КІБЕРНЕТИКА

УДК 519.17

С.М. НІКОЛАЄВ
Науково-дослідний інститут воєнної розвідки, Київ, Україна, e-mail: *divan24@i.ua*.
О.М. РОМАНОВ
Науково-дослідний інститут воєнної розвідки, Київ, Україна, e-mail: *rolex@i.ua*.
А.М. НИЩУК
Науково-дослідний інститут воєнної розвідки, Київ, Україна, e-mail: *svs14@ukr.net*.

МЕТОД МОДИФІКОВАНОГО ПОШУКУ У ГРАФІ ВГЛИБ ДЛЯ ПОБУДОВИ ВСІХ МОЖЛИВИХ КОДІВ ГРЕЯ ЗАДАНОЇ ДОВЖИНИ

Анотація. Розглянуто задачу пошуку можливих варіантів коду Грея для інтерпретації частотно-часових матриць, які застосовуються під час проєктування каналів передавання інформації. Побудовано неорієнтований однорідний неповний циркулянтний граф 4-го степеня. Запропоновано метод і алгоритм реалізації модифікованого пошуку у графі, за допомогою якого можна побудувати всі коди Грея заданої довжини. Наведено формулу для обчислення кількості варіантів цих кодів.

Ключові слова: бітовий потік, частотно-часова матриця, код Грея, неорієнтований граф.

ВСТУП

Дослідження бітових потоків з апріорно невідомою структурою, які містять різні варіанти завадостійких кодів, є однією із задач теорії кодування [1]. Станом на сьогодні під час побудови каналів передавання інформації зі швидким псевдовипадковим перелаштуванням робочої частоти (ППРЧ, або FHSS) широко застосовуються частотно-часові матриці, в яких кожний частотний стрибок кодується одним символом, що складається з декількох бітів [2]. Кількість бітів у символі визначається як $n = \log_2 M$, де M — кількість частот у каналі з ППРЧ.

Задачу доцільно сформулювати як пошук раціонального бітового кодування для кожного частотного стрибка (символа).

СУТЬ МЕТОДУ МОДИФІКОВАНОГО ПОШУКУ У ГРАФІ

Розглянемо задачу на прикладі побудови каналу передавання інформації з ППРЧ. На рис. 1 наведено варіант частотно-часової матриці для $M = 16$ і $n = 4$ (частотне рознесення між сусідніми частотами — 10 кГц, час випромінювання однієї частотної позиції — 100 мкс, швидкість перелаштування частот — 10000 стрибків на секунду).

Загальну кількість можливих варіантів двійкового кодування, коли символ складається з n бітів, визначають за відомою з комбінаторики формулою

$$K = (2^n)! = M!. \tag{1}$$

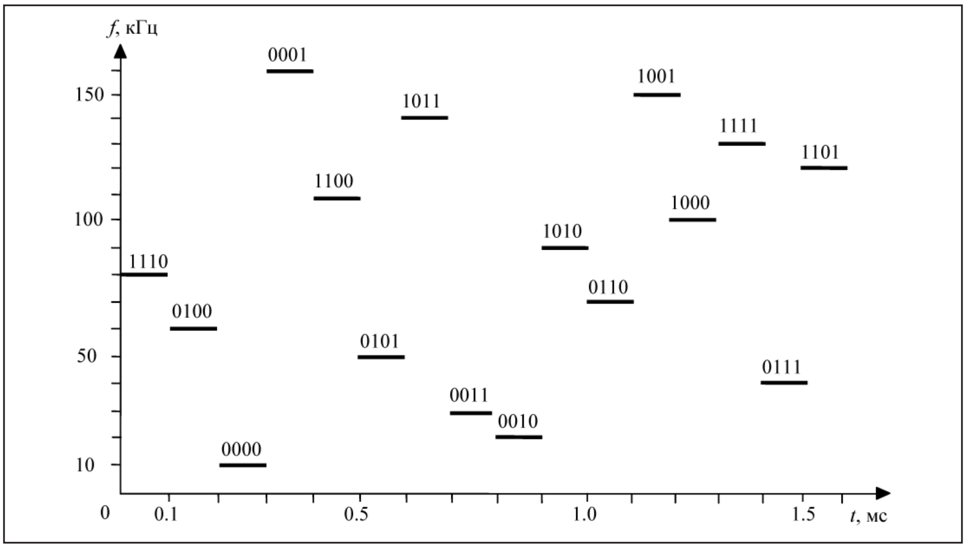

Рис. 1. Частотно-часова матриця сигналу з ППРЧ (над кожною частотною позицією вказано варіант можливого бітового кодування)

Очевидно, що навіть для відносно невеликого n значення K, обчислене за виразом (1), є достатньо великим. Задача пошуку можливих варіантів коду Грея, яким інтерпретують частотні позиції у вигляді бітового потоку, що міститься в каналі передавання інформації, є досить складною для $n \geq 4$. Тому розглянемо її на прикладі з $n = 4$, який відповідає рис. 1. Звісно, що у цьому випадку всі $(2^4)!$ варіантів кодування частотних позицій не можна вважати застосовними на практиці, оскільки для досягнення завадостійкого приймання сусідні частотні позиції мають відрізнятись лише одним бітом, що й передбачено кодом Грея. Наприклад, для 16 значень частот, якими закодовано комбінації з чотирьох бітів, наявний математичний апарат не дає змоги обчислити кількість усіх можливих варіантів кодів Грея (в них кодування двох сусідніх частот мають відрізнятися лише в одному з чотирьох бітів) [3]. Правила формування кодів такі: наприклад, бітові комбінації 0010 і 0011 можуть бути розміщені на сусідніх частотних позиціях (див. рис. 1, позиції 20 і 30 кГц відповідно), тому що $0010 \oplus 0011 = 0001$, а значення 0001 має вагу 1. Водночас, наприклад, бітові комбінації 0010 і 0100 не можуть бути розміщені на сусідніх частотних позиціях, оскільки $0010 \oplus 0100 = 0110$, а значення 0110 має вагу 2. Під вагою бітової комбінації розуміють кількість логічних одиниць у комбінації. Інакше кажучи, сусідні позиції частотно-часової матриці мають відрізнятися лише в одному розряді двійкового числа.

Важливою задачею є визначення кількості варіантів бітових потоків, що формуються кодами Грея, якими можна представити частотно-часову матрицю (див. рис. 1). Це дасть змогу оцінити розмірність задачі представлення частотно-часової матриці під час проєктування каналів передавання інформації.

У роботах [3, 4] викладено загальні результати щодо формування кодів Грея. У [5] описано спосіб побудови коду Грея на основі визначення того, який біт потрібно змінити у символі за допомогою операції $\oplus$. До того ж за оцінкою, наведеною у [5], кількість варіантів коду Грея перевищує $(2^n) \cdot n!$ для $n \geq 3$, але виразу для точного розрахунку немає. У [6] запропоновано алгоритм для створення кодів Грея та кодових слів фіксованої ваги, а у [7] наведено два швидкісні алгоритми формування бітових послідовностей на основі кодів Грея, що призначені для застосування, зокрема, під час проєктування засобів зв’язку. Проте результати цих досліджень не дають змоги побудувати всі можливі варіанти коду Грея та розрахувати (оцінити) їхню кількість.

Представимо всі можливі стани і переходи між бітовими комбінаціями для кількості бітів у символі $n = 4$ у вигляді графу (рис. 2). Вершини графу, яким поставлено у відповідність значення частот, позначено кодовими комбінаціями у десятковому вигляді (наприклад $13 = 1101_2$). Для наведеного графу матриця суміжності має такий вигляд:

$$\mathbf{C} = \begin{vmatrix} 0&1&1&0&1&0&0&0&1&0&0&0&0&0&0&0 \\ 1&0&0&1&0&1&0&0&0&1&0&0&0&0&0&0 \\ 1&0&0&1&0&0&1&0&0&0&1&0&0&0&0&0 \\ 0&1&1&0&0&0&0&1&0&0&0&1&0&0&0&0 \\ 1&0&0&0&0&1&1&0&0&0&0&0&1&0&0&0 \\ 0&1&0&0&1&0&0&1&0&0&0&0&0&1&0&0 \\ 0&0&1&0&1&0&0&1&0&0&0&0&0&0&1&0 \\ 0&0&0&1&0&1&1&0&0&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0 \\ 0&1&0&0&0&0&0&0&1&0&0&1&0&1&0&0 \\ 0&0&1&0&0&0&0&0&1&0&0&1&0&0&1&0 \\ 0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&1 \\ 0&0&0&0&1&0&0&0&1&0&0&0&0&1&1&0 \\ 0&0&0&0&0&1&0&0&0&1&0&0&1&0&0&1 \\ 0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&1 \\ 0&0&0&0&0&0&0&1&0&0&0&1&0&1&1&0 \end{vmatrix}.$$

Матрицю суміжності заповнюють так:

$\mathbf{C}[i, j] = 1$, якщо у графі є ребро (A_i, A_j);

$\mathbf{C}[i, j] = 0$, якщо у графі немає ребра (A_i, A_j).

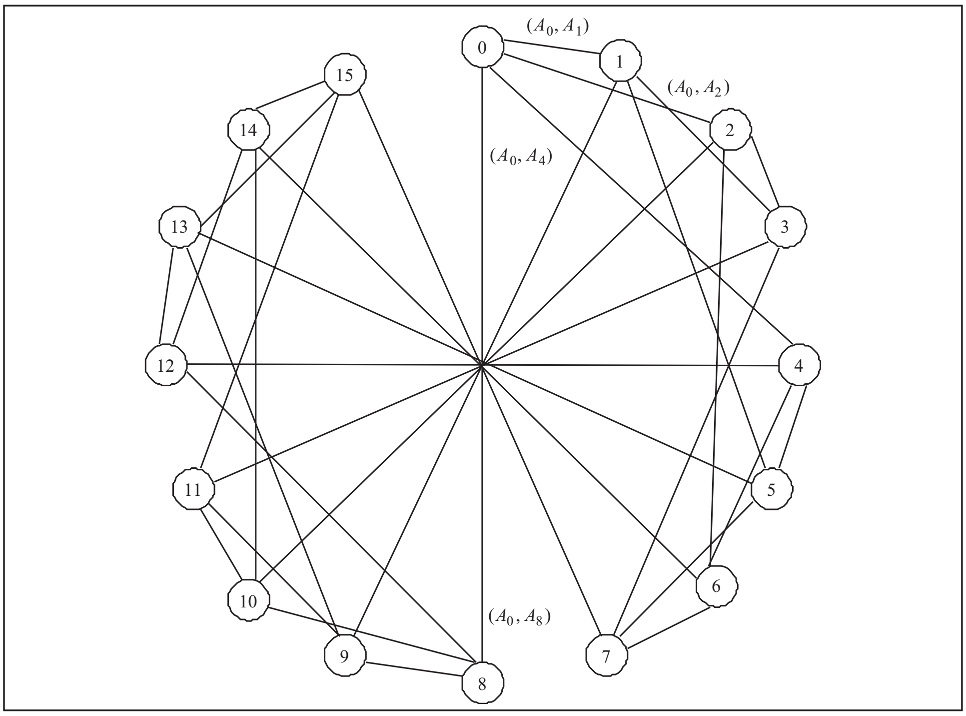

Рис. 2. Граф, яким представлено можливі варіанти кодів Грея для $M = 16$ і $n = 4$ (позначено лише ребра з вершини 0)

Кожен рядок матриці суміжності відповідає одній вершині графу і вказує можливі переходи з неї в інші вершини. Наприклад, перший рядок вказує, що з вершини номер 0 є можливими переходи до вершин з номерами 1, 2, 4 та 8 (на позиціях дозволених переходів у першому рядку матриці містяться одиниці, а на позиціях недозволених — нулі). Другий рядок вказує, що з вершини номер 1 є можливими переходи до вершин 0, 3, 5 та 9. Аналогічно в наступних 14 рядках матриці послідовно містяться можливі переходи для кожної з 14 вершин графу.

Результати аналізу матриці суміжності свідчать про те, що:

— головна діагональ матриці складається лише з нулів, що підтверджує відсутність петель у графі (відсутня можливість переходу вершини в саму себе);

— матриця є симетричною, а отже граф є неорієнтованим.

Цей граф має порядок $|G|=16$ (кількість вершин), кількість ребер $||G||=32$, степінь $d=4$ (кількість сусідів у кожної вершини). Він є однорідним неповним циркулянтним графом 4-го степеня. Задачу формулюють як пошук усіх можливих шляхів у графі $P=x_0x_1...x_{k-1}$, де $k=16$ — довжина шляху, причому перехід $x_{k-1}x_0$ є також обов'язковим. Інакше кажучи, потрібно визначити всі можливі циклічні послідовності вершин графу довжини 16 (кожну вершину обов'язково обходять один раз, повторні обходи заборонені).

Як відомо з теорії графів [8], для побудови всіх можливих шляхів між двома вершинами доцільно скористатися пошуком у графі вглиб [9], який виберемо як метод-прототип. Для цього потрібно запам'ятовувати пройдені вершини і не здійснювати повторні проходи ними. Пошук поточного шляху вважають завершеним у разі досягнення останньої вершини (в нашому випадку, 16-ї) або тоді, коли до шляху не можна додати ще одне ребро. Після успішного завершення побудови одного правильного шляху потрібно повернутися на один крок назад і намагатися побудувати інший правильний шлях. Створюємо масив-індикатор використання кожного ребра. Якщо воно не було використано, то мітка для цього ребра є істинною, в іншому разі — хибною. Під час пошуку шляху перш ніж перейти до вершини, потрібно перевірити, чи було використано поточне ребро (проаналізувати значення мітки). Якщо не було, то його додають до шляху і рекурсивно викликають пошук для наступної вершини. У разі досягнення тупика знаходження фінальної вершини роблять крок назад, при цьому останнє ребро у шляху вважають непройденим. Після кроку назад запропоновано враховувати не лише можливі дозволені переходи з поточної вершини, але й стан заборон, які зроблено на попередніх кроках (це є суттю модифікації пошуку). Узагальнений алгоритм, що реалізує запропонований метод модифікованого пошуку, наведено на рис. 3.

Основою порівняно простого алгоритму є три вкладені цикли, причому у самому внутрішньому циклі застосовано три умови, що спричиняють різні варіанти оброблення. За умови зміни параметрів циклів алгоритм можна використати для $n>4$, при цьому формувати відповідні матрицю суміжності та граф не потрібно.

На прикладі для $n=4$ оцінимо кількість варіантів коду Грея, що формуються запропонованим алгоритмом.

Кількість можливих шляхів у графі від вершини 0 до вершини 1 для $n=4$ становить 672 (в першій третині з них другою вершиною шляху є вершина 2, у другій третині — вершина 4, в останній третині — вершина 8; кількість сусідів у кожної вершини $d=4$). Аналогічно є три групи по 224 варіанти шляхів від вершини 0 до вершини 2, три групи по 224 варіанти шляхів до вершини 4 та три групи по 224 варіанти шляхів до вершини 8 (усього $n=4$). Інакше кажучи, щоб вийти з вершини 0 та успішно в неї повернутися, є $224\cdot(d-1)N=2688$ шляхів обходу графу. Якщо починати шлях від вершини 1, то для успішного повернення

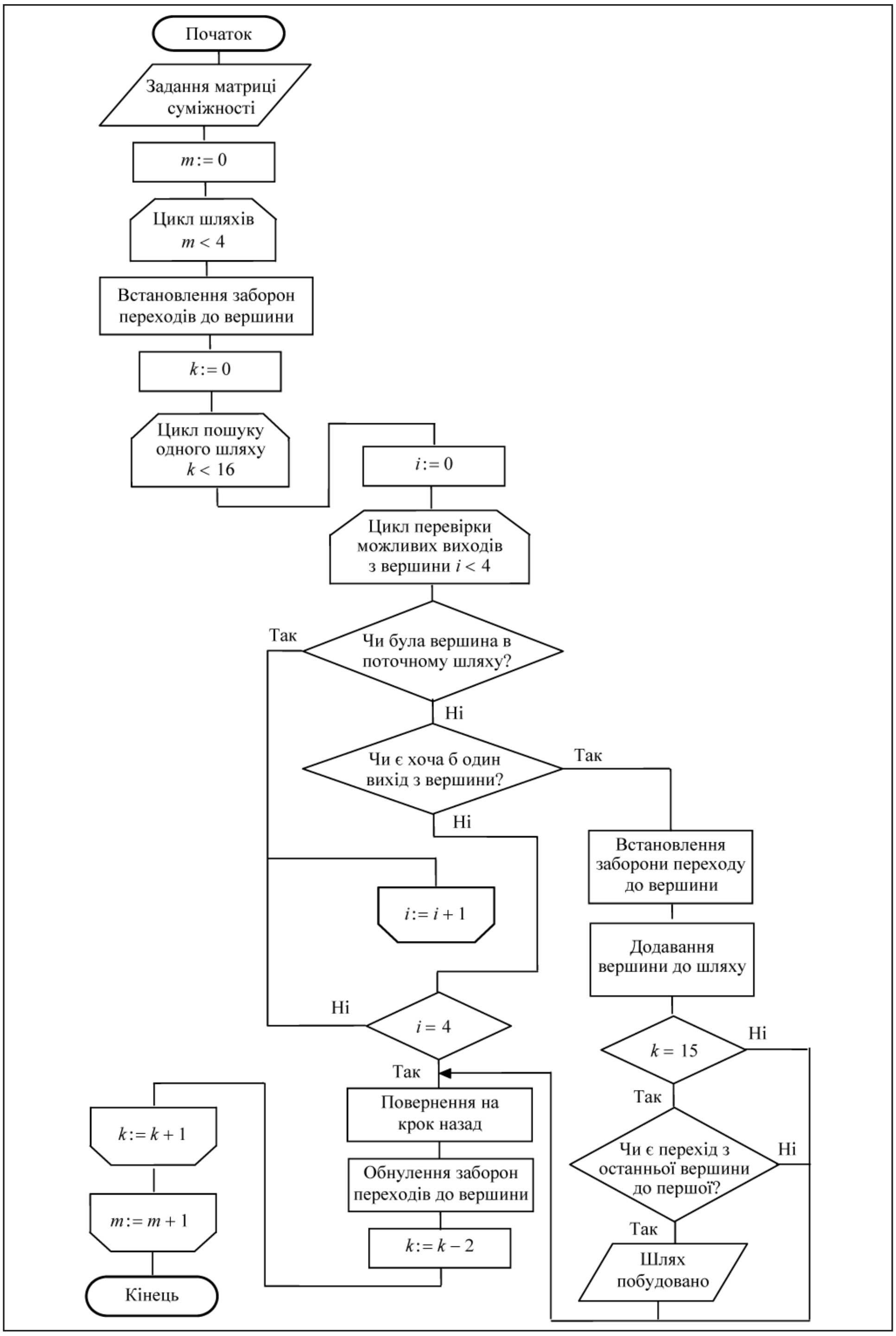

Рис. 3. Узагальнений алгоритм реалізації модифікованого пошуку у графі вглиб для $n = 4$

в неї також потрібно пройти 2688 шляхів. Отже, загалом для $M = 16$ є $W = 2688 \cdot M = 43008$ шляхів у графі.

Результати аналізу цього алгоритму свідчать про те, що метод на основі пошуку вглиб для $|G| = M = 16$, $||G|| = 32$, $n = 4$ і $d = 4$, для того, щоб відшукати 2688 варіантів виходу з вершини 0, виконує 585288 ітерацій (у середньому більше ніж 217 ітерацій на один варіант).

Таблиця 1

Кількість бітів n	Кількість варіантів W	Загальна кількість можливих варіантів K
4	43008	20922789888000
5	614400	32!
6	7618560	64!
7	86704128	128!
8	932184064	256!

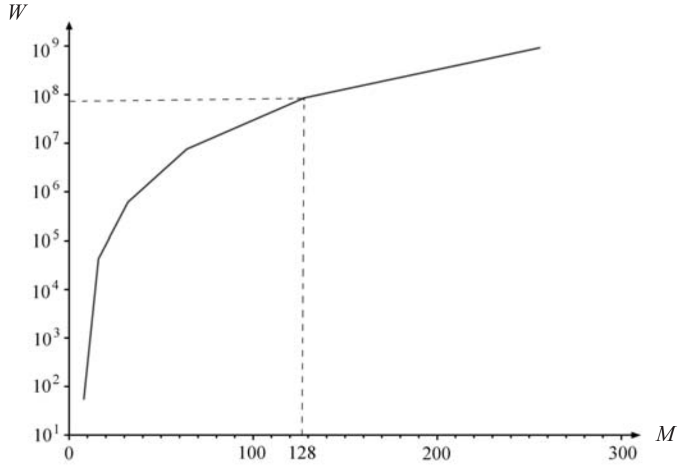

Рис. 4. Графік залежності кількості варіантів кодів Грея W від кількості частот M

Отже, з урахуванням попередніх міркувань загальну кількість можливих шляхів у графі W для довільних значень кількості вершин M, кількості бітів у символі n та кількості сусідів кожної вершини d можна обчислити за такою формулою:

$$W = M(M-2)n(d-1)M = (M^3 - 2M^2)n(d-1), \qquad (2)$$

де M — кількість вершин у графі (кількість частот сигналу з ППРЧ); n — кількість бітів у символі ($n > 3$); d — кількість сусідів кожної вершини графу.

У табл. 1 наведено обчислені за формулою (2) значення кількості варіантів кодів Грея W для різних значень n, якими можна представити частотно-часові матриці. Очевидно, що їхня кількість є значно меншою, ніж кількість варіантів K, обчислених за формулою (1).

На рис. 4 наведено графік залежності кількості варіантів кодів Грея W від кількості частот M, розрахований за виразом (2). Факт достатньо великого значення W для $n \geq 7$ можна використовувати під час проєктування каналів передавання інформації з ППРЧ задля ускладнення декодування у разі несанкціонованого доступу шляхом вибору одного з варіантів коду Грея, який не вказано у документації. Слід зазначити, що для поширеного виду модуляції КАМ-128 ($n = 7$) кількість варіантів перевищує 86 млн, що робить задачу пошуку всіх варіантів кодів Грея під час дослідження відповідних бітових потоків достатньо складною.

Для $n = 4$ запропонованим методом побудовано множину з 43008 варіантів кодів Грея, які збережено в табличному вигляді. Зазначену множину використано під час проєктування каналів передачі інформації з ППРЧ, в яких застосовується код Грея.

ВИСНОВКИ

Метод модифікованого пошуку доцільно застосовувати під час проєктування систем і засобів оброблення даних для інтерпретації частотно-часових матриць ППРЧ та інших бітових потоків кодами Грея. Розмірність задачі можна оцінити за допомогою запропонованої формули (2). Згодом доцільно дослідити використання методу модифікованого пошуку у випадку побудови графів 5-го та більшого степенів під час проєктування елементів каналів передачі інформації, зокрема модуляторів і демодуляторів (коли для забезпечення завадостійкого приймання сусідні символи фазового сузір'я представлені кодами Грея з $n \geq 5$).

СПИСОК ЛІТЕРАТУРИ

1. Nikolaev S.N., Romanov A.N. Method for recognition of parameters of error-correcting block-cyclic codes by a generator polynomial. *Cybernetics and Systems Analysis*. 2021. Vol. 57, N 1. P. 146–154. https://doi.org/10.1007/s10559-021-00338-w.
2. Єрохін В.Ф., Рома О.М., Василенко С.В., Бездрабко Д.Є. Математична модель перехоплення одиничного стрибка сигналу передавача з ППРЧ. *Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування*. 2016. № 64. С. 75–85. https://doi.org/10.20535/ RADAP.2016.64.75-85.
3. Mutze T., Nummenpalo J. Efficient computation of middle levels Gray codes. *ACM Trans. Algorithms*. 2018. Vol. 14, Iss. 2. Article 15. https://doi.org/10.1145/3170443.
4. Белецкий А.Я. Комбинаторика кодов Грея. Киев: Изд. комп. «КВІЦ», 2003. 506 с.
5. Уоррен Г. Алгоритмические трюки для программистов. Москва: ООО Диалектика-Вильямс, 2014. 512 с.
6. Bitner J.R., Ehrlich G., Reingold E.M. Efficient generation of the binary reflected Gray code and its applications. *Comm. ACM.* 1976. Vol. 19, N 9. P. 517–521. https://doi.org/10.1145/360336.360343.
7. Ali Md.M., Islam M.N., Foysal A.B.M. Algorithms for generating binary reflected Gray code sequence: Time efficient approaches. *Proc. 2009 International Conference on Future Computer and Communication* (03–05 April 2009, Kuala Lumpar, Malaysia). Kuala Lumpar, 2009. P. 79–83. https://doi.org/10.1109/ ICFCC.2009.41.
8. Balakrishnan R., Ranganathan K. A Textbook of Graph Theory. New York: Springer New York, 2012. XIII, 292 p. https://doi.org/10.1007/978-1-4614-4529-6.
9. Ashraf Iqbal M. Graph Theory and Algorithms. 2010. 522 p.

S. Nikolaev, O. Romanov, A. Nyshchuk

METHOD OF MODIFIED DEPTH GRAPH SEARCH FOR CONSTRUCTING ALL POSSIBLE GRAY CODES OF A SPECIFIED LENGTH

Abstract. The problem of finding possible variants of the Gray code for the interpretation of time-frequency matrices, which are used in the design of information transmission channels, is considered. An undirected homogeneous incomplete circulant 4-degree graph is constructed. A method and algorithm for implementing a modified search in the graph are proposed, which can be used to construct all the Gray codes of a given length. A formula for calculating the number of variants of these codes is given.

Keywords: bitstream, time-frequency matrix, Gray code, undirected graph.

Надійшла до редакції 03.01.2023