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

УДК 519.6

**В.К. ЗАДІРАКА**
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *zvk140@ukr.net.*

**А.М. ТЕРЕЩЕНКО**
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *teramidi@ukr.net.*

## ОПТИМІЗАЦІЯ БАГАТОРОЗРЯДНОЇ ОПЕРАЦІЇ МНОЖЕННЯ НА ОСНОВІ ДИСКРЕТНИХ ПЕРЕТВОРЕНЬ (ФУР'Є, КОСИНУСНИХ, СИНУСНИХ) У ПАРАЛЕЛЬНІЙ МОДЕЛІ ОБЧИСЛЕННЯ

**Анотація.** Розглянуто операцію багаторозрядного множення, від швидкодії якої залежить швидкодія асиметричних криптографічних програмно-апаратних комплексів. Запропоновано алгоритми реалізації операції множення двох $N$-розрядних чисел на основі дискретних косинусних та синусних перетворень (ДКП та ДСП). За рахунок використання ДКП та ДСП розділено обчислення для дійсної та уявної частин дискретного перетворення Фур'є (ДПФ) дійсного сигналу парної довжини, що дає змогу перевести обчислення з поля комплексних чисел у поле дійсних чисел та зменшити складність багаторозрядної операції множення за кількістю однорозрядних операцій комплексного множення. Проведено заміну операцій алгоритму для збереження симетрії у дійсній або уявній частинах багаторозрядних чисел, що дає змогу використовувати ДКП та ДСП меншої розрядності $N/2+1$ та розширює можливості з розпаралелювання під час реалізації багаторозрядного множення.

**Ключові слова:** багаторозрядне множення, багаторозрядна арифметика, асиметрична криптографія, дискретне косинусне перетворення, дискретне синусне перетворення, дискретне перетворення Фур'є, швидкий алгоритм обчислення Фур'є.

### ВСТУП

Поява нових паралельних обчислювальних систем, як-от багатоядерних процесорів, графічних прискорювачів, кластерів, розподілених систем, систем з розподіленою пам'яттю тощо зумовлена розв'язанням складних прикладних задач у різних галузях. Серед таких задач можна виділити задачі обчислення систем лінійних алгебраїчних рівнянь з кількістю невідомих 33–35 мільйонів, розрахунок оболонок ядерних реакторів, моделювання фізичних і хімічних процесів, аеродинаміки, гідродинаміки, захисту інформації тощо. Це значно розширює використання багаторозрядної арифметики [1–7], оскільки неврахування похибок заокруглення призводить до того, що іноді отримують комп'ютерні рішення, які не відповідають фізичному змісту. Багаторозрядна операція множення є складовою операції піднесення до степеня за модулем, від швидкодії якої залежить швидкодія асиметричних криптографічних програмно-апаратних комплексів.

У роботі Карацуби–Офмана [8] 1962 р. наведено опис алгоритму, який мав складність обчислення багаторозрядного множення за кількістю однорозрядних множень меншу ніж $O^{\text{стовпчик}}(N^2)$, де $N$ — кількість розрядів (слів) багаторозряд-

ного числа. Історично це був перший алгоритм, який відрізнявся від методу «множення у стовпчик». За своєю природою алгоритм Карацуби–Офмана є рекурсивним алгоритмом зі складністю $O^{\text{Карацуби}}(N^{\log_2 3})$, меншою ніж для методу «множення у стовпчик», оскільки на кожному рівні рекурсії обчислювали три операції множення замість чотирьох операцій. Використання рекурсії для обчислення операції множення було вже відомо Ч. Беббіджу, винахіднику першої аналітичної обчислювальної машини у 19-му сторіччі, але можливості заміни чотирьох операцій множення трьома не була приділена достатня увага. З 1962 р. почався активний пошук алгоритмів «швидкого множення». У 1965 р. Кулі та Тьюкі незалежно один від одного запропонували алгоритм [9], який дав змогу дискретне перетворення Фур'є довжини $N = N_1 \cdot N_2$ представити у вигляді дискретних перетворень меншої довжини $N_2$ рекурсивно та зменшити обчислювальну складність до $O^{\text{ШПФ}}(N \log N)$. Більш відомою назвою цього алгоритму є алгоритм «швидкого перетворення Фур'є» або ШПФ. Розробку швидкого алгоритму обчислення дискретного перетворення можна віднести до роботи Гауса 1805 р., де він хотів інтерполювати орбіту астероїдів Палас та Юна. Ця робота передує роботам Фур'є, але у ній не була розглянута обчислювальна складність та зрештою був використаний інший метод. У 1971 р., застосовуючи ШПФ, Шенхаге та Штрассен запропонували алгоритм зі складністю $O^{\text{Шенхаге–Штрассена}}(N \cdot \log N \cdot \text{loglog } N)$ у кільці з $2^N + 1$ елементів [10]. Цей алгоритм був найшвидшим відомим алгоритмом до 2007 р. Алгоритм Шенхаге–Штрассена фундаментально ґрунтується на такій теоремі про циклічну згортку для перетворення Фур'є: результат одновимірної циклічної згортки (наприклад, у вимірі часу) є результатом множення в іншому вимірі (наприклад, вимірі частоти). Цього ж року Пітассі опублікував роботу з описом швидкого алгоритму обчислення перетворення Уошла [11], на основі якого також можна побудувати багаторозрядну операцію множення [12]. У 1985 р. Монтгомері описав алгоритм, який дає змогу швидко обчислювати операцію множення, якщо вона є складовою операції множення за модулем [13]. З появою багатопроцесорних систем з'явилася можливість розпаралелити обчислення з лінійною складністю за кількістю однорозрядних операцій множення у межах одного процесора. У своїй дисертаційній роботі 1966 р. [14] Кук описав метод Тоома від 1963 р., який за своєю складністю $O^{\text{Тоома}}(N^{\log(2k-1)/\log k})$ для великих $k$ наближається до лінійної складності, де $k$ — кількість частин, на які розбивають велике число. Для $k = 2$ метод Тоома–Кука збігається з методом Карацуби–Офмана. Метод Тоома–Кука потребує здійснення більшої кількості операцій додавання та віднімання.

Досягнення в обчисленні ДПФ вплинули на розвиток інших дискретних перетворень. Швидкі обчислення ДКП та ДСП почали широко застосовувати у цифровому обробленні сигналів, починаючи з 1974 та 1976 рр. відповідно [15–19]. У більшості робіт ДКП обчислюють з використанням швидких алгоритмів обчислення ДПФ.

Натомість у цій роботі для обчислення ДПФ застосовано ДКП та ДСП. У роботі [20] запропоновано метод множення багаторозрядних чисел на основі використання уявної частини комплексного сигналу, що дає змогу використовувати ДПФ удвічі меншої розрядності порівняно з базовим методом. У роботі [21] запропоновано метод множення багаторозрядних чисел на основі ДКП та ДСП, у якому розділено обчислення для дійсної та уявної частин ДПФ. Завдяки цьому можна перевести обчислення з поля комплексних чисел у поле дійсних та цілих чисел та зменшити складність багаторозрядної операції множення за кількістю однорозрядних операцій множення. У цій роботі на основі поєднання

методів [20] та [21] запропоновано алгоритм множення багаторозрядних чисел, який зберігає симетрію у дійсній та уявній частинах багаторозрядних комплексних чисел. Це дає змогу використовувати вдвічі більшу кількість ДКП та ДСП з розрядностями вдвічі меншими, порівняно з методом [21]. Використання більшої кількості обчислювальних елементів, що мають менші розміри та складність, дає змогу задіяти більшу кількість процесорів у паралельній моделі обчислення для підвищення швидкодії багаторозрядного множення.

## ПОСТАНОВКА ЗАДАЧІ

Розглянемо обчислення $Z_{2N} = X_N \cdot Y_N$, де $X_N$, $Y_N$ — $N$-розрядні цілі додатні числа, а $Z_{2N}$ — $2N$-розрядне число. Ці числа можна представити у такому вигляді: $X_N = (x_{N-1}x_{N-2}\dots x_0) = \sum_{r=0}^{N-1} x_r 2^{r\omega}$, $Y_N = (y_{N-1}y_{N-2}\dots y_0) = \sum_{r=0}^{N-1} y_r 2^{r\omega}$, $Z_{2N} = (z_{2N-1}z_{2N-2}\dots z_0) = \sum_{r=0}^{2N-1} z_r 2^{r\omega}$,

де $\omega$ — довжина машинного слова у бітах (далі будемо вважати $\omega$=16, 24, 32 чи 64 біта), $0 \le x_r, y_r, z_r < 2^{\omega}$.

Необхідно розробити алгоритм реалізації операції множення двох $N$-розрядних чисел на основі ДКП та ДСП розрядністю $N/2+1$, у якому кількість елементів ДКП та ДСП, які обчислюються одночасно, збільшена вдвічі.

## СКОРОЧЕННЯ ТА ПОЗНАЧЕННЯ

$N$-розрядний сигнал — це послідовність $N$ комплексних чисел, дійсна та уявна частини яких не перевищують довжини машинного слова у бітах. $N$-розрядне число можна представити у вигляді $N$-розрядного сигналу, де уявна частина кожного розряду дорівнює нулю, тобто додавання нульової уявної частини до кожного розряду багаторозрядного числа переводить число у сигнал. Надалі $N$-розрядним числом будемо вважати дійсний $N$-розрядний сигнал, щоб не виділяти окремо операцію представлення багаторозрядного числа у вигляді дійсного багаторозрядного сигналу, та навпаки. Під $N$-розрядним комплексним числом будемо розуміти $N$-розрядний сигнал, у якого є розряди, що мають ненульові значення в уявній частині. У цій роботі використано такі позначення:

- ДПФ — дискретне перетворення Фур'є (у цій роботі термін ДПФ використовується, коли йдеться про перетворений сигнал на основі методу ДПФ, тобто далі його слід розуміти як ДПФ сигналу);
- ДКП — дискретне косинусне перетворення;
- ДСП — дискретне синусне перетворення;
- ОДПФ — обернене ДПФ;
- ШПФ — швидке перетворення Фур'є (швидкий алгоритм обчислення ДПФ сигналу);
- $E(X_{2N}), O(X_{2N})$ — оператори знаходження парних (even) та непарних (odd) елементів вектора $X_{2N}$. Нумерація починається з нуля, тому результатом виконання оператора $E(X_{2N})$ є елементи з індексами 0, 2, 4 тощо, а оператора $O(X_{2N})$ — елементи з індексами 1, 3, 5 тощо. Обчислення $E(X_{2N}), O(X_{2N})$ відповідає таким виразам: $[E(X_{2N})](r) = X_{2N}(2r)$, $[O(X_{2N})](r) = X_{2N}(2r+1)$, $r = \overline{0, N-1}$;

- $E(Z_{2N}) \leftarrow T_N$ — елементи $T_N$ записуються в елементи $Z_{2N}$ з парними індексами 0, 2, 4 тощо. Кількість елементів $T_N$ повинна бути вдвічі меншою за кількість елементів $Z_{2N}$;
- $O(Z_{2N}) \leftarrow T_N$ — аналогічно попередньому позначенню, тільки елементи $T_N$ записуються в елементи $Z_{2N}$ з непарними індексами 1, 3, 5 тощо;
- $I(\hat{X}_{2N})$ — повертає елементи у зворотному порядку за виключенням елементу з індексом нуль. Обчислення $I(\hat{X}_{2N})$ відповідає такому виразу: $[I(X_{2N})](r) = X_{2N}(\langle 2N - r\rangle_{2N})$, $r = \overline{0, 2N-1}$;
- $Z_N = X_N \otimes Y_N$ — значення збігаються з обох сторін поелементно;
- $W_{2N}^r = e^{-\frac{2\pi\cdot i}{2N}r} = e^{-\frac{\pi\cdot i}{N}r}$, $r = \overline{0, 2N-1}$; $W_N^r = e^{-\frac{2\pi\cdot i}{N}r}$.
- $W_{N,N}$ — квадратна матриця елементів $W_N^{\langle k\cdot r\rangle_N} = e^{-\frac{2\pi\cdot i}{N}k\cdot r}$, $k, r = \overline{0, N-1}$.

### БАЗОВИЙ АЛГОРИТМ МНОЖЕННЯ З ОБЧИСЛЕННЯМ ДПФ РОЗРЯДНІСТЮ $2N$ (ДПФ-$2N$)

В алгоритмі [3] до кожного з $N$-розрядних чисел додається $N$ старших нулів. Перехід від $N$- до $2N$-розрядних чисел пояснюється тим, що результатом множення двох $N$-розрядних чисел є число розрядністю $2N$. Отримані $2N$-розрядні числа представлено у вигляді дійсних $2N$-розрядних вектор-стовпців, які можна використовувати як вхідні параметри у ДПФ. Оперування числами розрядністю $2N$ потребує використання ДПФ розрядністю $2N$.

**Алгоритм 1.** Множення двох $N$-розрядних чисел з обчисленням ДПФ розрядністю $2N$ у полі комплексних чисел.

**Вхід:** числа $X_N = \sum_{r=0}^{N-1} x_r \cdot 2^{r\omega}$, $Y_N = \sum_{r=0}^{N-1} y_r \cdot 2^{r\omega}$, де $\omega$ — довжина машинного слова у бітах.

**Результат:** $Z_{2N} = \sum_{r=0}^{2N-1} z_r \cdot 2^{r\omega}$.

**Крок 1.** Ініціалізація та додавання старших нулів:

$$X_{2N}(r) \leftarrow X_N(r),\ Y_{2N}(r) \leftarrow Y_N(r),$$
$$X_{2N}(N+r) \leftarrow Y_{2N}(N+r) \leftarrow 0,\ r = \overline{0, N-1}.$$

**Крок 2.** Обчислення ДПФ розрядністю $2N$:

$$\hat{X}_{2N} \leftarrow W_{2N,2N} \cdot X_{2N},\ \hat{Y}_{2N} \leftarrow W_{2N,2N} \cdot Y_{2N},$$

де $W_{2N}^{\langle r\cdot k\rangle_{2N}} = e^{-\frac{2\pi\cdot i}{2N}\cdot r\cdot k} = e^{-\frac{\pi\cdot i}{N}\cdot r\cdot k}$, $i = \sqrt{-1}$, $r = \overline{0, 2N-1}$, $k = \overline{0, 2N-1}$, елементи матриці $W_{2N,2N}$.

**Крок 3.** Перемноження ДПФ розрядністю $2N$:

$$\hat{Z}_{2N}(r) \leftarrow \hat{X}_{2N}(r) \cdot \hat{Y}_{2N}(r),\ r = \overline{0, 2N-1}.$$

**Крок 4.** Обчислення ОДПФ:

$$Z_{2N} \leftarrow \frac{1}{2N} \cdot W_{2N,2N} \cdot \hat{Z}_{2N}^* \ \text{(або } \frac{1}{2N} \cdot W_{2N,2N}^* \cdot \hat{Z}_{2N}\text{)}.$$

**Крок 5.** Обчислення результату:

$$Z_{2N}(r) \leftarrow [\mathrm{Re}\, Z_{2N}(r)],\ r = \overline{0, 2N-1},$$

де $[\mathrm{Re}\, Z_{2N}(r)]$ — заокруглення до найближчого цілого дійсної частини $Z_{2N}(r)$.

### АЛГОРИТМ МНОЖЕННЯ З ОБЧИСЛЕННЯМ ДПФ РОЗРЯДНІСТЮ $N$ (ДПФ-$N$)

Наведений далі алгоритм [20] дає змогу провести обчислення з використанням ДПФ розрядністю $N$, що є вдвічі меншою ніж розрядність ДПФ, використана в алгоритмі 1. В алгоритмі 2 до кожного з $N$-розрядних чисел додається $N$ старших нулів. Перехід від $N$- до $2N$-розрядних чисел пояснюється тим, що результатом множення двох $N$-розрядних чисел є число розрядністю $2N$. Отримані $2N$-розрядні числа представлено у вигляді комплексних $N$-розрядних вектор-стовпців, які можна використовувати як вхідні параметри у ДПФ. Саме за рахунок задіяння уявної частини чисел довжину ДПФ зменшено вдвічі, що зменшує обчислювальну складність за кількістю однорозрядних операцій множення більше ніж у два рази порівняно з алгоритмом 1. Алгоритм 2 також відрізняється від алгоритму 1-м кроком поелементного множення. На цьому кроці алгоритм 2 має більше доданків, у яких здійснюється поелементне множення.

**Алгоритм 2.** Множення двох $N$-розрядних чисел з обчисленням трьох ДПФ розрядністю $N$.

**Вхід:** числа $X_N = \sum_{r=0}^{N-1} x_r \cdot 2^{r\omega}$, $Y_N = \sum_{r=0}^{N-1} y_r \cdot 2^{r\omega}$, де $\omega$ — довжина машинного слова у бітах.

**Результат:** $Z_{2N} = \sum_{r=0}^{2N-1} z_r \cdot 2^{r\omega}$.

**Крок 1.** Ініціалізація та додавання старших нулів:

$$X_{2N}(r) \leftarrow X_N(r),\ Y_{2N}(r) \leftarrow Y_N(r),$$
$$X_{2N}(N+r) \leftarrow Y_{2N}(N+r) \leftarrow 0,\ r = \overline{0, N-1}.$$

**Крок 2.** Обчислення ДПФ розрядністю N:

$$CX_N \leftarrow E(X_{2N}) - i \cdot O(X_{2N}),\ CY_N \leftarrow E(Y_{2N}) - i \cdot O(Y_{2N}).$$
$$\hat{X}_N \leftarrow W_{N,N} \cdot CX_N,\ \hat{Y}_N \leftarrow W_{N,N} \cdot CY_N.$$

де $W_N^{\langle r \cdot k \rangle_N} = e^{-\frac{2\pi \cdot i}{N} \cdot r \cdot k}$, $i = \sqrt{-1}$, $r = \overline{0, N-1}$, $k = \overline{0, N-1}$, — елементи матриці $W_{N,N}$, результатом виконання оператора $E$ (even) є парні елементи, а оператора $O$ (odd) — непарні.

**Крок 3.** Обчислення ДПФ непарних елементів чисел $X_{2N}$, $Y_{2N}$:

$$O\hat{X}_N \leftarrow (-i) \cdot \frac{1}{2} \cdot (\hat{X}_N - I(\hat{X}_N^*)),\ O\hat{Y}_N \leftarrow (-i) \cdot \frac{1}{2} (\hat{Y}_N - I(\hat{Y}_N^*)),$$

де результатом виконання оператора $I$ є елементи у зворотному порядку за винятком елементу з індексом нуль ($O\hat{X}_N = -W_{N,N} \cdot O(X_{2N})$, $O\hat{Y}_N = -W_{N,N} \cdot O(Y_{2N})$).

**Крок 4.** Обчислення ДПФ розрядністю $N$:

$$\hat{Z}_N(r) \leftarrow \hat{X}_N(r) \cdot \hat{Y}_N(r) + (1 + (W_{2N}^r)^2) \cdot O\hat{X}_N(r) \cdot O\hat{Y}_N(r),$$
$$W_{2N}^r = e^{-\frac{2\pi \cdot i}{2N} r},\ r = \overline{0, N-1}.$$

**Крок 5.** Обчислення ОДПФ та результату:

$$Z_N \leftarrow \frac{1}{N} \cdot W_{N,N} \cdot \hat{Z}_N^*.$$

$$E(Z_{2N}) \leftarrow [\mathrm{Re}\, Z_N],\ O(Z_{2N}) \leftarrow [\mathrm{Im}\, Z_N],$$

де $[\mathrm{Re}\, Z_N(r)]$, $[\mathrm{Im}\, Z_N(r)]$ — заокруглення до найближчого цілого дійсної та уявної частин $Z_N(r)$ відповідно.

### ПРИКЛАД ОБЧИСЛЕННЯ НА ОСНОВІ АЛГОРИТМУ 2

Покажемо роботу алгоритму 2 на прикладі множення 4-розрядних чисел $1112 \cdot 1112 = 1236544$, які можна представити у вигляді вектор-стовпців $X_4 = Y_4 = [2\ 1\ 1\ 1]^T$. Щоб полегшити сприйняття, виконуємо множення однакових чисел. Всі операції здійснюються з цілими числами, тому операцію заокруглення (крок 5) не позначено. Візьмемо до уваги, що $(W_{2N}^r)^2 = \left( e^{-\frac{2\pi \cdot i}{2N} r} \right)^2 = e^{-\frac{2\pi \cdot i}{N} r} = W_N^r$, тоді крок 4 алгоритму 2 можна задати таким виразом:

$$\hat{Z}_N \leftarrow \hat{X}_N \cdot \hat{Y}_N + (1 + W_N) \cdot O\hat{X}_N \cdot O\hat{Y}_N. \qquad (1)$$

Уведемо вектор-стовпець $W_4 = [1\ -i\ -1\ i]^T$, елементи якого обчислюються на основі виразу $(W_{2N}^r)^2 = W_N^r$, $r = \overline{0,3}$.

$$W_{4,4} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix},\ X_8 = [2\ 1\ 1\ 1\ 0\ 0\ 0\ 0]^T,\ Y_8 = X_8,$$

$$CX_4 = E(X_8) - i \cdot O(X_8) = \begin{bmatrix} 2 \\ 1 \\ 0 \\ 0 \end{bmatrix} - i \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 2-i \\ 1-i \\ 0 \\ 0 \end{bmatrix},\ CY_4 = CX_4,$$

$$\hat{X}_4 = W_{4,4} \cdot CX_4 = \begin{bmatrix} 3-2i \\ 1-2i \\ 1 \\ 3 \end{bmatrix},\ \hat{Y}_4 = \hat{X}_4,$$

$$O\hat{X}_4 = \frac{-i}{2} \cdot (\hat{X}_4 - I(\hat{X}_4^*)) = \frac{-i}{2} \cdot \left( \begin{bmatrix} 3-2i \\ 1-2i \\ 1 \\ 3 \end{bmatrix} - \begin{bmatrix} 3+2i \\ 3 \\ 1 \\ 1+2i \end{bmatrix} \right) = \begin{bmatrix} -2 \\ -1+i \\ 0 \\ -1-i \end{bmatrix},$$

$$O\hat{Y}_4 = O\hat{X}_4,\ O\hat{X}_4 \cdot O\hat{Y}_4 = \begin{bmatrix} -2 \\ -1+i \\ 0 \\ -1-i \end{bmatrix} \cdot \begin{bmatrix} -2 \\ -1+i \\ 0 \\ 1-i \end{bmatrix} = \begin{bmatrix} 4 \\ -2i \\ 0 \\ 2i \end{bmatrix},$$

$$\hat{X}_4 \cdot \hat{Y}_4 = \begin{bmatrix} 3-2i \\ 1-2i \\ 1 \\ 3 \end{bmatrix} \cdot \begin{bmatrix} 3-2i \\ 1-2i \\ 1 \\ 3 \end{bmatrix} = \begin{bmatrix} 5-12i \\ -3-4i \\ 1 \\ 9 \end{bmatrix},$$

$$\hat{Z}_4 = \hat{X}_4 \cdot \hat{Y}_4 + (1+W_4) \cdot O\hat{X}_4 \cdot O\hat{Y}_4 = \begin{bmatrix} 5-12i \\ -3-4i \\ 1 \\ 9 \end{bmatrix} + \begin{bmatrix} 1+1 \\ 1-i \\ 1-1 \\ 1+i \end{bmatrix} \cdot \begin{bmatrix} 4 \\ -2i \\ 0 \\ 2i \end{bmatrix} = \begin{bmatrix} 13-12i \\ -5-6i \\ 1 \\ 7+2i \end{bmatrix},$$

$$Z_4 = \frac{1}{4} \cdot W_{4,4} \cdot \hat{Z}_4^* = \frac{1}{4} \cdot W_{4,4} = \begin{bmatrix} 13+12i \\ -5+6i \\ 1 \\ 7-2i \end{bmatrix} = \tfrac{1}{4} \cdot \begin{bmatrix} 16+16i \\ 20+24i \\ 12+8i \\ 4 \end{bmatrix} = \begin{bmatrix} 4+4i \\ 5+6i \\ 3+2i \\ 1 \end{bmatrix},$$

$$E(Z_8) = [4\ 5\ 3\ 1]^{\mathrm{T}},\ O(Z_8) = [4\ 6\ 2\ 0]^{\mathrm{T}},\ Z_8 = [4\ 4\ 5\ 6\ 3\ 2\ 1\ 0]^{\mathrm{T}}.$$

**АНАЛІЗ СИМЕТРІЇ У ДІЙСНІЙ ТА УЯВНІЙ ЧАСТИНАХ ОПЕРАЦІЙ НАД БАГАТОРОЗРЯДНИМИ ЧИСЛАМИ**

У результаті порівняння кроків 4 алгоритмів 1 та 2 можна побачити, що алгоритм 2 має більшу кількість доданків, у яких здійснюється поелементне множення.

Формула Ейлера стверджує, що для будь-якого дійсного числа $x$ виконується рівність

$$e^{ix} = \cos x + i \sin x.$$

За допомогою формули Ейлера можна довести такі властивості ДПФ дійсного сигналу довжиною $N$, що дає змогу значно зменшити кількість комплексних множень:

$$\operatorname{Im} \hat{X}_{2N}(0) = 0,\ \operatorname{Im} \hat{X}_{2N}(N) = 0;$$

$$\operatorname{Re} \hat{X}_{2N}(r) = \operatorname{Re} \hat{X}_{2N}(2N-r),\ \operatorname{Im} \hat{X}_{2N}(r) = -\operatorname{Im} \hat{X}_{2N}(2N-r), \qquad (2)$$

$$r = \overline{1,\ N-1}.$$

Надалі властивості (2) будемо називати симетрією у дійсній частині багаторозрядного комплексного числа.

**Лема 1.** Якщо комплексні сигнали $\hat{X}_{2N}$ та $\hat{Y}_{2N}$ розрядністю $2N$ (парної довжини) мають властивості (2), то операції поелементного множення, додавання та віднімання утворюють комплексні сигнали $\hat{Z}_{2N} = \hat{X}_{2N} \cdot \hat{Y}_{2N}$ та $\hat{T}_{2N} = \hat{X}_{2N} \pm \hat{Y}_{2N}$, які також відповідають властивостям (2).

**Доведення.** Результатом додавання (віднімання) двох комплексних чисел з індексами $r = 0, N$, у яких уявна частина дорівнює нулю, також є число, у якого уявна частина дорівнює нулю. Справджуються такі вирази:

$$\hat{X}_{2N}^*(r) \pm \hat{Y}_{2N}^*(r) = (\hat{X}_{2N}(r) \pm \hat{Y}_{2N}(r))^* = \hat{X}_{2N}(2N-r) \pm \hat{Y}_{2N}(2N-r),$$

$$r = \overline{1,\ N-1}.$$

Множення двох комплексних чисел, в яких уявна частина дорівнює нулю, утворює також число з нульовою уявною частиною. Аналогічно операції додавання (віднімання) результат множення двох комплексно-спряжених чисел

дорівнює числу, в якого уявна частина також буде комплексно-спряженою, а саме

$$\hat{X}^{*}_{2N}(r)\cdot\hat{Y}^{*}_{2N}(r)=(\hat{X}_{2N}(r)\cdot\hat{Y}_{2N}(r))^{*}=$$

$$=(\hat{X}^{*}_{2N}(2N-r)\cdot\hat{Y}^{*}_{2N}(2N-r))^{*}=\hat{X}_{2N}(2N-r)\cdot\hat{Y}_{2N}(2N-r),\ r=\overline{1,\,N-1}.$$

Лему доведено.

**Лема 2.** Комплексний сигнал $SW_{2N}$ розрядністю $2N$ (парної довжини) з елементами $SW_{2N}(r)=W^{r}_{4N}=e^{-\frac{2\pi\cdot i}{4N}r}$, $r=\overline{0,\,2N-1}$, має такі властивості:

$$\begin{gathered}\operatorname{Im}SW_{2N}(0)=0,\ \operatorname{Re}SW_{2N}(N)=0,\\ \operatorname{Re}SW_{2N}(r)=-\operatorname{Re}W_{2N}(2N-r),\\ \operatorname{Im}SW_{2N}(r)=\operatorname{Im}SW_{2N}(2N-r),\ r=\overline{1,\,N-1}.\end{gathered}\tag{3}$$

**Доведення.** Обчислимо $SW_{2N}(0)=W^{r}_{4N}$ для $r=0$. Маємо, що $W^{0}_{4N}=e^{0}=1$. Для $r=N$ обчислимо

$$SW_{2N}(N)=W^{N}_{4N}=e^{-\frac{2\pi\cdot i}{4N}\cdot N}=e^{-\frac{\pi}{2}\cdot i}=\cos(-\pi/2)+i\sin(-\pi/2)=-i.$$

Далі обчислимо таке:

$$SW_{2N}(2N-r)=W^{2N-r}_{4N}=e^{-\frac{2\pi\cdot i}{4N}(2N-r)}=$$

$$=e^{-\frac{2\pi\cdot i}{4N}2N}\cdot e^{-\frac{2\pi\cdot i}{4N}(-r)}=e^{-\pi\cdot i}\cdot e^{-\frac{2\pi\cdot i}{4N}(-r)}=(\cos(-\pi)+i\sin(-\pi))\cdot W^{-r}_{4N}=$$

$$=-1\cdot W^{-r}_{4N}=-(W^{r}_{4N})^{-1}=-(W^{r}_{4N})^{*}=-SW^{*}_{2N}(r),\ r=\overline{1,\,N-1}.$$

Отримаємо, що $SW_{2N}(r)=-SW^{*}_{2N}(2N-r)$, $r=\overline{1,\,N-1}$. Цей вираз є аналогічним операції обчислення комплексно-спряженого значення, але для цього виразу знак змінюється на протилежний для дійсної частини комплексного числа замість уявної частини.

Лему доведено.

Властивості (3) далі будемо називати симетрією в уявній частині багаторозрядного комплексного числа.

**Лема 3.** Операція поелементного множення комплексних сигналів $\hat{X}_{2N}$ та $\hat{Y}_{2N}$ розрядністю $2N$ (парної довжини), які відповідають різним властивостям ((2) або (3)), утворює комплексний сигнал $\hat{Z}_{2N}=\hat{X}_{2N}\cdot\hat{Y}_{2N}$, який відповідає властивостям (3).

**Доведення.** Властивості (2) та (3) справджуються для елементів з індексом $r=0$. Є різниця у властивостях елементів з індексом $r=N$. У випадку множення чисел $\hat{X}_{2N}(N)\cdot\hat{Y}_{2N}(N)$ з властивостями $\operatorname{Im}\hat{X}_{2N}(N)=0$, $\operatorname{Re}\hat{Y}_{2N}(N)=0$ отримуємо число, яке буде мати властивість $\operatorname{Re}(\hat{Y}_{2N}(N)\cdot\hat{Y}_{2N}(N))=0$, що відповідає властивостям (3). У випадку поелементного множення $\hat{X}_{2N}(r)\cdot\hat{Y}_{2N}(r)$, $r=\overline{1,\,N-1}$ та $r=\overline{N+1,\,2N-1}$, з властивостями (2) для $\hat{X}_{2N}$ та властивостями (3) для $\hat{Y}_{2N}$

$$\operatorname{Re}\hat{X}_{2N}(r)=\operatorname{Re}\hat{X}_{2N}(2N-r),\ \operatorname{Im}\hat{X}_{2N}(r)=-\operatorname{Im}\hat{X}_{2N}(2N-r),$$

$$\operatorname{Re}\hat{Y}_{2N}(r)=-\operatorname{Re}\hat{Y}_{2N}(2N-r),\ \operatorname{Im}\hat{Y}_{2N}(r)=\operatorname{Im}\hat{Y}_{2N}(2N-r),\ r=\overline{1,\,N-1},$$

отримуємо число, яке буде мати властивості

$$\mathrm{Re}(\hat{X}_{2N}(r)\cdot\hat{Y}_{2N}(r)) = -\mathrm{Re}(\hat{X}_{2N}(2N-r)\cdot\hat{Y}_{2N}(2N-r)),$$

$$\mathrm{Im}(\hat{X}_{2N}(r)\cdot\hat{Y}_{2N}(r)) = \mathrm{Im}\,\hat{X}_{2N}((2N-r)\cdot\hat{Y}_{2N}(2N-r)),\ r=\overline{1,\,N-1},$$

що відповідає властивостям (3).

Доведення у тому випадку, коли $\hat{X}_{2N}$ відповідає властивостям (3) та $\hat{Y}_{2N}$ відповідає властивостям (2), є аналогічним.

Лему доведено.

**Лема 4.** Якщо комплексні сигнали $\hat{X}_{2N}$ та $\hat{Y}_{2N}$ розрядністю $2N$ (парної довжини) мають властивості (3), то операції поелементного множення утворюють комплексний сигнал $\hat{Z}_{2N} = \hat{X}_{2N}\cdot\hat{Y}_{2N}$, який відповідає властивостям (2).

**Доведення.** Властивості (2) та (3) справджуються для елементів з індексом $r=0$. Є різниця у властивостях елементів з індексом $r=N$. У випадку множення чисел $\hat{X}_{2N}(N)\cdot\hat{Y}_{2N}(N)$ з властивостями $\mathrm{Re}\,\hat{X}_{2N}(N)=0$, $\mathrm{Re}\,\hat{Y}_{2N}(N)=0$ отримуємо число, яке буде мати властивість $\mathrm{Im}\,(\hat{Y}_{2N}(N)\cdot\hat{Y}_{2N}(N))=0$, що відповідає властивості (2).

У випадку поелементного множення $\hat{X}_{2N}(r)\cdot\hat{Y}_{2N}(r)$, $r=\overline{1,\,N-1}$ та $r=\overline{N+1,2N-1}$, з властивостями (3) для $\hat{X}_{2N}$ та $\hat{Y}_{2N}$ маємо, що

$$\mathrm{Re}\,\hat{X}_{2N}(r) = -\mathrm{Re}\,\hat{X}_{2N}(2N-r),\ \mathrm{Im}\,\hat{X}_{2N}(r) = \mathrm{Im}\,\hat{X}_{2N}(2N-r),$$

$$\mathrm{Re}\,\hat{Y}_{2N}(r) = -\mathrm{Re}\,\hat{Y}_{2N}(2N-r),\ \mathrm{Im}\,\hat{Y}_{2N}(r) = \mathrm{Im}\,\hat{Y}_{2N}(2N-r)\ ,\ r=\overline{1,\,N-1},$$

отримуємо число, яке буде мати властивості

$$\mathrm{Re}(\hat{X}_{2N}(r)\cdot\hat{Y}_{2N}(r)) = \mathrm{Re}(\hat{X}_{2N}(2N-r)\cdot\hat{Y}_{2N}(2N-r)),$$

$$\mathrm{Im}(\hat{X}_{2N}(r)\cdot\hat{Y}_{2N}(r)) = -\mathrm{Im}(\hat{X}_{2N}(2N-r)\cdot\hat{Y}_{2N}(2N-r)),\ r=\overline{1,\,N-1},$$

що відповідає властивостям (2).

Лему доведено.

Операції, розглянуті у лемах 3 та 4, далі називатимемо операціями, які дають змогу зберігати симетричність (властивості (2) та (3)) у багаторозрядних комплексних числах розрядності парної довжини під час виконання операцій.

Далі проаналізовано властивості (2) (симетрія у дійсній частині) і розглянуто можливість заміни операцій, які не мають властивостей (2), на операції, які мають властивості (2). Це дає змогу використовувати ДКП та ДСП меншої розрядності на всіх кроках виконання алгоритму багаторозрядного множення.

## АНАЛІЗ ОБЧИСЛЕННЯ ДЛЯ ЗБЕРЕЖЕННЯ СИМЕТРИЧНОСТІ СИГНАЛІВ ПАРНОЇ ДОВЖИНИ

У результаті аналізу виразу (1) видно, що $\hat{Z}_N$ не відповідає властивостям симетрії (2) та (3), оскільки вирази $\hat{X}_N$ та $\hat{Y}_N$, використані в (1), не відповідають цим властивостям. Проаналізуємо вираз (1), щоб з'ясувати, чи можна здійснити заміну такими операціями, щоб проміжні результати відповідали властивостям симетрії.

Введемо нові позначення

$$EX_N \leftarrow E(X_{2N}),\ DX_N \leftarrow O(X_{2N}),$$

$$EY_N \leftarrow E(Y_{2N}),\ DY_N \leftarrow O(Y_{2N}),$$

$$X_N \leftarrow EX_N + i\cdot DX_N,\ Y_N \leftarrow EY_N + i\cdot DY_N.$$

Враховуючи, що $D\hat{X}_N = -O\hat{X}_N$, $D\hat{Y}_N = -O\hat{Y}_N$, у формулі (1) зробимо заміну у такий спосіб:

$$\hat{Z}_N = \hat{X}_N \cdot \hat{Y}_N + (1+W_N)\cdot O\hat{X}_N \cdot O\hat{Y}_N =$$

$$= (E\hat{X}_N - i\cdot O\hat{X}_N)\cdot(E\hat{Y}_N - i\cdot O\hat{Y}_N) + (1+W_N)\cdot(-D\hat{X}_N)\cdot(-D\hat{Y}_N) =$$

$$= (E\hat{X}_N + i\cdot D\hat{X}_N)\cdot(E\hat{Y}_N + i\cdot D\hat{Y}_N) + (1+W_N)\cdot D\hat{X}_N \cdot D\hat{Y}_N =$$

$$= E\hat{X}_N \cdot E\hat{Y}_N - D\hat{X}_N \cdot D\hat{Y}_N + i\cdot(E\hat{Y}_N \cdot D\hat{X}_N + D\hat{Y}_N \cdot E\hat{X}_N) +$$

$$+ D\hat{X}_N \cdot D\hat{Y}_N + W_N \cdot D\hat{X}_N \cdot D\hat{Y}_N =$$

$$= E\hat{X}_N \cdot E\hat{Y}_N + i\cdot(E\hat{Y}_N \cdot D\hat{X}_N + D\hat{Y}_N \cdot E\hat{X}_N) + W_N \cdot D\hat{X}_N \cdot D\hat{Y}_N .$$

Остаточно маємо, що

$$\hat{Z}_N = E\hat{X}_N \cdot E\hat{Y}_N + W_N \cdot D\hat{X}_N \cdot D\hat{Y}_N +$$

$$+ i\cdot(E\hat{Y}_N \cdot D\hat{X}_N + D\hat{Y}_N \cdot E\hat{X}_N). \qquad (4)$$

Обчислення виразу (4) є складнішим за обчислення (1), оскільки він має більше доданків, що потребує більшої кількості операцій поелементного множення. Введемо додаткові позначення, які дають змогу зменшити кількість цих операцій порівняно з їхньою кількістю у виразі (4):

$$S\hat{D}_N = (E\hat{X}_N - SW_N \cdot D\hat{X}_N)\cdot(E\hat{Y}_N - SW_N \cdot D\hat{Y}_N),$$

$$A\hat{D}_N = (E\hat{X}_N + SW_N \cdot D\hat{X}_N)\cdot(E\hat{Y}_N + SW_N \cdot D\hat{Y}_N),$$

де $SW_N(r) = W_{2N}^r = e^{-\frac{2\pi\cdot i}{2N}r}$, $r = \overline{0, N-1}$, є елементами вектор-стовпця $SW_N$.

Обчислимо додатково елементи

$$\hat{A}_N = \frac{1}{2}(A\hat{D}_N + S\hat{D}_N),$$

$$\hat{S}_N = \frac{1}{2\cdot SW_N}(A\hat{D}_N - S\hat{D}_N) = \frac{SW_N^*\cdot(A\hat{D}_N - S\hat{D}_N)}{2\cdot(\mathrm{Re}\,SW_N)^2 + 2\cdot(\mathrm{Im}\,SW_N)^2},$$

де елементи вектор-стовпця $SW_N^*$ є комплексно-спряженими з відповідними елементами вектор-стовпця $SW_N$.

Оскільки $(\mathrm{Re}\,SW_N(r))^2 + (\mathrm{Im}\,SW_N(r))^2 = 1$, $r = \overline{0, N-1}$, то можна записати, що $\hat{S}_N = \frac{SW_N^*}{2}(A\hat{D}_N - S\hat{D}_N)$.

За допомогою попередніх виразів значення $\hat{Z}_N$ у виразі (4) можна обчислити у такий спосіб:

$$\hat{Z}_N \leftarrow \hat{A}_N + i\cdot\hat{S}_N .$$

**Лема 5.** Числа $\hat{A}_N$ та $\hat{S}_N$ відповідають властивостям (2).

**Доведення.** Згідно з формулою (4) число $\hat{A}_N = (A\hat{D}_N + S\hat{D}_N)/2$ дорівнює виразу $E\hat{X}_N \cdot E\hat{Y}_N + W_N \cdot D\hat{X}_N \cdot D\hat{Y}_N$, кожен елемент якого відповідає властивостям (2), та, відповідно до леми 1, $\hat{A}_N$ також відповідає властивостям (2). Аналогічно доводять число $\hat{S}_N = (A\hat{D}_N - S\hat{D}_N)\cdot SW_N^*/2$, яке дорівнює $E\hat{Y}_N \cdot D\hat{X}_N + D\hat{Y}_N \cdot E\hat{X}_N$, кожен елемент якого також відповідає властивостям (2).

Лему доведено.

**Алгоритм 3.** Множення двох $N$-розрядних чисел з обчисленням трьох ДПФ розрядністю $N$ та поелементним множенням чисел, які зберігають симетрію (властивості (2) та (3)).

**Вхід:** числа $X_N = \sum_{r=0}^{N-1} x_r \cdot 2^{r\omega}$, $Y_N = \sum_{r=0}^{N-1} y_r \cdot 2^{r\omega}$, де $\omega$ — довжина машинного слова у бітах.

**Результат:** $Z_{2N} = \sum_{r=0}^{2N-1} z_r \cdot 2^{r\omega}$.

**Крок 1.** Ініціалізація та додавання старших нулів:

$$X_{2N}(r) \leftarrow X_N(r),\ Y_{2N}(r) \leftarrow Y_N(r),$$
$$X_{2N}(N+r) \leftarrow Y_{2N}(N+r) \leftarrow 0,\ r = \overline{0, N-1}.$$

**Крок 2.** Обчислення парних та непарних елементів:

$$EX_N \leftarrow E(X_{2N}),\ EY_N \leftarrow E(Y_{2N}),$$
$$DX_N \leftarrow O(X_{2N}),\ DY_N \leftarrow O(Y_{2N}),$$

де результатом виконання оператора $E$ (even) є парні елементи, а оператора $O$ (odd) — непарні.

**Крок 3.** Обчислення ДПФ парних та непарних елементів чисел $X_{2N}, Y_{2N}$:

$$E\hat{X}_N \leftarrow W_{N,N} \cdot EX_N,\ E\hat{Y}_N \leftarrow W_{N,N} \cdot EY_N,$$
$$D\hat{X}_N \leftarrow W_{N,N} \cdot DX_N,\ D\hat{Y}_N \leftarrow W_{N,N} \cdot DY_N.$$

де $W_N^{\langle r\cdot k\rangle_N} = e^{-\frac{2\pi\cdot i}{N}\cdot r\cdot k}$, $i = \sqrt{-1}$, $r = \overline{0, N-1}$, $k = \overline{0, N-1}$, — елементи матриці $W_{N,N}$.

**Крок 4.** Обчислення чисел, необхідних для ОДПФ:

$$SW_N(r) = W_{2N}^r,\ r = \overline{0, N-1},$$
$$S\hat{D}_N \leftarrow (E\hat{X}_N - SW_N \cdot D\hat{X}_N) \cdot (E\hat{Y}_N - SW_N \cdot D\hat{Y}_N),$$
$$A\hat{D}_N \leftarrow (E\hat{X}_N + SW_N \cdot D\hat{X}_N) \cdot (E\hat{Y}_N + SW_N \cdot D\hat{Y}_N).$$
$$\hat{A}_N \leftarrow \frac{1}{2}(A\hat{D}_N + S\hat{D}_N),$$
$$\hat{S}_N \leftarrow \frac{1}{2} \cdot SW_N^* \cdot (A\hat{D}_N - S\hat{D}_N),$$

де кожен елемент вектор-стовпця $SW_N^*$ є комплексно-спряженим до відповідних елементів вектор-стовпця $SW_N$.

**Крок 5.** Обчислення ОДПФ та результату:

$$A_N \leftarrow W_{N,N}^* \cdot \hat{A}_N,\ S_N \leftarrow W_{N,N}^* \cdot \hat{S}_N$$
$$(\text{або } A_N \leftarrow W_{N,N} \cdot \hat{A}_N^*,\ S_N \leftarrow W_{N,N} \cdot \hat{S}_N^*).$$
$$Z_N \leftarrow \frac{1}{N}(A_N + i \cdot S_N).$$

$$E(Z_{2N}) \leftarrow [\mathrm{Re}\, Z_N],\ O(Z_{2N}) \leftarrow [\mathrm{Im}\, Z_N],$$

де $[\mathrm{Re}\, Z_N(r)]$, $[\mathrm{Im}\, Z_N(r)]$ — заокруглення до найближчого цілого дійсної та уявної частин $Z_N(r)$ відповідно.

**ПРИКЛАД ОБЧИСЛЕННЯ НА ОСНОВІ АЛГОРИТМУ 3**

Покажемо роботу алгоритму 3 на прикладі множення 8-розрядних чисел $11111112 \cdot 11111112 = 123\,456\,809\,876\,544$, які можна представити у вигляді вектор-стовпців $X_8 = Y_8 = [2\,1111111]^T$. Щоб полегшити сприйняття, виконуємо множення однакових чисел.

$$W_{8,8} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & pm & -i & mm & -1 & mp & i & pp \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & mm & -i & pm & -1 & pp & i & mp \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & mp & -i & pp & -1 & pm & i & mm \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & pp & i & mp & -1 & mm & -i & pm \end{bmatrix},$$

$$pp = \frac{\sqrt{2}}{2}(1+i),$$
$$pm = \frac{\sqrt{2}}{2}(1-i),$$
$$mp = \frac{\sqrt{2}}{2}(-1+i),$$
$$mm = \frac{\sqrt{2}}{2}(-1-i),$$

$$SW_8,\quad \begin{bmatrix} 1 \\ 0.9239 - i0.3827 \\ 0.7071 - i0.7071 \\ 0.3827 - i0.9239 \\ -i \\ -0.3827 - i0.9239 \\ -0.7071 - i0.7071 \\ -0.9239 - i0.3827 \end{bmatrix}$$

$$EX_8,\ DX_8,\ E\hat{X}_8 = W_{8,8} \cdot EX_8,\ D\hat{X}_8 = W_{8,8} \cdot DX_8,$$

$$EX_8 = \begin{bmatrix} 2 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},\quad DX_8 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},\quad E\hat{X}_8 = \begin{bmatrix} 5 \\ 2 - i2.4142 \\ 1 \\ 2 - i0.4142 \\ 1 \\ 2 + i0.4142 \\ 1 \\ 2 + i2.4142 \end{bmatrix},\quad D\hat{X}_8 = \begin{bmatrix} 4 \\ 1 - i2.4142 \\ 0 \\ 1 - i0.4142 \\ 0 \\ 1 + i0.4142 \\ 0 \\ 1 + i2.4142 \end{bmatrix}$$

$$SW_8 \cdot D\hat{X}_8,\ E\hat{X}_8 - SW_{8,8} \cdot D\hat{X}_8,\ E\hat{X}_8 + SW_{8,8} \cdot D\hat{X}_8,$$

$$\begin{bmatrix} 4 \\ -i2.6132 \\ 0 \\ -i1.0824 \\ 0 \\ -i1.0824 \\ 1 \\ -i2.6132 \end{bmatrix},\quad \begin{bmatrix} 1 \\ 2.0000 + i0.1989 \\ 1 \\ 1.9999 + i0.6682 \\ 1 \\ 2.0000 + i1.4966 \\ 1 \\ 1.9998 + i5.0274 \end{bmatrix},\quad \begin{bmatrix} 9 \\ 1.9999 - i5.0274 \\ 1 \\ 2.0000 - i1.4966 \\ 1 \\ 1.9999 - i0.6682 \\ 1 \\ 2.0000 - i0.1989 \end{bmatrix}$$

$$EY_8 = EX_8,\ DY_8 = DX_8,\ E\hat{Y}_8 = E\hat{X}_8,\ D\hat{Y}_8 = D\hat{X}_8,$$

$$S\hat{D}_8 = (E\hat{X}_8 - SW_{8,8} \cdot D\hat{X}_8) \cdot (E\hat{Y}_8 - SW_{8,8} \cdot D\hat{Y}_8) = \begin{bmatrix} 1 \\ 3.9605 + i0.7958 \\ 1 \\ 3.5534 + i2.6728 \\ 1 \\ 1.7602 + i5.9865 \\ 1 \\ -21.2746 + i20.1094 \end{bmatrix},$$

$$A\hat{D}_8 = (E\hat{X}_8 + SW_{8,8} \cdot D\hat{X}_8) \cdot (E\hat{Y}_8 + SW_{8,8} \cdot D\hat{Y}_8) = \begin{bmatrix} 81 \\ -21.2746 - i20.1094 \\ 1 \\ 1.7603 - i5.9865 \\ 1 \\ 3.5534 - i2.6728 \\ 1 \\ 3.9605 - i0.7959 \end{bmatrix},$$

$$\hat{A}_8 = \frac{1}{2}(A\hat{D}_8 + S\hat{D}_8) = \quad \hat{S}_8 = \frac{1}{2}(A\hat{D}_8 - S\hat{D}_8)\cdot SW_8^* =$$

$$\begin{bmatrix} 41 \\ -8.6571 - i9.6567 \\ 1 \\ 2.6568 - i1.6568 \\ 1 \\ 2.6568 + i1.6568 \\ 1 \\ -8.6571 + i9.6567 \end{bmatrix}, \qquad \begin{bmatrix} 40 \\ -7.6571 - i14.4859 \\ 0 \\ 3.6571 - i2.4853 \\ 0 \\ 3.6571 + i2.4853 \\ 0 \\ -7.6571 + i14.4859 \end{bmatrix},$$

$$A_8 = W_{8,8}\cdot \hat{A}_8^* \quad S_8 = W_{8,8}\cdot \hat{S}_8^* \quad Z_8 = (A_8 + i\cdot S_8)/N$$

$$\begin{bmatrix} 31.995 \\ 39.9995 \\ 55.9998 \\ 71.9998 \\ 56.0005 \\ 40.0005 \\ 24.0002 \\ 8.0003 \end{bmatrix}, \quad \begin{bmatrix} 31.9999 \\ 48.0003 \\ 64.0012 \\ 80.0013 \\ 48.0001 \\ 31.9997 \\ 15.9988 \\ -0.001253 \end{bmatrix}, \quad \begin{bmatrix} 3.9999 + i3.9999 \\ 4.9999 + i6.0000 \\ 6.9999 + i8.0002 \\ 8.9999 + i10.0002 \\ 7.0001 + i6.0000 \\ 5.0001 + i3.9999 \\ 3.0000 + i1.9998 \\ 1.0000 - i0.0002 \end{bmatrix},$$

$$E(Z_{16}) = [\mathrm{Re}\, Z_8] = [4\ 5\ 7\ 9\ 7\ 5\ 3\ 1]^T,$$

$$O(Z_{16}) = [\mathrm{Im}\, Z_8] = [4\ 6\ 8\ 10\ 6\ 4\ 2\ 0]^T,$$

$$Z_{16} = [4\ 4\ 5\ 6\ 7\ 8\ 9\ (10-10)\ (7+1)\ 6\ 5\ 4\ 3\ 2\ 1\ 0]^T =$$

$$= [4\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 8\ 6\ 5\ 4\ 3\ 2\ 1\ 0]^T.$$

### ОПТИМІЗАЦІЯ ОБЧИСЛЕННЯ ДПФ ТА ОДПФ НА ОСНОВІ ДКП ТА ДСП

У роботі [21] розглянуто сигнали, які відповідають властивостям (2). Для цих сигналів обчислення ДПФ дійсного сигналу парної довжини можна реалізувати шляхом розділення обчислення для дійсної частини на основі ДКП та уявної частини на основі ДСП. Це дає змогу перевести обчислення з поля комплексних чисел у поле дійсних чисел та зменшити складність багаторозрядної операції множення за кількістю комплексних операцій множення майже на третину. Цей перехід зменшує зв'язність з комплексними операціями та дає змогу виконувати більше простіших операцій у полі дійсних чисел. Отже, можна задіяти більшу кількість процесорів у паралельній моделі обчислення.

Відповідно до [21] (див. алгоритм 3), ДПФ $\hat{X}_{2N}$ розрядністю $2N$ дійсного сигналу $X_{2N}$ можна обчислити з використанням матриць коефіцієнтів ДКП та ДСП розмірами $2N+1$ на $2N+1$. Якщо старші розряди мають нулі, то обчислення можна виконати ефективніше з використанням матриць коефіцієнтів ДКП та ДСП розмірами $N+1$ на $N+1$. Проведемо аналіз цього резерву оптимізації.

**Лема 6.** ДПФ дійсного сигналу $X_{2N}$ розрядністю $2N$, старші розряди якого мають нулі, може бути обчислено на основі виразів

$$X_{N+1}(r) \leftarrow X_{2N}(r),\ r = \overline{0,\ N-1},\ X_{N+1}(N) = 0;$$

$$\hat{X}_{N+1} \leftarrow (C_{N+1,N+1} - i\cdot S_{N+1,N+1})\cdot X_{N+1};$$

$$\hat{X}_{2N}(r) \leftarrow \hat{X}_{N+1}(r),\ r=\overline{0,\ N};$$

$$\hat{X}_{2N}(2N-r) \leftarrow \hat{X}^{*}_{N+1}(r),\ r=\overline{1,\ N-1},$$

де $C_{2N}^{\langle k\cdot r\rangle_{2N}} = \cos\left(\frac{k\cdot r\cdot\pi}{2N}\right)$, $S_{2N}^{\langle k\cdot r\rangle_{2N}} = \sin\left(\frac{k\cdot r\cdot\pi}{2N}\right)$, $k, r=\overline{0,\ N}$, є елементами матриць $C_{N+1,\,N+1}$ та $S_{N+1,\,N+1}$.

**Доведення.** За визначенням маємо, що

$$W_{2N}^{\langle k\cdot r\rangle_{2N}} = \cos\left(\frac{k\cdot r\cdot\pi}{2N}\right) - i\cdot\sin\left(\frac{k\cdot r\cdot\pi}{2N}\right) = C_{2N}^{\langle k\cdot r\rangle_{2N}} - i\cdot S_{2N}^{\langle k\cdot r\rangle_{2N}},$$

$$\hat{X}_{2N} \leftarrow W_{2N,2N}\cdot X_{2N} = (C_{2N,2N} - i\cdot S_{2N,2N})\cdot X_{2N}. \tag{5}$$

Оскільки $X_{2N}$ має $N$ старших нулів, операції множення на елементи з індексами більше $N-1$ дають нулі. Тому можна записати

$$\hat{X}_{2N} \leftarrow W_{2N,N+1}\cdot X_{N+1} = (C_{2N,N+1} - i\cdot S_{2N,N+1})\cdot X_{N+1},$$

де $X_{N+1}$ отримано з $N+1$ перших елементів $X_{2N}$ (хоча достатньо взяти $N$ перших елементів, використовуємо $N+1$ для того, щоб зберегти розміри для ДКП та ДСП). Матриці меншого розміру $W_{2N,N+1}$, $C_{2N,N+1}$, $S_{2N,N+1}$ отримано з матриць $W_{2N,2N}$, $C_{2N,2N}$, $S_{2N,2N}$.

ДПФ дійсного сигналу відповідає властивостям (2):

$$\hat{X}_{2N}(2N-r) \leftarrow \hat{X}^{*}_{N+1}(r),\ r=\overline{1,\ N-1}.$$

З використанням цього виразу матриці можна додатково зменшити до розмірів $N+1$ на $N+1$ до $W_{N+1,N+1}$, $C_{N+1,N+1}$, $S_{N+1,N+1}$.

Лему доведено.

**Лема 7.** Обчислення ОДПФ сигналу $\hat{X}_{2N}$ розрядністю $2N$, який відповідає властивостям (2), для знаходження дійсного сигналу $X_{2N}$ можна виконати у такий спосіб:

$$M\hat{X}_{N+1}(r) \leftarrow \hat{X}_{N+1}(0) + (-1)^{r}\cdot X_{N+1}(N),\ \hat{X}_{N+1}(r) \leftarrow \hat{X}_{2N}(r),\ r=\overline{0,\ N};$$

$$RX_{N+1} \leftarrow (2C_{N+1,N+1} - M\hat{X}_{N+1})\cdot \operatorname{Re}\hat{X}_{N+1},$$

$$IX_{N+1} \leftarrow i\cdot 2S_{N+1,N+1}\cdot \operatorname{Im}\hat{X}^{*}_{N+1};$$

$$X_{2N}(r) \leftarrow RX_{N+1}(r) - i\cdot IX_{N+1}(r),\ r=\overline{0,\ N};$$

$$\hat{X}_{2N}(2N-r) \leftarrow RX_{N+1}(r) + i\cdot IX_{N+1}(r),\ r=\overline{1,\ N-1},$$

де $C_{2N}^{\langle k\cdot r\rangle_{2N}} = \cos\left(\frac{k\cdot r\cdot\pi}{2N}\right)$, $S_{2N}^{\langle k\cdot r\rangle_{2N}} = \sin\left(\frac{k\cdot r\cdot\pi}{2N}\right)$, $k, r=\overline{0,\ N}$, є елементами матриць $C_{N+1,\,N+1}$ та $S_{N+1,\,N+1}$.

**Доведення.** Виходячи з (5), ОДПФ можна обчислити у такий спосіб:

$$X_{2N} \leftarrow W_{2N,2N}\cdot \hat{X}^{*}_{2N} = (C_{2N,2N} - i\cdot S_{2N,2N})\cdot \hat{X}^{*}_{2N}, \tag{6}$$

де $C_{2N}^{\langle k\cdot r\rangle_{2N}} = \cos\left(\frac{k\cdot r\cdot\pi}{2N}\right)$, $S_{2N}^{\langle k\cdot r\rangle_{2N}} = \sin\left(\frac{k\cdot r\cdot\pi}{2N}\right)$, $k, r=\overline{0,\ N}$, є елементами матриць $C_{2N,2N}$ та $S_{2N,2N}$.

Представимо (6) у такому вигляді:

$$X_{2N} \leftarrow (C_{2N,\,2N} - i \cdot S_{2N,\,2N}) \cdot \operatorname{Re} \hat{X}^{*}_{2N} + i \cdot (C_{2N,2N} - i \cdot S_{2N,2N}) \cdot \operatorname{Im} \hat{X}^{*}_{2N}. \quad (7)$$

Зрозуміло, що $\hat{X}^{*}_{2N}$ відповідає властивостям (2). Покажемо, що $X_{2N}$ також відповідає властивостям (2). Для цього треба з'ясувати, що кожен рядок матриці $W_{2N,2N}$ відповідає властивостям (2):

$$W_{2N,2N}(k, 2N - r) = W_{2N}^{\langle k \cdot (2N - r) \rangle_{2N}} = W_{2N}^{\langle -k \cdot r \rangle_{2N}} = W^{*}_{2N,2N}(k, r), \; r = \overline{1,\, N-1},$$

$$W_{2N,2N}(k,\, N) = W_{2N}^{\langle k \cdot N \rangle_{2N}} = e^{-\frac{2\pi \cdot i}{2N} \cdot k \cdot N} = e^{-\pi \cdot k \cdot i} =$$

$$= \cos(-\pi \cdot k) + i \sin(-\pi \cdot k) = \cos(-\pi \cdot k) = (-1)^{k},$$

$$W_{2N,2N}(k, 0) = 1.$$

Аналогічно можна дослідити рядки матриць $C_{2N,2N}$ та $S_{2N,2N}$:

$$C_{2N,2N}(k, 2N - r) = \cos\left(\frac{k \cdot (2N - r) \cdot \pi}{2N}\right) = \cos\left(-\frac{k \cdot r \cdot \pi}{2N}\right) = C_{2N,2N}(k, r),$$

$$S_{2N,2N}(k, 2N - r) = \sin\left(\frac{k \cdot (2N - r) \cdot \pi}{2N}\right) = \sin\left(-\frac{k \cdot r \cdot \pi}{2N}\right) = -S_{2N,2N}(k, r),$$

$$r = \overline{1,\, N-1}.$$

З урахуванням того, що $\operatorname{Im} \hat{X}^{*}_{2N}(0) = \operatorname{Im} \hat{X}_{2N}(N) = 0$, $\operatorname{Re} \hat{X}^{*}_{2N}(r) = \operatorname{Re} \hat{X}_{2N}(r)$, у формулі (7) можна зробити такі перетворення:

$$X_{2N}(k) \leftarrow \sum_{r=0}^{2N-1} (C_{2N,2N}(k, r) - i \cdot S_{2N,2N}(k, r)) \cdot \operatorname{Re} \hat{X}^{*}_{2N}(r) +$$

$$+ i \cdot \sum_{r=0}^{2N-1} (C_{2N,2N}(k, r) - i \cdot S_{2N,2N}(k, r)) \cdot \operatorname{Im} \hat{X}^{*}_{2N}(r) =$$

$$= \operatorname{Re} \hat{X}^{*}_{2N}(0) + \sum_{r=1}^{N-1} (C_{2N,2N}(k, r) - i \cdot S_{2N,2N}(k, r)) \cdot \operatorname{Re} \hat{X}^{*}_{2N}(r) +$$

$$+ (-1)^{k} \cdot \operatorname{Re} \hat{X}^{*}_{2N}(N) + \sum_{r=N+1}^{2N-1} (C_{2N,2N}(k, r) - i \cdot S_{2N,2N}(k, r)) \cdot \operatorname{Re} \hat{X}^{*}_{2N}(r) +$$

$$+ i \cdot \operatorname{Im} \hat{X}^{*}_{2N}(0) + \sum_{r=1}^{N-1} (C_{2N,2N}(k, r) - i \cdot S_{2N,2N}(k, r)) \cdot \operatorname{Im} \hat{X}^{*}_{2N}(r) +$$

$$+ i \cdot (-1)^{k} \cdot \operatorname{Im} \hat{X}^{*}_{2N}(N) + i \cdot \sum_{r=N+1}^{2N-1} (C_{2N,2N}(k, r) - i \cdot S_{2N,2N}(k, r)) \cdot \operatorname{Im} \hat{X}^{*}_{2N}(r) =$$

$$= \operatorname{Re} \hat{X}^{*}_{2N}(0) + \sum_{r=1}^{N-1} (C_{2N,2N}(k, r) - i \cdot S_{2N,2N}(k, r)) \cdot \operatorname{Re} \hat{X}^{*}_{2N}(r) +$$

$$+ (-1)^{k} \cdot \operatorname{Re} \hat{X}^{*}_{2N}(N) + \sum_{r=1}^{N-1} \begin{pmatrix} C_{2N,2N}(k, 2N - r) - \\ -i \cdot S_{2N,2N}(k, 2N - r) \end{pmatrix} \cdot \operatorname{Re} \hat{X}^{*}_{2N}(2N - r) +$$

$$+ i \cdot \sum_{r=1}^{N-1} (C_{2N,2N}(k, r) - i \cdot S_{2N,2N}(k, r)) \cdot \operatorname{Im} \hat{X}^{*}_{2N}(r) +$$

$$+i\cdot\sum_{r=1}^{N-1}\begin{pmatrix}C_{2N,2N}(k,2N-r)-\\-i\cdot S_{2N,2N}(k,2N-r)\end{pmatrix}\cdot\operatorname{Im}\hat{X}^{*}_{2N}(2N-r)=$$

$$=\operatorname{Re}\hat{X}^{*}_{2N}(0)+\sum_{r=1}^{N-1}(C_{2N,2N}(k,r)-i\cdot S_{2N,2N}(k,r))\cdot\operatorname{Re}\hat{X}^{*}_{2N}(r)+$$

$$+(-1)^{k}\cdot\operatorname{Re}\hat{X}^{*}_{2N}(N)+\sum_{r=1}^{N-1}(C_{2N,2N}(k,r)+i\cdot S_{2N,2N}(k,r))\cdot\operatorname{Re}\hat{X}^{*}_{2N}(r)+$$

$$+i\cdot\sum_{r=1}^{N-1}(C_{2N,2N}(k,r)-i\cdot S_{2N,2N}(k,r))\cdot\operatorname{Im}\hat{X}^{*}_{2N}(r)+$$

$$+i\cdot\sum_{r=1}^{N-1}(C_{2N,2N}(k,r)+i\cdot S_{2N,2N}(k,r))\cdot(-\operatorname{Im}\hat{X}^{*}_{2N}(r))=$$

$$=\operatorname{Re}\hat{X}^{*}_{2N}(0)+2\sum_{r=1}^{N-1}C_{2N,2N}(k,r)\cdot\operatorname{Re}\hat{X}^{*}_{2N}(r)+(-1)^{k}\cdot\operatorname{Re}\hat{X}^{*}_{2N}(N)+$$

$$+i\cdot 2\sum_{r=1}^{N-1}(i\cdot S_{2N,2N}(k,r))\cdot(-\operatorname{Im}\hat{X}^{*}_{2N}(r)),\ k=\overline{0,2N-1}.$$

Взявши до уваги те, що $S_{2N,2N}(k,r)=0$, за умови, що $k$ або $r$ дорівнюють 0 або $N$, та дотримуючись розрядності $N+1$ для ДКП та ДСП, попередній вираз можна записати так:

$$X_{2N}(k)\leftarrow 2\sum_{r=0}^{N}C_{2N,2N}(k,r)\cdot\operatorname{Re}\hat{X}_{2N}(r)-\operatorname{Re}\hat{X}_{2N}(0)-(-1)^{k}\cdot\operatorname{Re}\hat{X}_{2N}(N)-$$

$$-i\cdot 2\sum_{r=0}^{N}(i\cdot S_{2N,2N}(k,r))\cdot\operatorname{Im}\hat{X}^{*}_{2N}(r),\ k=\overline{0,2N-1}.$$

У результаті обчислення перших $N+1$ елементів $X_{2N}$ маємо, що значення під знаком суми відповідають ДКП та ДСП розрядності $N+1$:

$$MX_{2N}(k)\leftarrow\operatorname{Re}\hat{X}_{2N}(0)+(-1)^{k}\cdot\operatorname{Re}\hat{X}_{2N}(N),$$

$$X_{2N}(k)\leftarrow 2\sum_{r=0}^{N}C_{2N,2N}(k,r)\cdot\operatorname{Re}\hat{X}_{2N}(r)-MX_{2N}(k)-$$

$$-i\cdot 2\sum_{r=0}^{N}(i\cdot S_{2N,2N}(k,r))\cdot\operatorname{Im}\hat{X}^{*}_{2N}(r),\ k=\overline{0,N}.$$

Решту елементів $k=\overline{N+1,2N-1}$ можна обчислити, виходячи з того, що $X_{2N}$ відповідає властивостям (2).

Лему доведено.

### МНОЖЕННЯ ДВОХ $N$-РОЗРЯДНИХ ЧИСЕЛ НА ОСНОВІ ДКП ТА ДСП РОЗРЯДНІСТЮ $N/2+1$

На основі лем 5 та 6 нижче наведено алгоритм, який дає змогу виконувати обчислення з використанням ДКП та ДСП розрядності $N/2+1$, що вдвічі менше порівняно з [21].

**Алгоритм 4.** Множення двох $N$-розрядних чисел на основі ДКП та ДСП розрядністю $N/2+1$.

**Вхід:** числа $X_N=\sum_{r=0}^{N-1}x_r\cdot 2^{r\omega}$, $Y_N=\sum_{r=0}^{N-1}y_r\cdot 2^{r\omega}$, де $\omega$ — довжина машинного слова у бітах.

**Результат:** $Z_{2N} = \sum_{r=0}^{2N-1} z_r \cdot 2^{r\omega}$.

**Крок 1**. Ініціалізація та додавання старших нулів:

$$X_{2N}(r) \leftarrow X_N(r),\ Y_{2N}(r) \leftarrow Y_N(r),$$
$$X_{2N}(N+r) \leftarrow Y_{2N}(N+r) \leftarrow 0,\ r = \overline{0,\ N-1}.$$

**Крок 2.** Обчислення парних та непарних елементів:

$$EX_N \leftarrow E(X_{2N}),\ EY_N \leftarrow E(Y_{2N}),$$
$$DX_N \leftarrow O(X_{2N}),\ DY_N \leftarrow O(Y_{2N}),$$

де результатом виконання оператора $E$ (even) є парні елементи, а оператора $O$ (odd) — непарні.

$$EX_{N/2+1}(r) \leftarrow EX_N(r),\ EY_{N/2+1}(r) \leftarrow EY_N(r),$$
$$DX_{N/2+1}(r) \leftarrow DX_N(r),\ DY_{N/2+1}(r) \leftarrow DY_N(r),$$
$$r = \overline{0,\ N/2}.$$

**Крок 3.** Обчислення ДПФ парних та непарних елементів чисел $EX_{N/2+1}$, $EY_{N/2+1}$, $DX_{N/2+1}$, $DY_{N/2+1}$:

$$E\hat{X}_{N/2+1} \leftarrow (C_{N/2+1,N/2+1} - i \cdot S_{N/2+1,N/2+1}) \cdot EX_{N/2+1},$$
$$E\hat{Y}_{N/2+1} \leftarrow (C_{N/2+1,N/2+1} - i \cdot S_{N/2+1,N/2+1}) \cdot EY_{N/2+1},$$
$$D\hat{X}_{N/2+1} \leftarrow (C_{N/2+1,N/2+1} - i \cdot S_{N/2+1,N/2+1}) \cdot DX_{N/2+1},$$
$$D\hat{Y}_{N/2+1} \leftarrow (C_{N/2+1,N/2+1} - i \cdot S_{N/2+1,N/2+1}) \cdot DX_{N/2+1},$$

де $C_N^{\langle k \cdot r \rangle_N} = \cos\left(\frac{k \cdot r \cdot \pi}{N}\right)$, $S_N^{\langle k \cdot r \rangle_N} = \sin\left(\frac{k \cdot r \cdot \pi}{N}\right)$, $k, r = \overline{0,\ N/2}$, є елементами матриць $C_{N/2+1,\,N/2+1}$ та $S_{N/2+1,\,N/2+1}$.

**Крок 4.** Обчислення чисел, необхідних для ОДПФ:

$$E\hat{X}_N(r) \leftarrow E\hat{X}_{N/2+1}(r),\ E\hat{Y}_N(r) \leftarrow E\hat{Y}_{N/2+1}(r),$$
$$D\hat{X}_N(r) \leftarrow D\hat{X}_{N/2+1}(r),\ D\hat{Y}_N(r) \leftarrow D\hat{Y}_{N/2+1}(r),$$
$$r = \overline{0,\ N/2}.$$
$$E\hat{X}_N(N-r) \leftarrow E\hat{X}^*_{N/2+1}(r),\ E\hat{Y}_N(N-r) \leftarrow E\hat{Y}^*_{N/2+1}(r),$$
$$D\hat{X}_N(N-r) \leftarrow D\hat{X}^*_{N/2+1}(r),\ D\hat{Y}_N(N-r) \leftarrow D\hat{Y}^*_{N/2+1}(r),$$
$$r = \overline{1,\ N/2-1}.$$
$$SW_N(r) = W_{2N}^r,\ r = \overline{0,\ N-1}.$$
$$S\hat{D}_N \leftarrow (E\hat{X}_N - SW_N \cdot D\hat{X}_N) \cdot (E\hat{Y}_N - SW_N \cdot D\hat{Y}_N),$$
$$A\hat{D}_N \leftarrow (E\hat{X}_N + SW_N \cdot D\hat{X}_N) \cdot (E\hat{Y}_N + SW_N \cdot D\hat{Y}_N).$$
$$\hat{A}_N \leftarrow \frac{1}{2}(A\hat{D}_N + S\hat{D}_N),$$
$$\hat{S}_N \leftarrow \frac{1}{2} \cdot SW_N^* \cdot (A\hat{D}_N - S\hat{D}_N),$$

де елементи вектор-стовпця $SW_N^*$ є комплексно-спряженим до відповідних елементів вектор-стовпця $SW_N$.

$$\hat{A}_{N/2+1}(r) \leftarrow \hat{A}_N(r),\ \hat{S}_{N/2+1}(r) \leftarrow \hat{S}_N(r),\ r = \overline{0,\ N/2}.$$

**Крок 5.** Обчислення ОДПФ та результату:

$$M\hat{A}_{N/2+1}(r) = \hat{A}_{N/2+1}(0) + (-1)^r \cdot \hat{A}_{N+1}(N/2),\ r = \overline{0,\ N/2};$$

$$M\hat{S}_{N/2+1}(r) = \hat{S}_{N/2+1}(0) + (-1)^r \cdot \hat{S}_{N+1}(N/2),\ r = \overline{0,\ N/2};$$

$$RA_{N/2+1} \leftarrow (2C_{N/2+1,N/2+1} - M\hat{A}_{N/2+1}) \cdot \operatorname{Re} \hat{A}_{N/2+1},$$
$$RS_{N/2+1} \leftarrow (2C_{N/2+1,N/2+1} - M\hat{S}_{N/2+1}) \cdot \operatorname{Re} \hat{S}_{N/2+1},$$

$$IA_{N/2+1} \leftarrow i \cdot 2S_{N/2+1,N/2+1} \cdot \operatorname{Im} \hat{A}^*_{N/2+1},$$

$$IS_{N/2+1} \leftarrow i \cdot 2S_{N/2+1,N/2+1} \cdot \operatorname{Im} \hat{S}^*_{N/2+1};$$

$$A_N(r) \leftarrow RA_{N/2+1}(r) - i \cdot IA_{N/2+1}(r),\ r = \overline{0,\ N/2};$$

$$S_N(r) \leftarrow RS_{N/2+1}(r) - i \cdot IS_{N/2+1}(r),\ r = \overline{0,\ N/2};$$

$$A_N(N-r) \leftarrow RA_{N/2+1}(r) + i \cdot IA_{N/2+1}(r),\ r = \overline{1,\ N/2-1};$$

$$S_N(N-r) \leftarrow RS_{N/2+1}(r) + i \cdot IS_{N/2+1}(r),\ r = \overline{1,\ N/2-1};$$

$$Z_N \leftarrow \frac{1}{N}(A_N + i \cdot S_N).$$

$$E(Z_{2N}) \leftarrow [\operatorname{Re} Z_N],\ O(Z_{2N}) \leftarrow [\operatorname{Im} Z_N],$$

де $[\operatorname{Re} Z_N(r)]$, $[\operatorname{Im} Z_N(r)]$ — заокруглення до найближчого цілого дійсної та уявної частин $Z_N(r)$ відповідно.

**Теорема 1.** У послідовній моделі коефіцієнт прискорення обчислень ДПФ та ОДПФ на основі ДКП та ДСП за алгоритмом 4 порівняно з алгоритмом 2 можна виразити такою формулою:

$$k_{\text{послідовна}}(N) = 1 - \frac{1}{\log_2 N},$$

де $N$ — розрядність багаторозрядного числа.

**Доведення.** У реалізації операції множення двох $N$-розрядних чисел обчислення ДПФ та ОДПФ розрядністю $N$ згідно з [21] можна виконати на основі ДКП та ДСП розрядністю $N+1$. Загалом алгоритм 2 потребує обчислення трьох ДКП та трьох ДСП розрядністю $N+1$. Алгоритм 4 потребує загалом обчислення 12 ДКП та ДСП розрядністю $N/2+1$. Будемо вважати, що операції додавання (віднімання) та множення виконуються за однаковий час на сучасних комп'ютерах. Основою цього припущення є те, що сучасні процесори мають блоки прогнозування та паралельного виконання, а також те, що під час обчислення дискретного перетворення операції додавання (віднімання) та множення виконуються, змінюючи один одного, по черзі. Для обчислення складності дискретних перетворень в алгоритмі скористаємося таким виразом:

$$O(N) = D_N \cdot K \cdot N \cdot \log_2 N + D_N \cdot C_N,$$

де $D_N$ — загальна кількість ДКП та ДСП, $K$ — коефіцієнт для об'єднання операцій додавання (віднімання) та множення, $N$ — розрядність багаторозр-

рядного числа. Хоча розрядність ДКП та ДСП є більшою на одиницю, тобто становить $N+1$ та $N/2+1$ відповідно, вважаємо, що $N$ є дуже великим і неврахування одиниці не впливає на результат.

Використовуючи попередній вираз, коефіцієнт прискорення можна обчислити у такий спосіб:

$$k(N)=\frac{D_{N/2}\cdot K\cdot(N/2)\cdot\log_2 N/2+D_{N/2}\cdot C_{N/2}}{D_N\cdot K\cdot N\cdot\log_2 N+D_N\cdot C_N}, \qquad (8)$$

де $D_N$, $D_{N/2}$ — загальна кількість ДКП та ДСП розрядності $N+1$ та $N/2+1$, $C_N$, $C_{N/2}$ — константи в обчисленні ДКП та ДСП розрядностей $N+1$ та $N/2+1$.

Після підстановки значень отримаємо

$$k(N)=\frac{12\cdot K\cdot(N/2)\cdot\log_2 N/2+12\cdot C_{N/2}}{6\cdot K\cdot N\cdot\log_2 N+6\cdot C_N}=\frac{K\cdot N\cdot\log_2 N/2+2\cdot C_{N/2}}{K\cdot N\cdot\log_2 N+C_N}=$$

$$=\frac{K\cdot N\cdot\log_2 N+C_{N/2}+C_{N/2}-K\cdot N}{K\cdot N\cdot\log_2 N+C_N}=1+\frac{C_{N/2}-K\cdot N}{K\cdot N\cdot\log_2 N+C_N}.$$

Якщо вважати, що $C_{N/2}<<K\cdot N$ та $C_N<<K\cdot N$, то остаточно одержимо $k(N)=1-(1/\log_2 N)$.

Теорему доведено.

Для отримання достатньої стійкості криптографічних ключів використовують числа у діапазоні від 4000 до 8000. Для довжини машинного слова у 32 біти отримуємо діапазони $N$ від 128 до 256 розрядів. Відповідно до теореми 1 прискорення становитиме приблизно від 12.5% до 14.3%. У разі використання 64-бітної розрядності прискорення буде вдвічі ефективніше.

**Теорема 2.** У паралельній моделі коефіцієнт прискорення обчислень ДПФ та ОДПФ на основі ДКП та ДСП за алгоритмом 4 порівняно з алгоритмом 2 можна виразити такою формулою:

$$k_{\text{паралельна}}(N)=1/2-1/(2\log_2 N),$$

де $N$ — розрядність багаторозрядного числа.

**Доведення.** Розглянемо прискорення у випадку, коли для обчислення одного ДКП (або ДСП) виділено один паралельний процесор. Це дає можливість проаналізувати, наскільки швидше можна провести обчислення більшої кількості ДКП (або ДСП) меншого розміру. Порівняння для великої або необмеженої кількості процесорів не розглянуто, оскільки збільшення кількості задіяних процесорів призводить до збільшення кількості блокувань між процесорами, що зумовлює зростання накладних витрат і потребує додаткового врахування під час порівняння.

Використаємо (8) та врахуємо, що $D_{N/2}=D_N=1$. Вважаючи, що $C_{N/2}<<K\cdot N$ та $C_N<<K\cdot N$, отримуємо такий вираз:

$$k(N)=\frac{\log_2 N/2}{2\log_2 N}=\frac{\log_2 N-1}{2\log_2 N}=\frac{1}{2}-\frac{1}{2\log_2 N}.$$

Теорему доведено.

### ПРИКЛАД ОБЧИСЛЕННЯ НА ОСНОВІ АЛГОРИТМУ 4

Покажемо роботу алгоритму 4 на прикладі множення 8-розрядних чисел $11111112\cdot11111112=123\ 456\ 809\ 876\ 544$, які можна представити у вигляді

вектор-стовпців $X_8 = Y_8 = [2\,1111111]^T$. Щоб полегшити сприйняття, виконуємо множення однакових чисел.

$$X_{16} = Y_{16} = [2111111100000\ 000]^T,\ q = 1/\sqrt{2},$$

$$EX_8 = EY_8 = [21110000]^T,\ DX_8 = DY_8 = [11110000]^T,$$

$$EX_5 = EY_5 = [21110]^T,\ DX_5 = DY_5 = [11110]^T,$$

$$C_{5,5} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & q & 0 & -q & -1 \\ 1 & 0 & -1 & 0 & 1 \\ 1 & -q & 0 & q & -1 \\ 1 & -1 & 1 & -1 & 1 \end{bmatrix},\ S_{5,5} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & q & 1 & q & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & q & -1 & q & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$E\hat{X}_5 = E\hat{Y}_5 = (C_{5,5} - i \cdot S_{5,5}) \cdot EX_5 = \begin{bmatrix} 5 \\ 2 - i2.4142 \\ 1 \\ 2 - i0.4142 \\ 1 \end{bmatrix},\quad D\hat{X}_5 = D\hat{Y}_5 = (C_{5,5} - i \cdot S_{5,5}) \cdot DX_5 = \begin{bmatrix} 4 \\ 1 - i2.4142 \\ 0 \\ 1 - i0.4142 \\ 0 \end{bmatrix},$$

$$E\hat{X}_8 = E\hat{Y}_8 = \begin{bmatrix} 5 \\ 2 - i2.4142 \\ 1 \\ 2 - i0.4142 \\ 1 \\ 2 + i0.4142 \\ 1 \\ 2 + i2.4142 \end{bmatrix},\quad D\hat{X}_8 = D\hat{Y}_8 = \begin{bmatrix} 4 \\ 1 - i2.4142 \\ 0 \\ 1 - i0.4142 \\ 0 \\ 1 + i0.4142 \\ 1 \\ 1 + i2.4142 \end{bmatrix},\quad SW_8 = \begin{bmatrix} 1 \\ 0.9239 - i0.3827 \\ 0.7071 - i0.7071 \\ 0.3827 - i0.9239 \\ -i \\ -0.3827 - i0.9239 \\ -0.7071 - i0.7071 \\ -0.9239 - i0.3827 \end{bmatrix},\quad SW_8 \cdot D\hat{X}_8 = \begin{bmatrix} 4 \\ -i2.6132 \\ 0 \\ -i1.0824 \\ 0 \\ -i1.0824 \\ 1 \\ -i2.6132 \end{bmatrix},$$

$$E\hat{X}_8 - SW_{8,8} \cdot D\hat{X}_8 = \begin{bmatrix} 1 \\ 2.0000 + i0.1989 \\ 1 \\ 1.9999 + i0.6682 \\ 1 \\ 2.0000 + i1.4966 \\ 1 \\ 1.9998 + i5.0274 \end{bmatrix},\quad E\hat{X}_8 + SW_{8,8} \cdot D\hat{X}_8 = \begin{bmatrix} 9 \\ 1.9999 - i5.0274 \\ 1 \\ 2.0000 - i1.4966 \\ 1 \\ 1.9999 - i0.6682 \\ 1 \\ 2.0000 - i0.1989 \end{bmatrix},$$

$$S\hat{D}_8 = (E\hat{X}_8 - SW_{8,8} \cdot D\hat{X}_8) \cdot (E\hat{Y}_8 - SW_{8,8} \cdot D\hat{Y}_8) = \begin{bmatrix} 1 \\ 3.9605 + i0.7959 \\ 1 \\ 3.5534 + i2.6728 \\ 1 \\ 1.7602 + i5.9865 \\ 1 \\ -21.2746 + i20.1094 \end{bmatrix},$$

$$A\hat{D}_8 = (E\hat{X}_8 + SW_{8,8} \cdot D\hat{X}_8) \cdot (E\hat{Y}_8 + SW_{8,8} \cdot D\hat{Y}_8) = \begin{bmatrix} 81 \\ -21.2746 - i20.1094 \\ 1 \\ 1.7602 - i5.9865 \\ 1 \\ 3.5534 - i2.6728 \\ 1 \\ 3.9605 - i0.7959 \end{bmatrix}.$$

$$\hat{A}_8 = \frac{1}{2}(A\hat{D}_8 + S\hat{D}_8)\ \ \hat{S}_8 = \frac{1}{2}(A\hat{D}_8 - S\hat{D}_8)\cdot SW_8^*$$

$$\begin{bmatrix} 41 \\ -8.6571 - i9.6567 \\ 1 \\ 2.6568 - i1.6568 \\ 1 \\ 2.6568 + i1.6568 \\ 1 \\ -8.6571 + i9.6567 \end{bmatrix} \quad \begin{bmatrix} 40 \\ -7.6571 - i14.4859 \\ 0 \\ 3.6571 - i2.4853 \\ 0 \\ 3.6571 + i2.4853 \\ 0 \\ -7.6571 + i14.4859 \end{bmatrix}$$

$$\begin{matrix} \hat{A}_5 \\ \begin{bmatrix} 41 \\ -8.6571 - i9.6567 \\ 1 \\ 2.6568 - i1.6568 \\ 1 \end{bmatrix} \end{matrix} \quad \begin{matrix} \hat{S}_5 \\ \begin{bmatrix} 40 \\ -7.6571 - i14.4859 \\ 0 \\ 3.6571 - i2.4853 \\ 0 \end{bmatrix} \end{matrix} \quad \begin{matrix} M\hat{A}_5 \\ \begin{bmatrix} 42 \\ 40 \\ 42 \\ 40 \\ 42 \end{bmatrix} \end{matrix} \quad \begin{matrix} M\hat{S}_5 \\ \begin{bmatrix} 40 \\ 40 \\ 40 \\ 40 \\ 40 \end{bmatrix} \end{matrix}$$

$$RA_5 = \mathrm{Re}\,\hat{A}_5 \cdot (2C_{5,5} - M\hat{A}_5)\ \ RS_5 = \mathrm{Re}\,\hat{S}_5 \cdot (2C_{5,5} - M\hat{S}_5)$$

$$\begin{bmatrix} 73.9995 - 42 \\ 63.9999 - 40 \\ 82.0000 - 42 \\ 96.0001 - 40 \\ 98.0005 - 42 \end{bmatrix} = \begin{bmatrix} 31.9995 \\ 23.9999 \\ 40.0000 \\ 56.0001 \\ 56.0005 \end{bmatrix} \quad \begin{bmatrix} 71.9999 - 40 \\ 63.9995 - 40 \\ 80.0000 - 40 \\ 96.0005 - 40 \\ 88.0001 - 40 \end{bmatrix} = \begin{bmatrix} 31.9999 \\ 23.9995 \\ 40.0000 \\ 56.0005 \\ 48.0001 \end{bmatrix}$$

$$IA_5 = i \cdot \mathrm{Im}\,\hat{A}_5^* \cdot 2S_{5,5}\ \ IS_5 = i \cdot \mathrm{Im}\,\hat{S}_5^* \cdot 2S_{5,5}$$

$$\begin{bmatrix} 0 \\ i15.9997 \\ i15.9997 \\ i15.9997 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ i24.0008 \\ i24.0014 \\ i24.0008 \\ 0 \end{bmatrix}$$

$$A_8(r) = RA_5(r) - i \cdot IA_5(r),\ r = \overline{0,4} \quad S_8(r) = RS_5(r) - i \cdot IS_5(r),\ r = \overline{0,4}$$

$$\begin{bmatrix} 31.9995 + 0 \\ 23.9999 + 15.9997 \\ 40.0000 + 15.9997 \\ 56.0001 + 15.9997 \\ 56.0005 \end{bmatrix} = \begin{bmatrix} 31.9995 \\ 39.9996 \\ 55.9998 \\ 71.9998 \\ 56.0005 \end{bmatrix} \quad \begin{bmatrix} 31.9999 + 0 \\ 23.9995 + 24.0008 \\ 40.0000 + 24.0012 \\ 56.0005 + 24.0008 \\ 48.0001 \end{bmatrix} = \begin{bmatrix} 31.9999 \\ 48.0003 \\ 64.0012 \\ 80.0013 \\ 48.0001 \end{bmatrix}$$

$$A_8(r) = \qquad\qquad S_8(N - r) =$$

$$RA_5(r) + i \cdot IA_5(r),\ r = \overline{1,3} \qquad RS_5(r) + i \cdot IS_5(r),\ r = \overline{1,3}$$

$$\begin{bmatrix} 56.0001 - 15.9997 \\ 40.0000 - 15.9997 \\ 23.9999 - 15.9997 \end{bmatrix} = \begin{bmatrix} 40.0005 \\ 24.0002 \\ 8.0003 \end{bmatrix} \quad \begin{bmatrix} 56.0005 - 24.0008 \\ 40.0000 - 24.0014 \\ 23.9995 - 24.0008 \end{bmatrix} = \begin{bmatrix} 31.9998 \\ 15.9988 \\ -0.0012 \end{bmatrix}$$

$$Z_8 = (A_8 + i \cdot S_8)/8 = ,$$

$$\begin{bmatrix} 3.9999 + i3.9999 \\ 4.9999 + i6.0000 \\ 6.9999 + i8.0002 \\ 8.9999 + i10.0002 \\ 7.0001 + i6.0000 \\ 5.0001 + i3.9999 \\ 3.0000 + i1.9998 \\ 1.0000 - i0.0002 \end{bmatrix}$$

$$E(Z_{16}) = \mathrm{Re}\, Z_8 = [4\ \ 5\ \ 7\ \ 9\ \ 7\ \ 5\ \ 3\ \ 1]^T,$$
$$O(Z_{16}) = \mathrm{Im}\, Z_8 = [4\ \ 6\ \ 8\ \ 10\ \ 6\ \ 4\ \ 2\ \ 0]^T,$$

$$Z_{16} = [4\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9\ \ (10-10)\ \ (7+1)\ \ 6\ \ 5\ \ 4\ \ 3\ \ 2\ \ 1\ \ 0]^T =$$

$$= [4\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9\ \ 0\ \ 8\ \ 6\ \ 5\ \ 4\ \ 3\ \ 2\ \ 1\ \ 0]^T.$$

**ВИСНОВКИ**

Запропоновано способи оптимізації методів багаторозрядного множення двох $N$-розрядних чисел на основі дискретного перетворення Фур'є (ДПФ), дисккретного косинусного (ДКП) та синусного перетворень (ДСП). В алгоритмі реалізації множення на основі ДПФ проведено заміну операцій для збереження симетрії у дійсній або уявній частинах багаторозрядних чисел. Розділення обчислення ДПФ дійсного сигналу парної довжини для дійсної частини на основі ДКП та уявної частини на основі ДСП дає змогу перевести обчислення з поля комплексних чисел у поле дійсних чисел та зменшує складність багаторозрядної операції множення за кількістю одноразрядних операцій комплексного множення. Обчислення значень дискретних перетворень у поєднанні зі збереженням симетрії у багаторозрядних числах дає змогу використовувати ДКП та ДСП меншої розрядності $N/2+1$ замість $N+1$. Збільшення вдвічі кількості ДКП та ДСП меншої розрядності дало можливість удвічі зменшити обчислювальну складність, розраховану на один процесор у паралельній моделі. У вигляді теорем надано аналіз коефіцієнтів прискорення у послідовній та паралельній моделях обчислень.

СПИСОК ЛІТЕРАТУРИ


1. Анісімов А.В. Алгоритмічна теорія великих чисел. Модулярна арифметика великих чисел. Київ: Академперіодика, 2001. 153 с.
2. Задірака В., Олексюк О. Комп'ютерна арифметика багаторозрядних чисел. Київ: Наукова думка, 2003. 263 с.
3. Задирака В.К. Теория вычисления преобразования Фурье. Киев: Наукова думка, 1983. 213 с.
4. Задірака В.К., Терещенко А.М. Комп'ютерна арифметика багаторозрядних чисел у послідовній та паралельній моделях обчислень. Київ: Наукова думка, 2021. 136 с.
5. Качко Е.Г. Распараллеливание алгоритмов умножения чисел многократной точности. *Вестник Уфимского государственного авиационного технического университета*. 2011. Е 15, № 5 (45). С. 142–147.
6. Николайчук Я.М., Касянчук М.М., Якименко І.З., Івасьєв С.В. Ефективний метод модулярного множення в теоретико–числовому базисі Радемахера–Крестенсона. *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі*. 2014. № 806. С. 195–199.
7. Хіміч О.М., Сидорук В.А. Використання мішаної розрядності у математичному моделюванні. *Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки*. 2019. Вип. 19. С. 180–187.
8. Карацуба А.А., Офман Ю.П. Умножение многоразрядных чисел на автоматах. ДАН СССР. 1962. Т. 145, № 2. С. 293–294.

9. Cooley J.W., Tukey J.W. An algorithm for the machine calculation of complex Fourier series. *Mathematics of Computation*. 1965. Vol. 19, N 90. P. 297–301.
10. Schonhage A., Strassen V. Schnelle Multiplikation groβen Zahlen. *Computing*. 1971. Vol. 7, Iss. 3–4. P. 281–292.
11. Pitassi D.A. Fast convolution using the Walsh transform. *Proc. 1971 Symp. Applications of Walsh Functions* (13–15 April 1971, Washington, D.C., USA). Washington, D.C., 1971. P. 130–133.
12. Терещенко А.Н., Мельникова С.С., Гнатив Л.А., Задирака В. К., Кошкина Н.В. Реализация операции умножения с использованием преобразования Уолша. *Проблемы управления и информатики*. 2010. № 2. С. 102–126.
13. Montgomery P.L. Modular multiplication without trial division. *Mathematics of Computation*. 1985. Vol. 44, N 170. P. 519–521.
14. Cook S.A. On the minimum computation time of functions. PhD thesis. Harvard University, Department of Mathematics. 1966. URL: http://cr.yp.to/bib/1966/cook.html.
15. Ahmed N., Natarajan T., Rao K.R. Discrete cosine transform. *IEEE Transactions on Computers*. 1974. Vol. C–23, Iss. 1. P. 90–93. http://dx.doi.org/10.1109/T-C.1974.223784.
16. Jain A.K. A fast Karhunen–Loève transform for a class of random processes. *IEEE Transactions on Communications*. 1976. Vol. 24, N 9. P. 1023–1029.
17. Gluth R. Regular FFT–related transform kernels for DCT/DST – based polyphase filter banks. *Proc. IEEE 1991 International Conference on Acoustics, Speech and Signal Processing (ICASSP 1991)* (14–17 April 1991, Toronto, Canada). Toronto, 1991. P. 2205–2208.
18. Чичева М.А. Эффективный алгоритм дискретного косинусного преобразования четной длины. *Компьютерная оптика*. 1998. № 18. С. 147–149.
19. Гнатів Л.О., Луц В.К. Цілочислові модифіковані синус–косинусні перетворення типу VII. Метод побудови і роздільні направлені адаптивні перетворення для intra–прогнозування з блоками яскравості 8x8 у кодуванні зображень/відео. *Кібернетика та системний аналіз*. 2021. Т. 57, № 1. С. 178–190.
20. Терещенко А.М. Оптимізація багаторозрядного множення на основі ШПФ у паралельній моделі обчислень. *Захист інформації.* 2014. Т. 16, № 3. С.178–184.
21. Терещенко А.М., Задирака В.К. Реалізація багаторозрядної операції множення на основі дискретних косинусних та синусних перетворень. *Кібернетика та комп'ютерні технології.* 2021. № 4. С. 61–79.

**V.K. Zadiraka, A.M. Tereshchenko**

**OPTIMIZATION OF MULTIDIGIT MULTIPLICATION BASED ON DISCRETE TRANSFORMS (FURIE, COSINUS, SINUS) IN PARALLEL COMPUTATIONAL MODEL**

**Abstract.** This paper considers the multidigit multiplication operation, on whose speed the speed of asymmetric cryptographic software and hardware depends. Algorithms for implementation of the multiplication of two -digit numbers based on discrete cosine and sine transforms (DCT and DST) are proposed. Due to the use of DCT and DST, the calculations for the real and imaginary parts of the discrete Fourier transform (DFT) of a real even-length signal are separated, which allows translating the complex number calculations to real number calculations. Algorithm operations are replaced to preserve symmetry in real or imaginary parts of multidigit numbers, which allows the use of DCT and DST of lower length $N / 2 + 1$ and increases the possibility of parallelism in the implementation of multidigit multiplication.

**Keywords:** multidigit multiplication, multidigit arithmetic, asymmetric cryptography, discrete cosine transform, discrete sine transform, discrete Fourier transform, fast Fourier calculation algorithm..

*Надійшла до редакції 28.03.2022*