

ОБЩИЕ ЧИСЛЕННЫЕ МЕТОДЫ

УДК 519.113

ОБОБЩЕНИЕ БЫСТРОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ С ПОСТОЯННОЙ СТРУКТУРОЙ

© 2023 г. М. С. Беспалов^{1,*}

¹ 600000 Владимир, ул. Горького, 87, Владимирский гос. ун-т, Российская Федерация

*e-mail: bespalov@vlsu.ru

Поступила в редакцию 09.02.2023 г.
Переработанный вариант 14.03.2023 г.
Принята к публикации 28.04.2023 г.

Широко популярны знаменитые быстрые алгоритмы Кули–Тьюки для дискретного преобразования Фурье составного основания, представленные в двух видах — классическом и с постоянной структурой. В статье предложено матричное представление этих алгоритмов в обозначениях двух видов тензорного произведения матриц: кронекерова произведения и b -произведения. Предложенное матричное представление указывает на идентичность структуры этих алгоритмов с двумя быстрыми алгоритмами Гуда для кронекеровой степени матрицы. Продемонстрирована методика построения матричной формы быстрых алгоритмов для дискретных преобразований: Фурье и Крестенсона с составным основанием, а также Виленкина. Показана предпочтительность использования алгоритма с постоянной структурой в случаях более сложных конструкций. Библ. 13.

Ключевые слова: дискретное преобразование Фурье, дискретное преобразование Уолша, быстрый алгоритм, кронекерово произведение матриц.

DOI: 10.31857/S0044466923080033, **EDN:** WRXNSJ

ВВЕДЕНИЕ

Центральное место в теории алгоритмов цифровой обработки сигналов занимают быстрые алгоритмы Кули и Тьюки [1] для реализации дискретного преобразования Фурье (ДПФ) с составным основанием N . При практическом использовании наиболее популярными среди них служат алгоритмы быстрого преобразования Фурье (БПФ), соответствующие факторизации матриц ДПФ порядка $N = 2^n$. Из них выделяют [2] два основных БПФ с прореживанием по частоте и по времени, которые соответствуют одной и той же факторизации матриц ДПФ. Это объясняется тем, что матрица ДПФ $F = F_N$ симметрична; поэтому ДПФ можно считать для столбцов x , y по формуле $y = F \cdot x$ или для строк x , y по формуле $y = x \cdot F$. При переходе от одной формулы к другой меняется на противоположный порядок выполнения операций.

Другой подход к построению БПФ порядка $N = 2^n$ (с названием БПФ с постоянной структурой) не столь популярен, но более удобен при больших n . В данной статье проводится качественный анализ этих двух алгоритмов БПФ с представлением их в матричном виде. В основе построения первого из них лежит лемма факторизации кронекерова произведения $\otimes$ с добавлением диагональных матриц вращения. Формальное описание второго из них возможно с помощью нового тензорного произведения матриц $\oslash$, свойства которого получены в [3]. Естественно, что невозможно обойтись без сомножителей в виде диагональных матриц вращения и в алгоритме БПФ с постоянной структурой.

Если из каждого из этих двух вариантов факторизации матрицы ДПФ порядка $N = 2^n$ удалим все сомножители в виде диагональных матриц вращения, то получим два алгоритма Гуда [4] факторизации матрицы дискретного преобразования Уолша (ДПУ). Так как диагональные матрицы вращения не оказывают влияния на структуру алгоритма в виде блок-схем, то в качестве вывода получаем

Утверждение 1. *Скелет каждой из двух разновидностей БПФ составляют два алгоритма Гуда для ДПУ.*

Другой прием увеличения порядка матрицы ортогонального преобразования состоит в переходе от ДПФ к дискретному преобразованию Крестенсона (ДПК), матрица которого есть кронекерова степень матрицы ДПФ. При этом переходе возникает задача композиции двух быстрых алгоритмов – внутреннего для ДПФ и внешнего для кронекеровой степени. Внешний алгоритм можно построить по одному из алгоритмов Гуда, где в приоритете опять алгоритм с постоянной структурой. А конструкцию сопряжения этих алгоритмов можно провести с помощью свойств двух тензорных произведений матриц, описанных в [3].

1. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

1.1. В каждом варианте быстрого алгоритма ДПФ присутствует перестановка отсчетов сигнала, встречающаяся под названиями *разрядно-инверсная*, *реверсная* или *идеальная перетасовка*. Будем использовать более короткое название *реверсная* (применяемое в [5]), хотя название *разрядно-инверсная* более информативно. Вариант двоичной реверсной перестановки подробно описан в книге [5].

Рассмотрим общий случай реверсной перестановки относительно системы счисления по смешанному основанию.

Пусть $N = pq$ и $p \neq q$. Числа x от 0 до $N - 1$ представляются в виде $x = bp + a$ или $x = aq + b$, где $a = 0, 1, \dots, p - 1$, $b = 0, 1, \dots, q - 1$. Для представления $x = aq + b$ внутренний цикл по a , а внешний цикл по b приводит к одному реверсному порядку

$$\underbrace{0 \ q \ 2q \ \dots \ (p-1) \ q}_{\text{внутренний цикл}} \underbrace{1 \ q + 1 \ \dots \ (p-1)q + 1}_{\text{внешний цикл}} \dots \underbrace{q-1 \ 2q-1 \ \dots \ pq-1}_{\text{внешний цикл}}, \quad (1)$$

а реверсное прочтение другого представления $x = bp + a$ приводит к другому реверсному порядку того же набора чисел.

Если же $N = pqr$ для различных p, q, r , то получается уже шесть различных реверсных перестановок N чисел в соответствии с перестановкой порядка сомножителей в N .

Поскольку перестановки нам потребуется применять не к числам, а к строкам и столбцам матриц, то предложим описание реверсных перестановок через соответствующую перестановочную матрицу.

1.2. Напомним определения двух разных видов тензорного произведения матриц. Будем обозначать через $M_{n,m}$ множество матриц размера $n \times m$ и через $M_n := M_{n,n}$ множество квадратных матриц порядка n .

Если $A = (a_{kj}) \in M_{n,l}$, $B \in M_{m,s}$, то кронекерово произведение определяется в виде блочной матрицы

$$A \otimes B = (a_{kj} B)_{k,j=0}^{n-1,l-1} \in M_{nm,ls}.$$

Временно обозначим тем же символом с нижним индексом A_k строки матрицы A , а с верхним индексом A^j столбцы матрицы A . Тогда b -произведение $A \in M_{n,l}$ на $B \in M_{m,s}$ определяется в виде блочной матрицы (блок есть поэлементное произведение столбца на строку)

$$A \oslash B = (A^j B_k)_{k,j=0}^{m-1,l-1} \in M_{nm,ls}.$$

Быстрые алгоритмы первого типа ДПФ и ДПУ строятся на основе следующей леммы факторизации (доказательство приведено в [3]).

Лемма 1. *Если $A \in M_{n,l}$, $B \in M_{l,s}$, $C \in M_{m,k}$, $D \in M_{k,t}$, то*

$$\begin{aligned} (A \cdot B) \otimes (C \cdot D) &= (A \otimes C) \cdot (B \otimes D) = (C \oslash A) \cdot (B \oslash D), \\ (A \cdot B) \oslash (C \cdot D) &= (A \oslash C) \cdot (B \otimes D) = (C \otimes A) \cdot (B \oslash D). \end{aligned}$$

Следствие 1. Два вида тензорного произведения матриц связаны через реверсную перестановку строк

$$B \oslash D = (I_l \oslash I_k) \cdot (B \otimes D).$$

Доказывается подстановкой $A = I_l, C = I_k$.

Аналогично в общем случае матрица реверсной перестановки определяется как b -произведение единичных матриц, а в частном случае равных оснований – как b -степень единичной матрицы.

В [6] получено следующее свойство, где I_x – единичная матрица указанного порядка.

Лемма 2. Если $A \in M_m, B \in M_l$, то

$$(A \otimes I_x) \cdot (B \otimes I_{mx}) = (B \otimes A) \otimes I_x.$$

1.3. Матрица ДПУ (уровня n или порядка $N = 2^n$) в нумерации Адамара определяется как кронекерова степень $H_n = H^{\otimes n}$ матрицы

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (2)$$

Матрица ДПУ в нумерации Пэли (уровня n) определяется как b -степень той же матрицы $W_n = H^{\otimes n}$.

Матрица (обратного) ДПФ, которое берем в качестве основного,

$$F_N = \left(\omega_N^{jk} \right)_{j,k=0}^{N-1}, \quad \text{где} \quad \omega_N = \exp \frac{2\pi i}{N}. \quad (3)$$

Прямое ДПФ задается матрицей $\bar{F}_N$ или заменой ω_N на $\bar{\omega}_N = \omega_N^{-1}$ в (3).

Матрица дискретного преобразования Крестенсона (ДПК) определяется как кронекерова степень матрицы (3). Часто рассматривают другой вариант ДПК с матрицей в виде b -степени матрицы ДПФ, на который мы в данной статье отвлекаться не будем.

Строки (столбцы) матрицы (3) в [7], [2] названы дискретными экспоненциальными функциями (ДЭФ). Обозначим основную ДЭФ как вектор

$$\mathbf{r} = r_N = (1 \ \omega \ \omega^2 \ \dots \ \omega^{N-1}).$$

Остальные ДЭФ есть степени по Адамару основной ДЭФ:

$$\mathbf{r}^2 = \mathbf{r} \bullet \mathbf{r} = (1 \ \omega^2 \ \omega^4 \ \dots \ \omega^{2N-2}), \quad \mathbf{r}^3 = \mathbf{r} \bullet \mathbf{r} \bullet \mathbf{r} = (1 \ \omega^3 \ \omega^6 \ \dots \ \omega^{3N-3}), \dots$$

Для фиксированного N все ДЭФ образуют группу порядка N :

$$\mathbf{r}^k \bullet \mathbf{r}^m = \mathbf{r}^{k+m}, \quad \mathbf{r}^N = \mathbf{r}^0 = (1 \ 1 \ \dots \ 1) - \text{нейтральный элемент.}$$

Если N составное, т.е. $N = pq$, то введем понятие *срез дискретной экспоненциальной функции* (СДЭФ) с основным представителем

$$\mathbf{s} = s_{(p,q)} = (1 \ \omega \ \omega^2 \ \dots \ \omega^{q-1}), \quad \text{где} \quad \omega = \omega_N = \exp \frac{2\pi i}{N}.$$

Остальные СДЭФ также являются степенями по Адамару основной СДЭФ:

$$\begin{aligned} \mathbf{s}^0 &= (1 \ 1 \ \dots \ 1), \quad \mathbf{s}^2 = \mathbf{s} \bullet \mathbf{s} = (1 \ \omega^2 \ \omega^4 \ \dots \ \omega^{2q-2}), \quad \mathbf{s}^3 = \mathbf{s} \bullet \mathbf{s} \bullet \mathbf{s}, \dots \\ \dots, \mathbf{s}^{p-2}, \mathbf{s}^{p-1} &= (1 \ \omega^{p-1} \ \omega^{2p-2} \ \dots \ \omega^{(p-1)(q-1)}). \end{aligned}$$

Всего различных СДЭФ p штук. Отсчет с номером 1 служит образующим элементом как для ДЭФ, так и для СДЭФ.

Составим N -мерный вектор всех СДЭФ, определяемый по двум параметрам p, q таким, что

$$N = pq: \quad \mathbf{s}_{p,q} = (\mathbf{s}^0 \ \mathbf{s}^1 \ \mathbf{s}^2 \ \dots \ \mathbf{s}^{p-1}) = \left(\underbrace{1 \ 1 \ \dots \ 1}_p \underbrace{1 \ \omega \ \dots \ \omega^{q-1}}_q \underbrace{1 \ \omega^2 \ \dots \ \omega^{2q-2}}_q \dots \underbrace{1 \ \omega^{p-1} \ \dots \ \omega^{(p-1)(q-1)}}_q \right),$$

который является аналогом сигнала Франка [8].

Если N раскладывается на 3 сомножителя $N = pqr$, то обозначим $N_1 = pq$ и каждый блок в виде среза N_1 -мерного вектора СДЭФ повторим r раз

$$\mathbf{S}_{p,q,r} = \left(\underbrace{\mathbf{s}^0 \dots \mathbf{s}^0}_r \underbrace{\mathbf{s}^1 \dots \mathbf{s}^1}_r \dots \underbrace{\mathbf{s}^{p-1} \dots \mathbf{s}^{p-1}}_r \right). \quad (4)$$

2. БЫСТРЫЕ АЛГОРИТМЫ ОРТОГОНАЛЬНЫХ ПРЕОБРАЗОВАНИЙ

2.1. К быстрым алгоритмам для ортогональных преобразований в 1958 г. обратился Гуд, предложивший в [4] два варианта факторизации кронекеровой степени матрицы. Он отметил, что первый из алгоритмов есть следствие леммы факторизации кронекерова произведения. А второй алгоритм как раз и является алгоритмом с постоянной структурой, так как на каждом шаге не меняется вид матрицы сомножителя. Приведем эти алгоритмы в матричном виде применительно к ДПК.

Утверждение 2 (первый алгоритм Гуда). *Матрицу ДПК можно факторизовать в виде произведения слабозаполненных матриц*

$$F_p^{\otimes n} = T_n \cdot T_{n-1} \cdot \dots \cdot T_1, \quad \text{где} \quad T_j = E^{\otimes n-j} \otimes F_p \otimes E^{\otimes j-1},$$

E — единичная матрица p -го порядка. Причем матрицы T_j допускают любую перестановку сомножителей.

Алгоритм с постоянной структурой, выделенный Гудом как основной результат статьи [4], приведем в форме, полученной в [6].

Утверждение 3 (второй алгоритм Гуда). *Матрицу ДПК можно представить в виде степени слабозаполненной матрицы*

$$F_p^{\otimes n} = \left(F_p \otimes I_{p^{n-1}} \right)^n.$$

Замечание. В случае $p = 2$ в представленных алгоритмах приведены быстрые алгоритмы для ДПУ-Адамара, где $F_2 = H$ из (2).

Другой подход к этим алгоритмам, с построением соответствующих базисов, предложен в статьях [9], [10], а матричный вид первого алгоритма в [11].

Введем для случая порядка матрицы $N = pqr$ диагональные матрицы вращений $D_{p,q,r}$ с вектором $\mathbf{S}_{p,q,r}$ из (4) на диагонали: p групп по q элементов в группе с r повторами.

В частности,

$$D_{2,2^{j-1},1} = \text{diag} \left(\underbrace{1, 1, \dots, 1}_{2^{j-1}}, \omega^0, \omega^1, \dots, \omega^{2^{j-1}-1} \right)$$

для меняющихся порядков матриц $N_j = 2^j = pq$ с соответствующим $\omega = \omega_{pq} = \omega_{2^j}$. Это обозначение плюс запись матрицы реверсной перестановки в виде b -степени позволяют получить следующий (уточняющий предложенный в [12], [13]) матричный вариант алгоритма Кули-Тьюки для ДПФ порядка $N = p^n$.

Утверждение 4 (основной случай алгоритма Кули-Тьюки). *Пусть $N = p^n$. Допускается факторизация*

$$F_N = R_n \cdot R_{n-1} \cdot \dots \cdot R_1 \cdot L,$$

где $R_j = E^{\otimes n-j} \otimes ((F_p \otimes E^{\otimes j-1}) \cdot D_{p,p^{j-1},1})$ при $j > 1$, $R_1 = E^{\otimes n-1} \otimes F_p$, E — единичная матрица p -го порядка, $L = E^{\otimes n}$ — матрица реверсной перестановки.

Так как повторы здесь внешние, а не внутренние, то для их записи применен прием с помощью левого кронекерова произведения.

Утверждение 5 (алгоритм Кули-Тьюки с постоянной структурой). Пусть $N = p^n$. Допускается факторизация

$$F_N = L \cdot T \cdot D_{p,p,p^{n-2}} \cdot T \cdot D_{p^2,p,p^{n-3}} \cdot T \cdot D_{p^3,p,p^{n-4}} \cdot \dots \cdot T \cdot D_{p^{n-1},p,1} \cdot T,$$

где $T = F_p \otimes I_{p^{n-1}}$, $L = E^{\otimes n}$, E — единичная p -го порядка.

Вывод. Скелет стандартных видов алгоритма Кули-Тьюки составляют первый и второй алгоритмы Гуда. Добавлением к алгоритмам Гуда множителя в виде матрицы реверсной перестановки $L = E^{\otimes n}$ в начало алгоритма (умножение справа) для первого или в конец алгоритма (умножение слева) для второго алгоритма Гуда превращает алгоритм ДПУ-Адамара в алгоритм ДПУ-Пэли. Следующее добавление между каждой парой сомножителей алгоритма Гуда специально подобранных диагональных матриц вращений приводит к факторизации матрицы ДПФ порядка $N = p^n$.

Число сложений (вычитаний) в каждом из этих четырех алгоритмов одинаковое и равно $N \log_p N$. Для ДПУ это сложения действительных чисел, а для ДПФ комплексные сложения. Умножений для ДПУ нет. Для ДПФ число умножений вычисляется по числу комплексных множителей в диагональных матрицах вращений.

2.2. Наибольший практический интерес представляют случаи $p = 3$, как простейший модельный случай, и $p = 4$, как оптимальный по числу операций вариант основного случая $N = 2^n$. Замечание про случай $p = 4$ проиллюстрируем примерами.

Для вычисления $y = F_{16} \cdot x$ предложим две факторизации с постоянной структурой по утверждению 5. Первая факторизация

$$F_{16} = E^{\otimes 4} \cdot T \cdot D_{2,2,4} \cdot T \cdot D_{4,2,2} \cdot T \cdot D_{8,2,1} \cdot T,$$

где $T = H \otimes I_8$, $E = I_2$. Вторая факторизация

$$F_{16} = (I_4 \otimes I_4) \cdot (F_4 \otimes I_4) \cdot D_{4,4,1} \cdot (F_4 \otimes I_4)$$

дополняется факторизацией $F_4 = (H \otimes E) \cdot D_{2,2,1} \cdot (H \otimes E)$. Далее удобнее воспользоваться приемами параллельных вычислений, представив входной столбец $x \in \mathbb{C}^{16}$ в виде блочного столбца

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \text{ с элементами } a, b, c, d \in \mathbb{C}^4. \text{ Как первый шаг } (H \otimes E) \cdot \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a+c \\ a-c \\ b+d \\ b-d \end{pmatrix}, \text{ так и второй (после}$$

$$\text{умножения на i) шаг } (H \otimes E) \cdot \begin{pmatrix} a+c \\ a-c \\ b+d \\ i(b-d) \end{pmatrix} = \begin{pmatrix} a+b+c+d \\ a+ib-c-id \\ a-b+c-d \\ a-ib-c+id \end{pmatrix} \text{ состоит из 16 комплексных слагаемых}$$

(12 сложений). Умножение на числа i и $-i$ выполняется в виде перестановки элементов с изменением одного знака, что операцией не считается.

Из этих двух вариантов при первом варианте факторизации имеем 10 умножений: 4 в матрице $D_{4,2,2} = \text{diag}(1 \ 1 \ 1 \ 1 \ u \ 1 \ u \ 1 \ i \ 1 \ i \ 1 \ u^3 \ 1 \ u^3)$, где $u = \omega_8$, и 6 в матрице $D_{8,2,1} = \text{diag}(1 \ 1 \ 1 \ \omega \ 1 \ \omega^2 \ 1 \ \omega^3 \ 1 \ i \ 1 \ \omega^5 \ 1 \ \omega^6 \ 1 \ \omega^7)$, где $\omega = \omega_{16}$.

При втором варианте факторизации имеем 8 умножений ($\omega = \omega_{16}$): $D_{4,4,1} = \text{diag}(1 \ 1 \ 1 \ 1 \ 1 \ \omega \ \omega^2 \ \omega^3 \ 1 \ \omega^2 \ i \ \omega^6 \ 1 \ \omega^3 \ \omega^6 \ \omega^9)$.

3. ОСНОВНЫЕ ТЕОРЕМЫ О БЫСТРЫХ АЛГОРИТМАХ

Доказательство сформулированных выше утверждений 4 и 5, в которых приведены наиболее удобные и чаще применяемые БПФ, вытекает из следующего общего случая ДПФ с произвольным составным основанием $N = pqr$. Далее покажем переход к основанию $N = pqrs$.

Пусть $N = pqr$. Назовем *матрицей дискретного преобразования* Виленкина (ДПВ) кронекеро-произведение матриц ДПФ $F = F_p \otimes F_q \otimes F_r$.

Теорема 1. Данное ДПВ допускает факторизации Гуда

- 1) $F_p \otimes F_q \otimes F_r = (F_p \otimes I_q \otimes I_r) \cdot (I_p \otimes F_q \otimes I_r) \cdot (I_p \otimes I_q \otimes F_r),$
- 2) $F_p \otimes F_q \otimes F_r = (F_r \otimes I_{pq}) \cdot (F_q \otimes I_{pr}) \cdot (F_p \otimes I_{qr}).$

Доказательство. По лемме 1 получаем известную первую формулу

$$\begin{aligned} F_p \otimes F_q &= (F_p \cdot I_p) \otimes (I_q \cdot F_q) = (F_p \otimes I_q) \cdot (I_p \otimes F_q). \\ F &= ((F_p \otimes F_q) \cdot I_{pq}) \otimes (I_r \cdot F_r) = (((F_p \otimes I_q) \cdot (I_p \otimes F_q)) \otimes I_r) \cdot (I_{pq} \otimes F_r) = \\ &= (F_p \otimes I_q \otimes I_r) \cdot (I_p \otimes F_q \otimes I_r) \cdot (I_{pq} \otimes F_r). \end{aligned}$$

Для второй формулы по лемме 2 имеем

$$(F_p \otimes F_q) \otimes I_r = (F_q \otimes I_{pr}) \cdot (F_p \otimes I_{qr}),$$

при обозначении $B = F_p \otimes F_q \in M_{pq}$ по лемме 1 и этой формуле получим

$$F = B \otimes F_r = (F_r \otimes I_{pq}) \cdot (B \otimes I_r) = (F_r \otimes I_{pq}) \cdot (F_q \otimes I_{pr}) \cdot (F_p \otimes I_{qr}).$$

Замечание по терминологии. В технической литературе [2], следуя предложенному в [7], закрепился термин Виленкина-Крестенсона функции (ВКФ) как для ДПК, так и для их непрерывного аналога. Но Виленкин рассматривал мультипликативную систему функций в общем виде для смешанных оснований. Поэтому термин ВКФ воспринимался как те из функций Виленкина, которые изучались Крестенсоном (т.е. с постоянным основанием). Поэтому и предлагается вариант терминов с конкретизацией: ДПУ (основание 2), ДПК (основание $p > 2$) и ДПВ (случай смешанного основания). Если быть исторически точными, то дискретный вариант в виде кронекеровых произведений ДПФ нельзя приписывать Виленкину. Более правильно термином ДПВ для $N = pqr$ было бы называть преобразование с матрицей (соответствующее функциям Виленкина непрерывного аргумента)

$$F = F_p \otimes F_q \otimes F_r.$$

Утверждение 6. Два вида ДПВ связаны через матрицу реверсной перестановки

$$F_p \otimes F_q \otimes F_r = (I_p \otimes I_q \otimes I_r) \cdot (F_p \otimes F_q \otimes F_r).$$

Доказательство. По следствию 1 имеем $F_p \otimes F_q = (I_p \otimes I_q) \cdot (F_p \otimes F_q)$. Отсюда вновь по лемме 1 получим

$$F_p \otimes F_q \otimes F_r = ((I_p \otimes I_q) \cdot (F_p \otimes F_q)) \otimes (I_r \cdot F_r) = (I_p \otimes I_q \otimes I_r) \cdot (F_p \otimes F_q \otimes F_r).$$

Теорема 2. Две факторизации матрицы ДПФ основания $N = pqr$:

- 1) $F_N = (F_p \otimes I_{qr}) \cdot D_{p,qr,1} \cdot (I_p \otimes ((F_q \otimes I_r) \cdot D_{q,r,1})) \cdot (I_{pq} \otimes F_r) \cdot (I_r \otimes I_q \otimes I_p),$
- 2) $F_N = (I_r \otimes I_q \otimes I_p) \cdot (F_p \otimes I_{qr}) \cdot D_{p,q,r} \cdot (F_q \otimes I_{pr}) \cdot D_{pq,r,1} \cdot (F_r \otimes I_{pq}).$

Доказательство. Первый случай для двух сомножителей прямой проверкой

$$F_{pq} = (F_p \otimes I_q) \cdot D_{p,q,1} \cdot (I_p \otimes F_q) \cdot (I_q \otimes I_p) = (F_p \otimes I_q) \cdot D_{p,q,1} \cdot (F_q \otimes I_p).$$

Сначала дано представление с выделенной реверсной перестановкой, а потом последние два сомножителя объединены по лемме 1.

Теперь первый случай для трех сомножителей

$$F_{p(qr)} = (F_p \otimes I_{qr}) \cdot D_{p,qr,1} \cdot (I_p \otimes F_{qr}) \cdot (I_{qr} \otimes I_p),$$

где по лемме 1 имеем

$$\begin{aligned} I_p \otimes F_{qr} &= (I_p \cdot I_p \cdot I_p) \otimes ((F_q \otimes I_r) \cdot D_{q,r,1} \cdot (I_q \otimes F_r) \cdot (I_r \otimes I_q)) = \\ &= (I_p \otimes ((F_q \otimes I_r) \cdot D_{q,r,1})) \cdot (I_p \otimes I_q \otimes F_r) \cdot (I_p \otimes (I_r \otimes I_q)). \end{aligned}$$

Внесем в предыдущее выражение и преобразуем два последних множителя по лемме 1

$$(I_p \otimes (I_r \otimes I_q)) \cdot (I_{qr} \otimes I_p) = ((I_r \otimes I_q) \cdot I_{qr}) \otimes (I_p \cdot I_p) = I_r \otimes I_q \otimes I_p.$$

Второй случай для двух сомножителей имеет вид

$$F_{pq} = (I_q \otimes I_p) \cdot (F_p \otimes I_q) \cdot D_{p,q,1} \cdot (F_q \otimes I_p) \quad (5)$$

Обозначим через $\tilde{F}_{p,q}$ реверсную перестановку строк матрицы F_{pq} , равную произведению последних трех сомножителей в (5). Уточним вид этой реверсной перестановки на примере $p = 2, q = 3$:

$$F_2 \otimes I_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix},$$

$$S_{2,3,1} = (1 \ 1 \ 1 \ \omega^0 \ \omega^1 \ \omega^2),$$

$$(F_2 \otimes I_3) \cdot D_{2,3,1} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & \omega & 0 \\ 0 & 1 & 0 & 0 & -\omega & 0 \\ 0 & 0 & 1 & 0 & 0 & \omega^2 \\ 0 & 0 & 1 & 0 & 0 & -\omega^2 \end{pmatrix}, \quad F_3 \otimes I_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & q & 0 & q^2 & 0 \\ 1 & 0 & q^2 & 0 & q & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & q & 0 & q^2 \\ 0 & 1 & 0 & q^2 & 0 & q \end{pmatrix} = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix},$$

где $\omega = \omega_6 = e^{\frac{2\pi i}{6}}$, $q = \omega_3 = e^{\frac{2\pi i}{3}}$, $q = \omega^2$. Получили

$$\tilde{F}_{2,3} = (F_2 \otimes I_3) \cdot D_{2,3,1} \cdot (F_3 \otimes I_2) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \omega & q & q\omega & q^2 & q^2\omega \\ 1 & -\omega & q & -q\omega & q^2 & -q^2\omega \\ 1 & \omega^2 & q^2 & q^2\omega^2 & q & q\omega^2 \\ 1 & -\omega^2 & q^2 & -q^2\omega^2 & q & -q\omega^2 \end{pmatrix}.$$

Набор строк составляет полный набор различных ДЭФ порядка 6. В столбце с номером 1 приведены образующие этих ДЭФ в реверсном порядке:

$$\omega^0, \omega^3, \omega^1, \omega^4, \omega^2, \omega^5.$$

Умножение слева на перестановочную матрицу $I_3 \otimes I_2$ возвращает столбцу из этих элементов прямой порядок.

Аналогично в общем случае: матрицу $(F_p \otimes I_q)$ рассматриваем как блочную — в начальной блочной строке приведен прореженный нулями носитель в виде матрицы F_p , записанной по столбцам в начальном столбце каждого блока. Блочная строка с номером $j + 1$ получается циклическим сдвигом вправо j -й блочной строки. Поэтому в каждом блочном столбце идет повтор со сдвигом вправо носителя. Этот процесс лучше виден, если нули в матрицах убрать, оставив носитель и пустые клетки. Произведение трех матриц будем вычислять по столбцам по правилу:

j -й столбец произведения двух матриц есть линейная комбинация столбцов первого сомножителя с коэффициентами в j -м столбце второго. Поэтому предлагается элементы матрицы $D_{p,q,1}$ внести в столбцы первого сомножителя, а далее каждый j -й столбец последнего сомножителя выбирает (наложением носителя) и суммирует с указанными коэффициентами все столбцы j -го блока полученного первого сомножителя. При этом начальный столбец получается состоящим из единиц. А столбец с номером 1 (в нем образующие элементы) имеет вид $(r_p \ u r_p \ u^2 r_p \dots u^{q-1} r_p)^T$, где $r_p = (1 \ v \ v^2 \dots v^{p-1})$, $v = \omega_p$, $u = \omega_{pq}$. Если представим по правилу $v = u^q$ степени v как степени u , то относительно суммарных степеней u элементы этого столбца в реверсном порядке (1). Домножением слева на матрицу реверсной перестановки $I_q \otimes I_p$ восстанавливаем стандартный порядок элементов первого столбца.

Покажем, что если произвольный k -й элемент первого столбца (т.е. с номером $k, 1$) имеет вид $v^a u^b$, то элемент той же строки с номером k, j имеет вид $v^{aj} u^{bj}$. Для этого будем рассматривать u , v как не взаимосвязанные символы. Подставим вместо $D_{p,q,1} \cdot (F_q \otimes I_p)$ матрицу $K \otimes I_p$ той же структуры, где $K \in M_q$ и все элементы K единицы: $(F_p \otimes I_q) \cdot (K \otimes I_p) = K \otimes F_p$ – блочная матрица с одинаковыми блоками F_p . Для всех элементов этой матрицы степени v такие же, как и для $\tilde{F}_{p,q}$. Доказали, что $\tilde{f}_{k,j} = v^{aj} u^j$.

Повторим прием с заменой матрицы $F_p \otimes I_q$ на матрицу той же структуры $K \otimes I_q$, а множители диагональной матрицы $D_{p,q,1}$ внесем в строки матрицы $F_q \otimes I_p$. Если $k = a + bp$, то вносимые множители для k -й строки $1, u^a, u^{2a}, \dots, u^{(p-1)a}$ в строки с номерами $a, q + a, 2q + a, \dots, (p-1)q + a$. Умножаем $K \otimes I_q$ на $D_{p,q,1} \cdot (F_q \otimes I_p)$ по правилу: k -я строка есть линейная комбинация строк второго сомножителя с коэффициентами из k -строки первого сомножителя. Так как носители u слагаемых строк дизъюнктивны, то получаем строку

$$\begin{aligned} & (1 \ u^a \ u^{2a} \dots u^{(p-1)a} \quad w^a (u^a w^a) (u^{2a} w^a) \dots (u^{(p-1)a} w^a) \dots \\ & \dots w^{(q-1)a} (u^a w^{(q-1)a}) (u^{2a} w^{(q-1)a}) \dots (u^{(p-1)a} w^{(q-1)a})). \end{aligned} \quad (6)$$

В каждом блоке правой матрицы выбирали строку с одним и тем же номером a , поэтому начальные множители каждой группы есть элементы ДЭФ $\mathbf{r}^a = (1 \ w^a \ w^{2a} \dots w^{(q-1)a})$ (a -й строки матрицы F_q). Выразим все элементы через u из равенства $w = u^p$ и получим в (6) прямую нумерацию по степеням u^a , т.е. ДЭФ $\mathbf{r}^a$ порядка $N = pq$.

Перейдем к второму случаю для трех сомножителей $N = pqr$.

Из доказываемой формулы выделим три сомножителя:

$$(F_p \otimes I_{qr}) \cdot D_{p,q,r} \cdot (F_q \otimes I_{pr}) \quad (7)$$

и сравним со случаем $r = 1$: $\tilde{F}_{p,q} = (F_p \otimes I_q) \cdot D_{p,q,1} \cdot (F_q \otimes I_p)$. Простой структурный анализ проведем по формуле леммы 2 при $r = 1$ и в общем случае:

$$(F_p \otimes I_{qr}) \cdot (F_q \otimes I_{pr}) = (F_q \otimes F_p) \otimes I_r.$$

Чтобы в блочных столбцах матрицы (7) сохранялся вид столбца, каждый блок диагонали матрицы $D_{p,q,1}$ дублируем r раз, что приводит к $D_{p,q,r}$. Это приводит к формуле

$$\tilde{F}_{p,q} \otimes I_r = (F_p \otimes I_{qr}) \cdot D_{p,q,r} \cdot (F_q \otimes I_{pr}),$$

что аккуратно проверяется непосредственным просчетом.

При подстановке во вторую формулу утверждения теоремы получим

$$\tilde{F}_{p,q,r} = (\tilde{F}_{p,q} \otimes I_r) \cdot D_{p,q,r,1} \cdot (F_r \otimes I_{pq}),$$

что проверим далее.

Так как $\tilde{F}_{p,q}$ есть перестановка строк матрицы F_{pq} , то и $\tilde{F}_{p,q} \otimes I_r$ есть перестановка строк $F_{pq} \otimes I_r$. Следовательно, $(\tilde{F}_{p,q} \otimes I_r) \cdot D_{p,q,r,1} \cdot (F_r \otimes I_{pq})$ есть перестановка строк

$(F_{pq} \otimes I_r) \cdot D_{pq,r,1} \cdot (F_r \otimes I_{pq})$. Поэтому достаточно проанализировать первый (образующий) столбец этой матрицы.

В первом столбце матрицы $\tilde{F}_{p,q}$ приведены все различные степени (но в реверсном порядке) от 0 до $pq - 1$ элемента $\omega = \omega_{pq}$. В матрице $(\tilde{F}_{p,q} \otimes I_r)$ эти столбцы повторяются со смещением, а в произведении матриц $(\tilde{F}_{p,q} \otimes I_r) \cdot D_{pq,r,1}$ входят с множителями, собранными в векторе $s = (1 \ \omega \ \omega^2 \ \dots \ \omega^{r-1})$, где $\omega = \omega_{pqr}$. Таким образом, образующий столбец проверяемой матрицы содержит все степени ω в реверсном порядке. Теорема доказана.

Обобщение теоремы 1 для большого числа множителей очевидно. При обобщении теоремы 2 для четырех множителей остановимся только на формулировке результата.

Следствие 2. Для ДПФ порядка $N = pqr$ верны факторизации

$$F_N = (F_p \otimes I_{qrs}) \cdot D_{p,qrs,1} \cdot (I_p \otimes ((F_q \otimes I_{rs}) \cdot D_{q,rs,1})) \cdot (I_{pq} \otimes ((F_r \otimes I_s) \cdot D_{r,s,1})) \cdot L,$$

$$F_N = L \cdot (F_p \otimes I_{qrs}) \cdot D_{p,q,rs} \cdot (F_q \otimes I_{prs}) \cdot D_{pq,r,s} \cdot (F_r \otimes I_{pqs}) \cdot D_{pqr,s,1} \cdot (F_s \otimes I_{pqr}),$$

где $L = I_s \otimes I_r \otimes I_q \otimes I_p$.

4. БЫСТРОЕ ПРЕОБРАЗОВАНИЕ КРЕСТЕНСОНА С ОСНОВАНИЕМ p^n

В прикладных задачах часто исследуются сигналы с очень большим числом отчетов с помощью ДПФ такого же большого основания. Это вынуждает увеличивать разрядность чисел для сохранения точности вычислений. Альтернативой является замена ДПФ на дискретное преобразование Крестенсона (ДПК).

Рассмотрим возникающий при этом случай ДПК с матрицей $F_N^{\otimes m}$ при $N = p^n$, когда ставится вопрос о возможности применения суперпозиции рассмотренных быстрых алгоритмов из утверждений 5 и 3.

Теорема 3. *Предлагается следующая факторизация матрицы:*

$$F_{p^n}^{\otimes m} = \left((I_p^{\otimes n} \otimes I_{N^{m-1}}) \cdot (T \otimes I_{N^{m-1}}) \prod_{k=1}^{n-1} ((D_{p^k, p, p^{n-k-1}} \otimes I_{N^{m-1}}) \cdot (T \otimes I_{N^{m-1}})) \right)^m,$$

где $T = F_p \otimes I_{p^{n-1}}$, $N = p^n$.

Доказательство. Пусть

$$\tilde{F}_N = T \cdot D_{p,p,p^{n-2}} \cdot T \cdot D_{p^2,p,p^{n-3}} \cdot T \cdot D_{p^3,p,p^{n-4}} \dots \cdot T \cdot D_{p^{n-1},p,1} \cdot T$$

в утверждении 5, которое примет вид $F_{p^n}^{\otimes n} = I_p^{\otimes n} \cdot \tilde{F}_N$.

По утверждению 3 имеем $F_{p^n}^{\otimes m} = (F_{p^n}^{\otimes n} \otimes I_{N^{m-1}})^m$. Преобразуем выражение в скобках по второй формуле леммы 1

$$F_{p^n}^{\otimes n} \otimes I_{N^{m-1}} = (I_p^{\otimes n} \cdot \tilde{F}_N) \otimes (I_{N^{m-1}} \cdot I_{N^{m-1}}) = (I_p^{\otimes n} \otimes I_{N^{m-1}}) \cdot (\tilde{F}_N \otimes I_{N^{m-1}}).$$

По первой формуле леммы 1 к каждому сомножителю $\tilde{F}_N$ добавляется справа одинаковый кронекеров множитель

$$\tilde{F}_N \otimes I_{N^{m-1}} = (T \otimes I_{N^{m-1}}) \cdot (D_{p,p,p^{n-2}} \otimes I_{N^{m-1}}) \cdot (T \otimes I_{N^{m-1}}) \cdot \dots \cdot (D_{p^{n-1},p,1} \otimes I_{N^{m-1}}) \cdot (T \otimes I_{N^{m-1}}).$$

Далее согласно утверждению 3 проводится m итераций полученной формулы для $F_{p^n}^{\otimes n} \otimes I_{N^{m-1}}$. Теорема доказана.

Возможны и другие, более громоздкие, факторизации матрицы $F_{p^n}^{\otimes m}$. Именно постоянство структуры выбранного варианта алгоритма выделяет его как оптимальный вариант. Рекомендуется для сокращения числа операций при очень больших N брать $p = 4$, n равным 2 или 3 и варьировать m .

СПИСОК ЛИТЕРАТУРЫ

1. *Cooley J.W., Tukey J.W.* An algorithm for the machine calculation of complex Fourier series // *Math. Comput.* 1965. V. 19 (90). P. 297–301.
2. *Залманзон Л.А.* Преобразования Фурье, Уолша, Хаара и их приложения в управлении, связи и других областях. М.: Наука, 1989. 496 с.
3. *Беспалов М.С.* О свойствах тензорного произведения матриц // *Ж. вычисл. матем. и матем. физ.* 2014. Т. 54. № 4. С. 547–561.
<https://doi.org/10.1134/S0965542514040046>
4. *Good I.J.* The interaction algorithm and practical Fourier analysis // *J. Royal Stat. Soc.* 1958. Ser. B. V. 20. P. 361–372.
5. *Малоземов В.Н., Машарский С.М.* Основы дискретного гармонического анализа. СПб.: Лань, 2012. 304 с.
6. *Беспалов М.С.* Новые разложения кронекеровой степени по Гуду // *Проблемы передачи информации.* 2018. Т. 54. № 3. С. 62–66.
<https://doi.org/10.1134/S0032946018030043>
7. *Трахтман А.М., Трахтман В.А.* Основы теории дискретных сигналов на конечных интервалах. М.: Сов. радио, 1975.
8. *Малоземов В.Н., Машарский С.М., Цветков К.Ю.* Сигнал Франка и его обобщения // *Проблемы передачи информации.* 2001. Т. 37. № 2. С. 18–26.
9. *Малоземов В.Н., Машарский С.М.* Обобщенные вейвлетные базисы, связанные с дискретным преобразованием Виленкина–Крестенсона // *Алгебра и анализ.* 2001. Т. 13. Вып. 1. С. 111–157.
10. *Машарский С.М.* Быстрое преобразование Виленкуина – Крестенсона на основе факторизации Гуда // *Ж. вычисл. матем. и матем. физ.* 2002. Т. 42, № 6. с. 784–790.
11. *Беспалов М.С.* Дискретные преобразования Крестенсона // *Проблемы передачи информации.* 2010. Т. 46. № 4. С. 91–115.
<https://doi.org/10.1134/S003294601004006X>
12. *Johnson J., Johnson R.W., Rodriguez D., Tolimieri R.* A methodology for designing, modifying and implementing Fourier transform algorithms on various architectures // *Circuits, Systems and Signal Processing.* 1990. V. 9. № 4. P. 449–500.
13. *Малоземов В.Н., Просеков О.В.* Факторизация Кули–Тьюки матрицы Фурье // *Избранные главы дискретного гармонического анализа и геометрического моделирования.* Ч. I. Изд. 2-е. Под ред. проф. В. Н. Малоземова. СПб.: Изд-во ВВМ. 2014. С. 20–29.