**УДК 621.391**

**О.О.Чуприна**
КБ “Дніпровське”, м. Дніпропетровськ

# УДОСКОНАЛЕНИЙ АЛГОРИТМ ШПФ НА БАЗІ ШВИДКОЇ ЗГОРТКИ



**Наводиться удосконалений ефективний алгоритм обчислення ШПФ для великих обсягів даних. Алгоритм оснований на зведенні ДПФ до згортки та обчисленні коротких згорток з мінімальною кількістю множень.**

**The improved effective algorithm over of calculation is brought FFT for the large volumes of information. An algorithm is based on taking of discrete transformation of Fourier to package and calculation of short package with the minimum number of increases.**

Обчислення дискретного перетворення Фур’є (ДПФ) вигляду $S(x)=\sum_{i=0}^{I-1} s(i)e^{-j\left(\frac{2\pi}{I}\right)ix}$ – одна з основних операцій в цифровій обробці сигналів. Розвиток і широке використання швидкого перетворення Фур’є (ШПФ), якому сприяла поява статті Дж. Кулі та Дж. Такі [1], надало вирішального значення процедурі обробки сигналів. Числові обчислення, що раніше займали багато годин, з появою мікропроцесорних систем, що виконують цифрову обробку сигналів, потребували розроблення ефективних алгоритмів обчислення ШПФ в максимально короткі терміни і, по можливості, в реальному масштабі часу. Стосовно цифрової обробки сигналів це залишається одним з основоположних завдань сьогоденності, яке вимагає постійної уваги.

Досліджень і публікацій, які стосуються ефективних алгоритмів обчислення ДПФ, достатньо велика кількість. Зупинимося на аналізі основоположних напрямів, які торкаються обчислення ДПФ на основі згорток. Вперше така ідея була описана К. Рейдером в 1968 році і полягала в тому, що обчислення ДПФ може бути зведено до циклічної згортки за допомогою перестановки даних, коли обсяг даних $I$ – просте число. У роботі він показав, що швидкий спосіб обчислення згортки відкриває шлях до швидкого обчислення ДПФ [2].

У [3] С. Віноград визначив мінімальну кількість множень, необхідних для обчислення циклічної згортки. Алгоритми згортки, які у багатьох випадках реалізують цей мінімум, були розроблені Р. Агарвалом і Дж. Кулі [4]. Далі, в статті [5] для обсягу даних, що дорівнюють простому числу або ступеню простого числа, С. Віноград об’єднав зведення ДПФ до згортки з новими алгоритмами обчислення коротких згорток. Він запропонував обчислення довгих перетворень за допомогою *гніздового методу* визначення коротких (швидких) перетворень.

Далі дослідження у області обчислення ДПФ велися і ведуться у напрямі дослідження алгоритмів, найефективніших за критерієм швидкості обчислень.

*Невирішеною частиною загальної проблеми* є удосконалення алгоритмів обчислення ШПФ для великих обсягів даних.

*Постановкою завдання* для вирішення є отримання ефективного алгоритму [6] обчислення ШПФ для великих обсягів даних, який ґрунтується на зведенні ДПФ до згортки і її обчисленні з мінімальною кількістю множень.

## Розроблення алгоритму та математичне обґрунтування

Розглянемо два основні положення: перетворення ДПФ до циклічної згортки і згортку з мінімальною кількістю множень.

Альтернативним для *гніздового методу*, запропонованого С. Віноградом в [5], є алгоритм ШПФ для простих множників, що використовує швидку згортку для окремих множників. Цей алгоритм виділимо особливо як перспективний з погляду реалізації за допомогою ЕОМ мовами високого рівня, а також з погляду його виконання окремими мікропроцесорами (сигнальними, систолами тощо) [7] мовами низького рівня. Хоча сама ідея перетворення одновимірного перетворення на багатовимірне з простими множниками і не є новою [8], поєднання коротких швидких алгоритмів згортки з таким багатовимірним розкладанням видається перспективним новим способом обчислення ДПФ і надає додаткові достатні можливості для досліджень.

Виконаємо зведення ДПФ до згортки. Дискретне перетворення Фур'є

$$S(x)\sum_{i=0}^{I-1} s(i) Z^{ix}, \tag{1}$$

де $x = 0,...,I-1$; $Z = e^{-j\left(\frac{2\pi}{I}\right)}$ – лінійне перетворення вектора даних обсягу $I$

$\left.\begin{matrix} s(0) \\ s = s(1) \\ \vdots \\ s(I-1) \end{matrix}\right]$ на вектор $\left.\begin{matrix} S(0) \\ S = (1) \\ \vdots \\ S(I-1) \end{matrix}\right]$ коефіцієнтів Фур'є.

Матричне подання виду $\left.\begin{matrix} S(0) \\ S = (1) \\ \vdots \\ S(I-1) \end{matrix}\right] = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & Z^1 & Z^2\cdots & Z^{I-1} \\ \vdots & Z^2 & Z^4\cdots & Z^{2(I-1)} \\ & \vdots & \vdots & \vdots \\ 1 & Z^{I-1} & Z^{2(I-1)} \;\cdots & Z^{(I-1)(I-1)} \end{bmatrix} \left.\begin{matrix} s(0) \\ s(1) \\ \vdots \\ s(I-1) \end{matrix}\right]$

вказує на те, що складність алгоритму визначається правою нижньою частиною матриці, яка містить $(I-1)\times(I-1)$ комплексних експонент. Якщо

$$\overline{S}(x) = \sum_{i=1}^{I-1} s(i) Z^{xi}, \; x = 1, \dots I-1, \tag{2}$$

вдасться обчислити ефективно, то одержимо швидкий алгоритм для обчислення ДПФ (1), оскільки після обчислення (2) (1) можна отримати так:

$$S(0) = \sum_{i=0}^{I-1} s(i); \; S(x) = s(0) + \overline{S}(x), \; x = 1, 2, ..., I-1. \tag{3}$$

Щоб показати, як (2) можна звести до циклічної згортки, розглянемо матричне подання (2) для $I = 5$ з показниками комплексних експонент, приведеними за модулем 5:

$$\left.\begin{matrix} \overline{S}(1) \\ \overline{S}(2) \\ \overline{S}(3) \\ \overline{S}(4) \end{matrix}\right] = \begin{bmatrix} Z^1 & Z^2 & Z^3 & Z^4 \\ Z^2 & Z^4 & Z^1 & Z^3 \\ Z^3 & Z^1 & Z^4 & Z^2 \\ Z^4 & Z^3 & Z^2 & Z^1 \end{bmatrix} \left.\begin{matrix} s(1) \\ s(2) \\ s(3) \\ s(4) \end{matrix}\right] \tag{4}$$

Якщо переставити останні два стовпці в (4) і потім поміняти місцями останні два рядки, то отримаємо:

$$\left.\begin{matrix} \overline{S}(1) \\ \overline{S}(2) \\ \overline{S}(4) \\ \overline{S}(3) \end{matrix}\right] = \begin{bmatrix} Z^1 & Z^2 & Z^4 & Z^3 \\ Z^2 & Z^4 & Z^3 & Z^1 \\ Z^4 & Z^3 & Z^1 & Z^2 \\ Z^3 & Z^1 & Z^2 & Z^4 \end{bmatrix} \left.\begin{matrix} s(1) \\ s(2) \\ s(4) \\ s(3) \end{matrix}\right]. \tag{5}$$

Отже, ми одержали зворотну циклічну згортку або циклічну кореляцію. Залишаючи на місці $s(1)$ і розташовуючи вектор вхідних даних, що залишився, у зворотній послідовності, отримаємо звичайну циклічну згортку:

$$\begin{bmatrix} \bar{S}(1) \\ \bar{S}(2) \\ \bar{S}(3) \\ \bar{S}(4) \end{bmatrix} = \begin{bmatrix} Z^1 & Z^3 & Z^4 & Z^2 \\ Z^2 & Z^1 & Z^3 & Z^4 \\ Z^4 & Z^2 & Z^1 & Z^3 \\ Z^3 & Z^4 & Z^2 & Z^1 \end{bmatrix} \begin{bmatrix} s(1) \\ s(3) \\ s(4) \\ s(2) \end{bmatrix} \qquad (6)$$

Тобто обчислення (2) (і, отже, ДПФ) зведене до циклічної згортки (6) за допомогою перестановки вхідних і вихідних відліків і, отже, якщо ми отримали швидкий спосіб обчислення згорток, то тим самим ми одержали швидкий спосіб обчислення ДПФ. У [2] К. Рейдер показав, що подібні перестановки можна завжди зробити, коли $I$ – просте число. Але, оскільки $Z^I = 1$, то ми маємо справу з множенням цілих чисел за модулем $I$ в показнику комплексної експоненти $Z$ в (2). Отже, для зведення ДПФ до циклічної згортки можна використовувати відображення індексів, замінюючи множення індексів за модулем $I$ на складання індексів за модулем $I-1$. Як показано в [9], множина цілих чисел $(1, 2, ..., I-1)$ є циклічною групою з операцією множення за модулем $I$. Отже, ми завжди можемо знайти принаймні одне ціле число $A$ в цій групі, що володіє властивістю, що будь-яке ціле число, яке належить цій групі, може бути виражене у вигляді ступеня $A$. Упорядковувавши дані відповідно до показників $A$, зведемо (2) до циклічної згортки для простих $I$. Відповідність між новим індексом $k$ і початковим індексом $i$ запишемо так:

$$i = A^k \bmod I,\ i = 1, 2, ..., I-1;\ k = 0, 1, ..., I-2, \qquad (7)$$

де $A^{x\neq 1}$, для $0 < x < (I-1)$, і $A^{I-1} = 1.$ (8)

Відображення перестановки (7) – це ізоморфізм між мультиплікативною групою $I-1$ цілих чисел $\{1, 2, ..., I-1\}$ й адитивною групою $I-1$ цілих чисел $\{0, 1, ..., I-2\}$. Ціле $A$ з властивістю (8) в науковій літературі називається первісним коренем ступеня $I-1$ з одиниці, і є утворювальним елементом групи (генератором), оскільки будь-який елемент може бути записаний у вигляді ступеня $A$. Так само, як логарифмування зводить множення до складання, так і (7) замінює множення індексів їхнім складанням. Застосуємо (7) до індексів вхідних і вихідних даних. Тоді (2) набуває вигляду:

$$\bar{S}(A') = \sum_{k=0}^{I-2} s\left(A^k\right) Z^{A^{(v+k)}},\ v = 0, ..., I-2. \qquad (9)$$

В (9) показники $A$ обчислюються за модулем $I-1$. При $I-5$ і $A=2$ це дає зворотну циклічну згортку (5). Для отримання звичайної циклічної згортки ми міняємо знак $k$ в (9), що відповідає фіксації $s\left(A^0\right)$ і зверненню порядку решти значень вхідного вектора

$$\bar{S}(A') = \sum_{k=0}^{I-2} s\left(A^{-k}\right) Z^{A^{(v-k)}},\ v = 0, ..., I-2. \qquad (10)$$

У (10), як і вище, показники $A$ визначаються за модулем $I-1$. Об’єднуючи (10) і (3), можна звести обчислення ДПФ до циклічної згортки для простих $I$.

С. Віноград в [5], а також Дж. Макклеллан і К. Рейдер в [10] показали, що ДПФ може бути зведене до згортки, коли довжина перетворення дорівнює ступеню простого числа, тобто $I = d^q$, $d \neq 2$. Проте відзначимо, що для цього випадку з використанням ідеї перетворення одновимірного перетворення на багатовимірне з простими множниками із застосуванням поєднання коротких швидких алгоритмів згортки з багатовимірним розкладанням, перетворення стає складнішим, оскільки необхідно насамперед усунути з множини $\{1, 2, \ldots, I-1\}$ всі цілі числа, що містять множник $d$. Тільки в такому разі можемо отримати циклічну групу з $d^{q-1}(d-1)$ елементами. Ця циклічна група дає можливість отримати циклічну згортку довжини $d^{q-1}(d-1)$ так само, як було описано вище. Додаткові обчислення зводяться до обчислення двох ДПФ довжини $d^{q-1}$. Наприклад, при $I=9=3^2$ викидаємо цілі 3 і 6 для отримання множини $\{1, 2, 4, 5, 7, 8\}$, яка є циклічною групою щодо множення за модулем 9 й ізоморфна адитивній групі цілих чисел $\{0, 1, 2, 3, 4, 5\}$ щодо складання за модулем 6. Ціле 2 є утворювальний елемент мультиплікативної групи, оскільки ступені за модулем 9, $k=0,\ldots,5$ суть $1, 2, 4, 8, 7, 5$. У матричному виразі

$$\begin{bmatrix} S(0) \\ S(1) \\ S(2) \\ S(3) \\ S(4) \\ S(5) \\ S(6) \\ S(7) \\ S(8) \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & Z^1 & Z^2 & Z^3 & Z^4 & Z^5 & Z^6 & Z^7 & Z^8 \\ 1 & Z^2 & Z^4 & Z^6 & Z^8 & Z^1 & Z^3 & Z^5 & Z^7 \\ 1 & Z^3 & Z^6 & 1 & Z^3 & Z^6 & 1 & Z^3 & Z^6 \\ 1 & Z^4 & Z^8 & Z^3 & Z^7 & Z^2 & Z^6 & Z^1 & Z^5 \\ 1 & Z^5 & Z^1 & Z^6 & Z^2 & Z^7 & Z^3 & Z^8 & Z^4 \\ 1 & Z^6 & Z^3 & 1 & Z^6 & Z^3 & 1 & Z^6 & Z^3 \\ 1 & Z^7 & Z^5 & Z^3 & Z^1 & Z^8 & Z^6 & Z^4 & Z^2 \\ 1 & Z^8 & Z^7 & Z^6 & Z^5 & Z^4 & Z^3 & Z^2 & Z^1 \end{bmatrix} \begin{bmatrix} s(0) \\ s(1) \\ s(2) \\ s(3) \\ s(4) \\ s(5) \\ s(6) \\ s(7) \\ s(8) \end{bmatrix} \tag{11}$$

видаляємо рядки і стовпці, відповідні індексам 0, 3 і 6, та обчислюємо перетворення довжини 6, що залишилося

$$\begin{bmatrix} \bar{S}(1) \\ \bar{S}(2) \\ \bar{S}(4) \\ \bar{S}(5) \\ \bar{S}(7) \\ \bar{S}(8) \end{bmatrix} = \begin{bmatrix} Z^1 & Z^2 & Z^4 & Z^5 & Z^7 & Z^8 \\ Z^2 & Z^4 & Z^8 & Z^1 & Z^5 & Z^7 \\ Z^4 & Z^8 & Z^7 & Z^2 & Z^1 & Z^5 \\ Z^5 & Z^1 & Z^2 & Z^7 & Z^8 & Z^4 \\ Z^7 & Z^5 & Z^1 & Z^8 & Z^4 & Z^2 \\ Z^8 & Z^7 & Z^5 & Z^4 & Z^2 & Z^1 \end{bmatrix} \begin{bmatrix} s(1) \\ s(2) \\ s(4) \\ s(5) \\ s(7) \\ s(8) \end{bmatrix}$$

за допомогою відображення

$$i = 2^k \bmod 9, \; i = 1, 2, 4, 8, 7, 5; \quad k = 0, 1, 2, 3, 4, 5,$$

зводячи його до циклічної згортки (зі зверненням вхідного вектора описаним вище способом):

$$\begin{bmatrix} \bar{S}(1) \\ \bar{S}(2) \\ \bar{S}(4) \\ \bar{S}(8) \\ \bar{S}(7) \\ \bar{S}(5) \end{bmatrix} = \begin{bmatrix} Z^1 & Z^5 & Z^7 & Z^8 & Z^4 & Z^2 \\ Z^2 & Z^1 & Z^5 & Z^7 & Z^8 & Z^4 \\ Z^4 & Z^2 & Z^1 & Z^5 & Z^7 & Z^8 \\ Z^8 & Z^4 & Z^2 & Z^1 & Z^5 & Z^7 \\ Z^7 & Z^8 & Z^4 & Z^2 & Z^1 & Z^5 \\ Z^5 & Z^7 & Z^8 & Z^4 & Z^2 & Z^1 \end{bmatrix} \begin{bmatrix} s(1) \\ s(5) \\ s(7) \\ s(8) \\ s(4) \\ s(2) \end{bmatrix} \tag{12}$$

На доповнення до (12) виконаємо обчислення для рядків і стовпців, видалених з (11). Для видалених рядків обчислюємо:

$$\begin{bmatrix} S(0) \\ S(3) \\ S(6) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & Z^3 & Z^6 & 1 & Z^3 & Z^6 & 1 & Z^6 \\ 1 & Z^6 & Z^3 & 1 & Z^6 & Z^3 & 1 & Z^3 \end{bmatrix} \begin{bmatrix} s(0) \\ s(1) \\ s(2) \\ s(3) \\ s(4) \\ s(5) \\ s(6) \\ s(7) \\ s(8) \end{bmatrix}$$

Оскільки $Z^3 = e^{-j\left(\frac{2\pi}{9}\right)\cdot 3} = e^{-j\left(\frac{2\pi}{3}\right)} = Z_3$, то ця формула є просто ДПФ довжиною 3 для підсумованих вхідних значень:

$$\begin{bmatrix} S(0) \\ S(3) \\ S(6) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & Z^3 & Z_3^2 \\ 1 & Z_3^2 & Z^3 \end{bmatrix} \begin{bmatrix} s(0)+s(3)+s(6) \\ s(1)+s(4)+s(7) \\ s(2)+s(5)+s(8) \end{bmatrix}.$$

Для видалених стовпців знаходимо:

$$\begin{bmatrix} N(0) \\ N(1) \\ N(2) \\ N(3) \\ N(4) \\ N(5) \\ N(6) \\ N(7) \\ N(8) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & Z^3 & Z^6 \\ 1 & Z^6 & Z^3 \\ 1 & 1 & 1 \\ 1 & Z^3 & Z^6 \\ 1 & Z^6 & Z^3 \\ 1 & 1 & 1 \\ 1 & Z^3 & Z^6 \\ 1 & Z^6 & Z^3 \end{bmatrix} \begin{bmatrix} s(0) \\ s(3) \\ s(6) \end{bmatrix}$$

Для цього виразу здійснюємо обчислення другого ДПФ довжини 3:

$$\begin{bmatrix} N(0) \\ N(1) \\ N(2) \end{bmatrix} = \begin{bmatrix} N(3) \\ N(4) \\ N(5) \end{bmatrix} = \begin{bmatrix} N(6) \\ N(7) \\ N(8) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & Z_3 & Z_3^2 \\ 1 & Z_3^2 & Z_3 \end{bmatrix} \begin{bmatrix} s(0) \\ s(3) \\ s(6) \end{bmatrix}.$$

Для останнього обчислення (11) за допомогою (12) потрібні тільки два останні значення $N(1)$ і $N(2)$ з попереднього виразу:

$$\begin{bmatrix} S(1) \\ S(2) \\ S(4) \\ S(5) \\ S(7) \\ S(8) \end{bmatrix} = \begin{bmatrix} \overline{S}(1) \\ \overline{S}(2) \\ \overline{S}(4) \\ S(5) \\ \overline{S}(7) \\ \overline{S}(8) \end{bmatrix} + \begin{bmatrix} N(1) \\ N(2) \\ N(1) \\ N(2) \\ N(1) \\ N(2) \end{bmatrix}.$$

Отже, для обчислення ДПФ довжини 9 необхідно обчислити циклічну згортку довжини 6 і два триточкові ДПФ, які обчислюються за допомогою двоточкових циклічних згорток. Якщо $I = 3^3$, то ми отримуємо $3^2 \cdot 2 = 18$-циклічну згортку і дві ДПФ довжини $3^2 = 9$. Останні ДПФ можуть бути зведені до двох шеститочкових згортків і чотирьох триточкових ДПФ, які, своєю чергою, зводяться до обчислення двоточкових згорток.

**Висновки**

Аналізуючи наведені математичні перетворення, отримали, що перетворення довжини $I = d^q$ може бути обчислено за допомогою однієї циклічної згортки довжини $d^{q-1}(d-1)$, двох згорток довжини $d^{q-2}(d-1)$, чотирьох згорток довжини $d^{q-3}(d-1)$, восьми згорток довжини $d^{q-4}(d-1)\ldots$, і $2^{q-1}$ згорток довжини $d-1$, що є удосконаленням алгоритму С. Вінограда з погляду зменшення кількості операцій множення, який був запропонований ним в [5]. Подальшою перспективою для дослідження є знаходження інших ефективних алгоритмів обчислення ДПФ [11].

*1. Cooley J.W., Tukey J.W. An algorithm for the machine calculation of complex Fourier series. – Math. Comput., vol. 19, pp. 297-301, Apr. 1965. 2. Rader C.M. Discrete Fourier, transforms when, the number of data samples is prime. – Proc. IEEE, vol. 56, pp. 1107–1108, June 1968. 3. Winograd S. Some bilinear forms whose multiplicative complexity depends on the field of constants // IBM T.J. Watson-Res. Ctr., Yorktown Heights, NY, IBM Res. Rep. RC 5669, Oct. 10, 1975. 4. Agarwal R., Cooley J.W. New algorithms for digital convolution. Presented at the IEEE Arden House Workshop, Feb. 1971. 5. Winograd S. On computing the discrete Fourier transform. – Proc, Nat. Acad. Sci. USA, vol. 73, no. 4, pp. 1005–1006, Apr. 1976. 6. Казакова Н.Ф., Годулян И.О., Чуприна О.О. Установление критериев оптимизации алгоритмов при определении эффективности информационных систем // Наукові записки УНДІЗ.– 2007. – № 1. – С.62–71. 7. Чуприна А.А. Решение задачи вычисления дискретного преобразования Фурье, когда количество отсчетов – простое число // Наукові записки УНДІЗ. – 2008. – № 1(3). – С.75–79. 8. Чуприна А.А. Частный случай вычисления дискретного преобразования Фурье // Под ред. В.В. Шахгильдяна // Матер. науч.-техн. семин. "Системы синхронизации, формирования и обработки сигналов для связи и вещания", 1–4 июня 2007 г., Одесса: IEEE-РНТОРЭС им.А.С.Попова. – С.176–179. 9. Mostow C.D., Sampson J.H., Meyer J. Fundamental Structures of Algebra. New York: McGraw-Hill, 1993. 10. McClellan J., Rader C.M. There is something much faster than the fast Fourier transform. Seminar Notes, Oct. 21, 1976. 11. Чуприна А.А., Чунаев А.В. Вычисление дискретного преобразования Фурье, когда длина преобразуемой последовательности является циклической корреляцией / Матер. II наук.-практ. семін. молодих науковців та студентства "Сучасні телекомунікаційні та інформаційні технології", 12–14 грудня 2007 р., Київ: УНДІЗ.*