 = 55$ пар різних кодових комбінацій містить рівно три $(R_1 = 3)$ одиничні символи в однойменних розрядах коду, що випливає із властивостей ІКВ. Решта $n_1 - R_1 = 3$ символів однієї і стільки ж іншої кодових комбінацій відрізняються від символів, розміщених в однойменних розрядах. Тому мінімальна кодова відстань d_1для цього коду визначається за формулою

$$d_1 = 2(n_1 - R_1) \qquad (4)$$

Кількість t_1 помилок, які можна виявити за допомогою коректувального коду, і помилок, що підлягають виправленню t_2, визначається загальновідомими формулами [9]:

$$t_1 \le d_1 - 1,\ t_2 \le (d_1 - 1)/2 \qquad (5)$$

На підставі (4) і (5) просто визначається максимальна кількість виявлених і виправлених помилок оптимізованим ІКВ-кодом з параметрами S_n, n, R:

$$t_1 \le 2(n_1 - R_1) - 1,\ t_2 \le n_1 - R_1 - 1 \qquad (6)$$

Для оптимізованого циклічного коду з параметрами $S_n = 11$, $n_1 = 6$, $R_1 = 3$ мінімальна кодова відстань $d_1 = 2(n_1 - R_1) = 6$, кількість виявлених і виправлених помилок визначається за формулами (5) і (6) відповідно: $t_1 \le 5$, $t_2 \le 2$. Отже, завадостійкий ІКВ-код (1,1,2,1,2,4) з параметрами $S_n = 11$, $n_1 = 6$, $R_1 = 3$ може виявляти до п'яти помилок і виправляти одну або дві $(t_2 \le 2)$ помилки, а його потужність $P_1 = S_n = 11$.

Для збільшення потужності методу кодування вдвічі потрібно табл. 1 доповнити таблицею з такими ж розмірами, заповнену символами зі зміною їх знаків на протилежні. Після такої зміни ІКВ-код (1,1,2,1,2,4) з параметрами $S_n = 11$, $n_1 = 6$, $R_1 = 3$ перетворюється в ІКВ-код (4,3,2,1,1) з параметрами n і R: $n_2 = 5$, $R_2 = 2$.

Потужність методу кодування збільшується вдвічі, якщо кодові комбінації обох таблиць об'єднати. Однак, виникає питання стосовно мінімальної кодової відстані d_2 об'єднаних таблиць, яка визначається як менший з двох результатів, одержаних за формулами (4) і (7):

$$d_2 = S_n - d_1 \qquad (7)$$

При цьому потужність методу кодування оптимізованим циклічним ІКВ-кодом з комплексними параметрами зростає вдвічі. Із виразів (4)–(7) випливають формули для визначення кількості помилок, які можна виявити t_1 або виправити t_2 за допомогою оптимізованого циклічного коду вдвічі збільшеної потужності [27]:

$$\text{якщо } S_n \ge 4(n-R), \text{ то } \begin{cases} t_1 \le 2(n-R) - 1 \\ t_2 \le (n-R) - 1 \end{cases}; \qquad (8)$$

$$\text{якщо } S_n < 4(n-R), \text{ то } \begin{cases} t_1 \le S_n - 2(n-R) - 1 \\ t_2 \le \dfrac{S_n - 2(n-R+1)}{2} \end{cases}. \qquad (9)$$

Для прикладу розглянемо характеристики оптимізованого циклічного коду з параметрами ІКВ $S_n = 11$, $n_1 = 6$, $n_2 = 5$, $R_1 = 3$, $R_2 = 2$ $P_2 = 2S_n = 22$.

За формулами (4), а також (7)–(9) обчислюємо $d_1 = 2(n_1 - R_1) = 6$, $d_2 = S_n - d_1 = 5$, $S_n(n_1, R_1) = 4(n_1 - R_1) = 12$, $S_n(n_2, R_2) = 4(n_2 - R_2) = 12$.

Оскільки $S_n < 4(n-R)$, то знаходимо значення t_1 і t_2 за формулою (9), а саме:

$t_1 \le S_n - 2(n_1 - R_1) - 1 = 4$, або $t_1 \le S_n - 2(n_2 - R_2) - 1 = 4$;

$t_2 \le \frac{S_n - 2(n_1 - R_1 + 1)}{2} = 3{,}5$, або $\frac{S_n - 2(n_2 - R_2 + 1)}{2} = 3{,}5$.

Оптимізований ІКВ-код довжиною 11, може виявляти до 4 та виправляти до трьох помилок включно, маючи потужність 22. Збільшення вдвічі потужності методу кодування оптимізованим ІКВ-кодом призвело до зменшення мінімальної кодової відстані від 6 до 5, і відповідно зменшилась на одну позицію кількість виявлених і виправлених помилок.

Для дослідження коректувальної здатності оптимізованих ІКВ-кодів вищих порядків без збільшення їх потужності $P = S_n$ та з подвійною потужністю $P = 2S_n$ методу кодування розглянемо два варіанти кодів з однаковими параметрами $S_n = 31$, $n_1 = 15$, $n_2 = 16$, $R_1 = 7$, $R_2 = 8$.

Застосовуючи формули (4) і (7)–(9), знаходимо:

$$d_1 = 2(n_1 - R_1) = 16,\ d_2 = S_n - d_1 = 15,$$

$$S_n(n_1, R_1) = 4(n_1 - R_1) = 32,\ S_n(n_2, R_2) = 4(n_2 - R_2) = 32.$$

Оскільки $S_n < 4(n - R)$, знаходимо значення t_1 і t_2 за формулою (9), а саме:

$$t_1 \le S_n - 2(n_1 - R_1) - 1 = S_n - 2(n_2 - R_2) - 1 = 14;$$

$$t_2 \le \frac{S_n - 2(n_1 - R_1 + 1)}{2} = \frac{S_n - 2(n_2 - R_2 + 1)}{2} = 6{,}5.$$

Оптимізований ІКВ-код довжиною 31, може виявляти до 14 та виправляти помилки будь-якої кратності від одної до 6 включно. Потужність методу кодування становить 62. Якщо не ставити вимоги до подвоєння потужності, коректувальна спроможність цього коду визначається з (4)–(6): $t_1 \le 16, t_2 \le 7$. Збільшення вдвічі потужності методу кодування оптимізованим циклічним кодом з параметрами ІКВ мало впливає на його корегувальну здатність.

Окрему групу циклічних завадостійких кодів становлять ще мало вивчені монолітно-групові ІКВ-коди, комбінації яких формуються виключно з однойменних символів так, що всі дозволені кодові слова складаються не більш як із двох груп – в одній тільки одиниці, у другій – нулі [28], [27]. Теорія оптимальних монолітно-групових кодів базується на властивостях ІКВ. Оптимальний монолітно-груповий код – це зважений двійковий код, ваговим розрядам якого присвоєні числові значення елементів ІКВ, що забезпечує йому широкий діапазон різноманітності для завадостійкого кодування, збереження, опрацювання та пересилання повідомлень каналами зв'язку. Основною перевагою оптимальних монолітно-групових кодів є здатність автоматично виявляти і виправляти помилки за ознакою згуртованості однойменних символів не більше, ніж в одному пакеті дозволеного кодового слова. На помилку вказує поява хоча б одного символу "1" серед нулів, або символу "0" серед одиниць. Якщо в оптимальному монолітно-груповому коді з'являються хибні символи, вони виправляються за мажоритарним принципом. Ця властивість забезпечує високу швидкість завадостійкого кодування та декодування та самовиправлення помилок, що вигідно відрізняє оптимальні монолітно-групові коди від класичних аналогів.

Результати дослідження корегувальної спроможності оптимізованих циклічних ІКВ-кодів зведені в табл. 2.

Табл. 2. Результати дослідження корегувальної спроможності оптимізованих циклічних ІКВ-кодів

Довжина коду, S_n	Параметри ІКВ		Кодова відстань		Потужність коду, P	t_1	t_1/S_n, %	t_2	t_2/S_n, %
	n	R	d_1	d_2					
15	7	3	8	7	30	4	26,7	1	6,7
19	9	4	10	9	38	8	42,1	3	15,8
23	12	6	12	11	46	10	43,5	4	17,4
31	15	7	16	15	62	14	45,2	6	19,3
35	17	8	18	17	70	16	45,7	7	20,0
43	22	11	22	21	86	20	46,5	9	20,5
…	…	…	…	…	…	…	…	…	…
255	127	63	128	127	510	126	49,4	62	24,3

Із табл. 2 випливає, що зі збільшенням довжини S_n й відповідно потужності P оптимізованих ІКВ-кодів зростає їх спроможність виявляти і виправляти помилки з рівномірним приростом кількості виявлених і виправлених помилок. Приріст відповідає пропорційному закону 1:2:4, за яким для зростання числа виправлених помилок на одну, а виявлених на дві позиції достатньо збільшити довжину оптимізованого коду на чотири біти, не залежно від довжини оптимізованого ІКВ-коду. Збільшення потужності оптимізованих кодів доповненням множиною кодових комбінацій зі зміненими символами протилежного знаку забезпечує корегувальну спроможність коду з точністю до однієї виправленої помилки і не залежить від довжини коду.

Обговорення отриманих результатів дослідження. Оптимізовані циклічні коди об'єднують велику групу завадостійких кодів, пов'язаних із загальною теорією комбінаторних конфігурацій, циклічними групами розширених полів Галуа і досконалими комбінаторними конструкціями – "ідеальними кільцевими в'язанками" (ІКВ). Внаслідок проведеного дослідження ефективності циклічних кодів за трьома чинниками – коректувальною здатністю, потужністю методу кодування та складністю процедури декодування було з'ясовано, що за оцінкою коректувальної здатності оптимізовані ІКВ-коди і коди Боуза-Чоудхурі-Хоквінгема (БЧХ-коди) за однакової довжини кодових комбінацій приблизно рівноцінні, за потужністю методу кодування ІКВ-коди програють, однак виграють за простотою виконання процедур кодування – декодування. Це обумовлено спрощенням процедури перевірки прийнятих кодових слів, яка зводиться до простого порівняння прийнятих комбінацій зі списком дозволених комбінацій і визначення виправленого слова за мінімальним значенням кодової відстані. Асимптотична оцінка часової складності процедури декодування ІКВ-кодів становить менше $O(n^2)$, оскільки програма завчасу припиняє порівняння в момент виявлення виправленого слова. Натомість декодування класичних циклічних кодів вимагає здійснення матричних обчислень над поліномами вищих порядків, що відповідає поліноміальному рівню часової складності.

Зі збільшенням довжини коду складність декодування класичних циклічних кодів зростає за поліноміальним законом. Тому декодування повідомлень, закодованих циклічним ІКВ-кодом, здійснюється швидше, ніж кодами Голея [35], Боуза-Чоудхурі-Хоквінгема [4] та іншими кодами цього класу, а темпи зростання часової складності декодування класичних кодів вищі, ніж для оптимізованих ІКВ-кодів. Такими ж показниками опти-

мізовані ІКВ-коди вигідно відрізняються від кодів Голея, Ріда-Соломона та інших класичних аналогів. Наведені приклади, розрахунки і таблиці підтверджують правильність теоретичних висновків.

Монолітно-групові оптимізовані коди становлять підгрупу самокоректувальних кодів з кільцевою структурою та ймовірнісною оцінкою рівня завадостійкості. Ця властивість дає змогу миттєво виявляти певну частину, або усі хибні символи у кодовому слові за мажоритарним принципом.

Висновки

Встановлено, що основні переваги монолітного коду порівняно з класичними завадостійкими циклічними кодами – 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 даних і опрацювання великих обсягів інформації. Однак існують труднощі, пов'язані з виробленням методів розпізнавання помилок, коли вони виникають в розрядах на межі пакетів різнойменних символів.

З'ясовано, що використання комбінаторних методів оптимізації циклічних кодів дає змогу підвищити ефективність систем завадостійкого кодування, зменшивши часову складність обчислювальних процедур декодування. Розширення даного класу кодів розкриває нові перспективи для розвитку комбінаторних методів оптимізації інформаційно-комунікаційних систем.

References

[1] Akulinichev, Iu. P. (2010). *Teoriia elektricheskoi sviazi*. Tutorial. St. Petersburg: Lan, 240 p. [In Russian].

[2] Banket, V. L., Ivashchenko, P. V., & Ishchenko, M. O. (2011). *Zavadostiike koduvannia v telekomunikatsiinykh systemakh*. Odesa: ONAZ im. O. S. Popova, 100 p. [In Ukrainian].

[3] Banket, V. L., Ivashhenko, P. V., & Geer, A. E. (1996). *Tcifrovye metody peredachi informatcii v sputnikovykh sistemakh sviazi*. Odessa: UGAS, 180 p. [In Russian].

[4] BCH code. (2020). F*rom Wikipedia, the free encyclopedia*. Retrieved from: https://en.wikipedia.org/wiki/BCH_code

[5] Berrou C., Glavieux A., & Thitiumjshima, P. (1993). Near Shannon limit error correcting coding: Turbo codesiu *International Conf. on Commun. Geneva*, Switzerland, May 1993, pp. 1064–1070.

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

[7] Bleikhut, R. (1986). *Teoriia i praktika kodov, kontroliruiushhikh oshibki*. (Trans. from English). Moscow: Mir, 576 p. [In Russian].

[8] Consultative Committee for Space Data Systems (CCSDS). (1998). Recommendations for space data systems, telemetry channel coding. *Blue Book*. May 1998. Retrieved from: http://www.ccsds.org.

[9] DrM D Macleod, M. A. (1993). Cyclic Code. In: *Telecommunications Engineers Reference Book. MIEEE*. Retrieved from: https://www.sciencedirect.com/topics/engineering/cyclic-code

[10] Giancristofaro D., Giubilei R., Novello R., Piloni V., & Toush, J. (2000). Performances of Novel DVB-RCS Standard Turbo Code and its Use in On-Board Processing Satellites. *Proceedings of the EMPS workshop, in IEEE EMPS/PIMRC*. London, 17–21 September, pp. 345–349.

[11] Golay, M. J. E. (1949). NotesonDigitalCoding, *Proc. IRE journal*. Vol. 37, 657 p.

[12] Griess, R. L. (1998). TwelveSporadicGroups. *Springer*, 167 p.

[13] 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 TCSET'*2016, pp. 498–502. https://doi.org/10.1109/TCSET.2016.7452098

[14] 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 Conferenc*e (CSIT'2015), 14–17 September, 2015. pp. 67–69. https://doi.org/10.1109/stc-csit.2015.7325433

[15] Hall, M. Jr. (1986). Combinatorial Theory. *John Wiley & Sons*, 464 p.

[16] Hrebeniuk, O. P., Melenskyi, V. D., & Korinenko, V. I. (2015). Zastosuvannia zavadostiikoho koduvannia v systemakh zviazku i peredachi danykh kompleksiv radiomonitorynhu dlia zabezpechennia dostovirnosti informatsiinoho obminu. *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system*, *11*, 44–50. Retrieved from: http://nbuv.gov.ua/UJRN/Psvz_2015_11_7. [In Ukrainian].

[17] Hrytsiuk, Yu., & Bilas, O. (2019). Visualization of Software Quality Expert Assessment. *IEEE 2019 14th International Scientific and Technical Conference on Computer Sciences and Information Technologies* (CSIT 2019), (Vol. 2, pp. 156–160), 17–20 September, 2019. https://doi.org/10.1109/stc-csit.2019.8929778

[18] Ideal ring bundle. (2019). Retrieved from: https://en.wikipedia.org/wiki/Ideal_ring_bundle

[19] Klark, Dzh.-ml., & Kein, Dzh. (1987). *Kodirovanie s ispravleniem oshibok v sistemakh tcifrovoi sviazi*. (Trans. from English) (Tcybakova, B. S. Scientific Ed.). Moscow: Radio i sviaz, 392 p. [In Russian].

[20] Kuzmin, I. V., & Kedrus, V. A. (1986). *Osnovy teorii informatcii i kodirovaniia.* (2nd ed. add. and revised). Kyiv: Vishha shk. Golovnoe izd-vo, 238 p. [In Russian].

[21] Lagutenko, O. I. (2002). *Sovremennye modemy*. Moscow: EkoTrendz, 343 p. [In Russian].

[22] Morelos-Saragosa, R. (2005). *Iskusstvo pomekhoustoichivogo kodirovaniia. Metody, algoritmy, primenenie*. Moscow: Tekhnosfera, 320 p. [In Russian].

[23] Panfilov, I. P., Dyrda, V. Yu., & Kapatsin, A. V. (1998). *Teoriia elektrychnoho zviazku*: pidruchnyk dlia studentiv vuziv I ta II rivniv akredytatsii. Kyiv: Tekhnika, 328 p. [In Ukrainian].

[24] Panin, V. V. (2004). Osnovy teorii informatcii. Chast 2. *Vvedenie v teoriiu kodirovaniia.* Textbook. Moscow: MIFI, FGUP ISS, 391 p. [In Russian].

[25] Peterson, W. Wesley, & Weldon, E. J. (1972). *Error-correcting codes*, The MIT Press; secondedition, 560 p.

[26] Piterson, U., & Ueldon, E. (1976). *Kody, ispravliaiushhie oshibki*. (Trans. from English) (R. L. Dobrushina i S. I. Samoilenko Scientific Eds.). Moscow: Mir, 593 p. [In Russian].

[27] Riznyk, V. V. (2019). Combinatorial optimization of multidimensional systems. *Models of multidimensional intelligent systems* Lviv: Publishing Lvivskoji Politekhniky, 168 p. [In Ukrainian].

[28] Riznyk, V. V. (2019). Methods of multidimensional signal processing under toroidal coordinate systems. Kyiv: Bulletin of NTUU KPI, *Series Radiotekhnique. Radioapparatus building, 77*, pp. 5–12. [In Ukrainian].

[29] Rotman, J. (1998). GaloisExtensions. *Universitext*, pp. 79–82. https://doi.org/10.1007/978-1-4612-0617-0_15

[30] Sahalovich, Y. L. (2007). *The introduction to algebraic codes*. Moscow: MFTI, 262 p. [In Russian].

[31] Shvartcman, V. O., Emelianov, G. A. (1979). *Teoriia peredachi diskretnoi informatcii*. Textbook for universities. Moscow: Sviaz, 424 p. [In Russian].

[32] Sidelnikov, V. M. (2006). *Teoriia kodirovaniia. Spravochnik po printcipam i metodam kodirovaniia*. Moscow: Moskovskii gosudarstvennyi universitet im. M. V. Lomonosova (MGU), 289 p. [In Russian].
[33] Skliar, B. (2003). *Tcifrovaia sviaz. Teoreticheskie osnovy i prakticheskoe primenenie*. (2nd ed. add. and revised). (Trans. from English). Moscow: Publishing House "Viliams", 1104 p. [In Russian].
[34] Tsymbal, V. P. (1977). *Theory of information and coding*. Kyiv: Vyshcha shkola, 288 p. [In Russian].
[35] Wolfram Math World. (2019). *Built with Mathematical Technology*. Retrieved from: http://mathworld.wolfram.com/GolayCode.html
[36] Ziuko, A. G., & Klovskii, D. D. (1998). *Teoriia elektricheskoi sviazi*. Textbook for universities. (Klovskogo, D. D. Scientific Ed.). Moscow: Radio i sviaz, 432 p. [In Russian].
[37] Ziuko, A. G., Falko, A. I., & Panfilov, I. P. (1985). *Pomekhoustoichivost i effektivnost sistem peredachi informatcii*. (Ziuko, A. G. Scientific Ed.). Moscow: Radio i sviaz, 282 p. [In Russian].
[38] Ziuko, A. G., Klovskii, D. D., Nazarov, M. V., & Fink, L. M. (1986). *Teoriia peredachi signalov*. Textbook for universities. Moscow: Radio i sviaz, 304 p. [In Russian].
[39] Zolotarev, V. V., & Ovechkin, G. V. (2004). *Pomekhoustoichivoe kodirovanie. Metody i algoritmy*. Spravochnik. Moscow: Goriachaia liniia – Telekom, 126 p. [In Russian].

V. V. Riznyk, D. Yu. Skrybaylo-Leskiv

Lviv Polytechnic National University, Lviv, Ukraine

IMPROVEMENT OF CYCLIC CODES EFFECTIVENESS BY COMBINATORIAL OPTIMIZATION METHODS

The methods of improving the cyclic codes efficiency constructed on the basis of combinatorial configurations of the type "ideal ring bundles" (IRB) s by three factors – correction ability, power of coding method and complexity of the decoding procedure are considered. The method is based on the principle of combinatorial optimization, grounded on the algebraic theory of ordered integer sequences with a circular structure, all the numbers, as well as all sums of consecutive numbers exhaust the value sofnatural row numbers. Two theoretically grounded approaches to increase of noise immunity of cyclic codes are offered: implementation of optimized IRB-code, as well as monolithic and group one. Optimized cyclic IRB-code favorably differs from the rest of the codes of this class by the highest correction capacity at the same length of code words. Optimized IRB-codes constitute a large group of cyclic codes designed on a combinatorial models with selection of corresponding relationships between the parameters of the code to achieve its specified technical characteristics. Noise protected monolithic and group codes belong to the group of self-correcting codes with a ring structure and probabilistic assessment of the level of noise protection. This property allow so instant lydetect a particular part or all invalid characters in the code word by the majority principle. Mathematical calculations have been performed to calculate the optimized ratios between the parameters of cyclic IRB-codes, under which they reach maximum correction capacity. The algorithm of constructing and increasing the power of coding methods of optimized noise-resistant IRB-codes is examined and analyzed. The concrete examples of increase efficiency of combinatorial optimization cyclic codes methods with appropriate calculations and tables are given. The comparative analysis of the IRB-codes with the Golay codes and Bose – Chaudhuri – Hocquenghe (BCH) codes with respect to correction ability, power encoding method and computational complexity of decoding procedures is carried out. The advantages and disadvantages of cyclic, and ringmonolithic and group IRB-codes in comparison with classical analogues are determined. The prospect so fusing the research results in the problems of information and communication technologies are outlined.

***Keywords**:* combinatorial configuration, computational complexity, error-correcting code, optimized cyclic code, code effectiveness, self-correcting monolithic and group code.

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, асистент, кафедра автоматизованих систем управління. **Email:** skrybajlo.d.yu@gmail.com

Цитування за ДСТУ: Різник В. В., Скрибайло-Леськів Д. Ю. Підвищення ефективності циклічних кодів методами комбінаторної оптимізації. *Український журнал інформаційних технологій*. 2020, т. 2, № 1. С. 66–72.

Citation APA: Riznyk, V. V., & Skrybaylo-Leskiv, D. Yu. (2020). Improvement of cyclic codes effectiveness by combinatorial optimization methods. *Ukrainian Journal of Information Technology, 2*(1), 66–72. https://doi.org/10.23939/ujit2020.02.066