УДК 004.421.2:517.443

І. Процько
Національний університет "Львівська політехніка",
кафедра систем автоматизованого проектування

АНАЛІЗ АЛГЕБРАЇЧНОЇ СИСТЕМИ АРГУМЕНТІВ ДЛЯ ПРОСТОГО ОБСЯГУ ДПФ

Проаналізовано аргументи дискретного перетворення класу Фур'є (ДПФ) для простого обсягу, що задають частковий випадок алгебраїчної системи – абелеві групи. Визначено особливості та характер породжуючих елементів даної системи.

Ключові слова: дискретні перетворення Фур'є, абелева група, породжуючий елемент.

Arguments of DFT for prime size specifying partial case of algebraic systems – abel groups is analyzed. Features of generate element this algebraic systems are determined.

Keywords: discrete fourier transforms, abel group, generate element.

Вступ

У багатьох прикладних задачах для ефективного дослідження та аналізу систем сигнали складної форми відтворюють лінійним перетворенням над елементарними (базисними) функціями [1]. Під час проходження в системі неперервні сигнали складної форми представляють у вигляді зваженої суми базисних функцій

$$U(t) = \sum_k C_k \phi(t)_k, t \in [t_1, t_2]. \quad (1)$$

Отже, за вибраного базису сигнал *U(t)* повністю задається коефіцієнтами C_k. Таку сукупність чисел називають дискретним спектром сигналу. Спектри є зручною аналітичною формою зображення сигналів. Такий підхід на основі базисного набору особливо продуктивний для аналізу лінійних інваріантних до зсуву систем. Історично склалось, що співвідношення (1) називають узагальненим рядом Фур'є, а коефіцієнти C_k – узагальненими коефіцієнтами Фур'є. Адже вперше визначення C_k на основі властивості ортогональності було застосовано в ряді Фур'є. Визначення спектральних складових значно легше обчислюється в ортогональних базисах. Повні системи ортогональних функцій забезпечують як завгодно малу різницю між неперервною функцією та її рядом за необмеженого збільшення кількості його членів.

Широке визнання отримали зображення детермінованих сигналів експоненціальними базисними функціями (перетворення Фур'є, перетворення Лапласа). Перехід від експоненціальних базисних функцій через формули Ейлера відображає складний детермінований сигнал у вигляді суми гармонічних складових (cos ωt, sin ωt). Параметр ω відповідає круговій частоті, тому результат гармонічного перетворення часто називають частотною формою зображення сигналу. Для представлення, особливо дійсних даних в їх гармонічний спектральний образ поряд з швидким перетворенням Фур'є використовується дискретне косинусне перетворення, дискретне перетворення Хартлі, що мають відповідні базисні функції W, які складаються з певного набору гармонічних складових.

Розроблення узагальненої схеми ефективного обчислення дискретних гармонічних перетворень вимагає аналізування особливостей базису перетворення на основі періодичності та симетрії гармонік, що є елементами базису

$$X'(n) = \sum_{k=0}^{N-1} x(k) W^{nk}, \quad (2)$$

де W – лінійне гармонічне перетворення вхідних даних з аргументами n, k=1,2,...,N-1.

$$X(0) = \sum_{k=0}^{N-1} x(k); \; X(n) = X'(n) - x(0); \quad n=1,2,...,N-1.$$

Дискретне гармонічне перетворення в матричній формі:

$$X = W * x, \tag{3}$$

де W(kxn) – квадратна базисна матриця, x(N) and X(N) – матриці-стовпці вхідних та вихідних даних. Базисом дискретних гармонічних перетворень є функції синуса, косинуса та їхніх комбінацій з відповідними аргументами.

Аналіз останніх досліджень

У роботах [2, 3] розглянуто приведення обчислення перетворення (2) до циклічних згорток для значення простого обсягу за відповідними перестановками вхідних і вихідних даних. Відображення індексів для приведення використовують за первісним коренем (генератором, примітивним елементом) циклічної групи. Важливим питанням є подальше дослідження даних алгебр та особливостей первісних коренів у формуванні множин.

1. Формування алгебраїчної системи аргументів

Детально проаналізуємо основні аргументи φ=(2π×n×k/N), (n,k=1,(1),...,N-1), що є основою дискретної базисної функції перетворень класу Фур'є. Спрощено, без врахування $\Delta\varphi=(2\pi/N)$ аргументи задаються добутками цілих чисел (k×n) і є ключовими елементами матриці. Дискретні гармонічні базисні функції періодичні відносно N, тому можна подати елементи матриці аргументів базису порядку (N×N) у вигляді:

$$a_{kn} = (n \times k) \bmod N, \tag{4}$$

де a_{kn} цілочисельні значення аргументів базисної матриці по n=1(1)N-1 рядку та k =1(1)N-1 стовпцю. Тобто, одержали двовимірну матрицю цілих елементів, що належать множині $a_{kn} \in (1,2,..., N-1)$,

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1(n-1)} & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2(n-1)} & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3(n-1)} & a_{3n} \\ & & & \dots & & \\ a_{(n-1)1} & a_{(n-1)2} & a_{(n-1)3} & \dots & a_{(n-1)n} & \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{n(n-1)} & a_{nn} \end{pmatrix} . \tag{5}$$

З набору елементів множини (1,2,..., N-1), якими є n, k за (4) маємо матрицю значень a_{kn}, що також належать множині (1,2,..., N-1). Тобто, матрицю значень аргументів можна подати у вигляді таблиці для алгебраїчної операції множення за модулем N (*= (n x k) mod N)

$$\begin{array}{c|cccc} * & 1 & 2 & 3 \dots & N-1 \\ \hline 1 & a_{11} & a_{12} & a_{13} \dots & a_{1(N-1)} \\ 2 & a_{21} & a_{22} & a_{23} \dots & a_{2(N-1)} \\ 3 & a_{31} & a_{32} & a_{33} \dots & a_{3(N-1)} \\ \dots & & & \dots & \\ (N-1) & a_{(N-1)1} & a_{(N-1)2} & \dots & a_{(N-1)(N-1)} \end{array} \tag{6}$$

На перетині рядка *i* стовпця *j* знаходимо результат композиції і *j = a_{ij} . Приклад таблиці для N=11, алгебраїчної операції множення за модулем N (4):

*	1	2	3	4	5	6	7	8	9	10
1:	1	2	3	4	5	6	7	8	9	10
2:	2	4	6	8	10	1	3	5	7	9
3:	3	6	9	1	4	7	10	2	5	8
4:	4	8	1	5	9	2	6	10	3	7
5:	5	10	4	9	3	8	2	7	1	6
6:	6	1	7	2	8	3	9	4	10	5
7:	7	3	10	6	2	9	5	1	8	4
8:	8	5	2	10	7	4	1	9	6	3
9:	9	7	5	3	1	10	8	6	4	2
10:	10	9	8	7	6	5	4	3	2	1

Одержані матриці алгебраїчної операції (4) симетричні головній та бічній діагоналям, доповнено симетричні (mod N) відносно середини вертикалі ($a_{ik}+ a_{(N-i)k} =N$) та горизонталі ($a_{ki}+ a_{k(N-i)} =N$), крім елементів, що дорівнюють нулю.

Отже, значення аргументів базисної матриці ДГП відповідають заданій множині з (N-1) елементів та визначаються на основі операції (4), задаючи алгебраїчну систему.

2. Аналіз сформованих алгебраїчних систем

2.1. Властивості алгебраїчної системи

Проаналізуємо системи <N-1,*> задані множиною елементів (1,2…N-1) та операцією на відповідність до часткових випадків алгебр для конкретних значень обсягів перетворень.

У випадку N – простого числа в системі <N, * > , операція має властивості:

а) комутативності, для будь-яких елементів a, b з множини N виконується рівність a*b = b*a,

$$[(k \times n) \bmod N]*[(n \times k) \bmod N]= [(n \times k) \bmod N]*[(k \times n) \bmod N], \quad (7)$$

наприклад, система <11, x> на основі (6) маємо рівність,

$a_{57} * a_{35} = [(5 \times 7) \bmod 11]*[(3 \times 5) \bmod 11] = [(3 \times 5) \bmod 11]*[(5 \times 7) \bmod 11] = 2*4=4*2=8;$

б) асоціативності для будь-яких елементів a, b, c з множини N, (a*b)*c= a*(b*c),

$$\{[(k \times n) \bmod N)] * [(n \times k) \bmod N]\}*[(k \times n) \bmod N]=$$
$$= [(k \times n) \bmod N)] \times \{[(n \times k) \bmod N]x[(k \times n) \bmod N]\}, \quad (8)$$

наприклад, система <11,x> має одинаковий результат операцій,

$(a_{57} * a_{16}) * a_{92}=\{[(5x7)\bmod 11]*[(1x6) \bmod 11]\}*[(9x2) \bmod 11]=(2*6)*7=7,$

$a_{57} *(a_{16}* a_{92})=[(5x7)\bmod 11]*\{[(1x6) \bmod 11]*[(9x2) \bmod 11]\}=2*(6*7)=7;$

в) наявність нейтрального елемента множини N відносно операції a*e = a (e = a_{11}=1)

$$(k \times 1) \bmod N = k, \quad (9)$$

наприклад, система <11,x> , (1x6) mod 11= (6x1) mod 11= 6;

г) наявність оберненого елемента для будь-яких елементів з множини N,

$$a* a^{-1}=e, \quad (10)$$

наприклад, в системі <11,x >, елементи 2, 3, 5, 7, 10 мають обернені 6, 4, 9, 8, 10 відповідно, так як 2*6 = 3*4 = 5*9 =7*8 =10*10 =1.

Використовуючи мультиплікативну форму запису, нейтральний елемент відносно операції множения називають одиничним елементом, або одиницею групи. Елемент симетричний *a* позначають a^{-1} і називають оберненим елементу *a*. Натуральний степінь a^n елемента a мультипликативної групи визначається: $a^n = e$, $a^n = a*a*...* a$ для $n\in N-1\backslash\{0\}$.

Отже, значення аргументів базисної матриці ДГП для простого обсягу перетворення відповідають абелевій групі. Адже, система <N-1, *> абелева група порядку (N-1) — непуста множина з бінарною операцією, причому бінарна операція комутативна та асоціативна, наявний нейтральний елемент і кожен елемент групи має обернений йому елемент відносно бінарної операції (7–10).

2.2. Примітивні елементи алгебраїчної системи

Системи <N,*> з заданою операцією на множині елементів, коли порядок N – просте число, є циклічними групами G, причому таблиця операцій є ганкелевий циркулянт [4]. Розглянемо циклічні групи G з порядком N, що дорівнює простому числу, членами якої є результати операції (4).

Елементи циклічної групи G можна зобразити у вигляді натуральних степенів деякого елемента $\alpha \subset G$, який називають примітивним (породжуючим). Ясно, що породжуючий елемент α циклічної групи завжди примітивний елемент, але α – не єдиний примітивний елемент. Примітивним також є елемент α^{N-1}, де N – порядок циклічної групи.

Будь-яка кінечна група простого порядку являється циклічною. Мінімальне позитивне число *w* для якого $\alpha_j^w=\alpha_1$, називається мультиплікативним порядком елемента α_j. Якщо *x* – складене число, то відповідно до теореми Лагранжа: порядок будь-якого елемента α_j довільної кінечної

групи, а не тільки циклічної, є дільником порядка групи *x*. Тобто, порядок *w* будь-якого елемента a_j, крім a_1, дорівнює x/η_j, де η_j –НСД [*x*, j-1] – найбільший спільний дільник.

Наприклад, для обсягу перетворення N=11, за (4) мультиплікативна операція визначається без 0, то таблиця операції має порядок 10. Тобто, при *x*=10 маємо

η_2= НСД [*x* =10, j-1=1]=1; *w*(a_2)= x/η_2=10;
η_3= НСД [*x* =10, j-1=2]=2; *w*(a_3)= x/η_3=5;
η_4= НСД [*x* =10, j-1=3]=1; *w*(a_4)= x/η_4=10;
η_5= НСД [*x* =10, j-1=4]=2; *w*(a_5)= x/η_5=5;
η_6= НСД [*x* =10, j-1=5]=5; *w*(a_6)= x/η_6=2;
η_7= НСД [*x* =10, j-1=6]=2; *w*(a_2)= x/η_2=5;
η_8= НСД [*x* =10, j-1=7]=1; *w*(a_3)= x/η_3=10;
η_9= НСД [*x* =10, j-1=8]=2; *w*(a_4)= x/η_4=5;
η_{10}= НСД [*x* =10, j-1=9]=1; *w*(a_5)= x/η_5=10;

Елементи a_2, a_4, a_8, a_{10} – примітивні елементи (не єдиний примітивний елемент цієї циклічної групи).

Всі елементи циклічної групи можуть бути представлені степенями примітивних елементів a_2 або a_x , для *x*=10 і також a_4 , a_8 . Тобто:

$a_1= a_2^{10}$; $a_2= a_2^{1}$; $a_3= a_2^{2}$; $a_4= a_2^{3}$; $a_5= a_2^{4}$; $a_6= a_2^{5}$; $a_7= a_2^{6}$; $a_8= a_2^{7}$; $a_9= a_2^{8}$; $a_{10}= a_2^{9}$;

$a_1= a_{10}^{10}$; $a_2= a_{10}^{9}$; $a_3= a_{10}^{8}$; $a_4= a_{10}^{7}$; $a_5= a_{10}^{6}$; $a_6= a_{10}^{5}$; $a_7= a_{10}^{4}$; $a_8= a_{10}^{3}$; $a_9= a_{10}^{2}$; $a_{10}= a_{10}^{1}$;

Мінімальне позитивне число *w*, для якого $\alpha_j^w=\alpha_1$, називається мультиплікативним порядком елемента α_j. Порядки непримітивних елементів a_3; a_5; a_6; a_7; a_9 будуть *w*(a_3)=w(a_5)=w(a_7) =w(a_9)=5; w(a_6)= 2. Тобто, степені порядків непримітивних елементів у результаті обчислення дають a_1

$a_3^5= a_1$; $a_5^5= a_1$; $a_6^2= a_1$; $a_7^5= a_1$; $a_9^5= a_1$;

Відповідно у нашому випадку мультиплікативні порядки елементів a_2 та a_x ($a_1= a_2^{10}$, $a_1= a_{10}^{10}$) дорівнюють w=10 – порядку (числу елементів) циклічної групи, заданої (6).

Згенеруємо елементи групи за примітивними елементами:

1) примітивний елемент α =2, генерування α^i=4, 8, 5, 10, 9, 7, 3, 6, 1 (i=2,…,10) ;

$a_1= a_2^{10}$; $a_2= a_2^{1}$; $a_3= a_2^{2}$; $a_4= a_2^{3}$; $a_5= a_2^{4}$; $a_6= a_2^{5}$; $a_7= a_2^{6}$; $a_8= a_2^{7}$; $a_9= a_2^{8}$; $a_{10}= a_2^{9}$;

a_1= 1; a_2= 2; a_3= 4; a_4= 8; a_5= 5; a_6=10; a_7= 9; a_8= 7; a_9= 3; a_{10}= 6; (для N=11)

$a_3^5= a_1$; $a_5^5= a_1$; $a_6^2= a_1$; $a_7^5= a_1$; $a_9^5= a_1$; (непримітивні елементи)

4^5=1; 5^5=1; 10^2=1; 9^5=1; 3^5=1; (непримітивні елементи) (для N=11)

a_2 =2, a_4 =8, a_8 =7, a_{10} =6; (примітивні елементи)

2) примітивний елемент $a_{10}=\alpha^{x-1}=2^9$=6, генерування α^i=3, 7, 9, 10, 5, 8, 4, 2, 1 (i=2,…,10) ;

$a_1= a_{10}^{10}$; $a_2= a_{10}^{9}$; $a_3= a_{10}^{8}$; $a_4= a_{10}^{7}$; $a_5= a_{10}^{6}$; $a_6= a_{10}^{5}$; $a_7= a_{10}^{4}$; $a_8= a_{10}^{3}$; $a_9= a_{10}^{2}$; $a_{10}= a_{10}^{1}$;

a_1= 1; a_2= 3; a_3= 7; a_4= 9; a_5= 10; a_6= 5; a_7= 8; a_8= 4; a_9= 2; a_{10}= 6; (для N=11)

3) примітивний елемент a_8 =α=7, генерування α^i=5, 2, 3, 10, 4, 6, 9, 8, 1(i=2,…,10);

4) примітивний елемент $a_4= \alpha^{x-1}=7^9$=8, генерування α^i=9, 6, 4, 10, 23, 2, 5, 7, 1(i=2,…,10);

Непримітивні елементи a_3; a_5; a_6; a_7; a_9 виконують генерування не всіх елементів групи

α =3, α^i=9, 5, 4, 1 (1, 3, 9, 5, 4) доповнюючи [2*(1, 3, 9, 5, 4)mod11] = (2, 6, 7,10, 8);

α =4, α^i=5, 9, 3, 1 (1, 4, 5, 9, 3) доповнюючи [2*(1, 4, 5, 9, 3)mod11] = (2, 8, 10, 7, 6);

α =5, α^i=3, 4, 9, 1 (1, 5, 3, 4, 9) доповнюючи [2*(1, 5, 3, 4, 9)mod11] = (2, 10, 6, 8, 7);

α =9, α^i=4, 3, 5, 1 (1, 9, 4, 3, 5) доповнюючи [2*(1, 9, 4, 3, 5)mod11] = (2, 7, 8, 6, 10);

α =10, α^i=1, 10, (1, 10) доповнюючи 2*(1, 10)mod11=(2, 9), 2*(2, 9) mod11=(4,7), 2*(4, 7) mod11=(8, 3), 2*(8, 3) mod11= (5,6); Тобто, елементи групи дорівнюють (1, 10) (2, 9) (4, 7) (8, 3) (5, 6).

Отже, у разі генерування за непримітивними елементами решту елементів групи можна отримати, домножуючи отриману множину на два за модулем N.

Кількість примітивних елементів циклічної групи порядка N можна визначити через φ(*x*) функцією Ейлера, яка дорівнює кількості всіх натуральних чисел між 1 та N і взаємно простих з N. Для p- просте число функція дорівнює

$$\varphi(p)=(p-1);\ ;$$

Тобто, якщо x – просте число (кількість елементів групи), то будь-який елемент є примітивним (породжуючим) для будь-якого степеня a_2^i або a_x^i і, відповдно, $a_j = a_2^{j-1} = a_x^{x-j+1}$, крім елемента a_1, оскільки має порядок $w = w(a_j) = x$.

Наприклад, у цьому випадку мультиплікативна операція визначається без 0, то таблиця операції, заданої ганкелевим циркулянтом, має порядок 10 для обсягу перетворення N=11. Кількість примітивних елементів циклічної групи порядка 10, то

$\varphi(10) = \varphi(2) * \varphi(5) = 1 * 4 = 4$ (тобто відповідно a_2, a_4, a_8, a_{10}).

Отже, для цих алгебраїчних систем кількість примітивних елементів визначається за теоремою Лагранжа і може бути більша або дорівнювати функції Ейлера.

2.3. Аналіз алгебраїчної системи як сукупності підстановок

Аналізуючи ганкелеву матрицю значень аргументів базису ДГП для простого обсягу, кожен рядок (стовпець) матриці (5) a_i , $i \subset \{1,2,\ldots,x\}$ можна трактувати як підстановку π_i [5] відносно найвищого рядка (крайнього лівого стовпця):

$\begin{pmatrix} a_{11}\, a_{12}\, a_{13} \ldots a_{1x-1}\, a_{1x} \\ a_{22}\, a_{23} \ldots a_{2x-1}\, a_{2x}\, a_{21} \end{pmatrix} \equiv \pi_2(a_i)$ формування елементів другого рядка через підстановку π_2;

$\begin{pmatrix} a_{11}\, a_{12}\, a_{13} \ldots a_{1x-1}\, a_{1x} \\ a_{33} \ldots a_{3x-1}\, a_{3x}\, a_{31} a_{32} \end{pmatrix} \equiv \pi_3(a_i)$ формування елементів третього рядка через підстановку π_3;

…

$\begin{pmatrix} a_{11}\, a_{12}\, a_{13} \ldots a_{1x-1}\, a_{1x} \\ a_{xx}\, a_{x1}\, a_{x2}\, a_{x3} \ldots a_{xx-1} \end{pmatrix} \equiv \pi_x(a_i)$ формування елементів рядка через підстановку π_x;

Аналогічно перший рядок і перший стовпець можна розглядати як одиничні підстановки (називається тотожньою підстановкою і позначається: ().

$\begin{pmatrix} a_{11}\, a_{12}\, a_{13} \ldots a_{1x-1}\, a_{1x} \\ a_{11}\, a_{12}\, a_{13} \ldots a_{1x-1}\, a_{1x} \end{pmatrix} \equiv \pi_1(a_i) = ()$; *тотожня* підстановка містить всі фіксовані елементи.

На основі твердження підстановка π_2 та π_x є циклічними (круговими) – відповідно лівою та правою. Тобто нижній рядок відносно верхнього у підстановці формується круговим зсувом ліворуч та праворуч для ганкелевих матриць. Всі решта підстановок можуть бути представлені як степені циклічних підстановок, наприклад:

$$\pi_2^2 = \pi_2 \times \pi_2 = \pi_3;$$

$$\begin{pmatrix} a_1\, a_2\, a_3 \ldots a_{x-1}\, a_x \\ a_2\, a_3 \ldots a_{x-1}\, a_x a_1 \end{pmatrix} X \begin{pmatrix} a_1\, a_2\, a_3 \ldots a_{x-1}\, a_x \\ a_2\, a_3 \ldots a_{x-1}\, a_x a_1 \end{pmatrix} = \begin{pmatrix} a_1\, a_2\, a_3 \ldots a_{x-1}\, a_x \\ a_3\, a_4 \ldots\, a_x\, a_1\, a_2 \end{pmatrix}$$

$\pi_2^3 = \pi_4$; $\pi_2^4 = \pi_5$; … $\pi_2^{x-1} = \pi_x$; $\pi_2^x = \pi_1$; … $\pi_x^2 = \pi_{x-1}$; $\pi_x^3 = \pi_{x-2}$; … $\pi_x^{x-1} = \pi_2$; $\pi_x^x = \pi_1$;
$\pi_2^2 = \pi_3$; $\pi_3^2 = \pi_4$; $\pi_4^2 = \pi_5$; … $\pi_x^2 = \pi_1$;

Сукупність підстановок $\{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \ldots \pi_x\}$ утворює циклічну групу Gц.

Наприклад, для обсягу перетворення N=11, де мультиплікативна операція визначається без 0, таблиця операції має порядок 10, кожен рядок (стовпець) матриці (5) a_i , $i \subset \{1,2,\ldots,10\}$ можна трактувати як підстановку відносно найвищого рядка (крайнього лівого стовпця):

π_2 $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10 \\ 2\ 4\ 6\ 8\ 10\ 1\ 3\ 5\ 7\ 9 \end{pmatrix}$ π_9 $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10 \\ 3\ 6\ 9\ 1\ 4\ 7\ 10\ 2\ 5\ 8 \end{pmatrix}$

π_3 $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10 \\ 4\ 8\ 1\ 5\ 9\ 2\ 6\ 10\ 3\ 7 \end{pmatrix}$ π_5 $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10 \\ 5\ 10\ 4\ 9\ 3\ 8\ 2\ 7\ 1\ 6 \end{pmatrix}$

π_{10} $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10 \\ 6\ 1\ 7\ 2\ 8\ 3\ 9\ 4\ 10\ 5 \end{pmatrix}$ π_8 $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10 \\ 7\ 3\ 10\ 6\ 2\ 9\ 5\ 1\ 8\ 4 \end{pmatrix}$

π_4 $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\8&5&2&10&7&4&1&9&6&3\end{pmatrix}$ π_7 $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\9&7&5&3&1&10&8&6&4&2\end{pmatrix}$

π_6 $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\10&9&8&7&6&5&4&3&2&1\end{pmatrix}$ π_1 $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\1&2&3&4&5&6&7&8&9&10\end{pmatrix}$

Відповідно, твердження підстановка π_2 являється циклічною (круговою) – відповідно лівою. Тобто нижній рядок відносно верхнього у підстановці формується круговим зсувом вліво. Примітивні (породжуючі) елементи підстановок π_2 , π_{10} , π_4 , π_8 (2, 6, 7, 8)

$$\pi_2^2 = \pi_3 = \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\2&4&6&8&10&1&3&5&7&9\end{pmatrix} \text{x} \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\2&4&6&8&10&1&3&5&7&9\end{pmatrix} = \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\4&8&1&5&9&2&6&10&3&7\end{pmatrix}$$

$\pi_2^3 = \pi_4$; $\pi_2^4 = \pi_5$; $\pi_2^5 = \pi_6$; $\pi_2^6 = \pi_7$; $\pi_2^7 = \pi_8$; $\pi_2^8 = \pi_9$; $\pi_2^9 = \pi_{10}$; $\pi_2^{10} = \pi_1$

π_{10} $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\6&1&7&2&8&3&9&4&10&5\end{pmatrix}$

$\pi_{10}^2 = \pi_9$; $\pi_{10}^3 = \pi_8$; $\pi_{10}^4 = \pi_7$; $\pi_{10}^5 = \pi_6$; $\pi_{10}^6 = \pi_5$; $\pi_{10}^7 = \pi_4$; $\pi_{10}^8 = \pi_3$; $\pi_{10}^9 = \pi_2$; $\pi_{10}^{10} = \pi_1$;

π_4 $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\8&5&2&10&7&4&1&9&6&3\end{pmatrix}$ $\pi_4^{10} = \pi_1$;

π_8 $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\7&3&10&6&2&9&5&1&8&4\end{pmatrix}$ $\pi_8^{10} = \pi_1$;

Непримітивні (π_3 , π_5 , π_6 , π_7 , π_9) елементи підстановок: для підстановки π_9

π_9 $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\3&6&9&1&4&7&10&2&5&8\end{pmatrix}$

$\pi_9^2 = \pi_7$; $\pi_9^3 = \pi_5$; $\pi_9^4 = \pi_3$; $\pi_9^5 = \pi_1$;

Отже, аналіз значень аргументів базису ДГП для простого обсягу (5) з погляду операції підстановки показує, що сукупність підстановок $\{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \ldots \pi_{10}\}$ утворює циклічну групу. Кількість і нумерація породжуючих і непримітивних елементів як для операції підстановки, так і для операції (4) в системі елементів збігаються.

Висновки

У результаті аналізу значень аргументів базисної матриці ДГП простого обсягу отримуємо:

- задана множина з (N-1) елементів аргументів та мультиплікативної операції відповідає конкретному випадку алгебраїчної системи – абелевій групі;
- кількість примітивних елементів абелевої групи визначається за теоремою Лагранжа і може бути більша або дорівнювати функції Ейлера;
- генерування циклічної абелевої групи за непримітивними елементами дає змогу решту елементів групи отримати за модулем N, домножуючи сформовану множину на два;
- кількість і нумерація породжуючих і непримітивних елементів як для операції підстановки, так і для мультиплікативної операції в системі елементів збігаються.

Ці результати використовуються для формування базисних матриць дискретних перетворень класу Фур’є за примітивними і не примітивними елементами у вигляді циклічних згорток.

1. Оппенгейм А., Шафер Р., Цифровая обработка сигналов. – М.: Техносфера, 2006. 2. Макклеллан Дж., Рейдер Ч. Применение теории чисел в цифровой обработке сигналов. – М.: Радио и связь, 1983. 3. Чуприна О.О. Удосконалений алгоритм ШПФ на базі швидкої згортки // Вісник Нац. ун-ту "Львівська політехніка". – 2008. – № 618. – С. 174–179. 4. Муттер В.М. Основы помехоустойчивой телепередачи информации.– Л.: Энергоатомиздат, 1990. 5. Кнут Д.Э. Исскуство программирования для ЭВМ. – М.: Мир, 1977.