УДК 004.421.2:517.443

І. Процько, *Р. Рикмас
Національний університет “Львівська політехніка”,
кафедра інформаційних систем та технологій,
*ТОВ “Юнісервіс” (Львів)

РОЗВИТОК АЛГОРИТМУ ВІНОГРАДА ПЕРЕТВОРЕННЯ ФУР’Є НА БАЗІ ТВІРНОГО МАСИВУ

Розглянуто загальну методику ефективного обчислення ДПФ за допомогою циклічних згорток для обсягів, що дорівнюють цілому степеню два. Проаналізовано подальший розвиток алгоритму Віноградa перетворення Фур’є (WFTA). Застосовано твірний масив для стислого опису блочно-циклічної структури базисної матриці ДПФ. Визначено загальну блочно-циклічну структуру дискретної базисної матриці та обчислювальні затрати для ДПФ обсягів $N = 2^n$.

Ключові слова: швидке перетворення Фур’є (ШПФ), циклічна згортка, твірний масив.

The general technique of efficient computation DFT using of cyclic convolutions for sizes of integer power of two is considered. Further development of Winograd Fourier transform algorithm (WFTA) is analyzed. The hashing array for the compacting definition of the block-cyclic structure the basis matrix of DFT is proposed. The general block-cyclic structure of discrete basis matrix for the computation of DFT of sizes $N=2^n$ is determined.

Key words: fast Fourier transform, cyclic convolution, hashing array.

Вступ

Дискретне перетворення Фур’є (ДПФ) застосовують для спектрального аналізу різноманітних сигналів на основі існуючих швидких алгоритмів. Реалізацію методів ефективного обчислення ДПФ за допомогою алгоритмів називають швидкими перетвореннями Фур’є (ШПФ, FFT). ШПФ за алгоритмами Кулі–Тьюкі поділяють на: алгоритми з основою два, розщепленою основою, змішаною основою, алгоритми простих множників складеного обсягу перетворення та інші [1,2].

Значною подією, пов’язаною з іншою тенденцією розвитку ефективних алгоритмів, який відзначається в багатьох виданнях з цифрової обробки сигналів [3,4], є можливість обчислення ШПФ через циклічні згортки. Алгоритми на основі циклічних згорток дуже затребувані розробниками ДПФ на апаратному рівні завдяки високим характеристикам модульності, локальності та регулярності зв’язків між процесорними елементами в систолічних масивах реалізації циклічних згорток [5–7].

Аналіз літературних джерел

Піонерською в цьому напрямі є робота Ч. Рейдера про можливість ефективного обчислення ДПФ через циклічні згортки [8]. У 1968 р. Рейдер показав, як переформатувати ДПФ простого значення обсягу N до циклічної згортки обсягу (N-1). Це обчислення ДПФ ефективно реалізується через використання швидких згорток.

Подальший розвиток підходу відносіть до алгоритму Віноградa перетворення Фур’є (АВПФ, 1976) для значень обсягів, що дорівнюють степеню простого числа [9]. В алгоритмі Віноградa для специфічного перепорядкування даних перетворення використовують переіндексацію на основі китайської теореми про залишки, властивості прямого добутку матриць і алгоритми циклічних

згорток. Однак, АВПФ мають свої специфічні особливості для кожного обсягу N, пов'язаного з переіндексацією вхідної послідовності і, отже, мають деякі нерегулярні структури. Це потребує значних зусиль, щоб перевести цей теоретичний результат у реальний комп'ютерний код. Отже, алгоритми Рейдера–Віноградa досліджують і розвивають багато авторів [10–13]. Обчислення ДПФ через циклічні згортки ґрунтовно розглянуто в книгах [14, 15].

У цій роботі показано розвиток алгоритмів ДПФ на основі циклічних згорток для обсягів, що дорівнюють цілому степеню два. Розроблені алгоритми є загальнішими, ніж алгоритми Рейдера–Віноградa та вдосконалення алгоритмів АВПФ в роботі [16].

Постановка проблеми

Алгоритм Віноградa перетворення Фур'є (АВПФ) представляє переважно теоретичні результати, важливі для теорії складності обчислення перетворень. Алгоритм Віноградa [17] зменшує кількість множень порівняно з алгоритмом ШПФ за основою два [2] за коефіцієнтом, близьким до п'яти. Але практична реалізація АВПФ потребує подальших досліджень та розвитку.

Вдосконалений АВПФ розробив і детально розглянув С. Зохар у роботі [16, 18]. Алгоритм подано через послідовність таблиць, що зручно та компактно в графічній формі представляють послідовності арифметичних операцій відповідних частин алгоритму. Алгоритм складається з декількох підпрограм, які з погляду їх програмної реалізації призначені для практичної алгоритмічної ясності, а не для обчислень з погляду швидкодії. Розгляд АВПФ С. Зохар докладно і сповна провів з метою подальшого розвитку цього підходу.

Виведення алгоритмів Рейдера–Віноградa, відповідно до [8], ґрунтується на ідеї примітивного кореня g з теорії чисел. Примітивний корінь N є цілим числом, цілі степені за модулем N якого породжують всі цілі числа в інтервалі (1, N), за винятком значень, кратних p, де $N=p^k$; p – просте число, k – ціле число. Отже, кількість цілих чисел, породжена g, є

$$n= p^k - N/ p = p^k - p^k / p = p^k - p^{k-1}= (p -1) p^{k-1} \quad (1)$$

і послідовність (g^ρ mod N), ρ=0,1,2,…, n-1 – це просто перестановка цих чисел в інтервалі (1, N), що не кратні p.

У роботі [16, 18] достатньо детально розглянуто алгоритми ДПФ для обсягів N=8, 16. Під час розроблення алгоритму з використанням таблиць для N=8, 16 виникають ускладнення у зв'язку з тим, що обсяги перетворень $N=2^k$ (k > 2) не мають примітивних коренів. У роботі [16, 18] модернізовано схему індексації. У випадку ДПФ обсягу $N=16=2^4$ для елемента g=3 піднесенням до степеня за модулем N ($r= g^\rho$ mod N) генерує половину значень в інтервалі (1, N). Для іншої половини застосування ($s= g^\delta$ mod N) із складним визначенням степенів δ, що формує базисну матрицю з частиною лівоциркулянтних (ЛЦ) підматриць. У результаті алгоритм ДПФ для N=16 потребує 36 дійсних множень або 20 дійсних множень (з виключенням кількості множень на 1 і j) та 148 дійсних додавань.

Тобто, важливими є розвиток та спрощення розробленої схеми синтезу ШПФ на основі циклічних згорток.

Подальший розвиток АВПФ

АВПФ широко досліджується та узагальнюється для організації ефективних обчислень ДПФ різноманітних цілих значень обсягів. Розглянемо розвиток ефективного АВПФ і структур базису перетворення для випадку обсягів послідовностей перетворення, що дорівнюють цілому степеню два.

Дискретне перетворення Фур'є (ДПФ) відповідає сумі добутку значень вхідних сигналів на комплексні значення тригонометричних функцій і обчислюється за формулою

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

де W_N=exp (-j 2π/N); вхідні x (n) та вихідні X (n) дискретні сигнали перетворення обсягу N.

Дискретний комплексний експоненціальний базис W_N ДПФ можна подати у вигляді дійсної та уявної частин

$$X(k) = X1(k) + x(0) - jX2(k), \quad k = 0,1,\ldots,N-1, \tag{3}$$

де $X1(k) = \sum_{n=1}^{N-1} x(n)\cos(2p\,k\,n/N), \quad k = 0,1,\ldots,N-1,$ (4)

$$X2(k) = \sum_{n=1}^{N-1} x(n)\,\sin(2p\,k\,n/N), \quad k = 1,\ldots,N-1. \tag{5}$$

Всі N вихідних значень ДПФ можна отримати обчисленням $X1(k)$ та $X2(k)$ частин.

Ефективне ШПФ на основі циклічної згортки полягає в декомпозиції [19] матриці степенів дискретного експоненціального базису W^{kn} ДПФ (2) на матриці дійсної $X1(k)$ та уявної частин $X2(k)$ окремо.

Проаналізуємо аргументи функцій дискретного експоненціального базису

$$a_{k,n} = k*n*a_N, \quad k = 1,\ldots,N-1, \tag{6}$$

а точніше, цілі (k*n) компоненти, без

$$a_N = 2p/N. \tag{7}$$

Базисна функція періодична на періоді 2π. Тому відповідно до властивості періодичності, матриця аргументів функкій частин ДПФ міститиме елементи

$$X_a(k,n) = [(k*n) \bmod N] = [d_{k,n}], \quad k = 1,\ldots,N-1 \tag{8}$$

тобто, кожна з частин (4, 5) відповідно дорівнює матриці аргументів

$$X_a(k,n) = \begin{bmatrix} 1, & 2, & 3, & \ldots, & 1*(\mathrm{N}-1)\bmod\mathrm{N} \\ 2, & 4, & 6, & \ldots, & 2*(\mathrm{N}-1)\bmod\mathrm{N} \\ & & & \ldots & \\ ((\mathrm{N}-1)*1)\bmod\mathrm{N}, & \ldots, & ((\mathrm{N}-1)*(\mathrm{N}-1))\bmod\mathrm{N} & & \end{bmatrix}. \tag{9}$$

ДПФ є декомпозицією групового представлення <N-1, • > для простого обсягу N, де • – групова операція добутку за модулем. Відповідно до теореми Келі, алгебраїчна структура < Ψ, ○ >, де елементи підстановок {ψ_1, ψ_2, ψ_3,…, ψ_{N-1},} з відповідних рядків/стовпців матриці (9) та ○ - операція над підстановками, є ізоморфна до кінцевої групи <N-1, • >. Сформуємо підстановки $\psi_{k/n}$ у вигляді циклічного розкладу

$$D(n) = (d_{11}, d_{12},\ldots, d_{1L1})(d_{21}, d_{22},\ldots, d_{2L2})\ldots(d_{kL1}, d_{kL2},\ldots, d_{kLk}), \tag{10}$$

де d_{ij} – елемент підмасиву, k – кількість підмасивів, L_i – кількість елементів у підмасивах, n – обсяг циклічного розкладу. Вираз (10) є стислим представлення множини ЛЦ підмасивів у структурі базисної матриці ДПФ і називатимемо твірним масивом.

Застосуємо твірний масив $D(n)$ для переіндексації стовпців/рядків матриці аргументів ДПФ для обсягів $N=2^n$.

Властивості симетричності та періодичності базису ДПФ ведуть до зменшення значень елементів аргументів функцій ЛЦ підматриць з доповненням відповідними підматрицями знаків $Zc(k, n)$ і $Zs(k, n)$, що містять значення елементів +1, -1 0 (коротко позначено +, -, 0). Спрощені матричні елементи $d'_{k,n}$ аргументів визначають для обсягів $N = 2^n$ через послідовність операцій

$$d'_{k,n} = (d_{k,n} \bmod N) - N/2, \quad \text{if} \quad (d_{k,n} \bmod N) > N/2; \tag{11}$$

$$d'_{k,n} = \begin{cases} N/4 - (d_{k,n} \bmod N - N/2), \\ \qquad \text{if} \quad N/8 < (d_{k,n} \bmod N - N/2\} < N/4; \\ N/4 - [N/2 - (d_{k,n} \bmod N - N/2)], \\ \qquad \text{if} \quad 3N/8 < (d_{k,n} \bmod N - N/2\} < N/2; \\ d_{k,n}, \quad \text{otherwise.} \end{cases} \tag{12}$$

Спрощені матричні елементи $d'_{k,\,n}$ аргументів доповнюються значеннями знаків косинус і синус функцій, що визначаються за нерівностями

$$Zc[k,n]=\begin{cases}+1, & 3N/4< c_{k,n} < N/4;\\ 0, & c_{k,n}=N/4,\,3N/4;\\ -1, & N/4< c_{k,n} <3N/4.\end{cases} \quad (13)$$

$$Zs\,[k,n]=\begin{cases}+1, & 0< c_{k,n} < N/2;\\ 0, & c_{k,n}=0,\,N/2;\\ -1, & N/2< c_{k,n} < N.\end{cases} \quad (14)$$

Спрощена матриця степенів експоненціального базису визначає конкретні структури ЛЦ підматриць базисної квадратної матриці *W*. Підмасиви твірного масиву *D* (*n*) відтворюють ганкелеві підматриці в структурі базисної квадратної матриці *W*, що ведуть до обчислення циклічних згорток за значеннями функцій з аргументами *Zc, s* (*n*) *D*'(*n*) та вхідними даними *x* (*n*).

Наприклад, ДПФ для перетворення обсягу N = 16 твірний масив має вигляд:

D (15)=(0)(8) (4, 12) (2, 6) (10, 14) (1, 3, 9, 11) (15, 13, 7, 5).

Використовуючи властивість симетрії базису ДПФ, спрощений твірний масив *D*'(7) містить спрощені елементи $d'_{k,\,n}$, що доповнюються відповідними елементами знаків *Zc* (7) і *Zs* (7) функцій. У нашому випадку *D*'(7), *Zc* (7) і *Zs* (7) містить такі спрощені значення:

D'(7) = (0) (4) (2, 2) (1, 3, 1, 3),

Zc (7) = (1) (0) (+ -) (+ + - -), *Zs* (7) = (0) (+) (+ +) (+ + - -).

Застосовуючи твірні масиви, скорочують і визначають такі матриці (табл. 1) спрощених аргументів зі знаками *Zc, Zs,*.

У результаті аналізу даних табл. 1 одержаний алгоритм ДПФ для обсягу N = 16 зводиться до обчислення однієї 4-х точкової та двох 2-точкових циклічних згорток, що містять повторення групи коефіцієнтів базису. Для цього необхідно виконати кількість множень m = 8 для дійсних вхідних даних *x* (*n*) або m = 16 для комплексних вхідних даних *x* (*n*) із виключенням кількості множень на 1 і *j*.

Таблиця 1

Матриця спрощених аргументів *W* зі знаками *Zc, Zs, N*=16

$_k{}^n$	**0:**	**4:**	**2:**	**6:**	**1:**	**3:**	**9:**	**11:**
0:	+0	+0	+0	+0	+0	+0	+0	+0
4:	+0	+0	-8	-8	4	4	4	4
2:	+0	-8	4	4	+2	-2	+2	-2
6:	+0	-8	4	4	-2	+2	-2	+2
1:	+0	4	+2	-2	+1	+3	-1	-3
3:	+0	4	-2	+2	+3	-1	-3	+1
9:	+0	4	+2	-2	-1	-3	+1	+3
11:	+0	4	-2	+2	-3	+1	+3	-1
$_k{}^n$	**0:**	**4:**	**2:**	**6:**	**1:**	**3:**	**9:**	**11:**
0:	0	0	0	0	0	0	0	0
4:	0	0	8	8	+4	-4	+4	-4
2:	0	8	+4	-4	+2	+2	+2	+2
6:	0	8	-4	+4	+2	+2	+2	+2
1:	0	+4	+2	+2	+1	+3	-1	-3
3:	0	-4	+2	+2	+3	-1	-3	+1
9:	0	+4	+2	+2	-1	-3	+1	+3
11:	0	-4	+2	+2	-3	+1	+3	-1

Загальний АВПФ для N = 2^n

Застосовуючи підстановки, визначені через рядки/стовпці матриці аргументів базисної функції ДПФ, формують твірні масиви. Розглянемо специфіку структури ЛЦ підматриць у базисній квадратній матриці W для обсягів перетворення $N = 2^n$. На основі підстановки за рядками матриці аргументів базисної функції ДПФ сформуємо твірні масиви D (n).

Для N = 32 твірний масив складається з k = 4 підмасивів:

D (31)=(1,3,9,27,17,19,25,11)¦(5,15,13,7,21,31,29,23)(2,6,18,22)¦(10,30,26,14)(4,12)¦(20,28)(8,24)(16).

Спрощені елементи $d'_{k,n}$ аргументів D (31) відповідно до (11) матимуть значення:

D (31)=(1,3,9,5,15,13,7,11)¦(5,15,13,7,11,1,3,9) (2,6,14,10)¦(10,2,6,14)(4,12)¦(12,4)(8,8)(16).

Об'єднаємо ідентичні підмасиви в спрощеному твірному масиві D (31)

D'(15)=(1,3,9,5,15,13,7,11) (2,6,14,10)(4,12)(8)(16),

і далі за (12) спростимо елементи $d'_{k,n}$ аргументів:

D'(15)= (1,3,7,5, 1,3,7,5) (2,6,2,6) (4,4) (8) (0),

Zc (15)= (+ + - + - - + -) (+ + - -)(+ -) (-1),

Zs (15)= (+ + + - - - - +) (+ + - -) (+ +) (+) (0).

Для N = 64 твірний масив складається з k = 5 підмасивів:

D (63)=(1,3,9,27,17,51,25,11,33,35,41,59,49,19,57,43)¦(5,15,45,7,21,63,61,55,37,47,13,39,53,31,29,23) (2,6,18,54,34,38,50,22)¦(10,30,26,14,42,62,58,46) (4,12,36,44) ¦ (20,60,52,28) (8,24) ¦ (40,56) (16,48) (32).

Спрощений твірний масив і спрощені елементи $d'_{k,n}$ аргументів (11–14) мають значення:

D'(31)=(1,3,9,27,17,13,25,11,31,29,23,5,15,19,7,21)(2,6,18,10,30,26,14,22)(4,12,28,20)(8,24)(16)(32),

D'(31)=(1,3,9,5,15,13,7,11,1,3,9,5,15,13,7,11)(2,6,14,10,2,6,14,10) (4,12,4,12) (8,8) (0),

Zc (31)=(+ + + - - + - + - - - + + - + -) (+ + - + - - + -) (+ + - -) (+ -) (-1),

Zs (31)=(+ + + + + - + + - - - - - + - -)(+ + + - - - - +)(+ + - -) (+ +) (0).

Твірні масиви D (n) для ДПФ обсягу $N = 2^n$ можна в загальному описати в виді:

$$D\,(2^{n-1}-1) = D_1\{2^{n-1}\}\,D_2\{2^{n-2}\}\ldots D_{n-1}\{2^1\}\,D_n\,\{2^0\}, \qquad (15)$$

де D_i{кількість елементів аргументів} – твірні підмасиви.

Отже, загальну ЛЦ структуру базисної квадратної матриці W (nxn) можна подати у вигляді табл. 2.

Таблиця 2

Загальна ЛЦ структура базисної матриці ДПФ для обсягу N=2^n^

<table>
<tr><td colspan="4" rowspan="16">$D_1\{2^{n-1}\}$</td><td colspan="4" rowspan="8">$D_2\{2^{n-2}\}$</td><td colspan="4" rowspan="4">…</td><td colspan="2" rowspan="2">$D_{n-1}\{2^1\}$</td><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2" rowspan="2">$D_{n-1}\{2^1\}$</td><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="4" rowspan="4">…</td><td colspan="2" rowspan="2">$D_{n-1}\{2^1\}$</td><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2" rowspan="2">$D_{n-1}\{2^1\}$</td><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="4" rowspan="8">$D_2\{2^{n-2}\}$</td><td colspan="4" rowspan="4">…</td><td colspan="2" rowspan="2">$D_{n-1}\{2^1\}$</td><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2" rowspan="2">$D_{n-1}\{2^1\}$</td><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="4" rowspan="4">…</td><td colspan="2" rowspan="2">$D_{n-1}\{2^1\}$</td><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2" rowspan="2">$D_{n-1}\{2^1\}$</td><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="2">$D_n\,(2^0)$</td></tr>
<tr><td colspan="8">$D_2\{2^{n-2}\}$</td><td colspan="8">$D_2\{2^{n-2}\}$</td></tr>
<tr><td colspan="4">…</td><td colspan="4">…</td><td colspan="4">…</td><td colspan="4">…</td></tr>
<tr><td colspan="2">$D_{n-1}(2^1)$</td><td colspan="2">D_{n-1}</td><td colspan="2">D_{n-1}</td><td colspan="2">D_{n-1}</td><td colspan="2">D_{n-1}</td><td colspan="2">D_{n-1}</td><td colspan="2">D_{n-1}</td><td colspan="2">$D_{n-1}(2^1)$</td></tr>
<tr><td>D_n</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>D_n</td></tr>
</table>

Аналізом структури підматриць у базисній матриці ДПФ визначено, що багато ЛЦ підматриць є виду (15), що відповідає вдвічі зменшеному розміру циклічної згортки (17). Адже група елементів $d'(n, k)$ повторюється в (16) твірних підмасивах $D_i'(n)$, що визначають коефіцієнти ДПФ

$$D_i'(n_k) = (d'_{kL1,} d'_{kL2,} \ldots, d'_{kLj}, d'_{kL1,} d'_{kL2,} \ldots, d'_{kLj}). \quad (16)$$

$$\begin{pmatrix} d(m) - d(m) \\ -d(m)\, h(m) \end{pmatrix} \otimes \begin{pmatrix} x0 \\ x1 \end{pmatrix} = \begin{pmatrix} d(m) \otimes (x0 - x1) \\ -d(m) \otimes (x0 - x1) \end{pmatrix}. \quad (17)$$

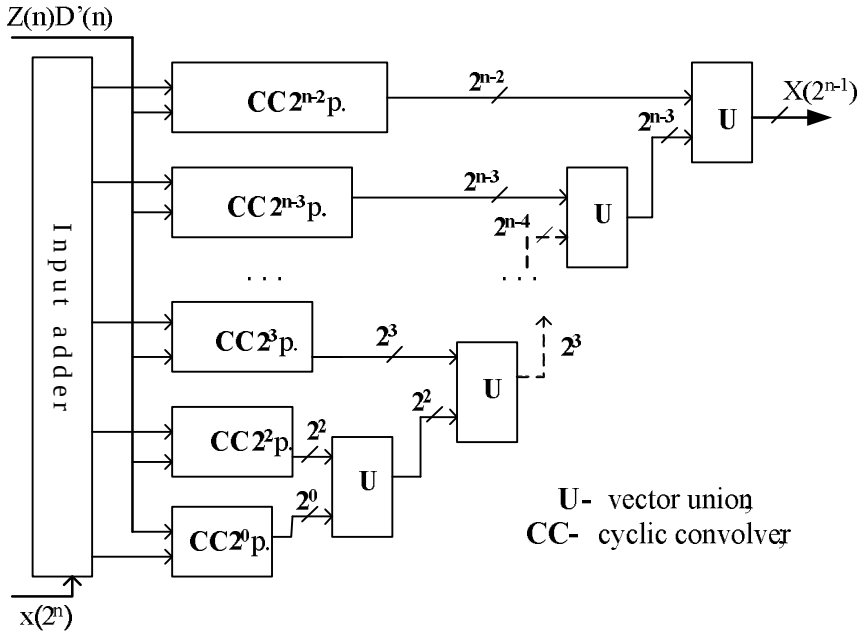
Обчислення окремо косинусної або синусної частини ДПФ ґрунтується на декомпозиції дискретної базисної матриці для обсягу перетворення $N=2^n$ і визначається k – кількістю твірних підмасивів, що задають t - точкові обсяги циклічних згорток (табл. 3).

Таблиця 3

Кількість твірних підмасивів в алгоритмі ДПФ для $N=2^n$

N	8	16	32	64	...	2^n
k	1	2	3	4	...	n-2
t	1	4,1 1	8,4,1 4,1 1	16,8,4,1 8,4,1 4,1 1	...	$2^{n-2}, 2^{n-3}, \ldots, 2^0$ $2^{n-3}, \ldots 2^2, 2^0$ $2^{n-4}, \ldots, 2^2, 2^0$ … $2^2, 2^0$ 2^0

Структурну схему обчислення косинусних або синусних частин ДПФ обсягу $N=2^n$, відповідно до табл. 7, подано на рисунку, що відповідає обчисленню половини значень вихідних даних.



Структурна схема обчислення косинусних/синусних частин ДПФ обсягу $N=2^n$

Матрична структура ДПФ для обсягу $N = 2^n$ визначає оптимальне послідовно-паралельне об'єднання (рисунок) в блоках U результатів циклічних згорток (блоки СС) обсягів $N= 2^i$, i = 2,3,..., n-2. Ефективно обчислюють СС за алгоритмами швидких циклічних згорток [3].

Аналіз результатів

Представлення блочно-циклічної структури базисної матриці ДПФ за допомогою твірних масивів охоплює ядро перетворення загалом, а не здійснює аналіз за окремими частинами, що є перевагою запропонованого розвитку АВПФ.

Обчислюють косинусну або синусну частини ДПФ традиційно в три послідовні етапи. Попередня обробка на етапі C_I являє собою об'єднання вхідних даних відповідно до ідентичності горизонтальних ЛЦ підматриць, що містить (18) лише операції додавання/віднімання:

$$C_I = N/2 + \sum_{i=3}^{n-1} \sum_{r=i}^{n-1} (2^{n-r}). \qquad (18)$$

Етап обробки C_{II} містить обчислення i - циклічних згорток (СС) із включенням арифметичних операцій (19) обчислення $p = 2^{n-i}$ - точкових циклічних згорток

$$C_{II} = CC_{(N/2^3)} + 2\sum_{i=4}^{n} CC_{(N/2^i)} + CC_{(N/2^n)}. \qquad (19)$$

Обчислення i-точкових циклічних згорток CC_i містить всі операції множення алгоритму ДПФ з використанням циклічних згорток.

Етап обробки C_{III} містить (20) операції додавання/віднімання результатів циклічних згорток та деяких вхідних даних для обчислення вихідних даних X (к) перетворення

$$C_{III} = 2^{n-2} + 2\sum_{r=0}^{n-3} 2^r. \qquad (20)$$

Кількість арифметичних операцій на основі цього підходу значною мірою залежить від вибору швидких алгоритмів циклічної згортки (з мінімальною кількістю множень або з балансом операцій додавання і множення тощо).

Розвинутий алгоритм ДПФ для обсягів N = 32, 64, 128 приводить до обчислення з числом дійсних множень m=24, 68, 198 для дійсних вхідних даних x (n) з виключенням з кількості множення на 1 і j. У результаті кількість множень менша порівняно з числами множень m = 34, 98, 258, отриманими у роботі [21].

Переформування базису ДПФ в ЛЦ структури виконують на основі твірного масиву. В результаті блочно-циклічні структури базисної матриці ДПФ для обсягів $N = 2^n$ можна описати версіями твірних масивів, поданими в табл. 4 (у {} – подається кількість елементів у твірному підмасиві).

Таблиця 4

Версії твірних масивів D (2^n-1) ДПФ для обсягів $N=2^n$

Версії	Твірні масиви D (2^n-1)
n-2) D (2^n-1)	$D\{2^{n-2}\}$ $D\{2^{n-2}\}$ $D\{2^{n-3}\}$ $D\{2^{n-3}\}$… $D\{2^1\}$ $D\{2^1\}$ $D\{2^0\}$;
n-3) D (2^n-1)	$D\{2^{n-3}\}$ $D\{2^{n-3}\}$ $D\{2^{n-3}\}$ $D\{2^{n-3}\}$ $D\{2^{n-4}\}$ $D\{2^{n-4}\}$ … $D\{2^1\}$ $D\{2^1\}$ $D\{2^0\}$;
…	…
1) D (2^n-1)	$D\{2^1\}$ $D\{2^1\}$... $D\{2^1\}$ $D\{2^0\}$... $D\{2^0\}$;

У випадку ДПФ для обсягів $N = 32 = 2^5$ маємо такі версії твірних масивів:

3) D (2^5-1)=(1,5,25,29,17,21,9,13)(3,15,11,23,19,31,27,7)
(2,10,18,26)(6,30,22,14)(4,20)(8)(24)(12,28) (16);

2) $D(2^5\text{-}1)$=(1,7,17,23)(3,21,19,5) (9,31,25,15)(11,13,27,29)
(2,14)(4,28)(6,10)(8,24)(12,20) (18,30)(22,26) (16);
1) $D(2^5\text{-}1)$=(1,15)(3,13)(5,11)(7,9)(17,31)(19,29)(21,27)
(23,5)(2,30)(4,28)(6,26)(8,24)(10,22)(12,20)(14,18)(16).

Окремі обчислення циклічних згорток, в які структуровано базисну матрицю ДПФ згідно з варіантами твірних масивів $D(2^n\text{-}1)$, а також об'єднання результатів згорток роблять важливим запропонований метод для реалізації в послідовно-паралельних та паралельних системах.

Висновки

Подано загальну методику ефективного обчислення ДПФ на основі циклічних згорток для обсягів цілого степеня два. Проаналізовано вдосконалений алгоритм Віноградa перетворення Фур'є [18] і розглянуто подальший розвиток АВПФ з використанням твірних масивів. Варіанти твірних масивів визначають стислий опис блочно-циклічних структур базисної матриці ДПФ для обсягів цілого степеня два. Аналіз виду спрощеного твірного масиву $D'(n)$ з доповненням відповідних підмасивів Zc (n), Zs (n) знаків зменшує кількість обчислення циклічних згорток в алгоритмі. Запропонований алгоритм порівняно з традиційними алгоритмами є гнучкішим, оскільки його можна застосувати для реалізації обсягів будь-якого степеня двійки. Порівняння числа множень відомих алгоритмів [18, 21] за цим підходом є меншим.

Подальші дослідження запропонованої методики будуть скеровані на обчислювальні структури обсягів $N=p^к$ та інших довільних розмірів дискретних перетворень Фур'є класу на основі циклічних згорток.

1. Duhamel P., Fast Fourier Transform: A tutorial Review and a State of the Art / P. Duhamel, M. Vitterli // Signal Processing. –1990. – Vol.19, – p. 259–299. 2. Chu Eleanor, Inside the FFT black box. Serial and Parallel Fast Fourier Transform Algorithms / Eleanor Chu, Alan George // CRC Press LLC, Boca Raton, 2000. 3. Tolimiery R. Algorithms for Discrete Fourier Transform and Convolution / R. Tolimiery, M. An, C. Lu // New York, Springer–Verlag, 1997 (s.ed.). 4. Prots'ko I., Becoming of Discrete Harmonic Transform Using Cyclic Convolutions / Ihor Prots'ko, Roman Rykmas // American Journal of Circuits, Systems and Signal Processing. – 2015. – August 2006. – Vol. 1, No. 3. – P. 114–119. 5. Chen H.-C., Distributed arithmetic realization of cyclic convolution and its DFT application. / H.-C. Chen, J.-I. Guo, C.-W. Jen and T.-S. Chang // IEE Proc.-Circuits Devices Syst. – December 2005. – Vol. 152, No. 6. – p. 615–629. 6. Meher P. K., Efficient Systolic Implementation of DFT using a Low-Complexity Convolution-like Formulation. / P. K. Meher // IEEE Transactions on Circuits & Systems-II: Express Briefs. – August 2006. – Vol. 53, No.8. – p. 702–706. 7. Cheng C., Low-Cost Fast VLSI Algorithm for Discrete Fourier Transform. / Chao Cheng, Keshab K. Parhi // IEEE Transactions on circuits and systems - I: regular papers. – April 2007. – Vol. 54, No. 4, – p. 791–806. 8. Rader C. M., Discrete Fourier Transforms When the Number of Data Samples is prime. / C. M. Rader // Proc. IEEE, – 1968. – 56, p. 1107–1108. 9. Winograd S., On computing the discrete Fourier transform. / S. Winograd // in Proc. Nat. Acad. Sci. USA. – April 1976, Mathematics. – Vol. 73, No. 4, – p. 1005–1006. 10. Lu C., Extension of Winograd Multiplicative Algorithm to Transform Size $N = p^2q$, p^2q^r and Their Implementation. / C. Lu, and R. Tolimieri // Proc. ICASSP 89. – Scotland, May 22-26, 1989. 11. Silverman H. F., An introduction to Programming the Winograd Fourier Transform algorithm (WFTA) / H. F. Silverman // IEEE Trans ASSSP. – 1977. – Vol. ASSSP- 25, No.2, – p.152–165. 12. Patterson R. W., Fixed Point Error Analysis of Winograd Fourier Transform Algorithms. / R. W. Patterson, J. H. McClellan // IEEE Trans. ASSP. – October 1978. – p.447–455. 13. Lavoie P., A high-speed CMOS implementation of the Winograd Fourier transform algorithm. / P. Lavoie // IEEE Trans. Signal Process. – Aug. 1996. – Vol. 44, No. 8. – p. 2121–2126. 14. Blahut R. E., Fast algorithms for signal processing. / R. E. Blahut // Cambridge University Press, 2010. – 469 p. 15. Nussbaumer Henri J. Fast Fourier Transform and Convolution Algorithms / Henri J. Nussbaumer // Springer-Verlag, Berlin, Heidelberg, 1982. 16. Zohar S., Faster Fourier Transformation: The Algorithm of S. Winograd. / Shalhav Zohar // Jet Propulsion Laboratory JPL

Publication 78–104, under NASA Contract No. NAS7-100, – February 15, 1979. – p. 1–93. 17. Winograd S., On computing the discrete Fourier transforms. / S. Winograd // Mathematics of Computation. – 1978. – Vol. 32. – p. 175–199. 18. Zohar S., Winograd's discrete Fourier transform algorithm. /Two-dimensional Digital Signal Processing. Transforms and Median Filters. Edited by T. S. Huang. Springer-Verlag, Berlin, Heidelberg, – New York, 1981. – 222 p. 19. Prots'ko I., The generalized technique of computation the discrete harmonic transforms / I. Prots'ko // Proceedings of the IVth International Conference (MEMSTECH'2008), Polyana, 21–24 may, 2008. – p. 101–102. 20. Thomas W. Judson, Abstract Algebra Theory and Applications. / W. Judson Thomas // Stephen F. Austin State University, February 14, 2009. – 428 p. 21. Duhamel P., Implementation of "Split-Radix" FFT Algorithms for Complex, Real, and Real-Symmetric Data. / P. Duhamel // IEEE Trans. on Acoustic, Speech, and Signal Processing, – April 1986, – Vol. ASSP-34, No. 2, – p. 285–295.

УДК 531.36+534

С. Носенко, Р. Оліярник, М. Назаркевич
Національний університет "Львівська політехніка",
кафедра інформаційних технологій видавничої справи

МЕТОД ПОБУДОВИ АНІМОВАНИХ ЗАХИСНИХ ЕЛЕМЕНТІВ ДЛЯ ДРУКОВАНИХ ТА ЕЛЕКТРОННИХ ВІДБИТКІВ

Розроблено спосіб захисту друкованих відбитків створенням анімованих об'єктів. Метод захисту полягає в тому, що статичне зображення створюють з "анімацією". Рух забезпечується за допомогою плівки, яка зміщується в горизонтальному напрямі. Розроблений метод можна використовувати як для електронних, так і для друкованих документів. Обгрунтовано вибір товщини лінії та прогалин для якісного відтворення засобами поліграфічної техніки.

Key words: image conversion, protection of printed documents, Hilbert curve.

The developed is the way of protection the printed impression by creating animated objects. The method of protection is a static image that created with "animation". Movement is provided through the plastic sheet, which is displaced in a horizontal direction. The method can be used for both electronic and printed documents. The choice line thickness and gaps for high-quality playback means printing equipment.

Key words: перетворення зображень, захист друкованих документів, крива Гільберта.

Вступ

Система захисту електронних та друкованих документів повинна забезпечити автентифікацію документів та службових повідомлень, що гарантує достовірність та цілісність у результаті неможливості підробки або викривлення документів у векторному вигляді. Доволі поширеною стала методика захисту з використанням електронного цифрового підпису (ЕЦП). Запропоновано інший підхід, який не потребує застосування ЕЦП, а охоплює графічні способи захисту електронної та друкованої інформації.