



# НОВІ ЗАСОБИ КІБЕРНЕТИКИ, ІНФОРМАТИКИ, ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ТА СИСТЕМНОГО АНАЛІЗУ

УДК 681.391

**І.О. ПРОЦЬКО**

Національний університет «Львівська політехніка», Львів, Україна,  
e-mail: [ihor.o.protsko@lpnu.ua](mailto:ihor.o.protsko@lpnu.ua).

**М.В. МІЩУК**

Національний університет «Львівська політехніка», Львів, Україна,  
e-mail: [myroslav.mishchuk.knm.2019@lpnu.ua](mailto:myroslav.mishchuk.knm.2019@lpnu.ua).

## БЛОЧНО-ЦИКЛІЧНА СТРУКТУРИЗАЦІЯ БАЗИСУ ПЕРЕТВОРЕННЯ КЛАСУ ФУР'Є НА ОСНОВІ ЦИКЛІЧНОЇ ПІДСТАНОВКИ

**Анотація.** Розглянуто використання підстановки як примітивного елемента для формування циклічної базисної матриці перетворення класу Фур'є. Застосовано циклічну підстановку для блочно-циклічної структуризації гармонічного базису, що надає змогу синтезувати алгоритми швидких дискретних перетворень класу Фур'є довільних обсягів на основі циклічних згорток. Показано, що внаслідок зміни порядку циклів та їхніх перших елементів у циклічних підстановках зменшується кількість обчислень циклічних згорток у швидких алгоритмах дискретних перетворень класу Фур'є.

**Ключові слова:** циклічна підстановка, дискретне косинусне перетворення, синтез алгоритму, блочно-циклічна структура базису, циклічні згортки.

### ВСТУП

У багатьох прикладних застосуваннях використовують комбінаторні множини як засоби математичного аналізу, розроблення обчислювального методу та моделювання [1, 2]. Найбільш поширеними серед комбінаторних скінченних множин підстановок, які виділяють у класи з урахуванням певних умов, є підстановки з різних елементів, підстановки з повтореннями з  $n$  елементів,  $k$  з яких є різними, циклічні підстановки, підстановки кортежів, композиції підстановок та інші [3, 4].

Аналіз і дослідження особливостей комбінаторних об'єктів у конкретних прикладних застосуваннях сприяють підвищенню ефективності розв'язання задач, особливо у випадку комбінаторної генерації та оптимізації.

У розробленні швидких перетворень класу Фур'є (дискретних косинусних і синусних перетворень, дискретних перетворень Хартлі), що є ключовими у цифровому обробленні сигналів, використовують прорідження та перестановки даних перетворення з метою переформування обчислень для отримання алгоритму з меншою обчислювальною складністю. Багатоваріантність алгоритмів ефективних обчислень (з основою два, розщепленою основою, змішаною основою, непарного чи складеного обсягу) охоплює різноманітні комбінаторні множини, що використовуються для їхнього синтезу.

Одним з підходів реалізації швидких перетворень класу Фур'є є приведення обчислення до виконання циклічних згорток [5], що ґрунтується на декомпозиції базисної матриці у набір циклічних структур. У цьому підході використано швидкі алгоритми обчислення згорток, серед яких найбільш відомими є алгорит-

© І.О. Процько, М.В. Міщук, 2021

ми Вінограда малих обсягів, алгоритм Агарвала–Кулі, алгоритм поліноміальних перетворень [6], алгоритм блочних псевдоциркулянтів [7], алгоритм парисекції (Пітасі) [8] або апаратні систолічні архітектури конвольверів з розподіленою арифметикою [9]. У результаті використання гнучкої організації виконання перетворень на основі сформованої блочно-циклічної структури базису перетворення класу Фур'є зменшується обчислювальна складність, виконується паралельне обчислення згорток, покращуються технічні показники (площа, затримка) обчислювача у процесі проектування надвеликих інтегральних схем [10].

#### ПОСТАНОВКА ЗАДАЧІ

У більшості публікацій [5, 11] для формування циклічної базисної матриці перетворення класу Фур'є використовують примітивний елемент  $\alpha_i$ , який визначається за виразом

$$\alpha_i^n \bmod T, \quad n = \varphi(T), \quad (1)$$

де  $\varphi(T)$  — функція Ейлера,  $T$  — період базисної функції перетворення. Однак, застосування примітивного елемента  $\alpha_i$  обмежується для обсягів перетворень  $N$ , що дорівнюють простому числу або конкретним числовим значенням [12].

У роботі [13] використано циклічну підстановку для синтезу швидких алгоритмів обчислення перетворень класу Фур'є на основі циклічних згорток. Основою побудови циклічної підстановки є рядки або стовпці квадратної матриці, що містять цілочисельні аргументи функцій базису дискретного перетворення класу Фур'є. Для компактнішого представлення підстановки використовують послідовність у вигляді циклу, що містить стислий опис блочно-циклічної структури ядра перетворення класу Фур'є. Це надає змогу надалі синтезувати ефективний алгоритм обчислення перетворень класу Фур'є через циклічні згортки.

Отже, актуальним є дослідження особливостей визначення та використання циклічної підстановки для формування блочно-циклічної структури ядра перетворення класу Фур'є, що забезпечить зменшення кількості циклічних згорток в алгоритмах обчислення швидких перетворень класу Фур'є.

#### ВИЗНАЧЕННЯ ЦИКЛІЧНОГО РОЗКЛАДУ ПІДСТАНОВКИ

У сучасних дослідженнях з узагальнення швидких дискретних перетворень класу Фур'є найчастіше використовують теорію алгебр. Розглянемо квадратні матриці  $C_a(k, n)$ , що містять цілочисельні аргументи функцій базису перетворень класу Фур'є,

$$C_a(k, n) = [(k * n) \bmod T], \quad n, k = 0, 1, \dots, T-1. \quad (2)$$

Множина цілочисельних елементів  $(T-1)$ , що є аргументами функцій базису, та алгебраїчна операція добутку за модулем задають алгебраїчну структуру. Для простого обсягу  $T$  алгебраїчна структура, згідно з властивостями, є Абелевою циклічною групою. Тому табличне подання алгебраїчної операції

$$a_{k,n} = (k * n) \bmod T, \quad n, k = 0, 1, \dots, T-1, \quad (3)$$

відповідає таблиці Келі, в якій в результаті переставлення стовпців та рядків на основі примітивного елемента двовимірний масив результатів операцій є Ганкелевим циркулянтом (табл. 1).

Для синтезу швидких алгоритмів обчислення перетворень класу Фур'є у структуризації базису у вигляді набору блочно-циклічних підматриць [14] використовують переставлення рядків та стовпців за допомогою підстановок  $\psi_i$ . Підстановку визначають за двома рядками або стовпцями базисної матриці (2) цілочисельних аргументів за модулем  $T$ .

**Таблиця 1.** Таблиця алгебраїчної операції над аргументами функцій базису

$n \backslash k$	1	2	3	...	$T-2$	$T-1$
1	$a_{11}$	$a_{12}$	$a_{13}$	...	$a_{1(T-2)}$	$a_{1(T-1)}$
2	$a_{12}$	$a_{13}$	$a_{14}$	...	$a_{1(T-1)}$	$a_{11}$
3	$a_{13}$	$a_{14}$	$a_{15}$	...	$a_{11}$	$a_{12}$
...	...	...	...	...	...	...
$T-1$	$a_{1(T-1)}$	$a_{11}$	$a_{12}$	...	$a_{1(T-3)}$	$a_{(T-2)}$

Для складеного обсягу перетворення  $N = N_1 * N_2 * \dots * N_k$ , де  $N_i$  — прості числа, результати операцій (3) відповідають квадратній матриці аргументів функцій базису перетворень класу Фур'є, що складається з множини підматриць. Одна підмножина підматриць містить елементи, які є взаємно простими множникам розкладу обсягу  $(N_i, a_{k,n}) = 1$ , а інша — елементи, кратні певним множникам  $N_i$  складеного обсягу перетворення. Скінченна множина з кратних елементів підматриць лінійно відображається у множину натурального ряду. Множина натурального ряду з операцією (3) є алгебраїчною структурою, що відповідає циклічній групі. Тому підматриці, що містять елементи, кратні певним множникам  $N_i$ , є Ганкелевими циркулянтами. Отже, для складеного обсягу за відповідною підстановкою  $\psi_i$  базисна матриця складатиметься з підматриць у матричній структурі базису перетворень класу Фур'є, що представляють набір Ганкелевих циркулянтів. Залежно від обсягу перетворення  $N$  циклічна підстановка  $P(h)$  може складатися з конкретної кількості циклів відповідної довжини  $t, \dots, m$ , що записуються у вигляді добутку циклів

$$P(h) = (1, \psi(1), \psi^2(1), \dots, \psi^{t-1}(1)) \dots (a_m, \psi(a_m), \psi^2(a_m), \dots, \psi^{m-1}(a_m)), \quad (4)$$

де  $h$  — загальна кількість елементів підстановки,  $t, \dots, m < h$ ;  $a_m$  — елемент аргументу. Кожен елемент аргументів функцій базису перетворення  $a_m = a_{k,n}$  міститься тільки в одному циклі. Наявність кількості циклів у циклічній підстановці (4), надає змогу зменшити обчислювальну складність алгоритму перетворення класу Фур'є.

#### ОБЧИСЛЕННЯ СТАНДАРТНОЇ ЦИКЛІЧНОЇ ПІДСТАНОВКИ

У стандартному вигляді циклічної підстановки, що містить кількість циклів більше одного, використовують запис, у якому цикли записують або в порядку зростання їхніх мінімальних елементів, причому в кожному циклі першим є його найменший елемент [15] або навпаки, цикли записують у порядку зростання їхніх максимальних елементів, причому в кожному циклі першим є його найбільший елемент. Наприклад, циклічна підстановка в першому випадку має вигляд  $P(7) = (1, 4) (2) (6) (3, 7, 5)$ , у другому —  $P(7) = (2) (4, 1) (6) (7, 5, 3)$ .

Є різні комбінаторні підходи до обчислення стандартної циклічної підстановки. У [16] розглянуто алгоритми з перебором елементів підстановки. Рекурсивний алгоритм, що використовує пошук у глибину в графі з вибором невикористаних вершин, описано в роботі [17]. Однак, його реалізація з використанням рекурсії потребує значних витрат часу для одержання циклічної підстановки великих обсягів.

Визначення циклічної підстановки для синтезу швидких алгоритмів обчислення перетворень класу Фур'є на основі циклічних згорток включає обчислювальні витрати, які залежать від періоду  $T$  періоду базисної функції. У роботі [18] описано особливості формування твірних масивів для синтезу швидких

алгоритмів дискретних косинусних перетворень чотирьох видів (ДКП I–IV) на основі циклічних згорток. Наведемо значення періоду  $T$  базисної функції перетворення залежно від обсягу перетворення  $N$  для дискретних косинусних перетворень різних видів:  $T = 2N$  для ДКП–I;  $T = 4N$  для ДКП–II;  $T = 4N$  для ДКП–III;  $T = 8N$  для ДКП–IV.

До обчислювальних витрат під час формування стандартної циклічної підстановки з перебором елементів входять:

1)  $T$  операцій за формулою (3) для одного обчислення рядка або стовпця підстановки, а інший рядок або стовпець підстановки відповідає натуральній послідовності;

2) від  $T$  до  $T^*$  ( $T/2$ ) доступів до елементів для формування  $P(h)$ .

Вважають, що максимальна кількість циклів є меншою ніж  $(T/2)$ . Кількість доступів  $T$  буде мінімальною у випадку, коли циклічна підстанова містить один цикл і перший рядок є натуральною послідовністю. Випадок, коли циклічна підстанова містить лише одні транспозиції з циклами довжини 2, не розглядається, оскільки синтезований алгоритм перетворення на основі циклічних згорток має найбільшу обчислювальну складність.

Розглянемо виконання блочно-циклічної структуризації базису для ДКП-II. Це перетворення застосовують для стиснення зображень та в багатьох стандартах відеокодування, особливо його цілочисельну апроксимацію [9, 19, 20]. Перетворення ДКП-II описують формулою

$$X^{c^2}(k) = \sqrt{\frac{2}{N}} \sum_{n=0}^{N-1} x(n) \cos \left[ \frac{(2n+1)k\pi}{2N} \right], \quad k = 0, 1, \dots, N-1, \quad (5)$$

де  $x(n)$  — вхідні дані перетворення,  $X^{c^2}(k)$  — частотні складові виконання перетворення. Відповідно,  $k$ -та компонента ДКП-II для кожного  $n$ -го базисного вектора матиме вигляд

$$c_{k,n} = \cos(k(2n+1) * n) \pi / (2N). \quad (6)$$

Обчислення стандартної циклічної підстановки виконаємо за цілочисельними аргументами  $c_a(k, n)$  компонент  $c_{k,n}$  ( $k, n = 0, 1, \dots, N-1$ ) базису

$$c_{k,n} = c_a(k, n) \Delta \varphi, \quad (7)$$

де  $c_a(k, n) = k(2n+1)$ ,  $\Delta \varphi = \pi / (2N)$  для цілого значення  $N$  обсягу ДКП-II.

Функція  $\cos(k(2n+1) * n) \pi / (2N)$  є періодичною відносно  $4N$  вибірок, тому, відповідно до (3) базисна матриця аргументів косинусу міститиме елементи аргументів у такому вигляді:

$$C_a^{\text{II}}(k, n) = [c_a(k, n) \bmod (4N)], \quad n, k = 0, 1, \dots, N-1. \quad (8)$$

Функція  $\cos(k(2n+1) * n) \pi / (2N)$  є симетричною відносно аргументу  $2N$ , тому елементи аргументів матриці (8) можна зменшити за такою умовою:

$$c_a^{\text{II}}(k, n) = 4N - [c_a(k, n) \bmod 4N], \quad \text{якщо } (c_a(k, n) \bmod 4N) > 2N. \quad (9)$$

Наприклад, для формування циклічної підстановки ДКП-II обсягу  $N = 20$  виберемо стовпці з  $n = 0$  і  $n = 1$  базисної матриці аргументів (8), зменшених за (9), з  $k = 0, 1, \dots, 2N-1$ , що задають підстановку

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39  
0 3 6 9 12 15 18 21 24 27 30 33 36 39 38 35 32 29 26 23 20 17 14 11 8 5 2 1 4 7 10 13 16 19 22 25 28 31 34 37

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	3	9	13	5	15	5	15	7	19	17	11	11	7	19	17	13	1	3	9
2	3	9	13	1	5	5	15	5	19	17	11	7	7	19	17	11	1	3	9	13
3	9	13	1	3	5	15	5	15	17	11	7	19	19	17	11	7	3	9	13	1
4	13	1	3	9	15	5	15	5	11	7	19	17	17	11	7	19	9	13	1	3
5	2	6	18	14	10	10	10	10	14	2	6	18	18	14	2	6	14	2	6	18
6	6	18	14	2	10	10	10	10	2	6	18	14	14	2	6	18	2	6	18	14
7	18	14	2	6	10	10	10	10	6	18	14	2	2	6	18	14	6	18	14	2
8	14	2	6	18	10	10	10	10	18	14	2	6	6	18	14	2	18	14	2	6
9	4	12	4	12	20	20	20	20	12	4	12	4	4	12	4	12	12	4	12	4
10	12	4	12	4	20	20	20	20	4	12	4	12	12	4	12	4	4	12	4	12
11	4	12	4	12	20	20	20	20	12	4	12	4	4	12	4	12	12	4	12	4
12	12	4	12	4	20	20	20	20	4	12	4	12	12	4	12	4	4	12	4	12
13	5	15	5	15	15	5	15	5	5	15	5	15	15	5	15	5	15	5	15	5
14	15	5	15	5	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15
15	5	15	5	15	15	5	15	5	5	15	5	15	15	5	15	5	15	5	15	5
16	15	5	15	5	5	15	5	15	15	5	15	5	5	15	5	15	5	15	5	15
17	7	19	17	11	5	15	5	15	9	13	1	3	3	9	13	1	11	7	19	17
18	19	17	11	7	15	5	15	5	13	1	3	9	9	13	1	3	7	19	17	11
19	17	11	7	19	5	15	5	15	1	3	9	13	13	1	3	9	19	17	11	7
20	11	7	19	17	15	5	15	5	3	9	13	1	1	3	9	13	17	11	7	19
21	8	16	8	16	0	0	0	0	16	8	16	8	8	16	8	16	8	16	8	16
22	16	8	16	8	0	0	0	0	8	16	8	16	16	8	16	8	16	8	16	8
23	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
24	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
25	11	7	19	17	15	5	15	5	3	9	13	1	1	3	9	13	17	11	7	19
26	7	19	17	11	5	15	5	15	9	13	1	3	3	9	13	1	11	7	19	17
27	19	17	11	7	15	5	15	5	13	1	3	9	9	13	1	3	7	19	17	11
28	17	11	7	19	5	15	5	15	1	3	9	13	13	1	3	9	19	17	11	7
29	13	1	3	9	15	5	15	5	11	7	19	17	17	11	7	19	9	13	1	3
30	1	3	9	13	5	15	5	15	7	19	17	11	11	7	19	17	13	1	3	9
31	3	9	13	1	15	5	15	5	19	17	11	7	7	19	17	11	1	3	9	13
32	9	13	1	3	5	15	5	15	17	11	7	19	19	17	11	7	3	9	13	1
33	14	2	6	18	10	10	10	10	18	14	2	6	6	18	14	2	18	14	2	6
34	2	6	18	14	10	10	10	10	14	2	6	18	18	14	2	6	14	2	6	18
35	6	18	14	2	10	10	10	10	2	6	18	14	14	2	6	18	2	6	18	14
36	18	14	2	6	10	10	10	10	6	18	14	2	2	6	18	14	6	18	14	2
37	16	8	16	8	0	0	0	0	8	16	8	16	16	8	16	8	8	16	8	16
38	8	16	8	16	0	0	0	0	16	8	16	8	8	16	8	16	16	8	16	8
39	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20

Рис. 1. Блочно-циклічна структуризація базису ДКП-II обсягу  $N = 20$  за стандартною циклічною підстановкою

На основі підстановки за алгоритмом з перебором елементів обчислимо стандартну циклічну підстановку

$$P(40) = (0) (13\ 9\ 27) (2\ 6\ 18\ 26) (4\ 12\ 36\ 28) (5\ 15\ 35\ 25) (7\ 21\ 17\ 29) (8\ 24) (10\ 30) (11\ 33\ 19\ 23) (13\ 39\ 37\ 31) (14\ 38\ 34\ 22) (16\ 32) (20).$$

Переставлення рядків за стандартною циклічною підстановкою  $P(40)$  та стовпців за циклічною підстановкою з циклів, що містять непарні елементи

$$(13\ 9\ 27) (5\ 15\ 35\ 25) (7\ 21\ 17\ 29) (11\ 33\ 19\ 23) (13\ 39\ 37\ 31),$$

забезпечує структуризацію базису ДКП-II для  $N = 20$  у вигляді набору циклічних підматриць (рис. 1).

У результаті аналізу блочно-циклічної структури, наведеної на рис. 1, для виконання обчислення ДКП-II обсягу  $N = 20$  необхідно обчислити одинадцять 4-точкових, сім 2-точкових циклічних згорток та чотири одноточкових циклічних згортки, що можуть мати значення множника  $\pm 1$ .

#### ОСОБЛИВОСТІ ФОРМУВАННЯ ЦИКЛІЧНОЇ ПІДСТАНОВКИ ДЛЯ БЛОЧНО-ЦИКЛІЧНОЇ СТРУКТУРИЗАЦІЇ БАЗИСУ ПЕРЕТВОРЕННЯ

Циклічну підстановку (4) можна розглядати як добуток різних циклів

$$P(h) = P_0(h_0)P_1(h_1)P_2(h_2)\dots P_l(h_l), \quad (10)$$

де  $P_i(h_i)$  — цикл;  $h_i$  — довжина циклу;  $l$  — загальна кількість циклів;  $h = h_0 + h_1 + \dots + h_l$ .

У структурі базису перетворення (див. рис. 1) наявні циклічні підматриці, що мають однаковий набір елементів, які належать одному циклу. Однак, ці циклічні підматриці починаються з різних елементів, тому в алгоритмі обчислення потрібно виконати більшу кількість циклічних згорток. Матрична структура базису перетворення у разі переставлення послідовності циклів  $P_i(h_i)$  в (10) не змінить результат перетворень за умови відповідного переставлення послідовності елементів у вхідних даних  $x(n)$ .

Отже, формуючи циклічну підстановку (4, 10) з метою зменшення обчислювальної складності перетворення, потрібно переформувати стандартну циклічну підстановку згідно з наведеною нижче умовою: кожен наступний цикл, якщо він існує, починається з першого елемента, що дорівнює  $(2N - a_{i1})$ , де  $a_{i1}$  — перший елемент попереднього  $i$ -го циклу:

$$P_i(h_i) = (a_{i1}, \psi(a_{i1}), \psi^2(a_{i1}), \dots, \psi^{h-1}(a_{i1})), \quad (11)$$

$$P_{i+1}(h_i) = (2N - a_{i1}, \psi(2N - a_{i1}), \psi^2(2N - a_{i1}), \dots, \psi^{h-1}(2N - a_{i1})).$$

Блок-схему алгоритму формування циклічної підстановки з розміщенням послідовності циклів, що відповідають умові (11), наведено на рис. 2. Знаходження циклічної підстановки визначається двома стовпцями  $A$  та  $B$  базисної матриці аргументів функцій ДКП-II обсягу  $N > 0$ , які позначені на блок-схемі як масиви  $A[]$  і  $B[]$ . Порядок перебору перших елементів задається масивом  $Et[N] = \{0, 1, (2N - 1), 2, (2N - 2), 3, (2N - 3), \dots, 2N\}$  відповідно до (11),  $sub[]$  — масив елементів циклічної підстановки з відповідними довжинами циклів  $block[]$ . Згідно з блок-схемою алгоритму, якщо елемент  $k \in$  в масиві  $Et[N]$  і відповідає умові  $A[k] \notin sub$ , то наявний цикл з першим елементом, що відповідає умові (11). Елементи, які містяться в попередніх циклах, надалі з  $Et[N]$  не використовуються. У результаті виконання функцій за блок-схемою алгоритму отримуємо масиви  $sub$  та  $block$ , які визначають циклічну підстановку  $P(h)$ .

Відповідно до блок-схеми (див. рис. 2) реалізовано функцію  $make\_hasharr()$  формування циклічної підстановки  $P(h)$  для синтезу алгоритмів швидких дискретних перетворень класу Фур'є довільних обсягів на основі циклічних згорток. Наприклад, для ДКП-II обсягу  $N = 20$  сформована циклічна підстановка після виконання функції  $make\_hasharr()$  матиме вигляд

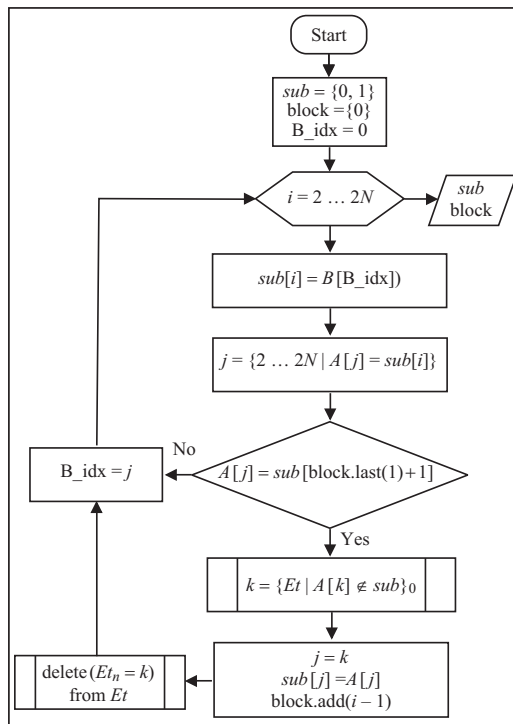


Рис. 2. Блок-схема алгоритму формування циклічної підстановки

$$P(40) = (0) \ (1 \ 3 \ 9 \ 27) \ (39 \ 37 \ 31 \ 13) \ (2 \ 6 \ 18 \ 26) \ (38 \ 34 \ 22 \ 14) \ (4 \ 12 \ 36 \ 28) \\ (5 \ 15 \ 35 \ 25) \ (7 \ 21 \ 17 \ 29) \ (33 \ 19 \ 23 \ 11) \ (8 \ 24) \ (32 \ 16) \ (10 \ 30) \ (20).$$



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	3	9	13	1	3	9	13	1	5	15	5	15	7	19	17	11	7	19	17
2	3	9	13	1	3	9	13	1	5	15	5	15	7	19	17	11	7	19	17	
3	9	13	1	3	9	13	1	3	5	15	5	15	17	11	7	19	17	11	7	
4	13	1	3	9	13	1	3	9	15	5	15	5	11	7	19	17	11	7	19	
5	1	3	9	13	1	3	9	13	5	15	5	15	7	19	17	11	7	19	17	
6	3	9	13	1	3	9	13	1	5	15	5	15	7	19	17	11	7	19	17	
7	9	13	1	3	9	13	1	3	5	15	5	15	17	11	7	19	17	11	7	
8	13	1	3	9	13	1	3	9	15	5	15	5	11	7	19	17	11	7	19	
9	2	6	18	14	2	6	18	14	10	10	10	10	14	2	6	18	14	2	6	
10	6	18	14	2	6	18	14	2	10	10	10	10	2	6	18	14	2	6	18	
11	18	14	2	6	18	14	2	6	10	10	10	10	6	18	14	2	6	18	14	
12	14	2	6	18	14	2	6	18	10	10	10	10	18	14	2	6	18	14	2	
13	2	6	18	14	2	6	18	14	10	10	10	10	14	2	6	18	14	2	6	
14	6	18	14	2	6	18	14	2	10	10	10	10	2	6	18	14	2	6	18	
15	18	14	2	6	18	14	2	6	10	10	10	10	6	18	14	2	6	18	14	
16	14	2	6	18	14	2	6	18	10	10	10	10	18	14	2	6	18	14	2	
17	4	12	4	12	4	12	4	12	20	20	20	20	12	4	12	4	12	4	12	
18	12	4	12	4	12	4	12	4	20	20	20	20	4	12	4	12	4	12	4	
19	4	12	4	12	4	12	4	12	20	20	20	20	12	4	12	4	12	4	12	
20	12	4	12	4	12	4	12	4	20	20	20	20	4	12	4	12	4	12	4	
21	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	
22	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15	
23	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	
24	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15	5	15	
25	7	19	17	11	7	19	17	11	5	15	5	15	9	13	1	3	9	13	1	
26	19	17	11	7	19	17	11	7	15	5	15	5	13	1	3	9	13	1	3	
27	17	11	7	19	17	11	7	19	5	15	5	15	1	3	9	13	1	3	9	
28	11	7	19	17	11	7	19	17	15	5	15	5	3	9	13	1	3	9	13	
29	7	19	17	11	7	19	17	11	5	15	5	15	9	13	1	3	9	13	1	
30	19	17	11	7	19	17	11	7	15	5	15	5	13	1	3	9	13	1	3	
31	17	11	7	19	17	11	7	19	5	15	5	15	1	3	9	13	1	3	9	
32	11	7	19	17	11	7	19	17	15	5	15	5	3	9	13	1	3	9	13	
33	8	16	8	16	8	16	8	16	0	0	0	0	16	8	16	8	16	8	16	
34	16	8	16	8	16	8	16	8	0	0	0	0	8	16	8	16	8	16	8	
35	8	16	8	16	8	16	8	16	0	0	0	0	16	8	16	8	16	8	16	
36	16	8	16	8	16	8	16	8	0	0	0	0	8	16	8	16	8	16	8	
37	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	
38	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	
39	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	

Рис. 3. Блочно-циклічна структуризація базису ДКП-II обсягу  $N = 20$  за сформованою циклічною підстановкою, що відповідає умові (11)

Переставлення рядків за сформованою циклічною підстановкою  $P(40)$  та стовпців за циклічною підстановкою з циклів, що містять непарні елементи

$$(1\ 3\ 9\ 27)\ (39\ 37\ 31\ 13)\ (5\ 15\ 35\ 25)\ (7\ 21\ 17\ 29)\ (33\ 19\ 23\ 11),$$

забезпечує структуризацію базису ДКП-II обсягу  $N = 20$  у вигляді набору циклічних підматриць (рис. 3).

У результаті аналізу блочно-циклічної структури, наведеної на рис. 3, для ефективного обчислення ДКП-II обсягу  $N = 20$  потрібно обчислити шість 4-точкових, сім 2-точкових циклічних згорток та чотири одноточкових циклічних згортки. Інакше кажучи, кількість 4-точкових згорток зменшилася відносно блочно-циклічної структуризації, наведеної на рис. 1, у результаті наявності циклів з першими елементами (1 і 29, 2 і 28, 7 і 33), що відповідають умові (11). Для 2-точкових циклічних згорток наявність циклів з першими елементами 8 і 32 залишається такою самою, бо враховується попередня наявність ідентичних згорток у процесі аналізу блочно-циклічної структури базису ДКП-II обсягу  $N = 20$ .

У табл. 2 наведено для порівняння значення загальної кількості циклічних згорток для обчислення ДКП-II коротких обсягів  $N$  з блочно-циклічною структуризацією за стандартною циклічною підстановкою та за сформованою циклічною підстановкою, що відповідає умові (11).

Загальна кількість циклічних згорток у випадку обчислення ДКП-II обсягу  $N = 20$  дорівнює  $17 = 6 + 7 + 4$ , в яку входять 4-точкові, 2-точкові та одноточкові циклічні згортки.

**Таблиця 2.** Значення загальної кількості циклічних згорток для обчислення ДКП-II малих обсягів  $N$

Обсяг $N$ ДКП-II	Загальна кількість циклічних згорток		Різниця загальних кількостей циклічних згорток
	за стандартною циклічною підстановкою	за циклічною підстановкою, за умовою (11)	
10	14	7	7
11	5	4	1
12	17	15	2
13	14	10	4
14	16	12	4
15	26	16	10
16	5	5	0
17	5	4	1
18	28	15	13
19	10	4	6
20	36	17	19
21	31	24	7
22	14	7	7
23	5	4	1
24	26	24	2
25	12	9	3
26	44	16	28
27	19	16	3
28	24	20	4
29	5	4	1
30	89	34	55
31	10	4	6
32	6	6	0
33	35	16	15
34	14	7	7
35	37	18	19

Аналіз табл. 2 показує, що в результаті формування блочно-циклічної структури базису ДКП-II за циклічною підстановкою, що відповідає умові (11), для обсягів перетворення  $N = 2^i$  ( $i = 4, 5, \dots$ ) загальна кількість циклічних згорток не змінюється, для простих обсягів  $N$  загальна кількість циклічних згорток зменшується від одиниці і більше, а для складених  $N$  загальна кількість циклічних згорток зменшується в межах 40–70 %.

Програмна реалізація синтезу алгоритмів ДКП-II надає змогу формувати різні підстановки за рядками або стовпцями квадратної матриці цілочисельних аргументів функцій базису, адже, відповідно до теорії, примітивний елемент може бути і не один. Це дасть можливість оптимізувати структуру під час проектування, зменшити обчислювальну складність та забезпечити високі показники швидкодії для малих обсягів перетворень ДКП-II [21].

#### ВИСНОВКИ

Для структуризації базису перетворення у вигляді набору блочно-циклічних підматриць визначення примітивних елементів за підстановками є більш ефектив-



ним порівняно зі знаходженням примітивних елементів  $\alpha_i$  (1) та визначенням переставленої послідовності  $a_i^t \bmod T$  ( $t=0, \dots, T-1$ ) з піднесенням  $\alpha_i$  до степеня. Це спричиняє пришвидшення синтезу швидких алгоритмів дискретних перетворень класу Фур'є довільних обсягів на основі циклічних згорток.

Синтез швидких алгоритмів дискретного косинусного перетворення на основі циклічних згорток з урахуванням умови (11) у процесі обчислення циклічної підстановки спричиняє зменшення кількості циклічних згорток і, відповідно, зниження обчислювальної складності перетворення, яка визначається обсягом перетворення (кількість елементів дорівнює простому числу, складений, такий, що дорівнює цілому степеню двійки). Значення обчислювальної складності алгоритму обчислення перетворень класу Фур'є на основі циклічних згорток, крім конкретного обсягу перетворення, визначається кількістю циклічних згорток, їхнім обсягом, алгоритмом швидких циклічних згорток та блочно-циклічною структурою базису.

Програмна реалізація блочно-циклічної структуризації базису перетворення на основі циклічних підстановок надає змогу вибрати циклічну підстановку, що мінімізує кількість та обсяг циклічних згорток, необхідних для обчислення, й оптимізує топологію на системному етапі проектування інтегральних схем обчислювачів дискретного перетворення класу Фур'є.

#### СПИСОК ЛІТЕРАТУРИ

1. Семенова Н.В., Колечкіна Л.М. Векторні задачі дискретної оптимізації на комбінаторних множинах: Методи дослідження та розв'язання. Київ: Наук. думка, 2009. 266 с.
2. Stoyan Yu.G., Grebennik I.V. Description and generation of combinatorial sets having special characteristics. *International Journal of Biomedical Soft Computing and Human Sciences, Special volume "Bilevel Programming, Optimization Methods, and Applications to Economics"*. 2013. Vol. 18, N 1. P. 83–88.
3. Bona M. Combinatorics of permutations. Boca Raton; London; New York: Chapman & Hall/CRC, 2004. 337 p. <https://doi.org/10.1201/b18255>.
4. Brualdi R.A. Introductory combinatorics. Upper Saddle River, NJ: Pearson Prentice Hall, 2010. 605 p.
5. Rader C.M. Discrete Fourier transform when the number of data samples is prime. *Proc. IEEE*. 1968. Vol. 56. P. 1107–1108.
6. Blahut R.E. Fast algorithms for signal processing. Cambridge: Cambridge University, 2010. 466 p.
7. Teixeira M., Rodríguez Y.I. Parallel cyclic convolution based on recursive formulations of block pseudocirculant matrices. *IEEE Trans. Signal Processing*. 2008. Vol. 56, N 7. P. 27–55.
8. Терещенко А.Н. Оптимизация метода Питасси вычисления свертки. *Искусственный интеллект*. 2009. № 1. С. 204–212.
9. Maher J., Meher P.K. Scalable approximate DCT architectures for efficient HEVC-compliant video coding. *IEEE Trans. Circuits Syst. Video Technol.* 2017. Vol. 27, N 8. P. 1815–1825.
10. Cotorobai L.-T., Chipper D.F. A new VLSI algorithm for type IV DCT for an efficient implementation of obfuscation technique. *Proc. 43rd International Conference on Telecommunications and Signal Processing (TSP) (7–9 July 2020, Milan, Italy)*. Milan, 2020. <https://doi.org/10.1109/TSP49548.2020.9163537>.
11. Chan Y.-H., Siu W.-C. Generalized approach for the realization of discrete cosine transform using cyclic convolutions. *Proc. IEEE Int. Conference Acoust., Speech, Signal Process.: Digit. Speech Processing (27–30 April 1993, Minneapolis, USA)*. Minneapolis, 1993. Vol. III. P. 277–280. <https://doi.org/10.1109/ICASSP.1993.319489>.
12. Meher P.K., Swamy M.N.S., New systolic algorithm and array architecture for prime-length discrete sine transform. *IEEE Transactions on Circuits and Systems II: Express Briefs*. 2007. Vol. 54, Iss. 3. P. 262–266. <https://doi.org/10.1109/TCSII.2006.889453>.

13. Prots'ko I. Generalized approach for synthesis and computation DST using cyclic convolutions. *Proc. VIII International Conference MEMSTECH'2012* (18–21 April 2012, Lviv, Poljana). Lviv, 2012. P. 66–67.
14. Пат. 96540 Україна, G06F 17/16 (2006.01), H03M 7/30 (2006.01). Процько І.О. Спосіб приведення дискретних гармонічних складових цифрових сигналів до циклічних згорток. Опубл. 10.11.2011, Бюл. № 21.
15. Knuth D. The art of computer programming. Vol. 4. Fascicle 2: Generating all tuples and permutations. Boston: Addison-Wesley, 2005. 144 p.
16. Kreher D.L., Stinson D.R. Combinatorial algorithms: Generation, enumeration and search. Boca Raton, FL: CRC Press, 1999. 329 p.
17. Permutation cycle. URL: <https://mathworld.wolfram.com/PermutationCycle.html>.
18. Процько І.О. Особливості обчислення твірних масивів для синтезу швидких алгоритмів ДКП І–IV. *Радіоелектроніка, інформатика, управління*. 2020. № 2. С. 149–157. <https://doi.org/10.15588/1607-3274-2020-2-15>.
19. Гнатив Л.А. Целочисленные косинусные преобразования для высокоэффективного кодирования изображений и видео. *Кибернетика и системный анализ*. 2016. Т. 52, № 5. С. 161–176.
20. Процько І.О., Кузьмінський Р.Д., Теслюк В.М. Ефективне обчислення цілочисельного ДКП-II для стиснення зображень. *Радіоелектроніка, інформатика, управління*. 2019. № 2. С. 151–157. <https://doi.org/10.15588/1607-3274-2019-2-16>.
21. Prots'ko I., Rykmas R. The runtime benchmarking of DCT-II based on cyclic convolutions. *International Journal of Condition Monitoring and Diagnostic Engineering Management*. 2018. Vol. 21, N 2. P. 11–16.

## I. Prots'ko, M. Mishchuk

### BLOCK-CYCLIC STRUCTURING OF THE BASIS OF FOURIER CLASS TRANSFORMS BASED ON CYCLIC SUBSTITUTION

**Abstract.** A cyclic substitution is used for block-cyclic structuring of the harmonic basis, which allows synthesizing the algorithms for fast discrete transforms of Fourier class of arbitrary size based on cyclic convolutions. The peculiarities of the form of recording of cyclic substitution for formation of block-cyclic structure of the basis are investigated. A special form of cyclic substitution notation is shown to reduce the amount of computation of cyclic convolutions in fast algorithms of discrete Fourier transforms.

**Keywords:** cyclic substitution, discrete cosine transform, synthesis of algorithm, block-cyclic structure, cyclic convolutions.

*Надійшла до редакції 20.10.2020*