

*О.Я.Різник, Національний університет “Львівська політехніка”*

*В.О.Парубчак, Національний університет “Львівська політехніка”*

*Д.Скрибайло-Леськів, Національний університет “Львівська політехніка”*

## **КОДУВАННЯ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ МОНОЛІТНОГО КОДУ**

Різник О.Я., Парубчак В.О., Скрибайло-Леськів Д.

Кодування інформації за допомогою монолітного коду

Стаття присвячена дослідженню методів кодування інформації за допомогою математичних моделей на основі комбінаторних конфігурацій з нееквідистантною структурою – числових лінійок-в’язанок.

*Ключові слова:* системи кодування, розряди коду, вага розряду, монолітний код, числові в’язанки, алгоритм кодування.

Ризник О.Я., Парубчак В.О., Скрыбайло-Лескив Д.

Кодировка информации с помощью монолитного кода

Статья посвящена исследованию методов кодировки информации с помощью математических моделей на основе комбинаторных конфигураций с неэквидистантной структурой – числовых линеек-вязанок.

*Ключевые слова:* системы кодировки, разряды кода, вес разряда, монолитный код, числовые вязанки, алгоритм кодировки.

Сьогодні вагомого значення набувають питання розробки математичних моделей та методів оптимізації систем кодування для забезпечення захисту інформації від несанкціонованого доступу. У зв’язку з цим актуальною проблемою постає дослідження методів кодування інформації за допомогою математичних моделей на основі комбінаторних конфігурацій з нееквідистантною структурою – числових лінійок-в’язанок [1].

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

Рішення задачі зводиться до пошуку такого комбінаторного варіанту ваг розрядів коду, при якому будь-яке натуральне число можна було б подати єдино можливим способом. Таким кодом є й монолітний код на основі числових лінійок-в'язанок.

Монолітний двійковий код має ряд 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 вказує на помилку. Помилка не виявляється лише у тих випадках, коли хибний сигнал виникає в першому або останньому символах пакету (на межі між пакетами нулів та одиниць). Якщо в монолітному коді з'являються хибні символи, то всі вони або частина з них зразу 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 побачити, що в деяких випадках розподілу ваг монолітний код виявляється надміру надлишковим, бо одні й ті ж числа подаються кількома різними кодовими комбінаціями двійкового позиційного коду.

Розв'язок поставленої задачі зводяться до пошуку оптимального комбінаторного варіанту ваг розрядів монолітного коду, при якому 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 базуються на застосуванні комбінаторних властивостей числових в'язанок [2]. Числова в'язанка (ЧВ) - це алгебраїчна структура, утворена на послідовності цілих

додатних чисел, значення яких, як і значення сум поруч розташованих між собою чисел, зустрічаються визначене число раз. Елементи ЧВ розміщені один біля одного у вигляді лінійки або кільця.

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

$$N(K)=n(n-1)+1.$$

Нижче наведена таблиця 1 кодових комбінацій монолітного коду, утворених на простій кільцевій ЧВ шостоного (n=6) порядку (1,3,2,7,8,10).

Таблиця 1

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

Число	Код	Число	Код
0	000000	16	111001
1	100000	17	001110
2	001000	18	000011
3	010000	19	100011
4	110000	20	011110
5	011000	21	111110
6	111000	22	110011
7	000100	23	111101
8	000010	24	111011
9	001100	25	000111
10	000001	26	100111
11	100001	27	001111
12	011100	28	101111
13	111100	29	110111
14	110001	30	011111
15	000110	31	111111

Завадостійкість монолітного коду можна оцінити за співвідношенням кількості помилкових кодових комбінацій, які виявляються  $M_{\text{виявл.}}$  (або виправляються  $M_{\text{випр.}}$ ), до загальної кількості усіх можливих комбінацій заданої розрядності. Нехай  $n$  - розрядність кодового слова, а  $r$  - число помилкових символів у кодовому слові. Ефективність КМК щодо можливості виявлення і виправлення помилок можна оцінити за допомогою наступних залежностей [2]:

$$M_{\text{виявл.}}^{(k)} = \frac{C_{n-4}^r}{C_n^r} 100\%, \quad r < n-4$$

$$M_{\text{випр.}}^{(k)} = \frac{C_{n-8}^r}{C_n^r} 100\%, \quad r < n-8$$

*Алгоритм кодування за допомогою числових лінійок-в'язанок.*

Алгоритм кодування за допомогою числових лінійок-в'язанок базується на основі поняття монолітного коду та представленні кодуючого числа ASCII – формату та запропонованого методу кодування з використанням числових лінійок-в'язанок та архівації отриманих даних.

Алгоритм кодування можна умовно розбити на три етапи:

- 1) ввід даних та ініціалізація бази даних в'язанок;
- 2) генерація кодової комбінації;
- 3) архівація отриманих кодів чисел.

Алгоритм кодування можна умовно розбити на блоки:

1) блок “Ініціалізація бази даних ІКВ” – завантаження ідеальних кільцевих в'язанок в масив рядків;

2) блок “Ввід поточної інформації для кодування. Обчислення суми елементів ІКВ” – Введення з клавіатури числа для кодування в полі Edit та вибір відповідної в'язанки. Здійснюється перевірка на пусті поля вводу (обробка виняткових ситуацій) та ознаку вибору в'язанки;

3) блок “Порівняння” – здійснюється перевірка суми елементів ІКВ з введеним числом. Якщо введене число більше суми елементів, то повторний ввід числа;

4) блок “Обчислення позицій суми проіндексованої в’язанки” – індексується позиції у в’язанці та знаходження відповідних індексів суми елементів, що відповідає введеному числу;

5) блок “Побудова таблиці циклічних та монолітного коду згідно позицій” – 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 позиціям діапазону індексів;

6) блок “Генерація кодових комбінацій відповідно до індексів числової в’язанки” - генерується таблиця кодових комбінацій, де кожна позиція-індекс відповідає коду числа;

7) блок “Побудова кодової комбінації згідно індексів в таблиці кодів” – остаточний результат згенерованого коду шляхом з’єднання двох кодів-позицій;

8) блок “Цикл Arch” – цикл обробки згенерованої комбінації. Заміна блоків “1” та “0” відповідними символами ASCII (груповані блоки “0” та “1” замінюються обраним відповідно для “0” та “1” ASCII-кодом та кількістю нулів та одиниць). В результаті зменшується об’єм закодованої інформації та ускладнюється процес підбору ключа для розшифровки.

Таким чином, алгоритм забезпечує захист даних від несанкціонованого доступу, завдяки їх проміжному перетворенню в код в’язанки, параметри якої відомі тільки користувачу. За допомогою монолітних кодів, побудованих за допомогою в’язанок є можливість застосовувати ефективні алгоритми кодування і декодування інформації, що розширює сферу практичних застосувань в задачах інформаційної техніки і проектування систем кодування.

Результати досліджень кодування інформації на основі числових в’язанок дають підстави стверджувати про можливість їх використання у сучасних інформаційних технологіях.

## Література

1. **Ризнык В.В., Ризнык О.Я., Бандырская О.В.** Синтез помехоустойчивых кодов на основе идеальных числовых отношений //Контрольно-измерительная техника. Вып.47. - Львов: Высшая школа, 1990.

2. **Різняк О.Я.** Завадостійкий спосіб перетворення сигналів // Матеріали Четвертої укр. конф. з автоматичного керування ("Автоматика-97"). - Черкаси. - 1997. - С.34.

Riznyk O.Y., Parubchak V.O. Skrybailo-Les'kiv D.

Information coding with the help of monolithic code

The article is devoted to research of methods of information coding with the help of mathematical models based on combinatorial configurations.

*Key words:* coding systems, code categories, category weight, monolithic code, coding algorithm.