МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ имени академика С.П.КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»

В.М. Чернов

Быстрые алгоритмы многомерного дискретного преобразования Фурье

Электронное учебное пособие

САМАРА

2010

Авторы: ЧЕРНОВ Владимир Михайлович,

Представленное учебное пособие относится к пограничной области между информатикой (теория и практика анализа и обработки многомерных цифровых сигналов) и математикой (абстрактная алгебра и теория чисел). Основное внимание в книге уделяется методам синтеза быстрых алгоритмов многомерного дискретного преобразования Фурье с представлением данных в виде элементов конечномерных алгебр специального вида.

Пособие предназначено для магистров направления 010400.68 “Прикладная математика и информатика”, обучающихся по программе «Математические и компьютерные методы обработки изображений и геоинформатики».

ВВЕДЕНИЕ

Преподавание математики все еще страдает от энтузиазма, вызванного открытием этого изоморфизма (сопоставляющего линейному преобразованию векторного пространства некоторую матрицу – В.Ч.). Следствием было то, что геометрия фактически исключалась и заменялась вычислениями. Вместо наглядных отображений пространства, сохраняющих сложение векторов и умножение их на скаляры <…>, в рассмотрение вводились матрицы.

Мой опыт показывает, что доказательства, включающие в себя матрицы, могут быть сокращены на 50%, если выбросить матрицы. Иногда это невозможно; бывает, например, что нужно вычислить определитель.

Э.Артин[1]

Приведем необходимые сведения из теории быстрых преобразований Фурье.

Одними из наиболее эффективных методов цифровой обработки сигналов являются методы, связанные с использованием дискретных ортогональных преобразований.

Определение В.1. Пусть $f(n) \in \mathbf{C}$ - периодическая с периодом N комплекснозначная последовательность, $\{h_m(n)\}_{m=0}^{N-1}$ - семейство N-периодических комплекснозначных функций с условием ортогональности

---

[1] Э.Артин. Геометрическая алгебра. - М.: Наука. - 1969.

$$\langle h_m, h_k \rangle = \sum_{n=0}^{N-1} h_m(n)\overline{h_k(n)} = \delta_{mk} \qquad \text{(B.1)}$$

(δ_{mk} - дельта-символ Кронекера, черта означает комплексное сопряжение).

Преобразование

$$\mathbf{f} = \big(f(0),..., f(N-1)\big) \mapsto \big(F(0),..., F(N-1)\big) = \mathbf{F}, \qquad \text{(B.2)}$$

определяемое соотношением,

$$F(m) = \sum_{n=0}^{N-1} f(n)\, h_m(n) \quad (m=0, 1, \ldots, N\text{-}1) \qquad \text{(B.3)}$$

называется *дискретным ортогональным преобразованием* (ДОП) с базисом $\{h_m(n)\}_{m=0}^{N-1}$.

Преобразование (B.3) линейно и может быть записано в матричной форме:

$$\mathbf{F}^T = \mathbf{H}\mathbf{f}^T, \qquad \text{(B.4)}$$

где $\mathbf{f}^T$, $\mathbf{F}^T$ - транспонированные к векторам (B.2) векторы-столбцы,

$$\mathbf{H} = \begin{pmatrix} h_0(0) & \ldots & h_0(N-1) \\ \ldots & \ldots & \ldots \\ h_{N-1}(0) & \ldots & h_{N-1}(N-1) \end{pmatrix}. \qquad \text{(B.5)}$$

Определение B.2. Матрица **H**, определенная равенством (B.5), называется *матрицей дискретного ортогонального преобразования* (B.3).

Пример B.1. Преобразование (B.3) с базисными функциями

$$h_m(n) = 1/\sqrt{N} \exp\{2\pi i\, mn/N\} \qquad \text{(B.6)}$$

называется дискретным преобразованием Фурье (ДПФ).

Пример B.2. Преобразование (B.3) с базисными функциями

$$h_m(n) = 1/\sqrt{N}\left(\cos 2\pi mn/N + \sin 2\pi mn/N\right) \qquad \text{(B.7)}$$

называется дискретным преобразованием Хартли.

Пример B.3. Преобразование (B.3) с базисными функциями

$$h_m(n) = \lambda_m \cos \pi(2n+1)m/2N, \qquad \text{(B.8)}$$

где нормирующие коэффициенты λ_m определены равенством

$$\lambda_m = \begin{cases} 2/\sqrt{N}, & \text{при} \quad m \neq 0, \\ 1/\sqrt{N}, & \text{при} \quad m = 0, \end{cases} \qquad \text{(B.9)}$$

называется дискретным косинусным преобразованием (ДКП).

Непосредственное матричное умножение в (B.4) или, что то же самое, вычисление массива $F(m)$ в (B.3) требует $\sim N^2$ арифметических операций. Поэтому в практических задачах предпочтение отдается таким ДОП, для которых арифметическая природа базисных функций позволяет синтезировать алгоритмы с существенно более низкой вычислительной сложностью. Отличительной особенностью преобразований примеров B.1-B.3 является возможность синтеза таких высокоскоростных алгоритмов.

Определение B.3. Число вещественных арифметических операций сложения и умножения, *достаточных* для реализации преобразования (B.3), будем называть (вещественной) *аддитивной и мультипликативной сложностью* алгоритма вычисления ДОП и обозначать $A(N)$ и $M(N)$, соответственно.

Если для данного алгоритма вычисления ДОП при $N \to \infty$ справедливо соотношение

$$\frac{A(N)+M(N)}{N^2} \to 0,$$

то алгоритм принято называть *быстрым* (БА ДОП).

Конечномерные ассоциативные алгебры

Пусть **A** – конечномерное векторное пространство над полем **F** с базисом:

$$\{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{d-1}\}$$

с обычными (покоординатными) правилами сложения и умножения на элемент поля **F**.

Определим бинарный закон $(\mathbf{e}_i, \mathbf{e}_j) \mapsto \mathbf{e}_i \mathbf{e}_j \in \mathbf{A}$ умножения базисных элементов и распространим его на все множество векторов из пространства **A** посредством равенства

$$\xi\eta = \sum_{k,j=0}^{d-1} \xi_k \eta_j \left(\mathbf{e}_k \mathbf{e}_j\right), \qquad \text{(B.10)}$$

где

$$\xi = \xi_0 \mathbf{e}_0 + \ldots + \xi_{d-1} \mathbf{e}_{d-1},$$

$$\eta = \eta_0 \mathbf{e}_0 + \ldots + \eta_{d-1} \mathbf{e}_{d-1}.$$

Определение В.4. Множество A с введенными операциями сложения, умножения на элемент из F, индуцированных операциями исходного векторного пространства, и умножением, определенным равенством (В.10), называется *конечномерной* (*d*-мерной) *ассоциативной алгеброй* над полем F (или, короче, F-алгеброй).

Определение В.5. Пусть **A** есть некоторая **F**-алгебра и $\mathbf{1} \in \mathbf{A}$ - такой элемент, что для всех $\mathbf{x} \in \mathbf{A}$ выполняются равенства

$$\mathbf{1} \cdot \mathbf{x} = \mathbf{x} \cdot \mathbf{1} = \mathbf{x}.$$

Такой элемент **1** называется *единицей* алгебры A, а сама алгебра – *алгеброй с единицей.*

Определение В.6. Пусть **A, B** – две **F**-алгебры. Взаимно однозначное отображение $\varphi : \mathbf{A} \mapsto \mathbf{B}$ называется *изоморфизмом* алгебр, если для любых $\xi, \eta \in \mathbf{A}$ и $\lambda \in \mathbf{F}$ выполняются равенства

$$\text{(a)}\ \varphi(\xi + \eta) = \varphi(\xi) + \varphi(\eta),$$

$$\text{(b)}\ \varphi(\lambda\xi) = \lambda\varphi(\xi),$$

$$\text{(c)}\ \varphi(\xi\eta) = \varphi(\xi) \cdot \varphi(\eta).$$

Если **A** = **B**, то отображение φ называется *автоморфизмом*.

Приведем несколько примеров конечномерных ассоциативных алгебр, рассматриваемых в настоящем разделе при синтезе БА ДОП.

Пример В.4. Четырехмерная **R**-алгебра с базисом $\{1,\ i,\ j,\ k\}$ и правилами умножения базисных элементов

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k$$

называется алгеброй кватернионов.

Пример В.5. Двумерные **R**-алгебры с базисом $\{\mathbf{1},\ \mathbf{e}\}$ называются *алгебрами комплексных, дуальных или двойных чисел*, если, соответственно, $\mathbf{e}^2=-\mathbf{1}$, $\mathbf{e}^2=\mathbf{1}$ или $\mathbf{e}^2=\mathbf{0}$.

Пример В.6. Пусть **G** – конечномерная *d*-элементная группа с групповой операцией (*) и нейтральным элементом $\mathbf{g}_0=\mathbf{1}\in\mathbf{G}$. Рассмотрим векторное пространство над **R** с базисом $\{\mathbf{1},\mathbf{g}_1,...,\mathbf{g}_{d-1}\}$ и определим умножение (В.10) элементов этого пространства равенством

$$\boldsymbol{\xi}\boldsymbol{\eta}=\sum_{\mathbf{g}\in\square}\left(\sum_{<\mathbf{g}_i\mathbf{g}_j=\mathbf{g}>}\xi_i\eta_j\right)\mathbf{g}.$$

Введенная алгебра называется *групповой алгеброй* группы **G**.

Другие необходимые примеры алгебр рассматриваются в разделе по мере их использования.

Декомпозиция Кули-Тьюки "по основанию 2"

Пусть $f(n)\in\mathbf{C}$ есть *N*-периодическая последовательность, $N=2^k$, $F(m)$ - её дискретный спектр Фурье:

$$F(m)=\sum_{n=0}^{N-1}f(n)\,w^{mn},\quad w=\exp\left\{2\pi i/N\right\},\quad 0\le m\le N-1. \qquad (В.11)$$

Сумма в правой части соотношения (В.11) может быть представлена для $0\le m\le N/2-1$ в виде двух сумм длиной $N/2$:

$$F(m)=\sum_{n=0}^{\frac{N}{2}-1}f(2n)\left(w^2\right)^{mn}+w^m\sum_{n=0}^{\frac{N}{2}-1}f(2n+1)\left(w^2\right)^{mn}=F_0(m)+w^mF_1(m). \qquad (В.12)$$

Здесь

$$F_0(m)=\sum_{n=0}^{\frac{N}{2}-1}f(2n)\left(w^2\right)^{mn},\quad F_1(m)=\sum_{n=0}^{\frac{N}{2}-1}f(2n+1)\left(w^2\right)^{mn}$$

- спектры Фурье $N/2$ -периодичных подпоследовательностей. Таким образом, ДПФ длиной N сведено к двум преобразованиям Фурье длиной $N/2$ и к $N/2$ дополнительным умножениям на степени w для $0 \le m \le N/2-1$. Так как $w^{N/2} = -1$, то вычисление $F(m)$ для $N/2 \le m \le N-1$ выполняется без дополнительных умножений:

$$F\left(m^* + N/2\right) = F_0(m^*) - w^{m^*} F_1(m^*), \quad 0 \le m^* \le N/2 - 1. \qquad \text{(B.13)}$$

Мультипликативная $M(N)$ и аддитивная $A(N)$ сложности такого алгоритма равны соответственно:

$$M(N) \le 3/2\, N\log_2 N - 9/2\, N, \quad A(N) \le 7/2\, N\log_2 N - 9/2\, N. \qquad \text{(B.14)}$$

Изложенный алгоритм принято называть быстрым преобразованием Фурье (БПФ) по основанию 2.

Декомпозиция Кули-Тьюки "по основанию 4"

Аналогичным образом строится алгоритм БПФ "по основанию 4" при $N = 4^k$. Сумма для $F(m)$ в (B.11) разбивается на четыре части:

$$\begin{aligned} F(m) = &\sum_{n=0}^{\frac{N}{4}-1} f(4n)\left(w^4\right)^{mn} + w^m \sum_{n=0}^{\frac{N}{4}-1} f(4n+1)\left(w^4\right)^{mn} + \\ &+ w^{2m} \sum_{n=0}^{\frac{N}{4}-1} f(4n+2)\left(w^4\right)^{mn} + w^{3m} \sum_{n=0}^{\frac{N}{4}-1} f(4n+3)\left(w^4\right)^{mn} = \\ &= F_0(m) + w^m F_1(m) + w^{2m} F_2(m) + w^{3m} F_3(m), \end{aligned} \qquad \text{(B.15)}$$

$$0 \le m \le N/4 - 1.$$

Соотношение (B.14) редуцирует вычисление ДПФ (B.11) к вычислению четырех ДПФ длиной $N/4$ и к $3N/4$ дополнительным умножениям на степени w. Так как при стандартном машинном представлении комплексных чисел умножения на

степени мнимой единицы i являются тривиальными, значения спектра при $N/4 \le m \le N-1$ вычисляются без дополнительных умножений следующим образом:

$$\begin{pmatrix} F(m^*) \\ F\left(\frac{N}{4}+m^*\right) \\ F\left(\frac{N}{2}+m^*\right) \\ F\left(\frac{3N}{4}+m^*\right) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} F_0(m^*) \\ w^{m^*} F_1(m^*) \\ w^{2m^*} F_2(m^*) \\ w^{3m^*} F_3(m^*) \end{pmatrix}, \quad 0 \le m^* \le N/4 - 1 . \qquad \text{(B.16)}$$

Оценки вычислительной сложности такого алгоритма имеют вид:

$$M(N) \le 9/8\, N\log_2 N - 13/4\, N , \quad A(N) \le 25/8\, N\log_2 N - 13/4\, N . \qquad \text{(B.17)}$$

Декомпозиция Кули-Тьюки с расщеплением основания

(сплит-радикс алгоритм)

Пусть $N = 2^k$, тогда преобразование (B.11) для $0 \le m \le N/4 - 1$ может быть записано в следующем виде [6]:

$$F(m) = \sum_{n=0}^{\frac{N}{2}-1} f(2n)\left(w^2\right)^{mn} + w^m \sum_{n=0}^{\frac{N}{4}-1} f(4n+1)\left(w^4\right)^{mn} + w^{3m} \sum_{n=0}^{\frac{N}{4}-1} f(4n+3)\left(w^4\right)^{mn} .$$

Здесь ДПФ длиной N сведено к одному ДПФ длиной $N/4$, двум ДПФ длиной $N/4$ и к $2N/4$ дополнительным умножениям на степени w. Вычисление $X(m)$ для $N/4 \le m \le N-1$ выполняются без дополнительных умножений:

$$\begin{pmatrix} F(m^*) \\ F\left(\frac{N}{4}+m^*\right) \\ F\left(\frac{N}{2}+m^*\right) \\ F\left(\frac{3N}{4}+m^*\right) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & i & 1 & -i \\ 1 & -1 & 0 & -1 \\ 0 & -i & 1 & i \end{pmatrix} \begin{pmatrix} F_0(m^*) \\ w^{m^*} F_1(m^*) \\ F_0\left(N/4+m^*\right) \\ w^{3m^*} F_3(m^*) \end{pmatrix}, \quad 0 \le m^* \le N/4 - 1 ,$$

где

$$F_0(m)=\sum_{n=0}^{\frac{N}{2}-1} f(2n)\left(w^2\right)^{mn},\quad F_1(m)=\sum_{n=0}^{\frac{N}{4}-1} f(4n+1)\left(w^4\right)^{mn},$$

$$F_3(m)=\sum_{n=0}^{\frac{N}{4}-1} f(4n+3)\left(w^4\right)^{mn}.$$

Оценки вычислительной сложности для этого алгоритма равны:

$$M(N)\le N\log_2 N-3N,\quad A(N)\le 3N\log_2 N-3N. \qquad \text{(B.18)}$$

Декомпозиция ДПФ Гуда-Томаса

Другим известным способом быстрого вычисления ДПФ является декомпозиция Гуда-Томаса [35, 42], применяемая в тех случаях, когда длина преобразования $N=P\cdot Q$, где P и Q - взаимно просты.

Пусть $\alpha=\exp\left\{2\pi i/P\right\}$, $\beta=\exp\left\{2\pi i/Q\right\}$ - первообразные комплексные корни из единицы степени P и Q соответственно. Представим индексы входной и выходной последовательности в виде:

$$\begin{cases} n\equiv Pn_1+Qn_2 \\ m\equiv Pam_1+Qbm_2 \end{cases}, \qquad \text{(B.19)}$$

где a и b определяются из условий

$$\begin{cases} P\,a\equiv 1\,(\mathrm{mod}\,Q) \\ Q\,b\equiv 1\,(\mathrm{mod}\,P) \end{cases}. \qquad \text{(B.20)}$$

После введения обозначений

$$\tilde{x}(n_1,n_2)=x(Pn_1+Qn_2),\quad \tilde{F}(m_1,m_2)=F(Pam_1+Qbm_2)$$

соотношение (B.11) примет вид:

$$\tilde{F}(m_1,m_2)=\sum_{n_1=0}^{Q-1}\sum_{n_2=0}^{P-1}\tilde{f}(n_1,n_2)\,w^{(Pn_1+Qn_2)(Pam_1+Qbm_2)}=$$

$$=\sum_{n_1=0}^{Q-1}\sum_{n_2=0}^{P-1}\tilde{f}(n_1,n_2)\,w^{P^2an_1m_1+PQ(bn_1m_2+an_2m_1)+Q^2bn_2m_2}.$$

В силу (В.20) справедливо равенство:

$$\tilde{F}(m_1, m_2) = \sum_{n_1=0}^{Q-1} \sum_{n_2=0}^{P-1} \tilde{f}(n_1, n_2)\, w^{Pn_1m_1}\, w^{PQ(bn_1m_2 + an_2m_1)}\, w^{Qn_2m_2} = \\ = \sum_{n_1=0}^{Q-1} \sum_{n_2=0}^{P-1} \tilde{f}(n_1, n_2) \beta^{n_1m_1} \alpha^{n_2m_2}, \tag{В.21}$$

где

$$\beta = \exp\left\{2\pi i P / N\right\} = \exp\left\{2\pi i / Q\right\} = w^P \ , \ \alpha = \exp\left\{2\pi i Q / N\right\} = \exp\left\{2\pi i / P\right\} = w^Q .$$

Из последнего равенства (В.21) следует:

$$\tilde{F}(m_1, m_2) = \sum_{n_2=0}^{P-1} \left(\sum_{n_1=0}^{Q-1} \tilde{f}(n_1, n_2) \beta^{n_1m_1} \right) \alpha^{n_2m_2} \tag{В.22}$$

или

$$F(Pam_1 + Qbm_2) = \sum_{n_2=0}^{P-1} \left(\sum_{n_1=0}^{Q-1} f(Pn_1 + Qn_2) \beta^{n_1m_1} \right) \alpha^{n_2m_2} . \tag{В.23}$$

Так как для описанного шага декомпозиции справедливо неравенство:

$$M(N) = M(P) \cdot Q + M(Q) \cdot P \le QP^2 + PQ^2 = N(P+Q) < N^2, \tag{В.24}$$

то применение этого приема тем эффективнее, чем на большее число взаимно простых сомножителей разлагается число *N*.

1. ПОСТАНОВКА ЗАДАЧИ, ОСНОВНЫЕ ИДЕИ

"Совмещенные" алгоритмы одномерного дискретного преобразования Фурье

$$\hat{x}(m) = \sum_{n=0}^{N-1} x(n)\ \omega^{mn},\ \omega \in \mathbf{C}, \omega^N = 1 \qquad (1)$$

вещественных N-периодических последовательностей хорошо известны и подробно описаны. В их основе лежит возможность получения дополнительных вычислительных преимуществ за счет избыточности представления вещественных чисел в комплексной арифметике. Эта "избыточность" заключается в том, что действительное число *не есть* частный случай комплексного. Строго говоря, двумерная алгебра $\mathbf{C}$ содержит "только" *изоморфную копию* одномерной алгебры действительных чисел, а именно алгебру $\mathbf{C}_0 = \{a + 0 \cdot i;\ a \in \mathbf{R}\}$.

Игнорирование этого, казалось бы малозначительного, факта вынуждает производить вычисления с действительными числами как с "полноценными" комплексными. В то же время, учет этой "неполноценности" позволяет получить некоторые вычислительные преимущества.

Типичный пример: представляя (1) в форме

$$\hat{x}(m) = \sum_{n=0}^{N/2-1} x(2n)\ \left(\omega^2\right)^{mn} + \omega^m \sum_{n=0}^{N/2-1} x(2n+1)\ \left(\omega^2\right)^{mn} \qquad (2)$$

и вводя комплекснозначную функцию

$$z(n) = x(2n) + i\ \ x(2n+1), \qquad (3)$$

можно свести вычисление преобразования (1) к вычислению дискретного Фурье-спектра $\hat{z}(m)$ комплексной последовательности $z(n)$ периода $N/2$ и некоторому (относительно небольшому) числу дополнительных вычислений, позволяющих найти известному спектру $\hat{z}(m)$ спектры $\hat{x}_0(m)$ и $\hat{x}_1(m)$ последовательностей $x(2n)$ и $x(2n+1)$, с последующей реконструкцией полного спектра $\hat{x}(m)$. В самом деле, такая возможность следует из равенств:

$$\begin{cases} \hat{x}_0(m) = \hat{z}(m) + \overline{\hat{z}(-m)}, \\ \hat{x}_1(m) = i\left(\hat{z}(-m) - \hat{z}(m)\right), \\ \hat{x}(m) = \hat{x}_0(m) + \omega^m \hat{x}_1(m). \end{cases} \qquad (4)$$

Выделение из $\hat{z}(m)$ частичных спектров $\hat{x}_0(m)$ и $\hat{x}_1(m)$ обеспечивается наличием в поле комплексных чисел **C** двух автоморфизмов (тождественного и комплексного сопряжения), действующих на **R** тождественно, причем переход к комплексно-сопряженному числу при стандартной машинной реализации не требует дополнительных арифметических действий.

Замечание 1. Аналогичный прием может использоваться, конечно, и для одновременного вычисления Фурье спектров двух вещественных $N/2$-периодических последовательностей $x_0(n)$ и $x_1(n)$. Первые два соотношения системы равенств (4) позволяют найти спектры $\hat{x}_0(m)$ и $\hat{x}_1(m)$ из спектра вспомогательной комплексной последовательности $z(n) = x_0(n) + ix_1(n)$.

В случае двумерного ДПФ, в частности, с реализацией быстрого алгоритма в простейшей построчно-столбцовой (каскадной) форме:

$$\hat{x}(m_1,\ m_2) = \sum_{n_1,\,n_2=0}^{N-1} x(n_1,\ n_2)\ \omega^{m_1 n_1 + m_2 n_2} = \sum_{n_1=0}^{N-1} \omega^{m_1 n_1} \left(\sum_{n_2=0}^{N-1} x(n_1,\ n_2)\ \omega^{m_2 n_2} \right), \qquad (5)$$

применение описанного выше приема затруднительно из-за невещественности внутренних сумм в правой части соотношения (5). Кроме того, поле **C** имеет "слишком мало" автоморфизмов, позволяющих осуществить многократное совмещение по каждому из аргументов с возможностью последующего разделения спектров.

<u>Основная идея.</u> Давайте вложим преобразуемый вещественный d-мерный массив $x(\mathbf{n})$ $\left(\mathbf{n} \in \mathbf{Z}^d\right)$ в другую, отличную от поля **C**, алгебру **A** с достаточным числом тривиально реализуемых автоморфизмов. Тогда при "разумном" выборе разбиения входного массива; алгебры **A**; множества автоморфизмов этой алгебры, дополнительные вычислительные затраты, связанные с увеличением вещественной сложности операций в алгебре **A** по сравнению с алгеброй комплексных чисел;

нахождением автоморфных образов элементов; реконструкцией спектра $\hat{x}(\mathbf{m})$ по известным частичным спектрам $A_t(\mathbf{m})$ (асимптотически) компенсируются, как и в каноническом случае, уменьшением объема области суммирования и учетом специфических свойств алгебры **A**.

2. ВСПОМОГАТЕЛЬНЫЕ СВЕДЕНИЯ

2.1. Общие принципы синтеза совмещенных алгоритмов

Определение 1. Конечномерную ассоциативную $\mathbf{R}$-алгебру $\mathbf{A}$ с единицей, содержащую изоморфную копию $\tilde{\mathbf{C}}$ алгебры комплексных чисел, будем далее называть для краткости гиперкомплексной алгеброй.

Пусть $\mathbf{E}_0 = 1,\ \mathbf{E}_1,\ \ldots,\ \mathbf{E}_{s-1}$ - базис алгебры $\mathbf{A}$ над $\mathbf{R}$:

$$a_0\mathbf{E}_0 + a_1\mathbf{E}_1 + \ldots a_{s-1}\mathbf{E}_{s-1} = \mathbf{a} \in \mathbf{A};$$

Δ - такое подмножество автоморфизмов алгебры $\mathbf{A}$, что система уравнений

$$\sigma(a) = b_\sigma,\ \sigma \in \Delta \tag{6}$$

разрешима относительно $a_0,\ \ldots,\ a_{s-1}$ при любых $b_\sigma \in \mathbf{A}$.

Пусть, далее, преобразуемый массив $X = \{x(\mathbf{n})\} \subset \mathbf{Z}^d$ представлен в виде объединения массивов X_t:

$$X = \bigcup_{t=0}^{s-1} X_t = \bigcup_{t=0}^{s-1} \{x(\mathbf{n}_t)\},$$

так что

$$\max_t\ card\ X_t = M < N,\ \mathbf{n}_t \in \Delta_t \subset \mathbf{Z}^d.$$

Введем обозначения:

$$\mathbf{n} = (n_1,\ \ldots,\ n_d),\ \mathbf{m} = (m_1,\ \ldots,\ m_d),\ \langle \mathbf{n},\ \mathbf{m} \rangle = n_1m_1 + \ \ldots + \ n_dm_d;$$

$$\Gamma_Q = \{\ \mathbf{k} = (k_1,\ \ldots,\ k_d) : 0 \le k_j \le Q-1,\ 1 \le j \le d\}.$$

Допустим, что $\omega \in \tilde{\mathbf{C}}$ - первообразный корень степени M из единицы с условием:

$$\sigma(\omega) = \omega^{r_\sigma},\ r_\sigma \in \mathbf{Z}, \sigma \in \Delta.$$

Для элементов

$$\mathbf{a}(\mathbf{n}_0, \ldots, \mathbf{n}_{s-1}) = x(\mathbf{n}_0)\mathbf{E}_0 + \ldots + x(\mathbf{n}_{s-1})\mathbf{E}_{s-1} \in \mathbf{A},\ x(\mathbf{n}_t) \in X_t$$

введем новую d-мерную индексацию

$$\mathbf{a}(\mathbf{n}_0, \ldots, \mathbf{n}_{s-1}) = \mathbf{a}(\mathbf{k}),\ \mathbf{k} \in \Gamma_M$$

и рассмотрим вспомогательное преобразование:

$$A(\mathbf{m}) = \sum_{\mathbf{k} \in \Gamma_M} \mathbf{a}(\mathbf{k})\ \omega^{\langle \mathbf{k}, \mathbf{m} \rangle}, \mathbf{m} \in \Gamma_M. \qquad (7)$$

Преобразование (7) может быть вычислено с помощью алгоритмов, аналогично обычным алгоритмам d-мерного ДПФ, но меньшего ($M<N$) объема. Применяя к равенству (7) автоморфизмы $\sigma \in \Delta$, получаем разрешимую систему уравнений для определения "частичных спектров" $A_t(\mathbf{m})$:

$$A_t(\mathbf{m}) = \sum_{\mathbf{n}_t \in \Delta_t} x(\mathbf{n}_t)\ \omega^{\langle \mathbf{n}_t, \mathbf{m} \rangle}. \qquad (8)$$

Таким образом, *возможность* синтеза быстрых алгоритмов с совмещением в алгебре **A** определяется существованием в ней множества Δ тривиально реализуемых автоморфизмов, формирующих разрешимую систему уравнений (6), а *эффективность* таких алгоритмов – сложностью реализации операций в алгебре **A**.

Рассмотрим свойства некоторых наиболее "популярных" алгебр, используемых в качестве алгебраических структур, в которых производится вычисление вспомогательного преобразования (7). Наиболее существенными характеристиками этих алгебр для нас являются:

- сложность арифметических операций;
- существование тривиально реализуемых автоморфизмов;
- факт единственности решения системы уравнений, порожденной этими автоморфизмами.

2.2. Алгебра кватернионов

Определение 2. Алгеброй **H** (гамильтоновых) кватернионов называется четырехмерная алгебра над **R**:

$$\mathbf{H} = \{ q = a + bi + cj + dk;\ a, b, c, d \in \mathbf{R} \} \tag{9}$$

с базисом $\{1, i, j, k\}$ и со следующими определяющими соотношениями для умножения базисных элементов:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k. \tag{10}$$

Поле комплексных чисел **C** канонически вкладывается в **H**:

$$a + bi \to a + bi + 0 \cdot j + 0 \cdot k. \tag{11}$$

Кроме того, справедливо соотношение

$$q = a + bi + cj + dk = (a + bi) + (c + di)\, j. \tag{12}$$

Кватернионы вида $a + bi$, $a + cj$, $a + dk$ будем называть *i*-, *j*- или *k*-кватернионами соответственно.

Замечание 2. Отметим, что далее, в рассматриваемом круге задач, арифметические операции над элементами гиперкомплексных алгебр, кватернионов, в частности, выполняются не для произвольных (переменных) элементов. Один из сомножителей (или слагаемых) – элемент, являющийся постоянным для данного алгоритма (корень соответствующей фиксированной степени из единицы, например). Операции над вещественными компонентами таких постоянных элементов могут быть выполнены заранее, вне рамок собственно алгоритма вычисления спектра. Поэтому далее мы не будем учитывать эти операции при анализе вычислительной сложности рассматриваемых алгоритмов.

С учетом соотношений (10) нетрудно показать, что умножение кватерниона (11) на кватернион

$$Q = x + iy + jz + kt, \tag{13}$$

то есть, вычисление произведения qQ, равносильно вычислению матричного произведения

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \tag{14}$$

и требует 16 вещественных умножений и 12 вещественных сложений. Покажем, что число умножений может быть несколько уменьшено с сохранением общего числа необходимых арифметических операций.

Лемма 1. Пусть q – постоянный кватернион (12), Q – переменный кватернион (13). Тогда для вычисления произведения qQ достаточно 12 вещественных умножений и 16 вещественных сложений.

Доказательство. Представляя кватернион (12) в форме

$$q = a + bi + cj + dk = (a + bi) + (c + di)\, j = A + Bj,$$

а кватернион (13) в форме

$$Q = x + iy + jz + kt = (x + iy) + j(z - kt) = V + jW,$$

получаем

$$(A + Bj)(V + jW) = (AV - BW) + j(\overline{A}W + \overline{B}V). \tag{15}$$

Утверждение леммы следует из того, что, с учетом Замечания 2, вычисление каждого из произведений комплексных чисел в (15) может быть реализовано посредством трех умножений и трех сложений. Действительно,

$$(\alpha + i\beta)(\eta + i\zeta) = [\beta(\eta - \zeta) + (\alpha - \beta)\eta] + i[\alpha(\eta + \zeta) - (\alpha - \beta)\eta]. \tag{16}$$

Лемма 2. Пусть $s = \alpha + \beta i$ есть i-кватернион; $t = \gamma + \delta j$ есть j-кватернион. Тогда для вычисления произведений sq и qt необходимо по шесть вещественных умножений и шесть вещественных сложений, а для одновременного вычисления произведения sqt - девять вещественных умножений и пятнадцать вещественных сложений.

Доказательство. Непосредственно проверяются равенства:

$$\begin{aligned} sq = {} & \big((\alpha - \beta)\, b + \alpha(a - b)\big) + \big(a(\alpha + \beta) - \alpha(a - b)\big) i + \\ & + \big((\alpha - \beta)\, d + \alpha(c - d)\big) j + \big(c(\alpha + \beta) - \alpha(c - d)\big) k; \end{aligned} \tag{17}$$

$$
\begin{aligned}
sqt = &\Big(\big[(\alpha-\beta)(b-d)+\alpha(a-b-c+d) \big]\delta + \big[(\alpha-\beta)b+\alpha(a-b) \big](\gamma-\delta) \Big) + \\
&+\Big(\big[(\alpha-\beta)(b-d)+\beta(a+b-c-d) \big]\delta + \big[(\alpha-\beta)b+\beta(a+b) \big](\gamma-\delta) \Big) i + \\
&+\Big(\big[(\alpha-\beta)(b-d)+\alpha(a-b-c+d) \big]\delta + \big[(\alpha-\beta)d+\alpha(c-d) \big](\gamma-\delta) \Big) j + \\
&+\Big(\big[(\alpha-\beta)(b-d)+\beta(a+b-c-d) \big]\delta + \big[(\alpha-\beta)d+\beta(c+d) \big](\gamma-\delta) \Big) k.
\end{aligned}
\tag{18}
$$

Далее, также непосредственно проверяется, что отображения

$$
\varepsilon_i : q \mapsto i^{-1}qi,\ \varepsilon_j : q \mapsto j^{-1}qj,\quad \varepsilon_k : q \mapsto k^{-1}qk,\ \varepsilon_0 : q \mapsto q
$$

являются автоморфизмами **H** над **R**, причем

$$
\begin{cases}
\varepsilon_0(q) = a+bi+cj+dk \\
\varepsilon_i(q) = a+bi-cj-dk \\
\varepsilon_j(q) = a-bi+cj-dk \\
\varepsilon_k(q) = a-bi-cj+dk.
\end{cases}
\tag{19}
$$

Система уравнений (19), рассматриваемая относительно *a*, *b*, *c*, *d*, разрешима при любых значениях левых частей и требует для решения только сложений и умножений на степени двойки:

$$
\begin{cases}
4a = \varepsilon_0(q)+\varepsilon_i(q)+\varepsilon_j(q)+\varepsilon_k(q) \\
4bi = \varepsilon_0(q)+\varepsilon_i(q)-\varepsilon_j(q)-\varepsilon_k(q) \\
4cj = \varepsilon_0(q)-\varepsilon_i(q)+\varepsilon_j(q)-\varepsilon_k(q) \\
4dk = \varepsilon_0(q)-\varepsilon_i(q)-\varepsilon_j(q)+\varepsilon_k(q).
\end{cases}
\tag{20}
$$

2.3. Четырехмерная коммутативная гиперкомплексная алгебра

Алгебра, рассматриваемая ниже, относительно редко используется в прикладных задачах. Несмотря на то, что простым линейным преобразованием она переводится в изоморфную ей алгебру $\mathbf{C} \oplus \mathbf{C}$ с покомпонентными сложением и умножением, относительная простота реализации операций в ней дает некоторые вычислительные преимущества в задачах синтеза быстрых алгоритмов дискретных ортогональных преобразований.

Определение 3. Четырехмерной коммутативной гиперкомплексной алгеброй $\mathbf{C}^2$ будем называть алгебру

$$\mathbf{C^2} = \{h = a + bi + cj + dij; \quad a, b, c, d \in \mathbf{R}\} \tag{21}$$

с базисом $\{1, i, j, ij\}$ и со следующими определяющими соотношениями для умножения базисных элементов:

$$i^2 = j^2 = -1; \quad ij = ji = k. \tag{22}$$

Поле комплексных чисел **C** канонически вкладывается в $\mathbf{C}^2$:

$$a + bi \to a + bi + 0 \cdot j + 0 \cdot k. \tag{23}$$

Кроме того, как и в кватернионном случае, справедливо соотношение (12). Элементы вида $a + bi, a + cj$ будем называть *i*-, или *j*- элементами, соответственно.

С учетом соотношений (22) нетрудно показать, что непосредственное умножение элемента (21) на элемент

$$H = x + yi + zj + tk, \tag{24}$$

то есть, вычисление произведения *hH,* равносильно вычислению матричного произведения

$$\begin{pmatrix} a & -b & -c & d \\ b & a & -d & -c \\ c & -d & a & -b \\ d & c & b & a \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \tag{25}$$

и требует 16 вещественных умножений и 12 вещественных сложений. Покажем, что число арифметических операций может быть еще более уменьшено, чем в кватернионном случае.

Лемма 3. Умножение двух элементов алгебры $\mathbf{C}^2$ общего вида может быть реализовано с помощью шести вещественных умножений и четырнадцати сложений.

Доказательство. Пусть $t = \alpha + \beta i + \gamma j + \delta ij$ и $h = a + bi + cj + dij$. Непосредственно проверяется равенство:

$$
\begin{aligned}
& t \cdot h = \\
& = \left[\left(\frac{\alpha+\delta}{2}-\frac{\beta-\gamma}{2}\right)(a+d)+\left(\frac{\beta+\gamma}{2}\right)((a-d)-(b+c))\right]+ \\
& +\left[\left(\frac{\alpha-\delta}{2}-\frac{\beta+\gamma}{2}\right)(a-d)+\left(\frac{\beta-\gamma}{2}\right)((a+d)-(b-c))\right]+ \\
& + \left[\left(\frac{\alpha+\delta}{2}+\frac{\beta-\gamma}{2}\right)(b-c)+\left(\frac{\beta-\gamma}{2}\right)((a+d)-(b-c))\right] i+ \\
& +\left[\left(\frac{\alpha-\delta}{2}+\frac{\beta+\gamma}{2}\right)(b+c)+\left(\frac{\beta+\gamma}{2}\right)((a-d)-(b+c))\right] i- \\
& -\left[\left(\frac{\alpha+\delta}{2}+\frac{\beta-\gamma}{2}\right)(b-c)+\left(\frac{\beta-\gamma}{2}\right)((a+d)-(b-c))\right] j+ \\
& +\left[\left(\frac{\alpha-\delta}{2}+\frac{\beta+\gamma}{2}\right)(b+c)+\left(\frac{\beta+\gamma}{2}\right)((a-d)-(b+c))\right] j+ \\
& +\left[\left(\frac{\alpha+\delta}{2}-\frac{\beta-\gamma}{2}\right)(a+d)+\left(\frac{\beta+\gamma}{2}\right)((a-d)-(b+c))\right] ij- \\
& -\left[\left(\frac{\alpha-\delta}{2}-\frac{\beta+\gamma}{2}\right)(a-d)+\left(\frac{\beta-\gamma}{2}\right)((a+d)-(b-c))\right] ij.
\end{aligned}
\tag{26}
$$

Второе утверждение леммы легко следует из (26) при $\gamma = \delta = 0$. Непосредственной проверкой легко убедиться также, что отображения

$$
\begin{cases}
\varepsilon_0(h) = a + bi + cj + dij, \\
\varepsilon_i(h) = a + bi - cj - dij, \\
\varepsilon_j(h) = a - bi + cj - dij, \\
\varepsilon_{ij}(h) = a - bi - cj + dij
\end{cases}
\tag{27}
$$

сохраняют сумму и произведение элементов алгебры $\mathbf{C}^2$, действуют тождественно на **R,** то есть являются автоморфизмами $\mathbf{C}^2$ над **R**.

Лемма 4. Система уравнений (27) относительно *a*, *b*, *c*, *d* разрешима при любых значениях левых частей и требует для решения не более двадцати четырех вещественных сложений.

Доказательство. Решения системы уравнений (27) определяются как

$$\begin{cases} 4a = \varepsilon_0(h) + \varepsilon_i(h) + \varepsilon_j(h) + \varepsilon_{ij}(h), \\ 4bi = \varepsilon_0(h) + \varepsilon_i(h) - \varepsilon_j(h) - \varepsilon_{ij}(h), \\ 4cj = \varepsilon_0(h) - \varepsilon_i(h) + \varepsilon_j(h) - \varepsilon_{ij}(h), \\ 4dij = \varepsilon_0(h) - \varepsilon_i(h) - \varepsilon_j(h) + \varepsilon_{ij}(h) \end{cases} \tag{28}$$

или

$$\begin{cases} 4a = \left(\varepsilon_0(h) + \varepsilon_i(h)\right) + \left(\varepsilon_j(h) + \varepsilon_{ij}(h)\right), \\ 4bi = \left(\varepsilon_0(h) + \varepsilon_i(h)\right) - \left(\varepsilon_j(h) + \varepsilon_{ij}(h)\right), \\ 4cj = \left(\varepsilon_0(h) - \varepsilon_i(h)\right) + \left(\varepsilon_j(h) - \varepsilon_{ij}(h)\right), \\ 4dij = \left(\varepsilon_0(h) - \varepsilon_i(h)\right) - \left(\varepsilon_j(h) - \varepsilon_{ij}(h)\right), \end{cases} \tag{29}$$

что и доказывает лемму.

Лемма 5. Алгебра $\mathbf{C}^2$ изоморфна прямой сумме двух алгебр комплексных чисел:

$$\mathbf{C}^2 \cong \mathbf{C} \oplus \mathbf{C}. \tag{30}$$

Доказательство. Представим элемент алгебры $\mathbf{C}^2$ в форме

$$h = a + bi + cj + dij = (a + bi) + (d - ci)ij = \alpha + \beta e, \;\; e = ij, \;\; e^2 = 1.$$

Непосредственно проверяется, что отображение $\Psi : \mathbf{C}^2 \to \mathbf{C} \oplus \mathbf{C}$, такое, что

$$h = \alpha + \beta e \mapsto (\alpha + \beta, \alpha - \beta) \in \mathbf{C} \oplus \mathbf{C} \tag{31}$$

реализует указанный изоморфизм.

Лемма 5 объясняет отчасти относительно редкое использование алгебры $\mathbf{C}^2$ в прикладных задачах. Тем не менее, у этой алгебры есть одно преимущество перед алгеброй кватернионов именно в контексте задачи синтеза совмещенных алгоритмов дискретного преобразования Фурье: при той же сложности операции сложения, операция умножения элементов алгебры $\mathbf{C}^2$ реализуется проще, чем умножение кватернионов.

2.4. Алгебры Клиффорда

Пусть **V** есть d-мерное векторное **R**-пространство с базисом $\{\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_d\}$; $Q(\mathbf{z})$ - квадратичная форма:

$$Q(\mathbf{z}) = \beta_1 z_1^2 + \ldots + \beta_d z_d^2.$$

Определение 4. Следуя [1], [2], определим алгебру Клиффорда $\mathbf{CL}(Q)$ формы $Q(\mathbf{z})$ как 2^d-мерную ассоциативную **R**-алгебру с базисом Λ из формальных произведений базисных векторов пространства **V**:

$$\Lambda = \left\{ \boldsymbol{\varepsilon}_1^{\alpha_1} \ \boldsymbol{\varepsilon}_2^{\alpha_2} \ldots \boldsymbol{\varepsilon}_d^{\alpha_d};\ \alpha_j = 0,\ 1 \right\}, \tag{32}$$

с принятыми соглашениями: $\boldsymbol{\varepsilon}_j^0 = 1, \boldsymbol{\varepsilon}_j^1 = \boldsymbol{\varepsilon}_j$.

Постулируем определяющие соотношения для умножения базисных элементов пространства **V**:

$$\boldsymbol{\varepsilon}_a \boldsymbol{\varepsilon}_b = -\boldsymbol{\varepsilon}_b \boldsymbol{\varepsilon}_a, \quad \boldsymbol{\varepsilon}_j^2 = \beta_j. \tag{33}$$

Связывая теперь с двоичными наборами индексов $(\alpha_1, \ldots, \alpha_d)$ целые числа t $(0 \le t \le 2^k - 1)$, занумеруем элементы множества Λ:

$$t = \alpha_1 + \alpha_2 \cdot 2 + \ldots + \alpha_d \cdot 2^{d-1}, \quad E_t = \boldsymbol{\varepsilon}_1^{\alpha_1} \boldsymbol{\varepsilon}_2^{\alpha_2} \ldots \boldsymbol{\varepsilon}_d^{\alpha_d}. \tag{34}$$

Соотношения (33) индуцируют правила умножения элементов базиса Λ и, следовательно, правила умножения произвольных элементов алгебры $\mathbf{CL}(Q)$

Рассмотрим несколько примеров алгебр Клиффорда.

Пример 1. Пусть d=1, $D = 2^d = 2$, $\boldsymbol{\varepsilon}_1^2 = -1$, $Q(t_1) = -t_1^2$. Тогда $\Lambda = \left\{ \boldsymbol{\varepsilon}_1^0, \boldsymbol{\varepsilon}_1^1 \right\}$; любой элемент алгебры $\mathbf{CL}(Q)$ представим в виде $\mathbf{Z} = x\boldsymbol{\varepsilon}_1^0 + y\boldsymbol{\varepsilon}_1^1$; соотношения (33) индуцируют в алгебре структуру алгебры комплексных чисел.

Пример 2. Пусть d=2, $D = 2^d = 4$, $\boldsymbol{\varepsilon}_1^2 = -1, \boldsymbol{\varepsilon}_2^2 = -1$, $Q(t_1, t_2) = -t_1^2 - t_2^2$. Тогда

$$\Lambda = \left\{ \boldsymbol{\varepsilon}_1^0 \boldsymbol{\varepsilon}_2^0, \quad \boldsymbol{\varepsilon}_1^1 \boldsymbol{\varepsilon}_2^0, \quad \boldsymbol{\varepsilon}_1^0 \boldsymbol{\varepsilon}_2^1, \quad \boldsymbol{\varepsilon}_1^1 \boldsymbol{\varepsilon}_2^1 \right\}; \tag{35}$$

любой элемент алгебры $\mathbf{CL}(Q)$ представим в виде $\mathbf{q} = x + y\boldsymbol{\varepsilon}_1 + z\boldsymbol{\varepsilon}_2 + w\boldsymbol{\varepsilon}_1\boldsymbol{\varepsilon}_2$; соотношения (33) индуцируют в алгебре структуру алгебры кватернионов.

Пример 3. Пусть d=2, $D = 2^d = 4$, $\boldsymbol{\varepsilon}_1^2 = -1, \boldsymbol{\varepsilon}_2^2 = +1, Q(t_1, t_2) = -t_1^2 + t_2^2$. Тогда, как и в предыдущем примере,

$$\Lambda = \left\{ \boldsymbol{\varepsilon}_1^0\boldsymbol{\varepsilon}_2^0, \quad \boldsymbol{\varepsilon}_1^1\boldsymbol{\varepsilon}_2^0, \quad \boldsymbol{\varepsilon}_1^0\boldsymbol{\varepsilon}_2^1, \quad \boldsymbol{\varepsilon}_1^1\boldsymbol{\varepsilon}_2^1 \right\};$$

любой элемент алгебры $\mathbf{CL}(Q)$ представим в виде $\mathbf{q} = x + y\boldsymbol{\varepsilon}_1 + z\boldsymbol{\varepsilon}_2 + w\boldsymbol{\varepsilon}_1\boldsymbol{\varepsilon}_2$.

Отображение, при котором базисные элементы преобразуются по правилам

$$\boldsymbol{\varepsilon}_1^0\boldsymbol{\varepsilon}_2^0 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \boldsymbol{\varepsilon}_1^1\boldsymbol{\varepsilon}_2^0 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$\boldsymbol{\varepsilon}_1^0\boldsymbol{\varepsilon}_2^1 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \boldsymbol{\varepsilon}_1^1\boldsymbol{\varepsilon}_2^1 \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

реализует изоморфизм алгебры $\mathbf{CL}(Q)$ и алгебры (2×2)-матриц над $\mathbf{R}$.

Далее будем предполагать, что, по крайней мере, одно из чисел $\beta_j < 0$, а остальные отличны от нуля. Положим, для определенности, что $\boldsymbol{\varepsilon}_1^2 = -1$.

Из предположений $\beta_1 = -1$, $\beta_j \neq 0$ следует:

(a) базисные элементы $\mathbf{E}_t$ обратимы;

(b) отображения

$$\sigma_j : \chi \mapsto \mathbf{E}_j^{-1} \ \chi \ \mathbf{E}_j \quad (\chi \in \mathbf{CL}(Q)) \tag{36}$$

являются (т.н. внутренними) автоморфизмами алгебры $\mathbf{CL}(Q)$;

(c) подалгебра $\mathbf{C}_1 = \{a + b\boldsymbol{\varepsilon}_1\} \subset \mathbf{CL}(Q)$ изоморфна алгебре комплексных чисел.

Лемма 6. Пусть в D-мерной ($D = 2^d$) алгебре Клиффорда $\mathbf{CL}(Q)$; выполняются условия $\beta_j \neq 0$ ($j = 1, \ldots, d$) и Δ - множество автоморфизмов (36). Пусть далее

$$\chi = f_0\mathbf{E}_0 + \ldots + f_{D-1}\mathbf{E}_{D-1}, \ f_j \in \mathbf{R} \ (\mathbf{E}_0 = 1).$$

Тогда система уравнений

$$\sigma_j(\chi) = \mathbf{b}_j, \sigma_j \in \Delta \tag{37}$$

разрешима относительно f_j при любых $\mathbf{b}_j \in \mathbf{CL}(Q)$.

Доказательство. Для d=2 разрешимость системы (37) показана ранее в разделах 2.2 и 2.3. Автоморфизмы σ_j являются линейными преобразованиями алгебры $\mathbf{CL}(Q)$, интерпретируемой как 2^d-мерное векторное пространство. Рассмотрим линейную оболочку $[\Delta]$ множества операторов σ_j. Для разрешимости системы (37) достаточно показать линейную независимость σ_j, для которой достаточно тривиальности ядра любого ненулевого оператора $\phi \in [\Delta]$. Предположим, что лемма доказана для всех $\delta < d$. Пусть Θ - ненулевой линейный оператор $\Theta : [\Delta] \to [\Delta]$ с ядром, содержащим автоморфизм

$$\sigma : \chi \mapsto \varepsilon_d^{-1} \ \chi \ \varepsilon_d,$$

и действующий тождественно на автоморфизм

$$\chi \mapsto \varepsilon_s^{-1} \chi \varepsilon_s \ \ (s \neq d).$$

Тогда равенство

$$(c_1\sigma_1 + \ldots + c_{D-1}\sigma_{D-1} + \mu_D\sigma_D)(\chi) = \mathbf{0}, \ \chi \neq \mathbf{0}, \tag{38}$$

влечет равенства

$$\Theta\big((c_1\sigma_1 + \ldots + c_{D-1}\sigma_{D-1} + \mu_D\sigma_D)(\chi)\big) = \mathbf{0},$$

$$\left(\sum_{\sigma_\tau \in T} c_\tau \sigma_\tau\right)(\chi) = \mathbf{0}. \tag{39}$$

Суммирование в (39) распространено на множество T таких автоморфизмов, для которых $\alpha_d = 0$ в произведении (34) для E_τ. Из индуктивного предположения следует, что $c_\tau = 0$ при всех $\sigma_\tau \in T$. Тогда справедливо равенство

$$\varepsilon_d^{-1}\left(\left(\sum_{\sigma_\rho \in \Sigma \setminus T} c_\rho \sigma_\rho\right)(\chi)\right)\varepsilon_d = \mathbf{0},$$

что также по индуктивному предположению влечет равенства $c_j = 0$ для остальных коэффициентов c_j в (38).

Замечание 3. Нетрудно показать, что решение линейной системы уравнений (37) требует только сложений и умножений на степени двойки. Доказательство в общем случае отличается от приведенных в разделах 2.2 и 2.3 только громоздкостью преобразований.

Лемма 7. Пусть в алгебре Клиффорда $\mathbf{CL}(Q)$ выполняются условия $\beta_1 = -1$, $\beta_j \neq 0$; $\mathbf{C}_1 \subset \mathbf{CL}(Q)$ - подалгебра с базисом $\{1, \boldsymbol{\varepsilon}_1\}$. Тогда умножение элемента $\mathbf{w} \in \mathbf{C}_1$ на элемент $\mathbf{Y} \in \mathbf{CL}(Q)$ требует $\mu = 3 \cdot 2^{d-1}$ вещественных умножений.

Доказательство. Пусть $\mathbf{w} = \mathbf{C} + \mathbf{S} \cdot \boldsymbol{\varepsilon}_1$ $(\mathbf{C}, \mathbf{S} \in \mathbf{R})$. Элемент $\mathbf{Y} \in \mathbf{CL}(Q)$ можно представить в форме $\mathbf{Y} = \mathbf{A} + \boldsymbol{\varepsilon}_1 \mathbf{B}$, где **A**, **B** - элементы подалгебры $\mathbf{CL}^{(2)}(Q)$ с базисом, порожденным элементами $\{\boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_d\}$.

Тогда, как и в случае комплексного умножения, показывается справедливость аналогов соотношений (16), откуда и следует утверждение леммы.

3. СИНТЕЗ СОВМЕЩЕННЫХ БА МНОГОМЕРНЫХ ДПФ

3.1. Двумерные алгоритмы ДПФ с совмещением в алгебре кватернионов

Теорема 1. Пусть $f(n_1, n_2)$ вещественная N-периодическая по каждому аргументу функция, N=2K, $\hat{f}(m_1,\ m_2)$- ее Фурье-спектр:

$$\hat{f}(m_1,\ m_2) = \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} f(n_1, n_2)\omega^{n_1 m_1 + n_2 m_2}\ , \tag{40}$$

$$0 \le m_1, m_2 \le N-1; \quad \omega^N = 1.$$

Тогда существует алгоритм вычисления массива $\hat{f}(m_1,\ m_2)$, требующий для реализации

$$M(N^2) = \frac{1}{2}\mu(N^2) + O(N^2), \quad A(N^2) = \frac{1}{2}\alpha(N^2) + O(N^2)$$

вещественных умножений и сложений, соответственно, где $\mu(N^2)$, $\alpha(N^2)$ есть мультипликативная и аддитивная сложности быстрого алгоритма двумерного ДПФ комплекснозначной функции.

Доказательство. Преобразуем выражение двумерного ДПФ (40) к виду:

$$\hat{f}(m_1,\ m_2) = \sum_{a,\ b=0}^{1} \omega^{am_1 + bm_2}\ \ S(m_1,\ m_2;\ a,\ b)\ , \tag{41}$$

где

$$S(m_1, m_2; a, b) = \sum_{n_1, n_2=0}^{K-1} x(2n_1 + a, 2n_2 + b)\left(\omega^2\right)^{m_1 n_1 + m_2 n_2}\ . \tag{42}$$

Положим $f_{ab}(n_1,\ n_2) = f(2n_1 + a,\ 2n_2 + b)$ и введем функцию $q(n_1,\ n_2)$ со значениями в алгебре **H**:

$$f_{00}(n_1, n_2) + f_{01}(n_1, n_2)i + f_{10}(n_1, n_2)j + f_{11}(n_1, n_2)k = q(n_1, n_2)\ . \tag{43}$$

Определим вспомогательное преобразование равенством:

$$Q(m_1,\ m_2)=\sum_{n_1,\ n_2=0}^{N_1-1} q(n_1,\ n_2)\ \left(w^2\right)^{m_1n_1+\ m_2n_2}. \qquad (44)$$

Для реконструкции $\hat{f}(m_1, m_2)$ достаточно вычислить $Q(m_1,\ m_2)$ для $m_1,\ m_2 = 0,\ 1,\ \ldots,\ N_1-1$, с помощью (44) найти $x(n_1, n_2)$:

$$\begin{aligned}
4S(m_1,\ m_2;\ 0,\ 0) &= Q(m_1,\ m_2)+Q^i(m_1,\ m_2)+Q^j(m_1,\ m_2)+Q^k(m_1,\ m_2);\\
4iS(m_1,\ m_2;\ 0,\ 1) &= Q(m_1,\ m_2)+Q^i(m_1,\ m_2)-Q^j(m_1,\ m_2)-Q^k(m_1,\ m_2);\\
4jS(m_1,\ m_2;\ 1,\ 0) &= Q(m_1,\ m_2)-Q^i(m_1,\ m_2)+Q^j(m_1,\ m_2)-Q^k(m_1,\ m_2);\\
4kS(m_1,\ m_2;\ 1,\ 1) &= Q(m_1,\ m_2)-Q^i(m_1,\ m_2)-Q^j(m_1,\ m_2)+Q^k(m_1,\ m_2),
\end{aligned} \qquad (45)$$

где

$$Q^i(m_1,\ m_2)=\varepsilon_i\left(Q(m_1,\ m_2)\right),\ Q^j(m_1,\ m_2)=\varepsilon_j\left(Q(-m_1,\ -m_2)\right),$$

$$Q^k(m_1,\ m_2)=\varepsilon_k\left(Q(-m_1,\ -m_2)\right),$$

а также выполнить $3(N_1-1)^2$ умножений на степени константы w в соотношении (41).

Таким образом, вычислительная сложность преобразований (44), следовательно и (40) определяется, в основном, сложностью кватернионного аналога двумерного БПФ.

Еще одним приложением алгебры кватернионов является развитие собственно кватернионного дискретного спектрального анализа. Рассмотрим дискретное ортогональное преобразование, значения базисных функций которого лежат в различных экземплярах алгебры комплексных чисел, вложенных в алгебру кватернионов.

Определение 5. Кватернионным ДПФ будем называть преобразование

$$F(m_1,\ m_2)=\sum_{n_1=0}^{N-1}\sum_{n_2=0}^{N-1} e^{2\pi i n_1 m_1/N} f(n_1, n_2) e^{2\pi j n_2 m_2/N}. \qquad (46)$$

Входной сигнал может быть вещественным, комплексным или кватернионным. Во всех случаях остаются в силе "стандартные" алгоритмы разной структуры, не

учитывающие специфику преобразуемого массива. Отличие от алгоритмов канонического двумерного ДПФ заключается только в учете некоммутативности умножения в алгебре кватернионов: при вынесении общего множителя i-кватернион выносится налево, j-кватернион – направо.

Если преобразуемый массив вещественный, то для вычисления кватернионного спектра применяется уже описанный метод совмещения: формируется вспомогательная последовательность (43) и т.д. Несколько иной вид приобретает система соотношений (45) для определения частичных кватернионных спектров.

3.2. Двумерные алгоритмы ДПФ с совмещением в коммутативной гиперкомплексной алгебре

Так как сложность операций умножения комплексного числа на гиперкомплексное такая же, как и у операции умножения комплексного числа на кватернион, то сложность "совмещенных" алгоритмов двумерного ДПФ вещественного массива с совмещением в алгебре $\mathbf{C}^2$ для вещественного входного сигнала примерно в два раза ниже, как и в случае одномерного совмещенного алгоритма, чем у алгоритма, в котором не учитывается вещественность входного сигнала, и зависит от структуры применяемого алгоритма вычисления вспомогательного гиперкомплексного ДПФ. Несколько иная ситуация возникает при рассмотрении "гиперкомплексных спектров".

Определение 6. Гиперкомплексным ДПФ будем называть преобразование

$$F(m_1,\ m_2) = \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} f(n_1, n_2) e^{2\pi i n_1 m_1 / N} e^{2\pi j n_2 m_2 / N}. \qquad (47)$$

С учетом Леммы 3 и с использованием рассмотренных во введении схем редукции и принципа совмещения, получаем алгоритмы вычисления преобразования (47).

3.3. Алгоритмы многомерных ДПФ с совмещением в алгебрах Клиффорда

Обобщением приведенного выше примера одномерного совмещенного БПФ является БА с многократным совмещением для d-мерного ДПФ (или для ДОП с базисом из функций Виленкина-Крестенсона):

$$\hat{f}(\mathbf{m}) = \sum_{\mathbf{n}\in\Gamma_N} f(\mathbf{n})\ \omega^{\langle \mathbf{n},\mathbf{m}\rangle},\ \mathbf{m}\in\Gamma_N, \omega = \exp\left\{2\pi i/N\right\} = \exp\left\{2\pi\varepsilon_1/N\right\}, N = 2^r. \quad (48)$$

Теорема 2. Пусть $g(\mathbf{n})\in\mathbf{R}$, $\mathbf{n}\in\mathbf{Z}^d$, $N=2^r$. Пусть далее $M\left(N^d\right)$ - вещественная мультипликативная сложность алгоритма d-мерного ДПФ (48) комплексного массива $f(\mathbf{n})$. Тогда существует алгоритм вычисления ДПФ вещественного массива $g(\mathbf{n})$ с мультипликативной сложностью

$$M_F^R(N\times N) = 4M_F^R\left(N/2\times N/2\right) + 6\cdot 2\cdot\left(N^2/2\right) + 9\left(N^2/16\right). \quad (49)$$

Доказательство. Рассмотрим алгебру Клиффорда $\mathbf{CL}(Q)$ с принятыми ранее условиями: $\beta_1 = -1, \beta_j \neq 0$. Пусть $\mathbf{w} = \cos 2\pi/N + \boldsymbol{\varepsilon}_1 \sin 2\pi/N$ - первообразный корень степени N из единицы в подалгебре $\mathbf{G}_1$ с базисом $\{1, \boldsymbol{\varepsilon}_1\}$. Пусть A - множество d-мерных бинарных векторов $\mathrm{A} = \left\{a = (\alpha_1, \ldots, \alpha_d);\ \alpha_j = 0, 1\right\}$. Представляя входной массив $G = g(\mathbf{n})$ в виде объединения массивов

$$G = \{g(\mathbf{n})\} = \bigcup_{\mathbf{a}\in\mathrm{A}} G_{\mathbf{a}} = \bigcup_{\mathbf{a}\in\mathrm{A}} \{g(2\mathbf{n}+\mathbf{a})\},$$

рассмотрим вспомогательную функцию $\mathbf{G}(\mathbf{n})$ со значениями в алгебре $\mathbf{CL}(Q)$:

$$\mathbf{G}(\mathbf{n}) = \sum_{\mathbf{a}\in\mathrm{A}} g(2\mathbf{n}+\mathbf{a})\mathbf{E}_{\mathbf{a}} \qquad (\mathbf{E}_{\mathbf{a}} = \boldsymbol{\varepsilon}_1^{\alpha_1}\boldsymbol{\varepsilon}_2^{\alpha_2}\ldots\boldsymbol{\varepsilon}_d^{\alpha_d}) \quad (50)$$

и вспомогательное преобразование функции $\mathbf{G}(\mathbf{n})$:

$$\hat{\mathbf{G}}(\mathbf{m}) = \sum_{\mathbf{n}\in\Gamma_K} \mathbf{G}(\mathbf{n})\mathbf{w}^{\langle \mathbf{n},\mathbf{m}\rangle} \qquad (\mathbf{m}\in\Gamma_K). \quad (51)$$

Пусть далее $\hat{\mathbf{G}}_{\mathbf{a}}(\mathbf{m})$ - "частичные спектры":

$$\hat{\mathbf{G}}_{\mathbf{a}}(\mathbf{m}) = \sum_{\mathbf{n}\in\Gamma_K} g(2\mathbf{n}+\mathbf{a})\ \mathbf{w}^{2\langle \mathbf{n},\ \mathbf{m}\rangle}. \quad (52)$$

Тогда ДПФ $\hat{g}(\mathbf{m})$ массива $g(\mathbf{n})$ и $\hat{\mathbf{G}}_{\mathbf{a}}(\mathbf{m})$ связаны соотношением:

$$\hat{g}(\mathbf{m}) = \sum_{\mathbf{a}\in \mathrm{A}} \hat{\mathbf{G}}_{\mathbf{a}}(\mathbf{m})\mathbf{w}^{\langle \mathbf{a},\mathbf{m}\rangle} \quad (\mathbf{m} \in \Gamma_N). \tag{53}$$

Вычисление преобразования (51) - "клиффордового аналога ДПФ" при $K = 2^{r-1}$, например, может быть проведено по схеме БПФ Кули-Тьюки или любой из его многочисленных модификаций. Объем области суммирования в (51) равен K^d, то есть в 2^d раз меньше, чем у преобразования (48). Сложность одного умножения на степень элемента $\mathbf{w}$ в 2^{d-1} раз больше, чем сложность одного комплексного умножения. Далее, из (52) следует возможность нахождения частичных спектров $\hat{\mathbf{G}}_{\mathbf{a}}(\mathbf{m})$ при известном $\hat{\mathbf{G}}(\mathbf{m})$. При решении системы уравнений для определения $\hat{\mathbf{G}}_{\mathbf{a}}(\mathbf{m})$ выполняются только умножения на степени двойки, которые, как обычно принято, не учитываются при анализе мультипликативной сложности алгоритма. Реконструкция полного спектра $\hat{g}(\mathbf{m})$ по формуле (53) требует $O\left(N^d\right)$ вещественных умножений, причем константа в символе "O" не зависит от N и d.

4. АЛГОРИТМЫ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ ПРЕОБРАЗОВАНИЙ, РЕАЛИЗУЕМЫЕ В ЦИКЛОТОМИЧЕСКИХ КОДАХ

4.1. Циклотомические коды

Рассмотрим схему декомпозиции ДПФ "по основанию p". Пусть $N = p^r$. Тогда для $m = 0, 1, ..., N/p - 1$ Фурье-спектр $\hat{f}(m)$ может быть представлен в виде:

$$\begin{pmatrix} \hat{f}(m) \\ \hat{f}\left(m + N/p\right) \\ \hat{f}\left(m + 2N/p\right) \\ \dots \\ \hat{f}\left(m + (p-1)N/p\right) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \gamma & \dots & \gamma^{p-1} \\ 1 & \gamma^2 & \dots & \gamma^{2(p-1)} \\ & & \dots & \\ 1 & \gamma^{p-1} & \dots & \gamma^{(p-1)^2} \end{pmatrix} \begin{pmatrix} \hat{f}_0(m) \\ \omega^m \hat{f}_1(m) \\ \omega^{2m} \hat{f}_2(m) \\ \dots \\ \omega^{(p-1)m} \hat{f}_{p-1}(m) \end{pmatrix}, \qquad (54)$$

где $\hat{f}_j(m)$ $(j = 0, 1, ..., p-1)$ - ДПФ длины N/p:

$$\hat{f}_j(m) = \sum_{n=0}^{\frac{N}{p}-1} f(pn + j)\left(\omega^p\right)^{mn}, \qquad (55)$$

а $\omega = \exp\left\{2\pi i/N\right\}$, $\gamma = \exp\left\{2\pi i/p\right\}$ есть первообразные корни из единицы степени N и p соответственно.

Равенства (54), (55) сводят вычисление ДПФ длины N к вычислению p раз ДПФ длины N/p с последующей последовательной редукцией к вычислению одноточечных преобразований. Спецификой случая $N = p^r$ при $p \neq 2, 4$ является наличие в правой части (54) умножений на степени константы γ, что увеличивает вычислительную сложность алгоритма по сравнению с БПФ по основанию 2 и 4, где аналогичные умножения тривиальны (умножение на $\pm 1, \pm i$).

В связи с этим возникает идея: коль скоро в общей вычислительной сложности алгоритма удельный вес умножения на константы γ относительно велик, то

преобразуемые данные надо представлять в таком виде, чтобы умножения на эти константы были бы, по возможности, просты в реализации.

Пусть, по-прежнему, $\gamma = \exp\left\{2\pi i/p\right\}$ - первообразный комплексный корень степени p из единицы. Тогда для комплексного числа c наряду с обычной алгебраической формой представления $c = a + bi$ возможна и форма

$$c = c_1\gamma + c_2\gamma^2 + \ldots + c_{p-1}\gamma^{p-1} = a + bi \ , \qquad (56)$$

где вещественные $c_1, \ldots, c_{p-1}$ связаны с вещественными a, b соотношениями

$$\begin{cases} a = \sum_{k=1}^{p-1} c_k \cos 2\pi k/p, \\ b = \sum_{k=1}^{p-1} c_k \sin 2\pi k/p. \end{cases}$$

Упорядоченный набор из (p-1) числа $\left(c_1, \ldots, c_{p-1}\right)$, ассоциированный с представлением числа c в форме (56), будем называть γ-кодом числа c.

Арифметические действия над комплексными числами индуцируют правила действий над кодами. Сложение чисел в γ-кодах производится покомпонентно, умножение чисел в γ-кодах сводится к нахождению циклической свертки γ-кодов. Умножения на $\gamma, \gamma^2, \ldots, \gamma^{p-1}$ выполняются с помощью γ-кодов без вещественных умножений и сводятся лишь к смене знака.

Пример 4. Пусть p=3, $N = 3^k$,

$$\gamma = \exp\left(2\pi i/3\right) = \tfrac{1}{2}\left(-1 + i\sqrt{3}\right), \quad \overline{\gamma} = \tfrac{1}{2}\left(-1 - i\sqrt{3}\right) \ ,$$

тогда соотношение (56) примет вид:

$$c = a + bi = x\gamma + y\overline{\gamma},$$

где

$$x = \left(b/\sqrt{3}\right) - a, \quad y = \left(-b/\sqrt{3}\right) - a \ .$$

Арифметические операции над кодами тогда реализуются по формулам:

$$(x, y)+(u, v)=(x+u, y+v) \quad , \tag{57}$$

$$(x, y)\cdot(u, v)=((y-x)(v-u)-xu, (y-x)(v-u)-yv) \quad ,$$

то есть сложность операций сложения и умножения в кодах совпадает со сложностью сложения и умножения комплексных чисел, а именно, сложение в кодах реализуется при помощи двух вещественных сложений, умножение в кодах реализуется через три вещественных умножения и три вещественных сложения (предполагается, что сложения компонент кода базисных функций выполнены заранее).

Умножение на числа γ и $\overline{\gamma}$, имеющие соответственно коды (1,0) и (0,1) реализуется наиболее просто:

$$\begin{aligned}(1,0)\cdot(u, v)&=(-v, u-v)\\ (0,1)\cdot(u, v)&=(v-u, -u)\end{aligned} \quad ,$$

и не содержит нетривиальных вещественных умножений.

4.2. Алгоритмы одномерных ДОП, реализуемые в циклотомических кодах

Указанное выше в Примере 4 представление комплексных чисел позволяет снизить вычислительную сложность алгоритма ДПФ именно благодаря простой реализации умножений на степени γ, удельный вклад которых в быстрый алгоритм ДПФ, реализуемый посредством (54), весьма высок.

Пример 5. Соотношение (54) при p=3 принимает вид:

$$\begin{pmatrix} \hat{f}(m) \\ \hat{f}\left(m+N/3\right) \\ \hat{f}\left(m+2N/3\right) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \gamma & \overline{\gamma} \\ 1 & \overline{\gamma} & \gamma \end{pmatrix} \begin{pmatrix} \hat{f}_0(m) \\ \omega^m \hat{f}_1(m) \\ \omega^{2m} \hat{f}_2(m) \end{pmatrix}. \tag{58}$$

Нетрудно показать, что оценки вычислительной сложности такого алгоритма для вещественного сигнала имеют вид:

$$M^R(N) \le N\log_3 N - N \, , \quad A^R(N) \le 3N\log_3 N + N/3 \, , \tag{59}$$

где $M^R(N)$, $A^R(N)$ - число вещественных умножений и сложений, соответственно.

Пример 6. Представим ненормированное дискретное косинусное преобразования (ДКП) нечетной длины N в форме

$$\hat{x}(m)=\sum_{n=0}^{N-1}x(n)\cos\left(\pi\frac{(2n+1)m}{2N}\right)=\mathrm{Re}\left\{\sum_{n=0}^{N-1}x(n)\omega^{(2n+1)m}\right\}, \tag{60}$$

где $\omega=\exp\left\{2\pi i/4N\right\}$ - первообразный корень степени $4N$ из единицы. Пусть

$$y(k)=\begin{cases}x(n) & \text{при } k=2n+1;\\ 0 & \text{при } k=2n;\end{cases}$$

тогда соотношение (60) примет вид:

$$\hat{x}(m)=\mathrm{Re}\left\{\sum_{n=0}^{2N-1}y(k)\omega^{km}\right\}. \tag{61}$$

При нечетном N числа 4 и N взаимно просты, декомпозиция Гуда-Томаса по формулам (11), (12) при P=4 и Q=N выполняется без дополнительных умножений. Преобразование индексов, ограничения на диапазон изменения индексов m и k, а также обращение в нуль функции $y(k)$ при четных k выделяют в двумерных массивах размера $4\times N$ “допустимые” подмножества K и M для пар (k_1,k_2) и (m_1,m_2). Тогда нетрудно показать, что вычисление ДКП (60) сводится к вычислению преобразования:

$$Y(m_1,m_2)=\sum_{k_2=0}^{3}\left(\sum_{k_1=0}^{N-1}\tilde{y}(k_1,k_2)\beta^{k_1m_1}\right)i^{k_2m_2}. \tag{62}$$

Так как “допустимое” подмножество индексов K сформировано так, что $\tilde{y}(k_1,k_2)$ отлично от нуля только для $(k_1,k_2)\in K$, то и суммирование в (62) выполняется только при $(k_1,k_2)\in K$, то есть при $k_2=1,3$. Этот факт позволяет привести выражение (62) к виду:

$$\hat{x}(m)=\mathrm{Re}\left\{i^{m_2}\sum_{k_1=0}^{N-1}z(k_1)\beta^{k_1m_1}\right\}, \tag{63}$$

где

$$z(k_1)=\begin{cases}\tilde{y}(k_1,1) & \text{при} \quad (k_1,1)\in K\\ \tilde{y}(N-k_1,3) & \text{при} \quad (k_1,3)\in K\end{cases},\quad \beta=\exp\left\{\frac{2\pi i}{N}\right\}.$$

Таким образом, ДКП нечетной длины N сведено к вещественному преобразованию Фурье той же длины. При $N=3^r$ и использовании ДПФ, описанного в Примере 2, оценки сложности вычисления массива (63) имеют вид :

$$M(N)=N\log_3 N-N,\quad A(N)=3N\log_3 N-\tfrac{2}{3}N. \tag{64}$$

При попытке непосредственного перенесения основной идеи алгоритма Примера 6 (представления данных в виде линейной комбинации корней третьей степени из единицы) на случай, когда преобразуемый массив принадлежит конечному полю **GF**(p) возникает ряд принципиальных затруднений.

Во-первых, для реализации метода совмещенного вычисления ТЧП-спектра

$$\hat{x}(m)=\sum_{n=0}^{N-1}x(n)\omega^{mn}\pmod{p},\ \omega^N\equiv 1\pmod{p}; \tag{65}$$

по аналогии с комплексным случаем, достаточно, чтобы корни γ_1,γ_2 сравнения

$$F(t)=t^2+t+1\equiv 0\pmod{p} \tag{66}$$

лежали в квадратичном расширении **GF**(p^2) поля **GF**(p), но не лежали в **GF**(p) (то есть, были бы "существенно модулярно-комплексными"). В этом случае основная идея вычисления ТЧП длины N=$2K$=$2\cdot 3^r$ является комбинацией идеи комплексного совмещения и идеи представления данных в γ-кодах.

Несколько иная ситуация и определенные трудности возникают при $\gamma_1,\gamma_2,\omega\in$ **GF**(p). В этом случае и преобразуемая последовательность, и параметры преобразования (65) имеют "однокомпонентное" представление, характерное для элементов поля **GF**(p), что исключает возможность непосредственного применения общей схемы для совмещенного вычисления спектра (65) (в поле **GF**(p) "мало автоморфизмов").

Так как при простом p число (p-1) всегда четно, то условие на p, разграничивающее эти два случая, следует из теоремы Лагранжа.

Предложение 1. Пусть $N=2K=2\cdot 3^r$, p – простое число.

(a) Если $(p-1)\neq 0 \pmod K$, но $(p+1)\equiv 0 \pmod K$, то корни γ_1,γ_2 сравнения (66) лежат в $\mathbf{GF}\left(p^2\right)\setminus\mathbf{GF}(p)$.

(b) Если $(p-1)\equiv 0 \pmod K$, то корни γ_1,γ_2 сравнения (66) лежат в **GF**(p).

Принципиальным для нас случаем является (b). Отметим, что алгоритм, который будет описан ниже, не дает ощутимого выигрыша в сложности по сравнению с "обычной" реализацией ТЧП длины $K=3^r$.

Рассмотрим двумерную алгебру **A** над **GF**(p) с базисом $\mathbf{g}_1,\mathbf{g}_2$:

$$\mathbf{A}=\{\mathbf{z}:\quad \mathbf{z}=z_1\mathbf{g}_1+z_2\mathbf{g}_2;\quad z_1,z_2\in\mathbf{GF}(p)\}$$

и правилами умножения базисных элементов

$$\mathbf{g}_1\cdot\mathbf{g}_1=\mathbf{g}_2,\quad \mathbf{g}_2\cdot\mathbf{g}_2=\mathbf{g}_1,\quad \mathbf{g}_1\cdot\mathbf{g}_2=-\mathbf{g}_1-\mathbf{g}_2.$$

(Иными словами, элементы $\mathbf{g}_1,\mathbf{g}_2$ "ведут себя" как корни уравнения (66) *не будучи таковыми*, они линейно независимы над **GF**(p)).

Отметим также, что отображение

$$\tau:\ \mathbf{z}=z_1\mathbf{g}_1+z_2\mathbf{g}_2\rightarrow\tau(\mathbf{z})=z_1\mathbf{g}_2+z_2\mathbf{g}_1 \qquad (67)$$

является автоморфизмом алгебры **A.**

Лемма 7. Для любой последовательности элементов $\mathbf{z}(n)\in$ **GF**(p) и первообразного корня $\omega\in$ **GF**(p) степени K существуют такие элементы $\mathbf{z}(n)$, $\mathbf{w}\in$ **A** и такое отображение $\Psi:\mathtt{A}\rightarrow\mathtt{GF}(p)$, что выполняются соотношения:

(a) $\Psi(\mathbf{z}(n))=z(n)$;

(b) $\Psi(\mathbf{w})=\omega$;

(c) если $\mathbf{w}=a\mathbf{g}_1+b\mathbf{g}_2$, то $\Psi(b\mathbf{g}_1+a\mathbf{g}_2)=\omega^{-1}$.

Доказательство. Условия (a)-(b) выполняются тривиально. Действительно, в силу простоты числа p, уравнение

$$A\gamma_1+B\gamma_2=C$$

в поле **GF**(p) относительно A, B имеет ровно p решений – пар (A, B). Единственным нетривиальным условием является (c). Оно равносильно существованию в поле **GF**(p) элементов с условием

$$(a\gamma_1 + b\gamma_2)(b\gamma_1 + a\gamma_2) = 1,$$

или, что тоже самое, с условием

$$(ab - a^2 - b^2)\gamma_1 + (ab - a^2 - b^2)\gamma_2 = -(\gamma_1 + \gamma_2),$$

что, в свою очередь, равносильно условию разрешимости уравнения

$$a^2 - ab + b^2 - 1 = 0.$$

Рассматривая последнее уравнение как квадратное относительно a, легко установить, что существование решения зависит от существования такого элемента b, что $\Delta = 4 - 3b^2$ является квадратом в **GF**(p). Но если b пробегает **GF**(p), то Δ принимает $\left(p+1/2\right)$ различных значений, а в **GF**(p) существует только $\left(p-1/2\right)$ элементов, не являющихся квадратами.

Опишем алгоритм вычисления ТЧП (65) для случая (b) Предложения 1. Будем считать, что соответствующие представления входных данных и параметров преобразования определены в соответствии с Леммой 7.

Шаг 1.Формирование вспомогательной функции.

Для входной последовательности преобразования (65) длины $N=2K=2\cdot 3^r$ положим:

$$\mathbf{z}(n) = x(2n)\mathbf{g_1} + x(2n+1)\mathbf{g_2}.$$

Шаг 2. Вычисление вспомогательного преобразования в алгебре **A**.

Вычисляем преобразование вспомогательной функции $\mathbf{z}(n)$:

$$\hat{\mathbf{z}}(m) = \sum_{n=0}^{K-1} \mathbf{z}(n)\mathbf{w}^{mn}.$$

Шаг 3. Формирование системы уравнений для "частичных спектров" в алгебре **A**.

Пусть автоморфизм τ определен равенством (67). Тогда система уравнений

$$\begin{cases} \hat{\mathbf{z}}(m) = \sum_{n=0}^{K-1} (x(2n)\mathbf{g_1} + x(2n+1)\mathbf{g_2})\mathbf{w}^{mn} \\ \tau(\hat{\mathbf{z}}(m)) = \sum_{n=0}^{K-1} (x(2n)\mathbf{g_2} + x(2n+1)\mathbf{g_1})\mathbf{w}^{mn} \end{cases}$$

равносильна системе уравнений

$$\begin{cases} \hat{\mathbf{z}}(m) + \tau(\hat{\mathbf{z}}(-m)) = (\mathbf{g_1} + \mathbf{g_2}) \sum_{n=0}^{K-1} (x(2n) + x(2n+1))\mathbf{w}^{mn} \\ \hat{\mathbf{z}}(m) - \tau(\hat{\mathbf{z}}(-m)) = (\mathbf{g_1} - \mathbf{g_2}) \sum_{n=0}^{K-1} (x(2n) - x(2n+1))\mathbf{w}^{mn}. \end{cases} \quad (68)$$

Шаг 4. Формирование системы уравнений для "частичных спектров" в **GF**(p). Действуя на уравнения системы (68) отображением Ψ, получаем систему уравнений в поле **GF**(p):

$$\begin{cases} \Psi(\hat{\mathbf{z}}(m) + \tau(\hat{\mathbf{z}}(-m))) = (\gamma_1 + \gamma_2)\left[\sum_{n=0}^{K-1} x(2n)\omega^{mn} + \sum_{n=0}^{K-1} x(2n+1)\omega^{mn}\right] \\ \Psi(\hat{\mathbf{z}}(m) - \tau(\hat{\mathbf{z}}(-m))) = (\gamma_1 - \gamma_2)\left[\sum_{n=0}^{K-1} x(2n)\omega^{mn} - \sum_{n=0}^{K-1} x(2n+1)\omega^{mn}\right]. \end{cases} \quad (69)$$

Шаг 5. Вычисление "частичных спектров" в поле **GF**(p).

Из системы уравнений (69) определяем "частичные спектры

$$\begin{cases} \hat{x}_0(m) = \sum_{n=0}^{K-1} x(2n)\omega^{mn} \\ \hat{x}_1(m) = \sum_{n=0}^{K-1} x(2n+1)\omega^{mn}. \end{cases}$$

Шаг 6. Реконструкция "полного" ТЧП - спектра.

Реконструкция ТЧП-спектра, как и в комплексном случае, осуществляется по формуле

$$\hat{x}(m) = \hat{x}_0(m) + \xi^m \hat{x}_1(m),$$

где ξ - первообразный корень степени N в поле **GF**(p).

4.3. Коды Гамильтона Эйзенштейна

Использование представлений элементов **R**-алгебр, размерностей больших двух приводит к синтезу БА многомерных ДОП с уменьшенной вычислительной сложностью.

Пусть кватернионы γ_1 и γ_2 - примитивные корни третьей степени из единицы, лежащие в различных экземплярах поля комплексных чисел $\mathbf{C}_1 = \mathbf{R}(i)$ и $\mathbf{C}_2 = \mathbf{R}(j)$, каноническим образом вложенных в **H**:

$$\gamma_1 = \exp\left\{2\pi i/3\right\}, \gamma_2 = \exp\left\{2\pi j/3\right\};$$

кватернионы $\overline{\gamma}_1$ и $\overline{\gamma}_2$ - соответствующие образы в **H** элементов, сопряженных в $\mathbf{C}_1$ и $\mathbf{C}_2$ элементами γ_1 и γ_2:

$$\overline{\gamma}_1 = \exp\left\{-2\pi i/3\right\}, \overline{\gamma}_2 = \exp\left\{-2\pi j/3\right\}.$$

Кватернионы $q = q_0 + q_1 i + q_2 j + q_3 k$ с $q_2 = q_3 = 0$ уже договорились называть *i*-кватернионами. Аналогично определяются *j*- и *k*-кватернионы.

Ряд свойств алгебры кватернионов сформулируем для удобства чтения в форме лемм. Автор счел возможным опустить доказательства, сводящиеся к непосредственной проверке тождеств для комплексных чисел.

Лемма 8. Для любого $q \in \mathbf{H}$ существуют единственные a, b, c, $d \in \mathbf{R}$ такие, что справедливо представление:

$$q = \left(a\gamma_1 + b\overline{\gamma}_1\right)\gamma_2 + \left(c\gamma_1 + d\overline{\gamma}_1\right)\overline{\gamma}_2. \qquad (70)$$

Определение 7. Четверку вещественных чисел (*a, b, c, d*) в представлении (70) для *q* назовем кодом Гамильтона-Эйзенштейна кватерниона *q* и будем обозначать $\langle q \rangle$.

В частности, кватернионы специального вида имеют коды:

$$\langle q_0 + q_1 \quad i \rangle = (a,\ b,\ a,\ b), \text{ где } q_0 = \frac{1}{2}(a+b),\ q_1 = \frac{\sqrt{3}}{2}(b-a),$$

$$\langle q_0 + q_2 \quad j \rangle = (a,\ a,\ c,\ c), \text{ где } q_0 = \frac{1}{2}(a+c),\ q_1 = \frac{\sqrt{3}}{2}(c-a),$$

$$\langle \gamma_1 \rangle = (-1,\ 0,\ -1,\ 0),\ \langle \overline{\gamma}_1 \rangle = (0,\ -1,\ 0,\ -1),$$
$$\langle \gamma_2 \rangle = (-1,\ -1,\ 0,\ 0),\ \langle \overline{\gamma}_2 \rangle = (0,\ 0,\ -1,\ -1).$$

Далее, если $q = a \in \mathbf{R}$, то $\langle q \rangle = (a,\ a,\ a,\ a)$.

Операции в теле кватернионов и автоморфизмы $\mathbf{H}$ как четырехмерной $\mathbf{R}$-алгебры индуцируют преобразования ассоциированных кодов.

Лемма 9. *Пусть* $\langle q \rangle = (a,\ b,\ c,\ d)$, $s \in \mathbf{C}_1$, $t \in \mathbf{C}_2$, $\langle s \rangle = (\alpha,\ \beta,\ \alpha,\ \beta)$, $\langle t \rangle = (\sigma,\ \sigma,\ \tau,\ \tau)$.

Тогда

$$\begin{aligned} \langle sq \rangle = &\big((\beta-\alpha)(a-b)+\alpha a,\ (\beta-\alpha)(a-b)+\beta b\big),\\ &(\beta-\alpha)(c-d)+\alpha c,\ (\beta-\alpha)(c-d)+\beta d, \end{aligned} \tag{71}$$

$$\langle qt \rangle = \begin{pmatrix} (\tau-\sigma)(a-c)+\sigma a,\ (\tau-\sigma)(b-d)+\sigma b,\\ (\tau-\sigma)(a-c)+\tau c,\ (\tau-\sigma)(b-d)+\tau d \end{pmatrix}. \tag{72}$$

В частности,

$$\langle \gamma_1\ \ q \rangle = (-b,\ a-b,\ -d,\ c-d),\ \langle \overline{\gamma}_1\ \ q \rangle = (b-a,\ -a,\ d-c,\ -c),$$

$$\langle\ q\ \ \gamma_2 \rangle = (-c,\ -d,\ a-c,\ b-d),\ \langle q\ \ \overline{\gamma}_2 \rangle = (c-a,\ d-b,\ -a,\ -b).$$

Таким образом, умножения (71) и (72) кватерниона q общего вида на i- или j-кватернионы требуют не более шести нетривиальных вещественных умножений и шести вещественных сложений (если считать, что сложения компонент кодов i- и j-кватернионов выполнены заранее); умножения кватернионов q общего вида на γ_1, $\overline{\gamma}_1$, γ_2 или $\overline{\gamma}_2$ требуют только двух вещественных сложений. Непосредственное последовательное умножение кватерниона общего вида на i- и j-кватернионы требует 12 вещественных умножений. Покажем, что одновременное выполнение такой пары умножений требует в 1,5 раза меньшего числа вещественных умножений.

Лемма 10. Пусть q – кватернион общего вида, s – i-кватернион, t – j-кватернион. Тогда вычисление кода произведения sqt требует не более девяти нетривиальных вещественных умножений и пятнадцати вещественных сложений.

Доказательство. Последовательным применением (71) и (72) получаем равенство:

$$\begin{aligned}\langle sqt\rangle = \big((\tau-\sigma)\big[(\beta-\alpha)(d-c-b+a)-\alpha\ \ (c-a)\big]-\sigma\ \ (\beta-\alpha)(b-a)+\sigma\alpha a+\\ +(\tau-\sigma)\big[(\beta-\alpha)(d-c-b+a)-\beta\ \ (d-b)\big]-\sigma\ \ (\beta-\alpha)(b-a)+\sigma\beta b+\\ +(\tau-\sigma)\big[(\beta-\alpha)(d-c-b+a)-\alpha\ \ (c-a)\big]-\tau\ \ (\beta-\alpha)(d-c)+\tau\alpha c+\\ +(\tau-\sigma)\big[(\beta-\alpha)(d-c-b+a)-\beta\ \ (d-b)\big]-\tau\ \ (\beta-\alpha)(d-c)+\tau\beta d\big).\end{aligned}$$

Также непосредственно легко убедиться, что автоморфизмы ε_i, ε_j и ε_k алгебры **H** над **R**:

$$\varepsilon_i : q \mapsto i^{-1}q\ \ i,\ \varepsilon_j : q \mapsto j^{-1}q\ \ j,\ \varepsilon_k : q \mapsto k^{-1}q\ \ k$$

индуцируют преобразования кодов, описываемые следующим предложением.

Лемма 11. Пусть $\langle q\rangle = (a,\ b,\ c,\ d)$, тогда

$$\langle \varepsilon_i(q)\rangle = (c,\ d,\ a,\ b),\ \langle \varepsilon_j(q)\rangle = (b,\ a,\ d,\ c),\ \langle \varepsilon_k(q)\rangle = (d,\ c,\ b,\ a),$$

и, следовательно, переход от кватерниона q к его автоморфному образу реализуется в кодах тривиально.

Лемма 12. Пусть $\langle q\rangle = (a,\ b,\ c,\ d)$, тогда

$$\langle (d-b-c)\ \ \gamma_1 + (a-b-c)\ \ \overline{\gamma}_1\rangle = (a,\ b,\ c,\ d)\ \ \mathbf{L},$$

где

$$\mathbf{L} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ 1 & 0 & 1 & 0 \end{pmatrix},$$

причем кватернион $(d-b-c)\ \ \gamma_1 + (a-b-c)\ \ \overline{\gamma}_1 = q'$ получен из кватерниона q формальной заменой в представлении (70) элементов γ_2 и $\overline{\gamma}_2$ элементами γ_1 и $\overline{\gamma}_1$ с последующим применением тождеств: $\gamma_1 + \overline{\gamma}_1 = -1,\ \gamma_1 \cdot \overline{\gamma}_1 = 1$.

Лемма 13. Пусть $s \in \mathbf{C}_1$, $\langle s\rangle = (\alpha,\ \beta,\ \alpha,\ \beta)$,

$$\mathbf{V}=\frac{1}{2}\begin{pmatrix}1+i & \sqrt{3}\\ 1-i & \sqrt{3}\\ 0 & \\ 0 & \end{pmatrix}.$$

Тогда справедливо равенство:

$$\mathrm{Re}\ \ s+i\ \mathrm{Im}\ \ s=(\alpha,\ \beta,\ \alpha,\ \beta)\mathbf{V}.$$

Леммы 12 и 13 обеспечивают возможность рассмотрения ДОП как "проекций" некоторых вспомогательных преобразований, базисные функции которых принимают значения не в изоморфных копиях алгебры **C**, а являются кватернионами общего вида. Это позволяет более полно учесть симметрии алгебры **H**, ассоциированные с ее автоморфизмами.

4.4. Быстрый алгоритм двумерного ДПФ

Пусть $f(n_1,\ n_2)\in\mathbf{R}$ - преобразуемый двумерный $(N\times N)$-массив, $N=3^r$, $F(m_1,\ m_2)$ - двумерный дискретный спектр Фурье:

$$F(m_1,\ m_2)=\sum_{n_1,\ n_2=0}^{N-1} f(n_1,\ n_2)\omega^{n_1m_1+\ n_2\ m_2},\ \omega=\exp\left\{2\pi i/N\right\}. \qquad (73)$$

Рассмотрим $\tilde{F}(m_1,\ m_2)$ - двумерный кватернионный спектр (46). Комплексные корни ω_1, ω_2 будем считать заданными кодами Гамильтона-Эйзенштейна. Из Лемм 12 и 13 следует следующее утверждение.

Лемма 14. Пусть матрицы **L** и **V** определены в Леммах 12 и 13. Тогда

$$F(m_1,\ m_2)=\left\langle\tilde{F}(m_1,\ m_2)\right\rangle\mathbf{LV}.$$

Таким образом, вычисление спектра $F(m_1,\ m_2)$ только $2N$ вещественными умножениями отличается от вычисления кватернионного спектра (46). Представление кватернионов кодами позволяет учесть мультипликативную тривиальность умножения на константы γ_1, γ_2 в быстрых алгоритмах. Вычисление спектра $F(m_1,\ m_2)$ с помощью кватернионного спектра позволяет в максимальной степени

использовать симметрии, связанные с автоморфизмами алгебры **H** при выборе фундаментальной области индексов выходного сигнала.

Например, нетрудно показать, что для наиболее простой построчно-столбцовой схемы вычисления БПФ-2 может быть получена мультипликативная сложность $M(N\times N)$, равная

$$M(N\times N)=3N^2\log_3 N+O(N^2).$$

С другой стороны, представляя (46) в форме

$$\tilde{F}(m_1,\ m_2)=\sum_{a,\ b=0}^{2}\omega_1^{am_1}\tilde{F}_{ab}(m_1,\ m_2)\omega_2^{bm_2}, \tag{74}$$

где

$$\tilde{F}_{ab}(m_1,\ m_2)=\sum_{n_1,\ n_2=0}^{N/3-1}\omega_1^{3n_1m_1}f(3n_1+a,3n_2+b)\omega_2^{3n_2m_2},$$

оценим мультипликативную сложность вычисления кватернионного спектра. Значения $\tilde{F}_{ab}(m_1,\ m_2)$ достаточно вычислить для пар $(m_1,\ m_2)=(\mu,\ \nu)\in\Delta$, где Δ - "фундаментальная область":

$$\Delta=\left\{(\mu,\ \nu):0\le\mu,\ \nu\le N/3-1\right\}.$$

Значения $\tilde{F}_{ab}(m_1,\ m_2)$ для пар$(m_1,\ m_2)$, лежащих в областях, полученных из Δ аддитивными сдвигами на векторы

$$\mathbf{a}=\left(\alpha\frac{N}{3},\ \beta\frac{N}{3}\right),\quad \alpha,\ \beta=0,\ 1,\ 2,$$

отличаются от соответствующих $\tilde{F}_{ab}(\mu,\ \nu)$ лишь множителями γ_1, $\overline{\gamma}_1$, γ_2, $\overline{\gamma}_2$ и не требуют для вычисления дополнительных вещественных умножений. При вычислении $\tilde{F}_{ab}(\mu,\ \nu)$ достаточно ограничиться значениями $(\mu,\ \nu)\in\Delta_0\subset\Delta$:

$$\Delta_0=\left\{(\mu,\ \nu):0\le\mu,\ \nu\le\frac{1}{2}\left(N/3+1\right)\right\}.$$

Действительно, непосредственно проверяются тождества:

$$\gamma_1^a \ \varepsilon_j\left(\omega_1^{a\mu} \ \tilde{F}_{ab}(\mu,\ v)\omega_2^{bv}\right) = \omega_1^{a\left(N/3-\mu\right)}\tilde{F}_{ab}\left(N/3-\mu,\ v\right)\omega_2^{bv},$$

$$\varepsilon_i\left(\omega_1^{a\mu} \ \tilde{F}_{ab}(\mu,\ v)\omega_2^{bv}\right) \ \gamma_2^b = \omega_1^{a\mu}\tilde{F}_{ab}\left(\mu,\ N/3-v\right)\omega_2^{b\left(N/3-v\right)}, \qquad (75)$$

$$\gamma_1^a \ \left(\varepsilon_i \circ \varepsilon_j\right)\left(\omega_1^{a\mu} \ \tilde{F}_{ab}(\mu,\ v)\omega_2^{bv}\right)\gamma_2^b = \omega_1^{a\left(N/3-\mu\right)}\tilde{F}_{ab}\left(N/3-\mu,\ N/3-v\right)\omega_2^{b\left(N/3-v\right)}.$$

И так как умножения на γ_1^a, γ_2^b и выполнение отображений ε_i и ε_j не требуют нетривиальных вещественных умножений, то для мультипликативной сложности $M(N)$ рассмотренного алгоритма вычисления спектра (73) имеем окончательно:

$$M \ (N\times N) = C \ N^2\log_3 N + O\left(N^2\right), \qquad (76)$$

где $C=\frac{5}{3}$ для вещественных и $C=\frac{10}{3}$ для комплексных входных данных.

4.5. Быстрый алгоритм дискретного косинусного преобразования

Известно, что одномерное дискретное косинусное преобразование нечетной длины N может быть сведено к ДПФ *вещественного* сигнала той же длины. Получим аналогичное утверждение для двумерного дискретного косинусного преобразования (ДКП-2).

Действительно, рассмотрим ДКП-2 в форме:

$$\hat{f}(m_1,\ m_2) = \sum_{n_1,\ n_2=0}^{N-1} f(n_1,\ n_2) \ \cos\ \pi\frac{(2n+1)\ \ m_1}{2N} \ \cos\ \pi\frac{(2n+1)\ \ m_2}{2N}.$$

Пусть

$$G(m_1,\ m_2) = \sum_{t_1,\ t_2=0}^{2N-1} \exp\left\{\pi i\frac{t_1 m_1}{2N}\right\} \ g(t_1,\ t_2) \ \exp\left\{\pi j\frac{t_2 m_2}{2N}\right\},$$

где

$$g(t_1,\ t_2)=\begin{cases} f(n_1,\ n_2), & \text{при } t_1=2n_1+1,\ t_2=2n_2+1;\\ 0, & \text{в остальных случаях;}\\ & t_1,\ t_2=0,\ 1,\ \ldots,\ 2N-1. \end{cases}$$

Тогда

$$\hat{f}(m_1,m_2)=\frac{1}{4}\Big[G(m_1,m_2)+\varepsilon_i\big(G(m_1,m_2)\big)+\varepsilon_j\big(G(m_1,m_2)\big)+\varepsilon_k\big(G(m_1,m_2)\big)\Big],\quad (77)$$

и основную трудность представляет вычисление $G(m_1,\ m_2)$.

Пусть целые α и β выбраны так, чтобы выполнялись соотношения

$$\begin{cases} 4^2\alpha\equiv 4 \pmod{4N};\\ N^2\beta\equiv N \pmod{4N}. \end{cases}$$

Находя для каждого нечетного числа t_s $(0\le t_s<2N;\ s=1,\ 2)$ пару $(t_{s1},\ t_{s2})$ как решение сравнения

$$t_s\equiv 4t_{s1}+Nt_{s2}\pmod{4N} \qquad (77)$$

и для каждого m_s $(0\le m_s<N)$ пару $(m_{s1},\ m_{s2})$ как решение сравнения

$$m_s\equiv 4\alpha\ \ m_{s1}+N\ \ \beta\ \ m_{s2}\pmod{4N} \qquad (78)$$

с условиями

$$0\le t_{s1},\ m_{s1}<N;0\le t_{s2},\ m_{s2}<4, \qquad (79)$$

получаем системы сравнений

$$\begin{cases} t_s\equiv 4\ \ t_{s1} \pmod{N};\\ t_s\equiv N\ \ t_{s2} \pmod{4}; \end{cases}\quad \begin{cases} m_s\equiv\ m_{s1} \pmod{N};\\ m_s\equiv m_{s2} \pmod{4}. \end{cases}$$

Пусть F - множество четверок чисел $(t_{11},\ t_{12};\ t_{21},\ t_{22})$, являющихся решениями сравнений (77)-(78) с условиями (79). Так как t_s нечетно, то t_{s2} также нечетные, поэтому множество F представимо в виде объединения четырех непересекающихся множеств $\mathsf{F}=\mathsf{F}_{11}\cup\mathsf{F}_{13}\cup\mathsf{F}_{31}\cup\mathsf{F}_{33}$, где

$$\mathsf{F}_{ab}=\big\{(t_{11},\ t_{12},\ t_{21},\ t_{22})\in\mathsf{F}:\ t_{12}=a,\ t_{22}=b\big\}.$$

Отметим ряд легко проверяемых свойств множеств F_{ab}:

(a) преобразования

$$(t_{11},\ 3,\ t_{21},\ 1) \mapsto (N - t_{11},\ 3,\ t_{21},\ 1); \tag{80}$$

$$(t_{11},\ 1,\ t_{21},\ 3) \mapsto (t_{11},\ 1,\ N - t_{21},\ 3); \tag{81}$$

$$(t_{11},\ 3,\ t_{21},\ 3) \mapsto (N - t_{11},\ 3,\ N - t_{21},\ 3) \tag{82}$$

являются биекциями множеств F_{31}, F_{13}, F_{33} соответственно;

(b) если *card A* - число элементов множества *A*, то

$$card\ \mathsf{F}_{13} = card\ \mathsf{F}_{31} = (N-1)(N+1)/4\ ;\ card\ \mathsf{F}_{33} = (N-1)^2/4\ ;$$

(c) при $(t_{11},\ t_{12};\ t_{21},\ t_{22}) \in \mathsf{F}$ переменные t_{11} и t_{21} принимают независимо все значения 0, 1, …, $N-1$ ровно по одному разу.

$$G(t_{11},\ t_{12};\ t_{21},\ t_{22}) = g(4t_{11} + N\ \ t_{12},\ 4t_{21} + N\ \ t_{22}),$$

$$F(m_{11},\ m_{12},\ m_{21},\ m_{22}) = \hat{f}(4\alpha\ \ m_{11} + N\ \beta\ \ m_{12},\ 4\alpha\ \ m_{21} + N\ \beta\ \ m_{22}).$$

Производя в (75) замены переменных (77) и (78), получаем после преобразований (декомпозиция Гуда-Томаса):

$$F(m_{11},\ m_{12},\ m_{21},\ m_{22}) = \frac{1}{4}\Big[Q(m_{11},\ m_{12},\ m_{21},\ m_{22}) + \varepsilon_i\big(Q(m_{11},\ m_{12},\ m_{21},\ m_{22})\big) +$$
$$+ \varepsilon_j\big(Q(m_{11},\ m_{12},\ m_{21},\ m_{22})\big) + \varepsilon_k\big(Q(m_{11},\ m_{12},\ m_{21},\ m_{22})\big)\Big]\ ,$$

где

$$\begin{aligned} &Q(m_{11},\ m_{12},\ m_{21},\ m_{22}) = \\ &= \sum_{(t_{11}, t_{12}, t_{21}, t_{22}) \in \mathsf{F}} i^{t_{12} m_{12}}\, \omega_1^{t_{11} m_{11}}\ G(t_{11},\ t_{12},\ t_{21},\ t_{22})\ \omega_2^{t_{21} m_{21}}\, j^{t_{22} m_{22}} = \\ &= \sum_{a,\ b=1,\ 3} \ \sum_{(t_{11}, t_{12}, t_{21}, t_{22}) \in \mathsf{F}_{ab}} i^{a m_{12}}\, \omega_1^{t_{11} m_{11}}\ G(t_{11},\ a,\ t_{21},\ b)\ \omega_2^{t_{21} m_{21}}\, j^{b m_{22}} = \\ &= \sum_{a,\ b=1,\ 3} Q_{ab}(m_{11},\ m_{12},\ m_{21},\ m_{22})\ . \end{aligned} \tag{83}$$

Так как $i^3 = -i = i^{-1}$, $j^3 = -j = j^{-1}$, то, производя в выражении для Q_{ab} при a и/или b равных трем замену переменных t_{11}, t_{21} согласно (80)-(82), получаем после несложных преобразований:

$$\hat{f}(m_1,\ m_2) = F(m_{11},\ m_{12},\ m_{21},\ m_{22}) =$$
$$= \frac{1}{4}\left[\sum_{r=o,i,j,k} \varepsilon_r \left(\sum_{n_1,\ n_2=0}^{N-1} i^{m_{12}}\ \omega_1^{n_1 m_{11}} Z(n_1,\ n_2)\ \omega_2^{n_2 m_{21}} j^{m_{22}} \right)\right], \qquad (84)$$

где

$$Z(n_1,\ n_2) = \begin{cases} G(n_1,\ 1,\ n_2,\ 1), & \text{при } (n_1,\ 1,\ n_2,\ 1) \in \mathsf{F}; \\ G(N-n_1,\ 3,\ n_2,\ 1), & \text{при } (N-n_1,\ 3,\ n_2,\ 1) \in \mathsf{F}; \\ G(n_1,\ 1,\ N-n_2,\ 3), & \text{при } (n_1,\ 1,\ N-n_2,\ 3) \in \mathsf{F}; \\ G(N-n_1,\ 3,\ N-n_2,\ 3), & \text{при } (N-n_1,\ 3,\ N-n_2,\ 3) \in \mathsf{F}. \end{cases}$$

Равенство (84) доказано для любого нечетного N. В случае $N = 3^r$ вычисление массива (84) можно реализовать в кодах с помощью алгоритма предыдущего раздела, что приводит к оценке

$$M(N \times N) = \frac{5}{3}\ N^2 \log_3 N + O\left(N^2\right).$$

В этом случае вычисление $\hat{f}(m_1,\ m_2)$ для m_1, m_2 одной четности не требует дополнительных умножений; при m_1, m_2 разной четности умножение на константу i в кодах требует не более одного умножения на отсчет выходного массива. В конкретных алгоритмах обработки сигналов эти умножения могут быть объединены с нормированием косинусного спектра.

5. СОВМЕЩЕННОЕ ВЫЧИСЛЕНИЕ СПЕКТРОВ МНОГОКАНАЛЬНОГО ИЗОБРАЖЕНИЯ

5.1 Алгебра Гурвица

Как уже отмечалось, общая схема совмещенного вычисления ДПФ может применяться как для снижения вычислительной сложности преобразования одного вещественного сигнала, так и для одновременного вычисления Фурье-спектров нескольких массивов. Необходимость одновременного решения обеих задач возникает при вычислении спектров многоканальных изображений. Эффективность соответствующих алгоритмов будет в этом случае определяться существованием "хорошей" многомерной алгебры с просто реализуемыми операциями и автоморфизмами.

В данном разделе рассматривается алгоритм совмещенного вычисления трех Фурье-спектров двумерного массива (цветного изображения, например).

Определение 8. Двенадцатимерную **R** – алгебру с базисом

$$E=\left\{\mathbf{e},\mathbf{i},\mathbf{j},\mathbf{k},\mathbf{w},\mathbf{w}^{\mathbf{i}},\mathbf{w}^{\mathbf{j}},\mathbf{w}^{\mathbf{k}},\overline{\mathbf{w}},\overline{\mathbf{w}}^{\mathbf{i}},\overline{\mathbf{w}}^{\mathbf{j}},\overline{\mathbf{w}}^{\mathbf{k}}\right\} \tag{85}$$

и правилами умножения базисных элементов, определенными табл. 1, будем называть алгеброй Гурвица и обозначать **Hz**. Элемент

$$\mathbf{g}=A\mathbf{e}+B\mathbf{i}+C\mathbf{j}+D\mathbf{k}+E\mathbf{w}+F\mathbf{w}^{\mathbf{i}}+G\mathbf{w}^{\mathbf{j}}+H\mathbf{w}^{\mathbf{k}}+P\overline{\mathbf{w}}+Q\overline{\mathbf{w}}^{\mathbf{i}}+R\overline{\mathbf{w}}^{\mathbf{j}}+S\overline{\mathbf{w}}^{\mathbf{k}} \tag{86}$$

алгебры **Hz** будем называть гурвицианом.

Анализ правил умножения, определенных табл. 1, позволяет сформулировать их неформальную интерпретацию: элементы $\mathbf{e},\mathbf{i},\mathbf{j},\mathbf{k}$ "ведут себя" относительно умножения как кватернионы *1, i, j, k* , соответственно, *не будучи таковыми.* Они становятся "настоящими" элементами четырехмерной алгебры кватернионов только под действием некоторого отображения $\Psi:\mathbf{Hz}\to\mathbf{H}$. Этот факт формально обеспечивается Леммой 15, которая, как и последующие, доказывается непосредственной проверкой.

Таблица 1. Умножение базисных гурвицонов

$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{w}$	$\mathbf{w}^{\mathbf{i}}$	$\mathbf{w}^{\mathbf{j}}$	$\mathbf{w}^{\mathbf{k}}$	$\bar{\mathbf{w}}$	$\bar{\mathbf{w}}^{\mathbf{i}}$	$\bar{\mathbf{w}}^{\mathbf{j}}$	$\bar{\mathbf{w}}^{\mathbf{k}}$
$\mathbf{i}$	$-\mathbf{e}$	$\mathbf{k}$	$-\mathbf{j}$	$\mathbf{w}^{\mathbf{k}}$	$\mathbf{w}^{\mathbf{j}}$	$-\mathbf{w}^{\mathbf{i}}$	$-\mathbf{w}$	$-\bar{\mathbf{w}}^{\mathbf{j}}$	$-\bar{\mathbf{w}}^{\mathbf{k}}$	$\bar{\mathbf{w}}$	$\bar{\mathbf{w}}^{\mathbf{i}}$
$\mathbf{j}$	$-\mathbf{k}$	$-\mathbf{e}$	$\mathbf{i}$	$\mathbf{w}^{\mathbf{i}}$	$-\mathbf{w}$	$\mathbf{w}^{\mathbf{k}}$	$-\mathbf{w}^{\mathbf{j}}$	$-\bar{\mathbf{w}}^{\mathbf{k}}$	$\bar{\mathbf{w}}^{\mathbf{j}}$	$-\bar{\mathbf{w}}^{\mathbf{i}}$	$\bar{\mathbf{w}}$
$\mathbf{k}$	$\mathbf{j}$	$\mathbf{i}-$	$-\mathbf{e}$	$\mathbf{w}^{\mathbf{j}}$	$-\mathbf{w}^{\mathbf{k}}$	$-\mathbf{w}$	$\mathbf{w}^{\mathbf{i}}$	$-\bar{\mathbf{w}}^{\mathbf{i}}$	$\bar{\mathbf{w}}$	$\bar{\mathbf{w}}^{\mathbf{k}}$	$-\bar{\mathbf{w}}^{\mathbf{j}}$
$\mathbf{w}$	$\mathbf{w}^{\mathbf{j}}$	$\mathbf{w}^{\mathbf{k}}$	$\mathbf{w}^{\mathbf{i}}$	$\bar{\mathbf{w}}$	$-\bar{\mathbf{w}}^{\mathbf{j}}$	$-\bar{\mathbf{w}}^{\mathbf{k}}$	$-\bar{\mathbf{w}}^{\mathbf{i}}$	$\mathbf{e}$	$-\mathbf{j}$	$-\mathbf{k}$	$-\mathbf{i}$
$\mathbf{w}^{\mathbf{i}}$	$\mathbf{w}^{\mathbf{k}}$	$-\mathbf{w}^{\mathbf{j}}$	$-\mathbf{w}$	$-\bar{\mathbf{w}}^{\mathbf{k}}$	$\bar{\mathbf{w}}^{\mathbf{i}}$	$-\bar{\mathbf{w}}$	$-\bar{\mathbf{w}}^{\mathbf{j}}$	$\mathbf{j}$	$\mathbf{e}$	$-\mathbf{i}$	$\mathbf{k}$
$\mathbf{w}^{\mathbf{j}}$	$-\mathbf{w}$	$\mathbf{w}^{\mathbf{i}}$	$-\mathbf{w}^{\mathbf{k}}$	$-\bar{\mathbf{w}}^{\mathbf{i}}$	$\bar{\mathbf{w}}^{\mathbf{k}}$	$\bar{\mathbf{w}}^{\mathbf{j}}$	$-\bar{\mathbf{w}}$	$\mathbf{k}$	$\mathbf{i}$	$\mathbf{e}$	$-\mathbf{j}$
$\mathbf{w}^{\mathbf{k}}$	$-\mathbf{w}^{\mathbf{i}}$	$-\mathbf{w}$	$\mathbf{w}^{\mathbf{j}}$	$-\bar{\mathbf{w}}^{\mathbf{j}}$	$-\bar{\mathbf{w}}$	$-\bar{\mathbf{w}}^{\mathbf{i}}$	$\bar{\mathbf{w}}^{\mathbf{k}}$	$\mathbf{i}$	$-\mathbf{k}$	$\mathbf{j}$	$\mathbf{e}$
$\bar{\mathbf{w}}$	$-\bar{\mathbf{w}}^{\mathbf{k}}$	$-\bar{\mathbf{w}}^{\mathbf{i}}$	$-\bar{\mathbf{w}}^{\mathbf{j}}$	$\mathbf{e}$	$\mathbf{k}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{w}$	$-\mathbf{w}^{\mathbf{k}}$	$-\mathbf{w}^{\mathbf{i}}$	$-\mathbf{w}^{\mathbf{j}}$
$\bar{\mathbf{w}}^{\mathbf{i}}$	$-\bar{\mathbf{w}}^{\mathbf{j}}$	$\bar{\mathbf{w}}$	$\bar{\mathbf{w}}^{\mathbf{k}}$	$-\mathbf{k}$	$\mathbf{e}$	$-\mathbf{j}$	$\mathbf{i}$	$-\mathbf{w}^{\mathbf{j}}$	$\mathbf{w}^{\mathbf{i}}$	$-\mathbf{w}^{\mathbf{k}}$	$-\mathbf{w}$
$\bar{\mathbf{w}}^{\mathbf{j}}$	$\bar{\mathbf{w}}^{\mathbf{i}}$	$-\bar{\mathbf{w}}^{\mathbf{k}}$	$\bar{\mathbf{w}}$	$-\mathbf{i}$	$\mathbf{j}$	$\mathbf{e}$	$-\mathbf{k}$	$-\mathbf{w}^{\mathbf{k}}$	$-\mathbf{w}$	$\mathbf{w}^{\mathbf{j}}$	$-\mathbf{w}^{\mathbf{i}}$
$\bar{\mathbf{w}}^{\mathbf{k}}$	$\bar{\mathbf{w}}$	$\bar{\mathbf{w}}^{\mathbf{j}}$	$-\bar{\mathbf{w}}^{\mathbf{i}}$	$-\mathbf{j}$	$-\mathbf{i}$	$\mathbf{k}$	$\mathbf{e}$	$-\mathbf{w}^{\mathbf{i}}$	$-\mathbf{w}^{\mathbf{j}}$	$-\mathbf{w}$	$\mathbf{w}^{\mathbf{k}}$

Лемма 15. Отображение $\Psi : \mathbf{Hz} \to \mathbf{H}$ такое, что

$$\Psi : \mathbf{e} \mapsto 1, \Psi : \mathbf{i} \mapsto i, \Psi : \mathbf{j} \mapsto j, \Psi : \mathbf{k} \mapsto k,$$

$$\mathbf{w} = \mathbf{e}^{-1}\mathbf{w}\mathbf{e} \mapsto \frac{1}{2}(-1+i+j+k), \quad \bar{\mathbf{w}} = \mathbf{e}^{-1}\bar{\mathbf{w}}\mathbf{e} \mapsto \frac{1}{2}(-1-i-j-k),$$

$$\mathbf{w}^{\mathbf{i}} = \mathbf{i}^{-1}\mathbf{w}\mathbf{i} \mapsto \frac{1}{2}(-1+i-j-k), \quad \bar{\mathbf{w}}^{\mathbf{i}} = \mathbf{i}^{-1}\bar{\mathbf{w}}\mathbf{i} \mapsto \frac{1}{2}(-1-i+j+k),$$

$$\mathbf{w}^{\mathbf{j}} = \mathbf{j}^{-1}\mathbf{w}\mathbf{j} \mapsto \frac{1}{2}(-1-i+j-k), \quad \bar{\mathbf{w}}^{\mathbf{j}} = \mathbf{j}^{-1}\bar{\mathbf{w}}\mathbf{j} \mapsto \frac{1}{2}(-1+i-j+k),$$

$$\mathbf{w}^{\mathbf{k}} = \mathbf{k}^{-1}\mathbf{w}\mathbf{k} \mapsto \frac{1}{2}(-1-i-j+k), \quad \bar{\mathbf{w}}^{\mathbf{k}} = \mathbf{k}^{-1}\bar{\mathbf{w}}\mathbf{k} \mapsto \frac{1}{2}(-1+i+j-k),$$

продолжается линейно до гомоморфизма алгебры $\mathbf{Hz}$ на алгебру $\mathbf{H}$.

Иными словами, как уже отмечалось, этот гомоморфизм переводит базисные элементы $\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ в кватернионы $1, i, j, k,$ а остальные восемь базисных элементов

$$\left\{\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{w}, \mathbf{w}^{\mathbf{i}}, \mathbf{w}^{\mathbf{j}}, \mathbf{w}^{\mathbf{k}}, \bar{\mathbf{w}}, \bar{\mathbf{w}}^{\mathbf{i}}, \bar{\mathbf{w}}^{\mathbf{j}}, \bar{\mathbf{w}}^{\mathbf{k}}\right\}$$

- в так называемые целые кватернионы Гурвица.

Лемма 16. Множество

$$\mathbf{H}^{*}\mathbf{z} = x\mathbf{e} + y(\mathbf{i}+\mathbf{j}+\mathbf{k}), \quad x, y \in \mathbf{R},$$

есть подалгебра алгебры $\mathbf{Hz}$.

Лемма 17. Гурвицион $\mathbf{W} \in \mathbf{H}^{*}\mathbf{z}$:

$$\mathbf{W} = \mathbf{e}\cos\frac{2\pi}{K} + \frac{1}{\sqrt{3}}(\mathbf{i}+\mathbf{j}+\mathbf{k})\sin\frac{2\pi}{K} \tag{87}$$

является первообразным корнем степени K из гурвиционной единицы $\mathbf{e} \in \mathbf{Hz}$.

Кватернион

$$w = \Psi(\mathbf{W}) = \cos\frac{2\pi}{K} + \frac{1}{\sqrt{3}}(i+j+k)\sin\frac{2\pi}{K} \tag{88}$$

является первообразным корнем степени K из единицы $1 \in \mathbf{H}$.

Лемма 18. Пусть

$$\mathbf{V} = \mathbf{w}\left(\frac{1}{\sqrt{3}}\sin\frac{2\pi}{K} - \cos\frac{2\pi}{K}\right) - \overline{\mathbf{w}}\left(\frac{1}{\sqrt{3}}\sin\frac{2\pi}{K} + \cos\frac{2\pi}{K}\right). \tag{89}$$

Тогда $\Psi(\mathbf{W}) = \Psi(\mathbf{V}) = w$.

Лемма 19. Существует такой кватернион $h \in \mathbf{H}$, что справедливо равенство

$$h^{-1}wh = \omega = \cos\frac{2\pi}{K} + i\sin\frac{2\pi}{K}. \tag{90}$$

Лемма 20. Пусть $\mathbf{g}, \mathbf{V} \in \mathbf{Hz}$ такие, что:

$$\mathbf{g} = A\mathbf{e}+B\mathbf{i}+C\mathbf{j}+D\mathbf{k}+E\mathbf{w}+F\mathbf{w}^{\mathbf{i}} + G\mathbf{w}^{\mathbf{j}} + H\mathbf{w}^{\mathbf{k}} + P\overline{\mathbf{w}} + Q\overline{\mathbf{w}}^{\mathbf{i}} + R\overline{\mathbf{w}}^{\mathbf{j}} + S\overline{\mathbf{w}}^{\mathbf{k}},$$

$$\mathbf{V} = x\mathbf{w} + y\overline{\mathbf{w}}.$$

Тогда для вычисления произведения $\mathbf{gV}$ достаточно 16 вещественных умножений.

Доказательство. С использованием табл. 1 имеем:

$$\mathbf{gV} = \left[(Px + Ey)\mathbf{e} + (Ax + Py)\mathbf{w} + (Ex + Ay)\bar{\mathbf{w}} \right] +$$
$$+ \left[(-Rx + Hy)\mathbf{i} + (-Hx - By)\bar{\mathbf{w}}^{\mathbf{i}} + (Bx - Ry)\mathbf{w}^{\mathbf{k}} \right] +$$
$$+ \left[(-Sx + Fy)\mathbf{j} + (Cx - Sy)\mathbf{w}^{\mathbf{i}} + (-Fx - Cy)\bar{\mathbf{w}}^{\mathbf{k}} \right] +$$
$$+ \left[(-Qx + Gy)\mathbf{k} + (Dx - Qy)\mathbf{w}^{\mathbf{j}} + (-Gx - Dy)\bar{\mathbf{w}}^{\mathbf{i}} \right].$$

Вещественные коэффициенты в последнем равенстве разбиваются на четыре группы (выделены квадратными скобками) по три коэффициента в каждой. Каждая такая тройка представляет собой компоненты трехточечной дискретной свертки, которая может быть вычислена посредством четырех умножений. Действительно, пусть элементы ζ, η, ξ определены равенствами:

$$\zeta = \beta x + \gamma y, \quad \eta = \alpha y + \gamma x, \quad \xi = \alpha x + \beta y,$$

то есть, матричным равенством

$$\begin{pmatrix} \zeta \\ \eta \\ \xi \end{pmatrix} = \begin{pmatrix} 0 & x & y \\ y & 0 & x \\ x & y & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix},$$

требующим для вычисления элементов ζ, η, ξ четырех вещественных умножений [3].

Через $Rot_{\mathbf{a}}(\mathbf{g})$ обозначим отображение (автоморфизм алгебры Гурвица)

$$Rot_{\mathbf{a}}(\mathbf{g}) = \mathbf{a}^{-1}\mathbf{g}\mathbf{a}, \quad \mathbf{g}, \mathbf{a} \in \mathbf{Hz}.$$

Замечание 4. Не останавливаясь на подробном обосновании, отметим, что группа отображений $Rot_{\mathbf{a}}(\mathbf{g})$ имеет интересную геометрическую интерпретацию. Пусть

$$\Re = \{ \pm Rot_{\mathbf{a}}(\bullet), \mathbf{a} \in E \},$$

тогда $\Re$ есть группа, изоморфная группе самосовмещений "кватернионного куба"

$$\Delta_{\pm 1} = \{ \delta: \quad \delta = \pm i \pm j \pm k \} \subset \mathbf{H}.$$

5.2. Алгоритм совмещенного вычисления трех Фурье-спектров цветного изображения

Пусть $x^{(\alpha)}(n_1, n_2)$ $(\alpha = 0,1,2)$ есть $RGB-$компоненты дискретного цветного изображения, $N = 2K = 2^r$. Пусть $\hat{x}^{(\alpha)}(m_1, m_2)$ - соответствующие Фурье-спектры:

$$\hat{x}^{(\alpha)}(m_1, m_2) = \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} x^{(\alpha)}(n_1, n_2) e^{2\pi i \frac{n_1 m_1 + n_2 m_2}{N}}; m_1, m_2 = 0, \ldots, N-1. \quad (91)$$

Основной целью этого раздела является конструктивное доказательство следующей теоремы.

Теорема 3. Существует совмещенный алгоритм одновременного вычисления трех двумерных Фурье-спектров, требующий не более

$$M^*(N^2) = \frac{1}{3} N^2 \log_2 N + O(N^2) \quad (92)$$

для каждого отдельного Фурье-спектра.

Доказательство. Дадим пошаговое описание алгоритма с анализом мультипликативной сложности каждого шага, откуда и будет следовать соотношение.

Шаг 1. Формирование вспомогательной функции со значениями в алгебре Гурвица.

Введем обозначения:

$$x_{\beta\gamma}^{(\alpha)}(n_1, n_2) = x_{\beta\gamma}^{(\alpha)}(2n_1 + \beta, 2n_2 + \gamma), \quad \alpha = 0,1,2; \beta, \gamma = 0,1,$$

$$\mathbf{X}^{(1)}(n_1, n_2) = \left(x_{00}^{(1)}\mathbf{e} + x_{10}^{(1)}\mathbf{i} + x_{01}^{(1)}\mathbf{j} + x_{11}^{(1)}\mathbf{k} \right)(n_1, n_2),$$

$$\mathbf{X}^{(2)}(n_1, n_2) = \left(x_{00}^{(2)}\mathbf{w} + x_{10}^{(2)}\mathbf{w}^{\mathbf{i}} + x_{01}^{(2)}\mathbf{w}^{\mathbf{j}} + x_{11}^{(2)}\mathbf{w}^{\mathbf{k}} \right)(n_1, n_2),$$

$$\mathbf{X}^{(3)}(n_1, n_2) = \left(x_{00}^{(3)}\bar{\mathbf{w}} + x_{10}^{(3)}\bar{\mathbf{w}}^{\mathbf{i}} + x_{01}^{(3)}\bar{\mathbf{w}}^{\mathbf{j}} + x_{11}^{(3)}\bar{\mathbf{w}}^{\mathbf{k}} \right)(n_1, n_2).$$

Образуем вспомогательную функцию со значениями в алгебре Гурвица

$$\mathbf{X}(n_1, n_2) = \mathbf{X}^{(1)}(n_1, n_2) + \mathbf{X}^{(2)}(n_1, n_2) + \mathbf{X}^{(3)}(n_1, n_2). \quad (93)$$

Шаг 2. Вычисление вспомогательного преобразования.

Пусть элемент $\mathbf{V}$ определен равенством (89) Леммы 18. Определим вспомогательное преобразование массива $\mathbf{X}(n_1, n_2)$:

$$\hat{\mathbf{X}}(m_1, m_2) = \sum_{n_1=0}^{K-1} \sum_{n_2=0}^{K-1} \mathbf{X}(n_1, n_2)\mathbf{V}^{n_1 m_1 + n_2 m_2}. \qquad (94)$$

Вычисление преобразования (94) по схеме декомпозиции

$$\hat{\mathbf{X}}(m_1, m_2) = \sum_{a,b=0}^{1} \mathbf{V}^{am_1 + bm_2} \sum_{n_1=0}^{K-1} \sum_{n_2=0}^{K-1} \mathbf{X}(2n_1 + a, 2n_2 + b)\mathbf{V}^{2(n_1 m_1 + n_2 m_2)}, \quad K = N/2$$

с учетом сложности умножений, указанной в Лемме 20, требует не более

$$\mu(K^2) = 12K^2 \log_2 K + O(K^2)$$

вещественных умножений.

Шаг 3. Выделение "частичных спектров"со значениями в алгебре Гурвица. Возможность такого выделения "частичных спектров"

$$\hat{\mathbf{X}}^{(\alpha)}_{\beta\gamma}(m_1, m_2) = \sum_{n_1=0}^{K-1} \sum_{n_2=0}^{K-1} x^{(\alpha)}_{\beta\gamma}(n_1, n_2)\mathbf{V}^{n_1 m_1 + n_2 m_2}; \ \alpha = 0,1,2; \ \beta, \gamma = 0,1$$

следует из существования единственного решения системы уравнений

$$Rot_{\mathbf{a}}\left(\hat{\mathbf{X}}(m_1, m_2)\right) = Rot_{\mathbf{a}}\left(\sum_{n_1=0}^{K-1} \sum_{n_2=0}^{K-1} \mathbf{X}(n_1, n_2)\mathbf{V}^{n_1 m_1 + n_2 m_2}\right), \quad \mathbf{a} \in E.$$

Для вычисления $\hat{\mathbf{X}}^{(\alpha)}_{\beta\gamma}(m_1, m_2)$ требуется не более, чем $O(N^2)$ вещественных арифметических операций.

Шаг 4. Вычисление "частичных кватернионных спектров".

В соответствии с Леммой 18, отображение Ψ преобразует $\hat{\mathbf{X}}^{(\alpha)}_{\beta\gamma}(m_1, m_2)$ в

$$\hat{\mathbf{X}}^{(\alpha)}_{\beta\gamma}(m_1, m_2) = \sum_{n_1=0}^{K-1} \sum_{n_2=0}^{K-1} x^{(\alpha)}_{\beta\gamma}(n_1, n_2)\omega^{n_1 m_1 + n_2 m_2}; \ \alpha = 0,1,2; \ \beta, \gamma = 0,1.$$

Это отображение не требует вещественных умножений.

Шаг 5. Выделение "частичных комплексных спектров".

Отображение

$$\hat{\mathbf{X}}^{(\alpha)}_{\beta\gamma}(m_1,m_2) \mapsto h^{-1}\hat{\mathbf{X}}^{(\alpha)}_{\beta\gamma}(m_1,m_2)h$$

преобразует $\hat{\mathbf{X}}^{(\alpha)}_{\beta\gamma}(m_1,m_2)$ в

$$\hat{x}^{(\alpha)}_{\beta\gamma}(m_1,m_2) = \sum_{n_1=0}^{K-1}\sum_{n_2=0}^{K-1} x^{(\alpha)}_{\beta\gamma}(n_1,n_2)\omega^{n_1m_1+n_2m_2};\ \alpha=0,1,2;\ \beta,\gamma=0,1.$$

Для вычисления $\hat{x}^{(\alpha)}_{\beta\gamma}(m_1,m_2)$ требуется $O(N^2)$ вещественных арифметических операций.

Шаг 6. Реконструкция трех "полных" комплексных спектров.

Три полных комплексных Фурье-спектра реконструируются по формуле

$$\hat{x}^{(\alpha)}(m_1,m_2) = \sum_{\beta,\gamma=0}^{1} e^{\frac{2\pi}{N}(\beta m_1+\gamma m_2)}\,\hat{x}^{(\alpha)}_{\beta\gamma}(m_1,m_2).$$

Эта реконструкция требует не более, чем $O(N^2)$ вещественных арифметических операций.

Окончательно, суммируя сложность каждого из описанных шагов, получаем утверждение теоремы.

6. АЛГОРИТМ ДПФ С "ЭКСТРЕМАЛЬНЫМ" СОВМЕЩЕНИЕМ В ГРУППОВОЙ АЛГЕБРЕ ЦИКЛИЧЕСКОЙ ГРУППЫ

Целью настоящего раздела является демонстрация принципиальной возможности синтеза алгоритма ДПФ с понижением порядка главного члена в оценке мультипликативной сложности. Сам алгоритм представляет скорее академический интерес, но принцип его синтеза иллюстрирует предельные, в некотором смысле, возможности метода совмещенного вычисления Фурье-спектров. Именно поэтому большинство промежуточных утверждений приводятся без доказательства. Полное и подробное доказательство опубликовано в [4].

6.1. Некоторые свойства групповых алгебр циклических групп

Ограничимся для простоты рассмотрением принципиального случая $N = p^r$ (p – простое нечетное число). Случай $N = 2^r$ будет рассмотрен специально.

Пусть $q = p^s$, $(2 \le s < r)$, $\mathbf{G}$ – циклическая группа из q элементов с образующим и нейтральным элементами $\mathbf{g}$ и $\mathbf{e}$, соответственно; $\mathbf{A} = \mathbf{A}(\mathbf{G}, \mathbf{R})$ - групповая $\mathbf{R}$-алгебра:

$$\mathbf{A} = \left\{ z = z_0\mathbf{e} + z_1\mathbf{g} + \ldots + z_{q-1}\mathbf{g}^{q-1};\ z_j \in \mathrm{R},\ 0 \le j \le q-1 \right\}. \tag{95}$$

Лемма 21. Пусть $z \in \mathbf{A}$,

$$w = w_1\mathbf{g}^{(q-1)/2} + w_2\mathbf{g}^{(q+1)/2} = w_1\mathbf{g}^{-} + w_2\mathbf{g}^{+}. \tag{96}$$

Тогда для вычисления произведения z w достаточно

$$\mu(q) = \frac{3}{2}(q-1) + 2$$

вещественных умножений.

Доказательство. Замечая, что

$$z = \left(\mathbf{g}^{-}\right)^{-1}\left[\mathbf{g}\left(z_1\mathbf{g}^{-} + z_2\mathbf{g}^{+}\right) + \ldots + \mathbf{g}^{q-2}\left(z_{q-2}\mathbf{g}^{-} + z_{q-1}\mathbf{g}^{+}\right)\right] + z_0\mathbf{e}, \tag{97}$$

получаем, что вычисление произведения zw сводится к $q-1/2$ умножениям элементов типа (96) и вычислению произведения $z_0 w$, требующего двух вещественных умножений.

Далее, так как справедливы равенства:

$$\begin{gathered}\left(u_1\mathbf{g}^- + u_2\mathbf{g}^+\right)\left(w_1\mathbf{g}^- + w_2\mathbf{g}^+\right) = u_1 w_1\mathbf{g}^{-1} + u_2 w_2\mathbf{g} + \left(u_1 w_2 + u_2 w_1\right)\mathbf{e}, \\ u_1 w_2 + u_2 w_1 = \left(u_1 - u_2\right)\left(w_2 - w_1\right) + u_1 w_1 + u_2 w_2,\end{gathered} \tag{98}$$

то вычисление произведения (98) требует не более трех вещественных умножений, что и доказывает лемму.

Множество автоморфизмов ε_τ алгебры **A**, индуцированных автоморфизмами $\mathbf{g} \to \mathbf{g}^\tau$, $(\tau, p) = 1$, группы **G**, будем далее обозначать $\boldsymbol{\varepsilon}$; через ε_τ^* обозначим автоморфизм, индуцированный отображением $\mathbf{g} \to \mathbf{g}^{-\tau}$.

Лемма 22. Пусть **J** – идеал алгебры A, порожденный элементами

$$c_\nu = \mathbf{g}^{2\nu} - 2\mathbf{g}^\nu \cos 2\pi\nu/q + \mathbf{e}, \tag{99}$$

C – двумерная R-алгебра комплексных чисел. Тогда имеет место изоморфизм R-алгебр: $\mathbf{A}/\mathbf{J} \cong \mathbf{C}$.

Доказательство. Пусть ω - первообразный корень степени q в C, $\omega_\nu = \omega^\nu$. Рассмотрим гомоморфизм $\rho : \mathrm{A} \to \mathrm{C}$, при котором $\rho(\mathbf{g}) = \omega$. Ядро этого гомоморфизма порождается элементами алгебры A, представления которых в виде линейных комбинаций степеней элемента **g** переходят под действием ρ в соотношения R-линейной зависимости между комплексными корнями степени q из единицы. А так как каждый такой невещественный корень ω_ν квадратичен над R и удовлетворяет соотношению

$$\omega_\nu^2 - 2\omega_\nu \cos 2\pi\nu/q + 1 = 0,$$

то $\mathbf{Ker}\,\rho$ порождается элементами c_ν, что доказывает лемму.

Лемма 23. Пусть элемент $b \in \mathbf{A}$ имеет вид:

$$b = \sum_{\substack{(\nu, p)=1 \\ 1 \le \nu \le p^{s-1}}} \beta_\nu \mathbf{g}^\nu , \quad \beta_\nu \in \mathbf{R} . \tag{100}$$

Тогда из системы уравнений

$$\sum_{\substack{(\nu, p)=1 \\ 1 \le \nu \le p^{s-1}}} \beta_\nu \, \rho \circ \varepsilon_\tau \left(\mathbf{g}^\nu \right) = \rho \circ \varepsilon_\tau (b) \text{ при } (\tau, p) = 1 \tag{101}$$

однозначно определяются константы β_ν.

Доказательство. Нетрудно показать (например, [5], гл.3, задача 12а) справедливость равенств:

$$\sum_{\substack{(\tau, q)=1 \\ 1 \le \tau \le p^s}} \omega_{-\nu\tau} \rho \circ \varepsilon_\tau (b) = p^{s-1} (p-1) \beta_\nu . \tag{102}$$

Лемма 24. Пусть $T = p^t \ (t > s)$, $w_m = w_m^+ \mathbf{g}^+ + w_m^- \mathbf{g}^-$,

$$w_m^+ = \left(\left(2\cos {2\pi(q-1)}/{2q} \right)^{-1} - \left(2\sin {2\pi(q-1)}/{2q} \right)^{-1} \right) \cos {2\pi m}/{T},$$

$$w_m^- = \left(\left(2\cos {2\pi(q-1)}/{2q} \right)^{-1} - \left(2\sin {2\pi(q-1)}/{2q} \right)^{-1} \right) \sin {2\pi m}/{T} .$$

Положим $w = w_1$; при $k = m \cdot n$ и обозначим $w_k = w_{mn}$.

Тогда $\rho(w_m) = \rho\left(w_1^m \right) = \varsigma^m$, где ζ - первообразный корень степени T в C.

Доказательство. Непосредственно проверяются тождества:

$$1 = \left(2\cos {2\pi(q-1)}/{2q} \right)^{-1} \rho\left(\mathbf{g}^+ + \mathbf{g}^- \right),$$

$$i = \left(2\sin {2\pi(q-1)}/{2q} \right)^{-1} \rho\left(\mathbf{g}^+ + \mathbf{g}^- \right),$$

и утверждение леммы следует из того, что

$$\rho\left(\mathbf{g}^{\pm}\right)=\omega^{\frac{q\pm1}{2}}. \tag{103}$$

Лемма 25. Пусть семейство функций $H(m,n)$ определено для $0\le m,n<{}^{T}\!/_{q}$ $\left(q<{}^{T}\!/_{q}\right)$ равенством $H(m,n)=w_{mn}$.

Тогда соотношения

$$H(m,qn+r)=H(qm,n)\,H(m,r), \tag{104}$$

$$H\left(m+{}^{aT}\!/_{q},n\right)=\mathbf{g}^{an}H(m,n) \tag{105}$$

однозначно продолжают функции $H(m,n)$ на область

$$\Lambda=\left\{(m,n):\ 0\le m,n<T;\ \ m,n\in \mathbb{Z}\right\},$$

причем $\rho\left(H(m,n)\right)=\varsigma^{mn}$.

Доказательство. Пусть $(m_1,n_1)\in\Lambda$, Тогда, применяя к $H(m,n)$ последовательно (104) и (105), получаем для $H(m_1,n_1)$ выражение через $H(m,n)$, где $0\le m,n<{}^{T}\!/_{q}$.

Пусть $\varepsilon_\tau\in\boldsymbol{\varepsilon}$, тогда отображение $\rho\circ\varepsilon_\tau$ индуцирует в алгебре комплексных чисел C линейную биекцию φ_τ. Из линейности φ_τ, и того, что элемент $\rho\circ\varepsilon_\tau^{*}(z)$ является комплексно-сопряженным к $\rho\circ\varepsilon_\tau(z)$, следует следующее утверждение.

Лемма 26. Для любого $\varepsilon_\tau\in$ E существуют независящие от m и n константы $b_\tau^{+},b_\tau^{-}\in$ R такие, что

$$\rho\left(H(m,n)\right)=b_\tau^{+}\left(\rho\circ\varepsilon_\tau\right)\left(H(m,n)\right)+b_\tau^{-}\left(\rho\circ\varepsilon_\tau^{*}\right)\left(H(m,n)\right). \tag{106}$$

6.2. Быстрый алгоритм вспомогательного преобразования со значениями в групповой алгебре

Рассмотрим преобразование T-периодической последовательности $\{a(n)\}$ элементов алгебры A:

$$A(m)=\sum_{n=0}^{T-1}a(n)H(m,n)\quad\left(m=0,1,...,T-1;\ T=p^t\right),\tag{107}$$

где семейство функций $H(m,n)$ определено в Лемме 25.

Теорема 4. Вычисление преобразования (107) требует не более

$$M^*(T)=\frac{1}{s}\left(1-\frac{1}{p^s}\right)\left(\frac{3}{2}(q-1)+2\right)T\left(\log_p T-s\right)\tag{108}$$

операций вещественного умножения.

Доказательство. Основой доказательства является конструктивное описание быстрого алгоритма "по основанию q" преобразования (107).

Пусть $T_1=T/q$; представляя $A(m)$ в форме:

$$A(m)=\sum_{n=0}^{T_1-1}a(qn)H(qm,n)+\sum_{v=1}^{q-1}H(m,v)\sum_{n=0}^{T_1-1}a(qn+v)H(qm,n),\tag{109}$$

получаем, что суммы в правой части (109) достаточно вычислить для значений m, лежащих в фундаментальной области

$$\Omega_0=\{0\le m<T_1\}.$$

Значения сумм для m, лежащих в областях Ω_j, полученных из Ω_0 аддитивными сдвигами на $j=T_1,2T_1,...,\left(p^s-1\right)T_1$, отличаются от соответствующих сумм для $m\in\Omega_0$ множителями $\mathbf{g}^{jv}$, умножения на которые в алгебре A реализуются тривиально.

Соотношение (109) редуцирует вычисление преобразования (107) длины T к вычислению $q=p^s$ преобразований длины T_1 и некоторому числу дополнительных умножений на w^{vm}. Отсюда следует:

$$M^*(T)=p^sM(T_1)+\frac{p^s-1}{p^s}T\mu(q)$$

и, окончательно,

$$M^*(T)=\frac{p^s-1}{sp^s}T\mu(q)\left(\log_p T-s\right),$$

что, с учетом лемм, сформулированных выше, дает соотношение (108).

6.3. Быстрый алгоритм ДПФ с асимптотическим понижением порядка мультипликативной сложности

Теорема 5. Пусть $x(n)$ - вещественная N-периодическая последовательность, $N=p^r, r>s$. Тогда для любого натурального s с условием $2\le s<r$ существует БА ДПФ длины N с мультипликативной сложностью

$$M(N)\le\frac{\kappa_1}{s}N\log_p N+\kappa_2 p^s N \tag{110}$$

с константами κ_1 и κ_2, зависящими только от p.

Доказательство. Вычисление ДПФ

$$X(m)=\sum_{n=0}^{N-1}x(n)\gamma^{mn},\quad \gamma=\exp\left\{2\pi i/N\right\}, \tag{111}$$

проведем с помощью рассмотренного преобразования (107).

При фиксированном *s*, вводя обозначения

$$x_y(n)=x\left(p^{s-1}n+y\right),\quad T=p^{r-s+1}=p^t,$$

получаем из (111):

$$X(m)=\sum_{n=0}^{N/p-1}x(pn)\left(\gamma^p\right)^{mn}+\sum_{\substack{n=0\\(n,p)=1}}^{N-1}x(n)\gamma^{mn}. \tag{112}$$

Первая сумма в (112) сводится к ДПФ длины N/p; вторая сумма преобразуется к виду:

$$X_y(m)=\sum_{n=0}^{T-1}x_y(n)\left(\gamma^{p^{s-1}}\right)^{mn}.$$

Для вычисления "частичных спектров" $X_y(m)$ при $(y, p)=1$ воспользуемся преобразованием (107). Занумеруем натуральные числа, взаимно простые с числом p, в порядке возрастания. Пусть $d(\nu)$ - функция-нумератор. Определим последовательность $a(n)$ элементов из A равенствами:

$$a(n)=a_0(n)\mathbf{e}+a_1(n)\mathbf{g}+\ldots+a_{q-1}(n)\mathbf{g}^{q-1},$$

$$a_\nu(n)=\begin{cases} x_y(n), & \text{при } (\nu, p)=1,\ d(\nu)=y,\ 1\le\nu\le p^{s-2}(p-1); \\ 0, & \text{в остальных случаях.}\end{cases}$$

Пусть вычисление спектра $A(m)$ этой последовательности производилось в соответствии с доказательством Теоремы 4 и потребовало $M^*(T)$ операций вещественного умножения.

Далее, положим для $\varepsilon_\tau\in\boldsymbol{\varepsilon}$:

$$D_\tau(m)=b_\tau^+\varepsilon_\tau(A(m))+b_\tau^-\varepsilon_\tau^*(A(m)). \tag{113}$$

Для дальнейших вычислений воспользуемся Леммой 23. Определим последовательности $\Delta_\nu(m)\in\mathbb{A}$ равенствами:

$$\Delta_\nu(m)=\sum_{\substack{(\tau,q)=1\\ 1\le\tau\le p^s}}\mathbf{g}^{-\nu\tau}D_\tau(m). \tag{114}$$

Тогда из Леммы 26 следует:

$$\rho(\Delta_\nu(m))=p^{s-1}(p-1)X_\nu(m). \tag{115}$$

Получение последовательностей $D_\tau(m)$ в алгебре A требует не более

$$M_1(N)=2p^{s-1}(p-1)p^sT\le 2p^{2s}T=2p^{s+1}N$$

вещественных умножений; переход от последовательности (114) к (115), то есть реализация гомоморфизма ρ, представляет собой формальную замену элементов $\mathbf{g}^k\in\mathbb{A}$ для $1\le k<p^s$ элементами ω^k с последующим преобразованием результатов

(по желанию пользователя) к стандартной алгебраической форме записи комплексных чисел.

Так как множество $\left\{\omega^k\right\}$ разбивается на пары комплексно-сопряженных чисел, то для получения комплексных последовательностей $X_\nu(m)$ требуется не более

$$M_2(N) = p^{2s}(p-1)T = p^{2s}(p-1)p^{r-s+1} \le p^{s+1}N$$

операций вещественного умножения. Далее, учитывая, что умножение комплексных чисел требует выполнения трех вещественных умножений, получаем для мультипликативной сложности $M(N)$ вычисления полного спектра $X(m)$ рекуррентное соотношение:

$$M(N) = M\left(N/p\right) + M^*(T) + 3M_2(T) + 3p^{s-2}(p-1)N.$$

Отсюда получаем

$$M(N) - M\left(N/p\right) \le \frac{1}{s}\left(1 - 1/p^s\right)\mu(q)T\left(\log_p T - s\right) + 3p^{s-1}N\left(p^2+1\right) \qquad (116)$$

и, после несложных преобразований, оценку теоремы 5.

Пусть $s = s(N)$. Тогда для фиксированного p при

$$p^s \sim \log_p^\theta N; \quad 0 < \theta < 1; \quad N \to \infty$$

в (110) доминирует первое слагаемое. Поэтому справедливо следующее утверждение.

Теорема 6. Для любого простого нечетного числа p существуют положительные константы δ_1 и δ_2, зависящие только от p и θ, и алгоритм вычисления ДПФ для которого при $N = p^r > N_0(\theta)$ справедливо асимптотическое соотношение:

$$M(N) \le \delta_1 \frac{N\log_p N}{\log_p \log_p N} + \delta_2 N \log_p^\theta N. \qquad (117)$$

6.4. Некоторые специальные случаи

При доказательствах Теорем 4 – 6 было сделано два допущения:

- p является простым нечетным числом;

- в условиях Теоремы 5 предполагалось, что $s > 2$.

Эти ограничения не являются существенными, но доказательства лемм и теорем требуют некоторой корректировки. Так как такая корректировка достаточно очевидна, автор счел возможным ограничиться лишь соответствующими формулировками и минимальными комментариями.

Случай А. Если $p = 2$, то специфической особенностью является наличие двух вещественных корней степени N из единицы.

Пусть $q = 2^s \ (2 \le s < r)$, G – циклическая группа из q элементов с образующим и нейтральным элементами **g** и **e**, соответственно; $\mathbf{A}_2 = \mathbf{A}_2(\mathbf{G},\mathbf{R})$ - групповая R – алгебра.

Лемма 21А. Пусть $w, z \in \mathrm{A}_2$,

$$w = w_1\mathbf{g}^{q/2-1} + w_2\mathbf{g}^{q/2+1} = w_1\mathbf{g}^{-} + w_2\mathbf{g}^{+}. \qquad (118)$$

Тогда для вычисления произведения zw достаточно

$$\mu_2(q) = 3(q/2-1)+4$$

вещественных умножений.

Доказательство. Аналогично доказательству Леммы 21, вычисление произведения zw сводится к $(q-2)/2$ умножениям элементов типа (118) и вычислению произведений $z_0 w$ и $w z_{q/2}$, требующих четырех вещественных умножений.

Лемма 22А. Пусть $\mathbf{J}_2$ - идеал алгебры $\mathbf{A}_2$, порожденный элементами

$$c_\nu = \mathbf{g}_\nu^2 - 2\mathbf{g}_\nu \cos 2\pi\nu/q + \mathbf{e},$$

тогда имеет место изоморфизм R-алгебр: $\mathbf{A}_2/\mathbf{J}_2 \cong \mathbf{C}$.

Лемма 23А. Пусть элемент $b \in \mathbf{A}_2$ имеет вид:

$$b = \sum_{\substack{1 \le \nu \le 2^{s-2} \\ \nu \equiv 1 (\mathrm{mod}\, 2)}} \beta_\nu \mathbf{g}^\nu, \quad \beta_\nu \in \mathbf{R}.$$

Тогда из системы уравнений

$$\sum_{\substack{1 \le \nu \le 2^{s-2} \\ \nu \equiv 1 (\mathrm{mod}\, 2)}} \beta_\nu \rho \circ \varepsilon_\tau \left(\mathbf{g}^\nu \right) = \rho \circ \varepsilon_\tau (b) \qquad (\tau, q) = 1$$

однозначно определяются коэффициенты β_ν.

Лемма 24А. Пусть $T = 2^t \ (t > s)$,

$$w_m = w_m^+ \mathbf{g}^+ + w_m^- \mathbf{g}^-,$$

$$w_m^+ = \left(\left(2\cos 2\pi (q-1)/2q \right)^{-1} - \left(2\sin 2\pi (q-1)/2q \right)^{-1} \right) \cos 2\pi m/T,$$

$$w_m^- = \left(\left(2\cos 2\pi (q-1)/2q \right)^{-1} - \left(2\sin 2\pi (q-1)/2q \right)^{-1} \right) \sin 2\pi m/T.$$

Тогда $\rho(w_m) = \rho\left(w_1^m\right) = \zeta^m$, где ζ - первообразный корень степени T в C.

Теорема 4А. Вычисление спектра $A(m)$ при $T = 2^t$ требует не более

$$M_2^*(T) = s^{-1}\left(1 - 2^{-s}\right)\left(3\left(q/2 - 1\right) + 2\right) T(\log_2 T - s)$$

операций вещественного умножения.

Теорема 5А. Для любого натурального $N = 2^r$ и s с условием $2 \le s < r$ существует БА ДПФ с мультипликативной сложностью

$$M(N) \le K s^{-1} N \log_2 N + K_2 2^s N,$$

где K_1 и K_2 - абсолютные константы.

Выбирая далее $s = s(N)$ как в Теореме 6, аналогично получаем справедливость (116) и при $p = 2$.

Случай В. Основное отличие этого случая состоит в несколько иной правой части равенства (102), которое справедливо в форме:

$$\sum_{\substack{(\tau,\,p)=1\\ 1\le\tau\le p}} \rho\left(\mathbf{g}^{a\tau}\right)=\begin{cases}-1, & \text{если } a\neq 0\,(\mathrm{mod}\ p);\\ p-1, & \text{если } a\equiv 0\,(\mathrm{mod}\ p).\end{cases} \tag{119}$$

Решение соответствующей системы линейных уравнений с матрицей

$$\begin{pmatrix} p-1 & -1 & \dots & -1\\ -1 & p-1 & \dots & -1\\ \dots & \dots & \dots & \dots\\ -1 & -1 & \dots & p-1 \end{pmatrix} \tag{120}$$

требует только сложений и умножений на одну и ту же константу, которые могут быть объединены с умножениями при реконструкции полного спектра.

Доказательство Теоремы 5 корректируется следующим образом.

Вводя обозначения $x_y(n)=x(pn+y)$, $T=p^{r-1}=p^t$, получаем из (111)

$$X(m)=\sum_{n=0}^{N/p-1} x(pn)\left(\gamma^p\right)^{mn}+\sum_{\substack{n=0\\(n,\,p)=1}}^{N-1} x(n)\gamma^{mn}. \tag{121}$$

Первая сумма в (121) сводится к ДПФ длины $T=N/p$; вторая преобразуется к виду:

$$\sum_{\substack{n=0\\(n,\,p)=1}}^{N-1} x(n)\gamma^{mn}=\sum_{y=1}^{p-1}\gamma^{my}\sum_{n=0}^{T-1} x_y(n)\left(\gamma^p\right)^{mn}=\sum_{y=1}^{p-1}\gamma^{my}X_y(m), \tag{122}$$

где

$$X_y(m)=\sum_{n=0}^{T-1} x_y(n)\left(\gamma^p\right)^{mn}.$$

Определим последовательность $a(n)$ элементов из A равенством

$$a(n)=x_1(n)\mathbf{g}+\dots+x_{p-1}(n)\mathbf{g}^{p-1}.$$

Пусть вычисление спектра $A(m)$ этой последовательности производилось в соответствии с доказательством Теоремы 4 и потребовало $M_1^*(T)$ операций вещественного умножения.

Положим для $\varepsilon_\tau \in \boldsymbol{\varepsilon}$:

$$D_\tau(m) = b_\tau^+ \varepsilon_\tau\big(A(m)\big) + b_\tau^- \varepsilon_\tau^*\big(A(m)\big).$$

Определим последовательности $\Delta_\nu(m) \in \mathbf{A}$ равенствами:

$$\Delta_\nu(m) = \sum_{\substack{(\tau,q)=1 \\ 1\le\tau\le p}} \mathbf{g}^{-\nu\tau} D_\tau(m). \tag{123}$$

Тогда, действуя на (123) гомоморфизмом ρ, получаем для определения массивов $X_\nu(m)$ линейную систему уравнений с матрицей (120). Получение последовательностей $D_\tau(m)$ в алгебре **A** требует не более

$$M_1'(N) = 2(p-1)\,pT \le 2p^2T = 2pN$$

вещественных умножений. Реализация гомоморфизма ρ, то есть замена элементов $\mathbf{g}^k \in \mathtt{A}$ элементами $\omega^k \in \mathbf{C}$ и получение массивов $X_\nu(m)$ требует не более $M_2'(N) = (p-1)^2\,T \le pN$ операций вещественного умножения. Далее, учитывая, что умножение комплексных чисел требует трех вещественных умножений, получаем для мультипликативной сложности $M(N)$ вычисления полного спектра $X(m)$ рекуррентное соотношение:

$$M(N) \le M\left(N/p\right) + M_1'(T) + 3M_2'(T) + 3(p-1)N.$$

Отсюда получаем

$$M(N) - M\left(N/p\right) \le \left(1-p^{-s}\right)\mu(p)\,T\left(\log_p T - 1\right) + 6p^2T$$

и, после несложных преобразований, асимптотическую оценку

$$M(N) = \left(3p+1/2p\right)N\log_p N + O(N). \tag{125}$$

КОММЕНТАРИИ К ТЕКСТУ

Содержание книги относится к пограничной области между информатикой (теория и практика анализа и обработки многомерных цифровых сигналов) и математикой (абстрактная алгебра и теория чисел).

Специалисты в области анализа и обработки цифровой информации давно и успешно используют алгебраические и теоретико-числовые методы, прежде всего, в таких областях, как криптография, корректирующие коды, синтез быстрых алгоритмов дискретных ортогональных преобразований. Несмотря на это, существует относительно мало доступной монографической литературы, охватывающей не только одну или несколько из указанных уже традиционных областей применения методов абстрактной алгебры и теории чисел к решению задач информатики, но и рассматривающей относительно новые приложения указанных математических методов и теорий к решению перспективных задач анализа цифровых сигналов. Ряд монографий отечественных или зарубежных авторов давно уже стал библиографической редкостью, а книги, изданные за рубежом, практически недоступны широкому кругу специалистов.

Данное пособие ставит своей целью отчасти восполнить указанный пробел. Оно предназначается для специалистов в области цифровой обработки сигналов и изображений, в области прикладной математики, а также для использования в учебном процессе - студентам и аспирантам по прикладной математике и информатике.

Автор не нашел слов более точных, чем прочитанные им в книге Г.Вейля "Классические группы, их инварианты и представления", которыми по мере возможностей руководствовался при написании этой книги:

"…предмет этой книги довольно специальный. Как бы важны ни были общие понятия и предложения, которыми одарило нас современное деятельное увлечение аксиоматизированием и обобщениями, распространенное в алгебре, быть может, большее, чем в какой бы ни было другой области, - все же я убежден в том, что именно специальные проблемы во всей их сложности составляют опору и стержень математики; и преодоление их трудностей требует, вообще говоря, наиболее серьезных усилий <…>. Общие теории показаны здесь в их возникновении из специальных проблем, анализ которых приводит к этим теориям как действенному инструменту решения, с почти принудительной необходимостью; но, однажды

появившись, эти теории освещают широкую область за пределами ограниченного участка их возникновения. <…> Книга предназначена, главным образом, для тех, кто скромно хочет узнать изложенные в ней новые вещи, а не для гордых ученых, уже знакомых с предметом и желающих получить лишь быструю или точную справку о той или иной детали. Она не является ни элементарным учебником, ни монографией. В том же духе выдержаны ссылки на литературу".

Автор затрудняется установить авторство совмещенного алгоритма вычисления ДПФ вещественного сигнала. Такой алгоритм описан, в частности, в монографии [22], но уже в то время рассматривался как фольклорный. Общие принципы синтеза быстрых алгоритмов многомерных совмещенных ДПФ были опубликованы автором в [10]. Также в [10] было введено "кватернионное ДПФ" как вспомогательное преобразование при вычислении комплексного двумерного ДПФ. Впоследствии как самостоятельное преобразование кватернионное ДПФ было введено в работе [23] и получило достаточно широкое распространение [24]. Использование других алгебр для реализации различных версий базовой идеи совмещенного вычисления дискретных ортогональных преобразований описаны в [13]-[19].

В монографиях [20],[21] для БА "по основанию p" ДПФ комплексной входной последовательности приведены оценки мультипликативной сложности $M^c(N)$, из которых следует асимптотическое соотношение

$$M^c(N) = \lambda N \log_p N + O(N), \quad \lambda = \lambda_1(p) = \left(3(p-1) + M(p)\right) p^{-s}. \qquad (126)$$

Из (125) для комплексной входной последовательности следует асимптотическое соотношение (126), где

$$\lambda = \lambda_0(p) = (3p+1)\, p^{-s}. \qquad (127)$$

Сравнение (126) с (127) показывает, что $\lambda_0 < \lambda_1$ при всех p, для которых $M(p) > 4$. С учетом известных нижних оценок Винограда мультипликативной сложности ДПФ длины, равной простому числу [3], для $M(p)$ получаем, что при $p > 3$ даже наиболее структурно простая версия БА, рассмотренного в разд. 3.3, требует асимптотически меньшего числа умножений, чем БА ДПФ по "основанию p" с оптимальной реализацией коротких ДПФ длины p.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ван Дер Варден, Б.Л. Алгебра / Б. Л. Ван Дер Варден - М.: Наука, 1976.-648с.
2. Артин, Э. Геометрическая алгебра / Э.Артин - М.: Наука, 1969. – 312 с.
3. Блейхут, Р. Быстрые алгоритмы цифровой обработки сигналов / Р.Блейхут - М.: Мир, 1987. - 448с
4. Chernov, V.M. Parametrization of some classes of fast algorithms of discrete orthogonal transforms /V.M.Chernov // Pattern Recogn. and Image Analysis. N 2. V.5, 1995. P.238-245.
5. Виноградов, И.М. Основы теории чисел / И.М.Виноградов - М.: Наука, 1965. - 172с.
6. Chernov, V.M. Fast algorithms of discrete orthogonal transforms for data represented in cyclotomic fields / V.M.Chernov // Pattern Recogn. and Image Analysis. N 4. V.3, 1993. P.455-458.
7. Чернов, В.М. Быстрый алгоритм дискретного косинусного преобразования нечетной длины / В.М.Чернов // Автоматика и вычислительная техника. N 3, 1994. С.62-70.
8. Чернов В.М. Алгоритмы дискретного преобразования Фурье с представлением данных в полях алгебраических чисел. / В.М.Чернов // Автоматика и выч. Техника. N 4, 1994. С.64-69.
9. Чернов, В.М. Новый алгоритм дискретного преобразования Фурье по основанию пять / В.М.Чернов // Компьютерная оптика. N 14, 1995. С.4-12.
10. Chernov, V.M. Arithmetic method in the theory of discrete orthogonal transforms / V.M.Chernov // SPIE. V.2363, 1995. P.134-141.
11. Чернов В.М. Алгоритмы дискретных ортогональных преобразований, реализуемые в кодах Гамильтона-Эйзенштейна. / В.М.Чернов // Пробл. передачи информ. N 3. Т.31, 1995. С. 38-46.
12. Chernov, V.M. Discrete orthogonal transforms with data representation in composition algebras / V.M.Chernov // Proc.of the 9th Scandinavian Conference on Image Analysis (SCIA'95). V 1, 1995. P. 357-364.

13. Chernov, V.M. Synthesis of fast algorithms for discrete Fourier-Clifford transform /V.M.Chernov, T. Buelov, G.Sommer // Pattern.Recognition and Image Analysis. N 2. V.8, 1998. P. 274-275.
14. Felsberg, M. Fast Algorithms of Hypercomplex Fourier Transforms / M.Felsberg, G.Sommer, V.M.Chernov // Geometric Computing with Clifford Algebras. Springer Verlag, 2000. P. 231-254.
15. Chernov, V.M. Clifford algebras are group algebras projections / V.M.Chernov, E.Bayro-Corrochano, G.Sobczyk // Advanches in Geometric Algebra with Applications in Science and Engineering.-Birkhauser, Boston, 2001. - P.467-482.
16. Чернов, В.М. Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М.Чернов. - М.:Наука, – 2007. - 328 с.
17. Aliev, M.V. Two-dimensional FFT-Like Algorithms with Overlapping in Some Hypercomplex Algebras / M. V. Aliev, V. M. Chernov // Optical Memory and Neural networks, N 1, V.11, 2002. P.29-38.
18. Chernov, V.M Two FFT-like algorithms for calculation of multi-channel spectra/ V.M.Chernov // Proc. of Int. Conf. "Automation, Control, and Information Technology". 2002. P.560-565.
19. Chernov, V. Some FFT-Like Algorithms for RGB-Spectra Calculation / V.Chernov // Machine GRAPHIC&VISION. V.11, 2002. P. 139-151.
20. Власенко, В. А. Методы синтеза быстрых алгоритмов свертки и спектрального анализа сигналов / В.А.Власенко, Ю.М.Лаппа, Л.П.Ярославский. - М.: Наука, 1990. - 180с.
21. Крот, А. М. Дискретные модели динамических систем на основе полиномиальной алгебры /А.М.Крот. - Минск: Навука і тэхніка, 1990. - 311 с.
22. Ярославский, Л.П. Введение в цифровую обработку изображений / Л.П.Ярославский. - М.: Радио и связь, 1987. – 287 с.
23. Sangwine, S.J. Fourier transform of color images using quaternion or hypercomplex numbers / S.J.Sangwine // Electron. Letters. N 21. v32, 1996. P.1979-1980.
24. Sommer, G. Geometric Computing with Clifford Algebras / G.Sommer. - Springer Verlag, 2000. – 765 с.

СОДЕРЖАНИЕ