змогу чітко виділяти контури. Обидва типи модифікацій без жодних застережень можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення, може зрости розмір шифрованого зображення.

Вказаний алгоритм може бути використаний при передачі графічних зображень.

1. Шнайер Б. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 2. Яне Б. Цифровая обработка изображений. – М.: Техносфера, 2007. – 583 с. 3. Рашкевич Ю.М., Пелешко Д.Д., Ковальчук А.М., Пелешко М.З. Модифікація алгоритму RSA для деяких класів зображень // Технічні вісті. – 2008/1(27). – 2(28). – С. 59 – 62. 4. Rashkevych Y., Kovalchuk A., Peleshko D., Kupchak M. Stream Modification of RSA Algorithm For Image Coding with precize contour extraction. Proceedings of the X-th International Conference CADSM 2009. 24–28 February 2009, Lviv-Polyana, Ukraine, Pp. 469–473.

УДК 681.3:519.15

В. Різник[*], Д. Скрибайло-Леськів, О. Ляхович
[*]Технологічно-природничий університет, м. Бидгощ (Польща)
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

СТРУКТУРНИЙ АНАЛІЗ МЕТОДІВ ОПТИМАЛЬНОЇ ПОБУДОВИ ЦИКЛІЧНИХ КОДІВ З ПОЛІПШЕНИМИ ХАРАКТЕРИСТИКАМИ

Досліджуються циклічні коди, побудовані на основі математичних конструкцій з унікальними комбінаційними властивостями – «ідеальних кільцевих в'язанок» (ІКВ) – та розглядаються методи оптимального синтезу за допомогою ІКВ циклічних кодів з поліпшеними можливостями щодо виправлення багаторазових помилок.

The cyclic coded design based on the mathematical constructions with special combinative properties, namely the "ideal ring bundles" (IRB)s are studied, and techniques for optimum synthesis of the cyclic codes with improved possibilities for correcting the multiple errors are regarded in this paper.

Вступ

Комбінаторні структури і методи комбінаторної оптимізації широко застосовують в інформаційних технологіях під час кодування, перетворення та пересилання даних, в інформаційно-вимірювальній та обчислювальній техніці, радіотехніці, зв'язку та суміжних галузях науки і техніки. Приклади постановки таких задач: проектування завадостійких систем кодування, розроблення ефективних технологій захисту цінних паперів від несанкціонованого доступу, удосконалення компонентів комп'ютерних систем, проектування радіосистем з високою роздільною здатністю. Тому актуальними є синтез математичних моделей систем та дослідження їх комбінаторних властивостей з метою поліпшення технічних характеристик систем та пристроїв комп'ютерної техніки та інформаційних технологій за такими показниками, як забезпечення достовірності інформації, підвищення надійності, функціональної безпеки і живучості інформаційних та інформаційно-управляючих систем, зокрема вдосконалення інформаційних технологій для створення гарантоздатних автоматизованих систем перероблення інформації та

управління критичного застосування. При цьому необхідно враховувати оптимальне розміщення елементів проектованих систем чи відповідних компонентів у просторово-часовому вимірі та характер взаємозв'язків між ними як систем інцидентності.

Постановка задачі

Циклічні коди, які спроможні виправляти більше двох помилок, в літературі відомі як коди Боуза, Чоудхурі, Хоквінхема – авторів методики побудови цих кодів (скорочено – коди БЧХ). Суть методики полягає в побудові твірного полінома, вигляд якого залежить від двох параметрів: довжини кодового слова S та максимально можливої кількості виправлених помилок t. Решта параметрів, що беруть участь у побудові твірного полінома, можуть визначатися за допомогою спеціальних таблиць і допоміжних співвідношень [1]. При цьому необхідно дотримуватися таких залежностей:

$$d = 2t + 1, \qquad S = 2^h - 1, \tag{1}$$

де d – мінімальна кодова відстань; h – величина, яка визначає вибір обрання числа контрольних символів k і пов'язана з h та t таким співвідношенням:

$$k \le ht = [\log_2 (S+1)]t. \tag{2}$$

З іншого боку, кількість контрольних символів визначається твірним поліномом і дорівнює його степеню. Зі збільшенням значення h довжина коду S стає дуже великою, що ускладнює технічну реалізацію пристроїв кодування та декодування. Побудова твірного полінома здійснюється за допомогою простих незвідних поліномів. Твірний поліном є добутком непарних мінімальних поліномів, що становить найменше спільне кратне. Максимальний порядок мінімальних поліномів

$$\rho = 2t - 1. \tag{3}$$

Порядок полінома використовують для визначення числа співмножників. Для побудови твірного полінома зазвичай користуються спеціальною таблицею мінімальних незвідних в полі Ґалуа GF (2) поліномів. В окремих випадках допускається використання поліномів й меншого степеня [2]. Декодування кодів БЧХ, які спроможні виправляти більше чотирьох помилок, є достатньо складною задачею і здійснюється, як правило, на основі алгоритму Берлекемпа [3] або його модифікацій. Легше комбінацію, одержану після K-кратного зсуву і додавання до залишку, зсувати не праворуч, а ліворуч на S- K циклічних зсувів, але це доцільно робити за умови, коли $K > S/2$ [1]. Теоретично БЧХ-коди можуть виправляти довільну кількість помилок, однак зі збільшенням кратності помилки значно зростає складність пристроїв декодування. Це приводить до зменшення швидкості пересилання повідомлень та ускладнення приймально-передавальної апаратури.

Інший підхід до побудови завадостійкого циклічного коду ґрунтується на використанні унікальних властивостей «ідеальних кільцевих в'язанок» (ІКВ) – впорядкованих цілочислових послідовностей з кільцевою структурою, причому всі числа разом з усіма сумами поруч розміщених чисел вичерпує значення чисел натурального ряду. Для побудови циклічного коду з довжиною кодових комбінацій S_n за допомогою ІКВ достатньо виділити рядок із S_n пронумерованих клітинок одновимірного масиву та заповнити інформаційними одиницями клітинки, номери яких збігаються з числом x_j , що знаходять із залежності

$$x_j - 1 \equiv \sum_{i=1}^{j} k_i \,(\mathrm{mod}\, S_n\ ), j=1,2,\ldots,n, \tag{4}$$

$$S_n = n\,(n-1)/\,R + 1, \tag{5}$$

де k_j – i-й елемент обраного ІКВ, S_n, n, R – параметри ІКВ [4].

Решта клітинок заповнюють інформаційними нулями. Утворена послідовність двійкових символів є твірною комбінацією коду, циклічним зсувом якої можна отримати решту S_n -1 кодових комбінацій.

Мінімальна кодова відстань для цього коду визначається за залежністю

$$d_{min} = 2(n - R). \tag{6}$$

Число помилок, які можна виправити за допомогою даного коду, залежить від параметрів n і R [4]:

$$t \le (n - R - 1) \tag{7}$$

Аналіз методів побудови циклічних завадостійких кодів

Для порівняння методів побудови циклічних кодів розглянемо кілька прикладів. Нехай треба побудувати циклічний код завдовжки 15 символів, який виправляє одну або дві помилки.

Розв'язання цієї задачі за методом авторів коду БЧХ передбачає такі дії:

1) згідно із залежностями (1)

$$h = \log_2 (S + 1) = \log_2 16 = 4;$$

2) за формулою (2) число контрольних символів

$$k \le ht \le ht = 8;$$

3) порядок старшого з мінімальних поліномів, згідно з (3),

$$\rho = 2t - 1;$$

4) за допомогою таблиці мінімальних незвідних в полі Ґалуа GF (2) поліномів (табл. додатка 4 [1]) обирають два (t =2) мінімальні поліноми, порядок старшого з яких дорівнює 3 (ρ= 3), тобто поліноми 10011 та 11111;

5) перший рядок твірної матриці одержують додаванням зліва від послідовності 10011×11111= 111010001 такої кількості нулів, щоб загальна довжина кодової комбінації дорівнювала S= 15; твірна матриця будується k- разовим циклічним зсувом кодової комбінації відносно першого рядка твірної матриці:

000000111010001
000001110100010
000011101000100
000111010001000
001110100010000
011101000100000
111010001000000

Решта кодових послідовностей утворюється додаванням усіх можливих комбінацій рядків твірної матриці [1].

Для побудови циклічного коду завдовжки S= 15 за допомогою ІКВ необхідно виконати такі дії:

1) побудувати ІКВ, сума усіх чисел якої збігається з довжиною кодових комбінацій $S_n = S$ = 15, а параметри n, R визначаються зі співвідношень (5) і (6) за дотримання вимоги $d_{min} = (d_{min})$ = max; легко знайти, що ця вимога задовольняється за умови, коли n= 7, R=3, оскільки тоді $d_{min} = 2(n - R) = 8$, досягаючи свого максимального значення;

2) за допомогою залежності (4) побудувати циклічний код з параметрами S_n= 15, n= 7, R= 3.

Кілька методів побудови ІКВ описано в монографії [4]. Одним з найпростіших серед них є метод вибіркових переміщень, який ґрунтується на принципі «вирощування» впорядкованих числових послідовностей шляхом складання чисел у зростаючому порядку їх значень за дотримання певних правил, описаних в [4].

Одним з можливих варіантів побудованої за таким способом ІКВ є послідовність (1,1,2,1,3,2,5), на основі якої легко скласти повну систему циклічного коду, що відповідає параметрам S_n= 15, n= 7, R= 3:

111011001010000
011101100101000
001110110010100
……..
110110010100001

Циклічний код завдовжки S_n= 15 побудовано.

Структурний аналіз порівнюваних кодів

Для здійснення структурного аналізу досліджуваних кодів доцільно скористатися залежностями (4)–(7). На основі здійснених нами досліджень можна показати, що будь-якій кодовій комбінації побудованого циклічного коду БЧХ зі заданими вхідними даними S= 15, t= 2 відповідає одна і та сама кільцева послідовність чисел (1,1,2,4,7), сума яких збігається зі заданою довжиною коду БЧХ. Розглянемо комбінаційні можливості цієї послідовності з погляду теорії ІКВ, в основу яких покладено вимогу щодо впорядкованості елементів структури за критерієм досягнення максимальної взаємно однозначної відповідності між числом способів послідовного додавання чисел (елементів структури) та множиною утворених цими способами сум, що збігаються з рядом натуральних чисел. В ідеалі йдеться про «вичерпування» усіх можливих способів послідовного додавання чисел для автентичного переліку отриманих сум. Для зручності досліджень скористаємося методом табличного запису кільцевих сум для кожної зі згаданих послідовностей, причому під кільцевою слід розуміти не лише суми усіх послідовно впорядкованих чисел послідовності, але й числа, з яких ці суми утворюються.

а)

1	1	2	4	7
2	3	6	11	8
4	7	13	12	9
8	14	13	11	8

б)

1	1	2	1	3	2	5
2	3	3	4	5	7	6
4	4	6	6	10	8	7
5	7	8	11	11	9	9
8	9	13	12	12	11	10
10	14	14	13	14	12	13

У перших рядках таблиць а) і б) записані послідовності чисел, що описують циклічний код БЧХ довжиною в 15 символів (а) та порівнюваний з ним циклічний ІКВ код з тією ж довжиною (б). Другі рядки заповнені числами, що дорівнюють сумам двох, треті – трьох і т.д. послідовно складаних чисел послідовності, яка записана у першому рядку кожної таблиці. В останніх рядках таблиць знаходяться числа, що дорівнюють сумам чотирьох (а) та шести (б) елементів відповідної послідовності. Здійснюючи порівняльний аналіз, легко побачити, що в таблиці (а) числа 3, 6, 9, 12, 14 трапляються один раз, тоді як числа 1, 2, 4, 7, 11 і 13 – двічі, число 8 – тричі, натомість відсутні числа 5 і 10. Такий «розкид» кільцевих сум не задовольняє вимоги щодо їх зрівноваженого розподілу за натуральним рядом чисел, а степінь цього «розкиду» може слугувати певним критерієм того, наскільки ця послідовність відповідає (або не відповідає) досягненню максимальної взаємно однозначної відповідності між числом способів послідовного додавання чисел (елементів структури) та множиною утворених цими способами сум, що збігаються з рядом натуральних чисел. На відміну від таблиці (а) таблиця (б) містить усі числа натурального ряду від 1 до 14, кожне з яких трапляється рівно тричі (R=3), що є ознакою довершеності цієї числової моделі у порівнянні з попередньою. Легко переконатися у вищій порівняно зі згаданим кодом БЧХ ефективності циклічного коду довжиною 15, побудованого на основі ІКВ (1,1,2,1,3,2,5), який може виявляти до семи (d_{min} –1=2n –2R –1=7) і виправляти до трьох ($t \leq 3$) помилок, а код БЧХ такої ж довжини виправляє лише одну чи дві помилки [1]. Переваги циклічного ІКВ- коду над кодом БЧХ ще яскравіше проявляються зі зростанням кратності помилки. Так, наприклад, циклічний ІКВ-код з довжиною кодових комбінацій 63 може виправляти до 15 помилок, тоді як код БЧХ з такою

довжиною комбінацій – лише до шести помилок [1]. За цим показником циклічний ІКВ- код є в 2,5 разів ліпший від коду БЧХ. Теоретичні розрахунки показують, що зі зростанням кратності помилки ця перевага може обчислюватися в 10 і більше разів. Серед інших переваг методу побудови циклічних кодів на основі ІКВ слід відзначити спрощення алгоритму і високий рівень досконалості теорії кодів цього класу . Однак слід враховувати обмеження, пов'язані зі швидкістю передавання та ускладненням приймально-передавальної апаратури.

Висновки

Дослідження структури та порівняльний аналіз методів побудови циклічних кодів з високими можливостями щодо виявлення і виправлення багаторазових помилок дозволяє стверджувати доцільність застосування апарату теорії ІКВ, що дозволяє:

1) **збільшити в декілька разів ефективність** циклічного коду щодо спроможності виправлення багатократних помилок за наявності обмеження на довжину кодових комбінацій;

2) **спростити методику побудови** циклічних кодів, які забезпечують можливість виправляти десятки і більше помилок;

3) **вдосконалити алгоритм виправлення** багаторазових помилок;

4) **підвищити рівень досконалості теорії завадостійких кодів** цього класу.

Запропонований метод синтезу циклічного коду не вимагає обов'язкового пошуку твірного полінома та побудови мінімальних незвідних в полі Ґалуа GF (2) поліномів, як це передбачає алгоритм синтезу кодів БЧХ. Результати наших досліджень можуть знайти практичне застосування для розроблення інформаційних технологій та систем з поліпшеними технічними характеристиками за такими показниками як забезпечення достовірності інформації, підвищення надійності, функціональної безпеки і живучості інформаційних та інформаційно-управляючих систем, зокрема вдосконалення інформаційних технологій захисту інтелектуальної власності та цінних паперів, а також для створення гарантоздатних автоматизованих систем переробки інформації.

1. Цымбал В.П. Теория информации и кодирование. – К.: Вища школа, 1982. – 304 с. 2. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Сов. Радио, 1974. – 590 с. 3. Берлэкэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971. – 478 с. 4. Різник В.В. Синтез оптимальних комбінаторних систем. – Львів: Вища школа, 1989. – 168 с.