УДК 004.056.5

О.Я. Різник[1], І.Ю. Юрчак[2], В.О. Парубчак[3]
Національний університет "Львівська політехніка",
[1]кафедра автоматизованих систем управління
[2]кафедра систем автоматизованого тпроектування

АЛГОРИТМИ КОДУВАННЯ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ЧИСЛОВИХ В'ЯЗАНОК

Розглянуто подання чисел на основі числових в'язанок для кодування інформації. Розглянуто ефективність монолітного коду за евристичними оцінками. Розроблено методику побудови кодових комбінацій чисел на основі теорії числових в'язанок, що уможливлює подання кодових комбінацій чисел у вигляді монолітного коду.

In the article presentations of numbers are examined on the basis of numerical bundles for conducting of code of information. The considered efficiency of monolithic code is after heuristic estimations. Developed method of construction of codes combinations of numbers on the basis of theory of numerical bundles, that enables presentation of codes combinations of numbers as a monolithic code.

Вступ

Сьогодні вагомого значення набуває розроблення математичних моделей та методів оптимізації систем кодування для забезпечення захисту інформації від несанкціонованого доступу. У зв'язку з цим актуальною проблемою стає дослідження методів кодування інформації за допомогою математичних моделей на основі комбінаторних конфігурацій з нееквідистантною структурою – числових лінійок-в'язанок [1, 2, 4].

У системах кодування інформації з різними законами розподілу ваг розрядів коду в деяких випадках цей код виявляється надмірно надлишковим, тому що одні і ті самі числа подаються різними кодовими комбінаціями.

Метою цієї роботи є розроблення та пошук такого комбінаторного варіанта ваг розрядів коду, за якого будь-яке натуральне число можна було б подати єдино можливим способом. Таким кодом є й монолітний код на основі числових лінійок-в'язанок [3].

Монолітний двійковий код має багато переваг перед іншими кодами. Одна з них – простота виявлення та виправлення помилок на приймальній стороні, бо поява хоча б одного символу "1" серед нулів або символу "0" серед одиниць у прийнятій кодовій комбінації свідчить про помилку. Помилка не виявляється, лише коли хибний сигнал виникає в першому або останньому символах пакета (на межі між пакетами нулів та одиниць). Якщо в монолітному коді з'являються хибні символи, то всі вони або частина з них одразу ж виявляються, що спрощує виявлення помилок і забезпечує високу завадостійкість монолітного коду.

Використання монолітного коду на основі числових лінійок-в'язанок для кодування інформації

Досліджуючи системи кодування інформації з різними законами розподілу ваг розрядів монолітного коду, легко помітити, що в деяких випадках розподілу ваг монолітний код виявляється надміру надлишковим, бо одні й ті самі числа подаються кількома різними кодовими комбінаціями двійкового позиційного коду [1, 3].

Розв'язання поставленої задачі зводиться до пошуку оптимального комбінаторного варіанта ваг розрядів монолітного коду, за якого будь-яке натуральне число можна було б подати в монолітному коді єдино можливим способом.

Виникає проблема вибору оптимальної системи ваг розрядів, суть якої полягає в тому, щоб множині кодових комбінацій монолітного коду взаємно однозначно відповідала множина чисел натурального ряду.

Інтерес для дослідження становлять системи кодування, які ґрунтуються на застосуванні комбінаторних властивостей числових в'язанок [3]. Числова в’язанка (ЧВ) – це алгебраїчна структура, утворена на послідовності N цілих додатних чисел, значення яких, як і значення сум поруч розташованих чисел, відзначаються визначену кількість разів R. Елементи ЧВ розміщені один біля одного у вигляді лінійки (ЧЛВ) або кільця (ЧКВ).

Нижче наведена табл. 1 кодових комбінацій монолітного коду, утворених на ЧКВ шостого (n=6) порядку (**1,3,2,7,8,10**):

Таблиця 1

Кодові комбінації кільцевого монолітного коду (1, 3, 2, 7, 8, 10)

Число	Код
0	000000
1	100000
2	001000
3	010000
4	110000
5	011000
6	111000
7	000100
8	000010
9	001100
10	000001
11	100001
12	011100
13	111100
14	110001
15	000110

Число	Код
16	111001
17	001110
18	000011
19	100011
20	011110
21	111110
22	110011
23	111101
24	111011
25	000111
26	100111
27	001111
28	101111
29	110111
30	011111
31	111111

Потужність кільцевого монолітного коду (КМК), реалізованого на ЧВ n-го порядку, визначається загальною кількістю способів утворення кодових слів:

$$N^{(K)}=n(n-1)+1.$$

Завадостійкість монолітного коду можна оцінити за співвідношенням кількості помилкових кодових комбінацій, які виявляються $M_{виявл.}$ (або виправляються $M_{випр.}$), до загальної кількості усіх можливих комбінацій заданої розрядності. Нехай n – розрядність кодового слова, а r – кількість помилкових символів у кодовому слові. Ефективність КМК щодо можливості виявлення і виправлення помилок можна оцінити за допомогою таких залежностей:

$$M^{(k)}_{\text{виявл.}} = \frac{C^r_{n-4}}{C^r_n}100\%, \qquad r < n-4$$

$$M^{(k)}_{\text{вип р.}} = \frac{C^r_{n-8}}{C^r_n}100\%, \qquad r < n-8$$

Ефективність КМК за евристичними оцінками для n=5 - 10, 15, 20, 25, 30; r=1, 2, 3 наведена у табл. 2.

Таблиця 2

Ефективність КМК за евристичними оцінками

C	n									
M, %	5	6	7	8	9	10	15	20	25	30
C_n^1	5	6	7	8	9	10	15	20	25	30
C_{n-4}^1	1	2	3	4	5	6	11	16	21	26
C_{n-8}^1	-	-	-	-	1	2	7	12	17	22
$M_{виявл},\%$	20	33,3	42,8	50	55,5	60	73,3	80	84	86,7
$M_{випр},\%$	-	-	-	-	11,1	20	46,7	60	68	73,3
C_n^2	10	15	21	28	36	45	105	190	300	435
C_{n-4}^2	-	1	3	6	10	15	55	120	210	325
C_{n-8}^2	-	-	-	-	-	1	21	66	136	231
$M_{виявл},\%$	-	6,7	14,3	21,4	27,8	33,3	52,4	63,2	70	74,7
$M_{випр},\%$	-	-	-	-	-	2,2	20	34,7	45,3	53,1
C_n^3	10	20	35	56	84	120	455	1140	2300	4060
C_{n-4}^3	-	-	1	4	10	20	165	560	1330	2600
C_{n-8}^3	-	-	-	-	-	-	35	220	680	1540
$M_{виявл},\%$	-	-	2,8	7,1	11,9	16,7	36,3	49,1	57,8	64
$M_{випр},\%$	-	-	-	-	-	-	7,7	19,3	29,6	37,9

Алгоритм синтезу числових лінійок-в'язанок

Алгоритм побудови кільця монолітного коду складається з таких кроків:

Крок 1. За потужністю КМК вибирають ЧЛВ порядку N кратності R.

Крок 2. Заготовляється масив із N комірок, пронумерованих за зростанням.

Крок 3. В перші R комірок масиву записується число, з якого починається відлік у ЧЛВ, в $(R+1)$-у – наступне, в решту заносяться нулі.

Крок 4. Перший раз число A визначається як збільшене на одиницю найбільше число найкоротшого ряду послідовності чисел, утвореного на множині сум, які знайдені на всіх окремих послідовностях, що належать масиву. Наступний раз число A з тим самим значенням визначається як збільшене на одиницю наступне за найбільшим числом найкоротшого ряду послідовності чисел. Якщо є вільні комірки масиву, число A записується у вільну комірку з найменшим порядковим номером.

Крок 5. Обчислюється нове значення суми елементів масиву ЧЛВ. Якщо у масиві є вільні комірки, знаходять всі суми на всіх послідовностях, а за їхньої відсутності – всі лінійні суми на єдиній послідовності:

а) якщо кожна зі знайдених сум зустрічається не більше ніж R разів і є вільні комірки, то здійснюється перехід до кроку 4. За відсутності вільних комірок і при виконанні умови, що нове значення суми не більше від попереднього, отримується варіант ЧЛВ, після чого виконується крок 7. В іншому разі виконується крок 6;

б) якщо хоча б одна зі знайдених сум з'являється більше ніж R разів, то виконується крок 6.

Крок 6. Знаходять найбільше число B, потім визначають, чи є вільний номер комірки з номером, більшим, ніж той, де розташоване число B; якщо така комірка існує, то з комірки з меншим номером число B переноситься у вільну комірку з більшим номером, після чого виконується крок 5; у протилежному випадку виконується крок 7.

Крок 7. Звільняється комірка з числом B і виконується крок 6. Ознакою закінчення обчислень при побудові повної сім'ї ЧЛВ слугує поява числа, з якого починається відлік в ЧЛВ в комірці $\frac{N+3}{2}$ за умови його відсутності в попередніх комірках для непарних значень N і аналогічно в комірці $\frac{N+2}{2}$ для парних значень N.

Алгоритм кодування за допомогою числових лінійок-в'язанок

Алгоритм кодування за допомогою числових лінійок-в'язанок ґрунтується на понятті монолітного коду та поданні кодуючого числа ASCII-формату та запропонованого методу кодування з використанням числових лінійок-в'язанок та архівації отриманих даних.

Алгоритм кодування можна умовно розділити на три етапи:

- введення даних та ініціалізація бази даних в'язанок.
- генерація кодової комбінації.
- архівація отриманих кодів чисел.

Алгоритм кодування можна умовно розділити на блоки:

- Блок "Ініціалізація бази даних ЧЛКВ" – завантаження ідеальних кільцевих в'язанок у масив рядків.
- Блок "Ввід поточної інформації для кодування. Обчислення суми елементів ЧЛВ" – Введення з клавіатури числа для кодування в полі Edit та вибір відповідної в'язанки. Здійснюється перевірка на порожні поля введення (обробка виняткових ситуацій) та ознаку вибору в'язанки.
- Блок "Порівняння" – здійснюється перевірка суми елементів ІКВ з введеним числом. Якщо введене число більше від суми елементів, то повторне введення числа.
- Блок "Обчислення позицій суми проіндексованої в'язанки" – індексуються позиції у в'язанці та знаходять відповідні індекси суми елементів, що відповідає введеному числу.
- Блок "Побудова таблиці монолітного коду згідно з позиціями ЧЛВ" – генерується таблиця можливих комбінацій в'язанки та монолітний код (від першої позиції індексів до другої заповнюються "1", все решта "0"), який визначає другий варіант в'язанки по позиціях діапазону індексів.
- Блок "Генерація кодових комбінацій відповідно до індексів числової в'язанки" – генерується таблиця кодових комбінацій, де кожна позиція-індекс відповідає коду числа.
- Блок "Побудова кодової комбінації згідно з індексами в таблиці кодів" – остаточний результат згенерованого коду з'єднанням двох кодів-позицій.
- Блок "Цикл Arch" – цикл обробки згенерованої комбінації. Заміна блоків "1" та "0" в 3D-просторі відповідними символами ASCII (груповані блоки "0" та "1" заміняються вибраним відповідно для "0" та "1" ASCII-кодом та кількістю нулів та одиниць). У результаті зменшується обсяг закодованої інформації та ускладнюється підбір ключа для розшифрування.

Висновок

Алгоритм забезпечує захист даних від несанкціонованого доступу завдяки їхньому проміжному перетворенню на код в'язанки, параметри якої відомі тільки користувачу. За допомогою монолітних кодів, побудованих за допомогою в'язанок, можна застосовувати ефективні алгоритми кодування і декодування інформації, що розширяє сферу практичних застосувань у задачах інформаційної техніки і проектування систем кодування [6, 7].

Результати досліджень кодування інформації на основі числових в'язанок дають підстави стверджувати про можливості їхнього використання у сучасних інформаційних технологіях для задач захисту інформації [1, 5].

1. Дурняк Б.В., Різник О.Я., Різник В.В., Я.П. Кісь Я.П., Парубчак В.О.. Захист даних методом комбінаторної оптимізації // Праці третьої міжнародної наукової конференції ISDMIT'2007, м.Євпаторія. т.2, с.152–153. 2. Ризныk О.Я. Комбинаторные модели для синтеза технических устройств и систем на основе числовых линейных сцепок // Контрольно-измерительная техника. – Львов: Вища школа. – 1989. – Вып.45. – С.23–25. 3. Різник В.В. Синтез оптимальних комбінаторних систем. – Львів, 1989. 4. Різник О.Я. Завадостійкий спосіб перетворення сигналів // Матеріали Четвертої укр. конф. з автоматичного керування ("Автоматика-97"). – Черкаси. – 1997. – С.34. 5. Різник О.Я., Парубчак В.О., Скрибайло-Леськів Д.Ю. Використання числових в'язанок для кодування інформації // Праці міжнародної конференції "Сучасні комп'ютерні системи та мережі: розробка та використання" (ACSN'2007). С.112–114. 6. Різник О.Я., Парубчак В.О., Скрибайло-Леськів Д.Ю. Кодування інформації за допомогою монолітного коду. Праці 2-ї міжнародної науково-практичної конференції "Інформаційні технології в наукових дослідженнях і навчальному процесі", м. Луганськ, 2007, т.2. С.88–92. 7. Різник О.Я., Стасевич С.П., Парубчак В.О., Скрибайло-Леськів Д.Ю. Швидкий синтез подібних кодів Баркера // Праці міжнародної конференції з математичного моделювання AMSE'2007, м. Алушта. – С. 23–24.

УДК 004.421

О.В. Бандирська[1], В.В. Різник[2], І.Ю. Юрчак[3]
Національний університет "Львівська політехніка",
[1]кафедра інформаційно-вимірювальних технологій,
[2]кафедра автоматизованих систем управління,
[3]кафедра систем автоматизованого проектування

АЛГЕБРИЧНИЙ МЕТОД ПРОЕКТУВАННЯ КРУГОВИХ ШКАЛ З ВИСОКОЮ РОЗДІЛЬНОЮ ЗДАТНІСТЮ

Розглядається алгебричний метод проектування нееквідистантних кругових шкал з підвищеною роздільною здатністю. Ці шкали ґрунтуються на так званих "ідеальних кільцевих в'язанках". Використовується принцип "оптимальних структурних пропорцій".

Algebraic method for design of non-uniform ring scales with improved resolving ability is described. These scales has been based on the so-called "Gold Ring Bundles". The principle of the "optimum structural proportions" (OSP) is applicated.

Алгебричні моделі та методи проектування систем будь-якого призначення широко застосовуються в радіоелектроніці, технічній кібернетиці, інформаційно-вимірювальній та обчислювальній техніці, а комбінаторні конфігурації широко використовуються для оптимального