УДК 681.3:519.15

В.В. Різник[1], Д.Ю. Скрибайло-Леськів[1], О.В. Ляхович[1], І.Ю. Юрчак[2]
Національний університет "Львівська політехніка",
[1]кафедра автоматизованих систем управління,
[2]кафедра систем автоматизованого проектування

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАВАДОСТІЙКОСТІ БАГАТОПОЗИЦІЙНИХ ЦИКЛІЧНИХ КОДІВ

Досліджено різновиди завадостійких циклічних кодів, побудованих за допомогою незвідних поліномів та нестандартних математичних конструкцій з унікальними комбінаційними властивостями – «ідеальних кільцевих в'язанок» (ІКВ). Розглянуто методи оптимального синтезу за допомогою ІКВ циклічних кодів з поліпшеними можливостями щодо виправлення багаторазових помилок.

Ключові слова – циклічні коди, ідеальні кільцеві в'язанки, ІКВ, оптимальний синтез.

Various types of correcting cyclic codes design using the primitive multinomial and non-standards mathematical constructions with special combinative properties, namely the "ideal ring bundles" (IRB)s are studied. The techniques for optimum synthesis of the cyclic codes with improved possibilities for correcting the multiple errors are regarded in this paper.

Keywords – cyclic codes, ideal ring bundles, IRB, optimum synthesis.

Вступ

Циклічні коди дістали свою назву, тому що в них усі комбінації або частину з них можна утворити циклічним зсувом однієї чи кількох комбінацій коду. Згідно з загальноприйнятою класифікацією найпоширеніших дискретних кодів циклічні коди належать до систематичних кодів. Останні, як відомо, будуються так, щоб інформаційні та корегувальні символи знаходилися на чітко визначених місцях у кодових комбінаціях. До систематичних циклічних кодів належать коди Боуза-Чоудхурі, коди Фаєра і коди Міласа-Абрамсона [1]. Поряд зі згаданими до сім'ї циклічних кодів належать коди, які не можна зарахувати до систематичних, оскільки для них не виконується правило щодо розмежування інформаційних та корегувальних символів на визначених місцях у кодових комбінаціях. Йдеться про коди, які побудовані за допомогою нестандартних математичних конструкцій з унікальними комбінаційними властивостями – так званих «ідеальних кільцевих в'язанок» (ІКВ) [2]. Приклади можливого застосування таких кодів: 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 актуальним є здійснення порівняльного аналізу стандартних та нестандартних кодів, побудованих на основі ІКВ.

Постановка задачі та мета досліджень

В основу постановки задачі покладено дослідження корегувальних властивостей циклічних кодів ІКВ порівняно з кодами БЧХ. Метою дослідження є поліпшення технічних характеристик 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 автоматизованих систем переробки інформації та управління критичного застосування.

Коди Боуза-Чоудхурі-Хоквінхема

Помилки у циклічних кодах Боуза-Чоудхурі-Хоквінхема (коди БЧХ) виявляються і виправляються за допомогою лишків від ділення отриманої комбінації на твірний поліном. Залишки від ділення виконують роль засобу розпізнавання помилок, але не вказують безпосередньо на місце помилки в циклічному коді. Ідея виправлення полягає у тому, що помилкова комбінація після певної кількості циклічних зсувів припасовується до залишка так, що в сумі з залишком вона дає виправлену комбінацію. При цьому залишок є різницею між хибними і правильними символами, де одиниці стоять на позиціях хибних розрядів у припасованій циклічними зсувами комбінації, причому помилкову комбінацію припасовують до того часу, поки число одиниць у залишку не дорівнюватиме числу помилок, яке цей код ще взмозі виправити. Розрахунок співвідношення між числом і інформаційних та числом k корегувальних символів у кодовій комбінації завдовжки n, яка може виправляти не менше s помилок, здійснюється на підставі таких виразів:

$$n = i + k; \quad (1)$$

$$2^k \geq n + 1; \quad (2)$$

$$2^i \leq 2^n / (n + 1); \quad (3)$$

$$s = \text{ent}\,(d - 1)/2, \quad (4)$$

де d – мінімальна кодова відстань.

Якщо відома довжина повної кодової комбінації, для визначення потрібної кількості контрольних розрядів з мінімальною кодовою відстанню $d = 3$ використовують залежність

$$k_{(3)} = \text{ent}\,[\log_2 (n + 1)], \quad (5)$$

що дає змогу виправляти одну помилку.

Для виявлення трьох помилок і виправлення однієї помилки потрібно збільшити кодову відстань до $d = 4$. Тоді число контрольних розрядів визначають із залежності

$$k_{(4)} \geq 1 + \log_2 (n + 1). \quad (6)$$

Для кодів завдовжки в n символів, що повинні виправляти одну чи дві помилки ($d = 5$), можна використати вираз

$$k_{(5)} \geq \log_2 (C^2_n + C^4_n + 1). \quad (7)$$

Для кодів, які виправляють s помилок, справедливим є вираз

$$\log_2 (C^s_n + C^{s-1}_n + \ldots + 1) < k_{(2s+1)} < \log_2 (C^{2s-1}_{n-1} + C^{2s-2}_{n-1} + \ldots + 1), \quad (8)$$

де ліва частина становить нижню границю Хеммінга [3], а права – верхню границю Варламова-Гілберта [4].

Для виправлення числа помилок більше двох необхідно, щоб довжина коду задовольняла умову

$$n = 2^r - 1, \quad (9)$$

причому n завжди буде непарним числом.

Величина r визначає обрання числа контрольних символів k і зв'язана з k і s співвідношенням

$$k \leq rs. \quad (10)$$

З іншого боку, число k контрольних символів визначається твірним поліномом і дорівнює його степеню. Зі збільшенням значення r довжина коду n 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

$$\rho = 2t - 1. \quad (11)$$

Порядок полінома використовують для визначення числа співмножників. Для побудови твірного полінома переважно 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. Певне полегшення може бути, коли комбінацію, одержану після K-кратного

зсуву і додавання до залишку, зсувати не вправо, а вліво на S- K циклічних зсувів, але це доцільно робити за умови, коли $K > S/2$ [1].

Побудова і декодування систематичних циклічних кодів зводиться до виконання багатьох стандартних процедур, таких як розрахунок співвідношення між контрольними та інформаційними символами, обрання твірного полінома, обрання параметрів одиничної транспонованої матриці, визначення елементів додаткової матриці за залишками від ділення останнього рядка транспонованої матриці на твірний поліном, побудова твірної матриці за допомогою додаткової матриці, знаходження дозволених кодових комбінацій. Виявлення і виправлення помилок здійснюють за залишками від ділення прийнятої комбінації на твірний поліном. Якщо прийнята комбінація ділиться на твірний поліном без залишку, то код прийнято без помилок. Наявність залишку від ділення свідчить про помилку, але не вказує на її місцезнаходження. Щоб знайти помилковий розряд і виправити його, потрібно поділити прийняту комбінацію на твірний поліном, обчислити кількість одиниць у залишку (вага залишку) з перевіркою багатьох вимог щодо дотримання відповідного співвідношення (більше – менше) між знайденою кількістю одиниць і допустимим числом помилок, що виправляються; якщо ця кількість виявиться не більшою від допустимого числа виправлень, то прийнята комбінація складається по модулю 2 з отриманим залишком, і сума дасть виправлену комбінацію; в протилежному випадку слід ділити отриману в результаті циклічного зсуву комбінацію на твірний поліном, і якщо в залишку знайдена кількість одиниць буде не більшою від цього допустимого числа, то складають ділене з залишком, а потім здійснюють циклічний зсув комбінації, отриманої в результаті додавання останнього діленого з залишком, дістаючи комбінацію без помилок; якщо ж після першого циклічного зсуву і наступного ділення залишок виявиться таким, що його вага буде більшою від допустимого числа виправлень, то повторюється вищезгадана процедура ділення дого часу, поки вага залишку не буде меншою або дорівнюватиме допустимій кількості виправлень; у цьому випадку комбінація, отримана в результаті останнього циклічного зсуву, додається до залишку від ділення цієї комбінації на твірний поліном, а потім здійснюється циклічний зсув на стільки розрядів, на скільки була зсунута складена з останнім залишком комбінація стосовно прийнятої комбінації, в результаті чого отримають виправлену комбінацію.

Твірний поліном є добутком непарних мінімальних поліномів, що становить найменше спільне кратне. Максимальний порядок мінімальних поліномів

$$\rho = 2t - 1. \qquad (12)$$

Порядок полінома використовують для визначення числа співмножників. Для побудови твірного полінома переважно користуються спеціальною таблицею мінімальних незвідних в полі Ґалуа GF (2) поліномів. В окремих випадках допускається використання поліномів й меншого степеня [3]. Декодування кодів БЧХ, які спроможні виправляти більше ніж чотири помилки, є достатньо складною задачею і здійснюється, як правило, на основі алгоритму Берлекемпа [4] або його модифікацій. Певне полегшення може бути, коли комбінацію, одержану після K-кратного зсуву і додавання до залишку, зсувати не вправо, а вліво на S- K циклічних зсувів, але це доцільно робити за умови, коли $K > S/2$ [1]. Отже, теоретично БЧХ-коди можуть виправляти довільну кількість помилок, однак зі збільшенням кратності помилки значно зростає складність пристроїв декодування. Це призводить до зменшення швидкості пересилання повідомлень та ускладнення приймально-передавальної апаратури.

Несистематичні циклічні коди

Сьогодні розроблено десятки кодів, які теоретично можуть виявляти довільну кількість помилок. За наявності такої різноманітності завадостійких кодів здійснити їхній чіткий розподіл на групи за ознаками, що взаємно не перекриваються, є нереальною задачею.

Інший підхід до побудови завадостійкого циклічного коду ґрунтується на використанні унікальних властивостей «ідеальних кільцевих в’язанок» (ІКВ) – впорядкованих цілочислових послідовностей з кільцевою структурою, причому усі 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

$$x_j - 1 \equiv \sum_{i=1}^{j} k_i \,(\mathrm{mod}\, S_n\ ),\ j=1,2,\ldots,n; \tag{13}$$

$$S_n = n\,(n\text{-}1)/\,R + 1, \tag{14}$$

де k_j – i-й елемент обраного ІКВ; S_n, n, R – параметри ІКВ [2].

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 згідно з залежністю

$$d_{min} = 2(n - R). \tag{15}$$

Кількість помилок, які можна виправити за допомогою цього коду, залежить від параметрів n і R [2]:

$$t \le (n - R - 1). \tag{16}$$

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

Розв’язок цієї задачі за методом авторів коду БЧХ зводиться до таких дій:

1) згідно з залежністю (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 стосовно 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 (14) і (15) 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 (14) побудувати циклічний код з параметрами S_n= 15, n= 7, R= 3.

Кілька методів побудови ІКВ описано в [2]. 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 [2]. За таким способом легко знайти послідовність (1,1,2,1,3,2,5), з якої випливає повна система циклічного коду, що відповідає параметрам S_n= 15, n= 7, R= 3:

111011001010000
011101100101000
001110110010100
……..
110110010100001

Циклічний код завдовжки S_n= 15 побудовано.

Для здійснення порівняльного аналізу досліджуваних кодів доцільно скористатися такими залежностями:

$$N = 2^n - 1; \quad (17)$$

$$t = 2^{n-2} - 1; \quad (18)$$

$$P = 2^{n+1}; \quad (19)$$

$$N^* = 2n \pm 1; \quad (20)$$

$$t^* = (N^* - 3)/4; \quad (21)$$

$$P^* = 2(N^* + 1), \quad (22)$$

де N і N^* – довжини кодових комбінацій порівнюваних циклічних кодів; t і t^* – кількість помилок, що виправляється; P і P^* – потужність циклічних кодів БЧХ і ІКВ відповідно.

Формули (17) – (19) випливають зі співвідношень, які описують параметри кодів БЧХ [1], а (20) – (22) – віддзеркалюють оптимальні пропорції між параметрами циклічного коду ІКВ, що забезпечують досягнення його максимальної завадостійкості за обмежень на довжину кодових комбінацій [2].

Висновок

Аналіз результатів порівняння обох кодів, здійснених на основі залежностей (17) – (22), показує, що за фіксованої довжини кодових комбінацій максимально досяжна завадостійкість циклічного коду ІКВ не поступається властивостям коду БЧХ за однакової потужності цих кодів. Певною перевагою коду БЧХ є можливість забезпечення стрімкого зростання потужності (19), але коштом втрати його завадостійкості. Крім того, зі збільшенням кратності помилки значно зростає складність пристроїв декодування, що призводить до зменшення швидкості пересилання повідомлень та ускладнення приймально-передавальної апаратури. На відміну від кодів БЧХ для побудови кодів ІКВ з високим рівнем завадостійкості не потрібні складні обчислення, а довжина кодових комбінацій визначається лінійною залежністю (20), що дало змогу значно розширити спектр побудови кодів з високим рівнем захищеності від завад. Результати 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.

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