*В.М. Чернов*

# НОВЫЙ АЛГОРИТМ ДИСКРЕТНОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ ПО ОСНОВАНИЮ ПЯТЬ

## ВВЕДЕНИЕ

При реализации хорошо известных и подробно описанных [1,2] "совмещенных" алгоритмов дискретного преобразования Фурье (ДПФ) вещественных последовательностей четной длины N используется избыточность представления входных данных по отношению к комплексным значениям базисных функций преобразования. Точнее, преобразование последовательности длины N сводится к преобразованию комплексной последовательности длины $N/2$, связанной с исходной, и некоторому (не очень большому) числу дополнительных умножений. Независимо от выбранной схемы совмещения, возможность применения такого приема обеспечивается наличием в поле комплексных чисел C нетождественного автоморфизма, реализуемого тривиально. Попытка синтеза быстрых алгоритмов ДПФ (БПФ) с "многократным совмещением", реализуемых в комплексной арифметике, наталкивается на принципиальные трудности, связанные с отсутствием в поле C достаточного числа тривиально реализуемых автоморфизмов. Синтез БПФ с многократным совмещением в иной, отличной от C, алгебраической структуре рассматривался автором в [3,4]. В качестве таких структур использовались композиционные алгебры [3], циклотомические расширения поля рациональных чисел [4].

Следует также отметить, что наиболее сильные в количественном отношении результаты относятся к синтезу быстрых алгоритмов ДПФ длины $N = 2^k$. В этом случае асимптотическая при $N \to \infty$ оценка вещественной мультипликативной сложности M(N) алгоритмов имеет вид:

$$M(N) = CN\log_2 N + O(N). \tag{1}$$

Для большинства современных алгоритмов $C = 1/2$. Алгоритмы работы [4], для которых $C = 3/7, 2/5$ и т. д. представляют, по всей видимости, примеры БПФ, для которых снижение значения константы C в (1) все еще компенсирует увеличение структурной сложности алгоритма в разумном для пользователя диапазоне значений N.

В отличие от случая $N = 2^k$, БПФ для $N = p^k$ ( p − простое ) разработаны менее детально и по своим вычислительным характеристикам относительно уступают БПФ для $N = 2^k$. Например, наилучшая известная автору оценка мультипликативной сложности БПФ комплексной входной последовательности при $N = 5^k$ имеет вид [2]:

$$M(N) = 4{,}4N\log_5 N - 3N + 3. \tag{2}$$

Как справедливо утверждается в [5], популярность БПФ алгоритма Кули–Тьюки привела к тому, что БПФ–алгоритмы стали диктовать параметры применяемых устройств вместо того, чтобы приложения диктовали выбор подходящего алгоритма БПФ.

В настоящей работе синтезируются алгоритмы ДПФ для $N = 5^k$ с многократным (точнее, восьмикратным) совмещением в алгебре матриц второго порядка над квадратичным полем, у которых оценка для M(N) асимптотически лучше чем (2).

Возможность построения таких БПФ обеспечивается, в основном, тремя факторами: во–первых, возможностью вложения поля комплексных чисел в алгебру матриц второго порядка с коэффициентами из $\mathbf{R}$; во–вторых, наличием в этой алгебре четырех автоморфизмов, реализуемых без вещественных умножений; в–третьих, уникальным арифметическим свойством первообразного корня пятой степени из единицы, вещественная часть которого является элементом квадратичного расширения поля рациональных чисел с минимальным многочленом, имеющим коэффициенты, равные (±1).

## 1. НЕКОТОРЫЕ СВОЙСТВА АЛГЕБР $(2 \times 2)$–МАТРИЦ

Отметим ряд известных или легко доказываемых свойств алгебры $(2 \times 2)$–матриц $\mathbf{M}_2(\mathbf{R})$. Автор счел возможным опустить доказательства, сводящиеся к непосредственной проверке матричных тождеств.

Предложение 1.1. Алгебра $\mathbf{M}_2(\mathbf{R})$ является четырехмерной ассоциативной $\mathbf{R}$–алгеброй. Матрицы

$$\mathbf{E} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{T} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{R} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{I} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

образуют базис $\mathbf{M}_2(\mathbf{R})$ над $\mathbf{R}$, то есть любая матрица $\mathbf{A}$ из $\mathbf{M}_2(\mathbf{R})$ представима в виде

$$\mathbf{A} = \gamma_0\mathbf{E} + \gamma_1\mathbf{T} + \gamma_2\mathbf{R} + \gamma_3\mathbf{I}$$

с подходящими $\gamma_0, \gamma_1, \gamma_2, \gamma_3 \in \mathbf{R}$.

Предложение 1.2. Базисные матрицы **E**, **T**, **R**, **I** имеют конечные мультипликативные порядки:

$$\mathbf{E} = \mathbf{T}^2 = \mathbf{R}^2 = \mathbf{I}^4.$$

Отображения $\theta$, $\rho$, $\iota$ алгебры $\mathbf{M}_2(\mathbf{R})$ на себя:

$$\theta\colon \mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \mathbf{TAT} = \begin{pmatrix} d & c \\ b & a \end{pmatrix}, \quad \rho\colon \mathbf{A} \mapsto \mathbf{RAR} = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}, \quad \iota\colon \mathbf{A} \mapsto \mathbf{I}^{-1}\mathbf{AI} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

являются (внутренними) автоморфизмами алгебры $\mathbf{M}_2(\mathbf{R})$.

Предложение 1.3. Автоморфизмы $\theta$, $\rho$, $\iota$ действуют на базисные элементы **T**, **R**, **I** следующим образом:

$$\theta(\mathbf{T}) = \mathbf{T}, \quad \rho(\mathbf{T}) = -\mathbf{T}, \quad \iota(\mathbf{T}) = -\mathbf{T};$$
$$\theta(\mathbf{R}) = -\mathbf{R}, \quad \rho(\mathbf{R}) = \mathbf{R}, \quad \iota(\mathbf{R}) = -\mathbf{R};$$
$$\theta(\mathbf{I}) = -\mathbf{I}, \quad \rho(\mathbf{I}) = -\mathbf{I}, \quad \iota(\mathbf{I}) = \mathbf{I}.$$

Предложение 1.4. Пусть $\mathbf{A} \in \mathbf{M}_2(\mathbf{R})$:

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

тогда справедливы соотношения:

$$\begin{cases} \mathbf{A} + \rho(\mathbf{A}) + \theta(\mathbf{A} + \rho(\mathbf{A})) = 2(a + d)\mathbf{E}, \\ [\mathbf{A} - \rho(\mathbf{A}) + \theta(\mathbf{A} - \rho(\mathbf{A}))]\mathbf{T} = 2(b + c)\mathbf{E}, \\ [\mathbf{A} - \theta(\mathbf{A}) + \rho(\mathbf{A}) - \iota(\mathbf{A})]\mathbf{R} = 2(a - d)\mathbf{E}, \\ [\mathbf{A} - \theta(\mathbf{A}) - \rho(\mathbf{A}) + \iota(\mathbf{A})]\mathrm{I}^{-1} = 2(b - c)\mathbf{E}, \end{cases} \tag{3}$$

и решение системы (3) требует вещественных умножений только на степени двойки, которые считаются более элементарной операцией.

Отметим, что соотношения (3) справедливы и для матриц над кольцом достаточно общего вида.

Предложение 1.5. Пусть $c = \cos 2\pi/5$, $s = \sin 2\pi/5$, $\beta = 2c$,

$$\mathbf{S} = \begin{pmatrix} c & s \\ -s & c \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} \beta & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathrm{A} = \begin{pmatrix} \alpha & 1 \\ -1 & 0 \end{pmatrix}.$$

Тогда существует невырожденная матрица $\mathbf{C}$ такая, что

$$\mathbf{B} = \mathbf{C}^{-1}\mathbf{S}\,\mathbf{C}.$$

Доказательство. Утверждение непосредственно следует из того, что матрицы $\mathbf{S}$ и $\mathbf{B}$ имеют одно и то же характеристическое уравнение $\lambda^2 - \beta\lambda + 1 = 0$ с корнями

$$\lambda_{1,2} = \exp\{\pm 2\pi/5\}.$$

Предложение 1.6. Матрица $\mathbf{B}$ имеет мультипликативный порядок, равный пяти, причем:

$$\mathbf{B}^5 = \mathbf{E}, \quad \mathbf{B}^{-1} = \mathbf{B}^4, \quad \mathbf{B}^2 = \beta\mathbf{B} - \mathbf{E}, \quad \mathbf{B}^3 = \beta\mathbf{B}^{-1} - \mathbf{E}.$$

Пусть $\alpha$ и $\beta$ являются корнями уравнения

$$t^2 + t - 1 = 0,$$

$\mathbf{Q}(\alpha)$ и $\mathbf{Q}(\beta)$ – алгебраические расширения поля рациональных чисел с примитивными элементами $\alpha$ и $\beta$ соответственно:

$$\mathbf{Q}(\alpha) = \{\ w = u + v\alpha;\ u, v \in \mathbf{Q}\ \};\ \mathbf{Q}(\beta) = \{\ w = u + v\beta;\ u, v \in \mathbf{Q}\ \}. \tag{4}$$

Пару чисел $(u,v)$, ассоциированную с представлением (4) элементов полей $\mathbf{Q}(\beta)$ и $\mathbf{Q}(\alpha)$, будем называть кодом элемента $w$ и обозначать $<w>$.

Так как $\alpha$ и $\beta$ являются корнями одного и того же уравнения, то сложение и умножение в кодах для $\mathbf{Q}(\alpha)$ и $\mathbf{Q}(\beta)$ определяются с помощью одних и тех же правил:

$$(u_1, v_1) + (u_2, v_2) = ((u_1 + u_2), (v_1 + v_2)), \tag{5}$$

$$\left(u_1,v_1\right)\times\left(u_2,v_2\right)=\left(\left(u_1u_2+v_1v_2\right),\left(u_1v_2+u_2v_1-v_1v_2\right)\right). \tag{6}$$

Распространим правила сложения и умножения (5)–(6) пар на $\mathbb{R}\times\mathbb{R}$, задав тем самым структуру кольца, которое обозначим $\mathbb{J}$. Кольцо матриц с коэффициентами из кольца $\mathbb{J}$ обозначим $\mathbf{M}_2(\mathbb{J})$; матрицы $\mathbf{X}$, компоненты которых заданы кодами, будем обозначать $<\mathbf{X}>$.

Предложение 1.7. Пусть $\mathbf{W}$ – матричный корень степени N = 5K из E:

$$\mathbf{W}=\begin{pmatrix} c_N & s_N \\ -s_N & c_N \end{pmatrix},$$

где $c_N=\cos{}^{2\pi}\!/_N$, $s_N=\sin{}^{2\pi}\!/_N$. Тогда матрица $\mathbf{V}=\mathbf{C}^{-1}\mathbf{W}\,\mathbf{C}$, где $\mathbf{C}$ – матрица, определенная в предложении 1.5, является корнем уравнений $\mathbf{V}^K=\mathbf{B}$, $\mathbf{V}^N=\mathrm{E}$.

Предложение 1.8. Существуют $q_0,q_1\in\mathbb{R}$ такие, что матрица $\mathbf{V}$ представима в виде

$$\mathbf{V}=q_0\mathbf{E}+q_1\mathbf{B}. \tag{7}$$

Доказательство. В самом деле, так как

$$\left(c_N\mathbf{E}+s_N\mathbf{I}\right)^K=\mathbf{S},$$

то

$$\left(c_N\mathbf{E}+s_N\mathbf{C}^{-1}\mathbf{I}\,\mathbf{C}\right)^K=\mathbf{B},$$

а так как из предложения 1.5 следует, что

$$c\,\mathbf{E}+s\,\mathbf{C}^{-1}\mathbf{I}\,\mathbf{C}=\mathbf{B},$$

то, полагая

$$q_1={}^{s_N}\!/_s,\quad q_0=c_N-{}^{cs_N}\!/_s,$$

получаем требуемое. Отсюда следует также справедливость представления (6) с подходящими $q_{0m},q_{1m}\in\mathbb{R}$ и для матриц $\mathbf{V}^m$.

Непосредственное умножение матрицы из $\mathbf{M}_2(\mathbb{J})$ на степени матрицы $<\mathbf{V}>$ требует шестнадцати вещественных умножений. Но, в силу предложения 1.8, матрица $<\mathbf{V}^m>$ имеет специфический вид:

$$<\mathbf{V}^m>=\begin{pmatrix} (x,y) & (y,0) \\ (-y,0) & (x,0) \end{pmatrix}$$

с некоторыми $x,y\in\mathbb{R}$. Эта специфика позволяет построить алгоритм сокращенного умножения.

Предложение 1.9. Умножение матрицы из $\mathbf{M}_2(\mathbb{J})$ на степени матрицы $<\mathbf{V}>$ требует четырнадцати вещественных умножений.

Доказательство. Действительно, так как

$$\left((a,b);(c.d)\right)\begin{pmatrix}(x,y) & (y,0)\\ (-y,0) & (x,0)\end{pmatrix} = \tag{8}$$
$$= \left((ax + by - cy, bx - dy + ay - by);(ay + cx, by + dx)\right) = \left((X,Y);(Z,T)\right),$$

то при

$$a_1 = (a-b)y, \quad a_2 = bx, \quad a_3 = dy, \quad a_4 = y(b-c), \tag{9}$$
$$a_5 = ax, \quad a_6 = c(x+y), \quad a_7 = x(d-c)$$

имеем

$$X = a_4 + a_5, \quad Y = a_1 - a_3 + a_2, \tag{10}$$
$$Z = a_1 + a_4 + a_6, \quad T = a_4 + a_6 + a_7.$$

Поэтому вычисление левой части (8) требует, согласно (9) и (10), семи вещественных умножений, а умножение матрицы из $\mathbf{M}_2(\mathbb{J})$ на степени матрицы <V> – четырнадцати вещественных умножений.

Пусть далее $<\mathbf{x}> = (x_1, x_2) \in \mathbb{J}$,

$<\mathbf{x}>_\alpha = x_1 + x_2\alpha, \quad <\mathbf{x}>_\beta = x_1 + x_2\beta;$

аналогичный смысл имеют обозначения $<\mathbf{V}>_\alpha$ и $<\mathbf{V}>_\beta$ для матриц.

Предложение 1.10. Существуют невырожденная матрица $F \in \mathbf{M}_2(\mathbb{R})$ и целое число d, такие что справедливо соотношение

$<\mathbf{V}^d>_\alpha = \mathbf{F}^{-1}\,\mathbf{W}\,\mathbf{F}.$

Доказательство. Достаточно показать, что $<\mathbf{V}>_\alpha$ является первообразным матричным корнем степени N из E. А это следует из предложения 1.7 и непосредственно проверяемых равенств:

$$\left[<\mathbf{V}>_\alpha\right]^N = \left[<\mathbf{V}^K>_\alpha\right]^5 = \left[<\mathbf{B}>_\alpha\right]^5 = \left[<\mathbf{A}>_\alpha\right]^5 = \left[<\mathbf{A}>_\alpha\right]^5 = \mathbf{A}^5 = \mathbf{E}.$$

## 2. БЫСТРЫЙ АЛГОРИТМ ВЫЧИСЛЕНИЯ ОДНОГО МАТРИЧНОГО ПРЕОБРАЗОВАНИЯ

Основную роль при синтезе рассматриваемого алгоритма ДПФ длины $N = 5^k$ играет следующее утверждение.

Предложение 2.1. Пусть $<\mathbf{h}(n)>$ – последовательность матриц периода $N = 5^k$ с коэффициентами из $\mathbb{J}$. Пусть $\{<H(m)>\}$ – "матричный спектр" последовательности $\{\mathbf{h}(n)\}$:

$$\langle H(m)\rangle = \sum_{n=0}^{N-1}\langle \mathbf{h}(n)\rangle\langle V^{mn}\rangle, \quad (m = 0, 1, \ldots, N-1), \tag{11}$$

где V – матрица, определенная в предложении 1.8. Тогда для вычисления $\{<H(m)>\}$ достаточно

$$M^{*}(N)=\frac{56}{5}N\left(\log_5 N-1\right) \tag{12}$$

вещественных умножений.

Доказательство. Представим $\langle \mathbf{H}(m)\rangle$ в форме:

$$<\mathbf{H}(m)>=\sum_{a=0}^{4}\left[\sum_{n=0}^{N/5-1}<\mathbf{h}(5n+a)><\mathbf{V}^{5mn}>\right]<\mathbf{V}^{am}>=\sum_{a=0}^{4}<\mathbf{H}_a(m)><\mathbf{V}^{am}>. \tag{13}$$

Внутренние суммы в (13) представляют собой преобразования (11) длины N/5. Их достаточно вычислить для значений m, лежащих в "фундаментальной области":

$$\Delta_0=\left\{0,1,\ldots,N/5-1\right\}.$$

Действительно, значения $<\mathbf{H}_a(m)\mathbf{V}^{am}>$ для m, лежащих в областях $\Delta_b$, полученных из $\Delta_0$ аддитивным сдвигом на $Nb/5$ (b = 1, 2, 3, 4 ), отличаются от соответствующих значений $<\mathbf{H}_a(m)\mathbf{V}^{am}>$ только умножениями на степени матрицы $\langle \mathbf{B}\rangle$, которые реализуются без нетривиальных вещественных умножений. Соотношение (13), таким образом, редуцирует вычисление матричного спектра длины N к вычислению матричных спектров пяти последовательностей длины N/5 и некоторому числу дополнительных умножений на $<\mathbf{V}^{am}>$ для $m\in\Delta_0$. Считая, что умножения матриц на степени $\langle \mathbf{V}\rangle$ реализованы согласно предложению 1.9, получаем для $M^{*}(N)$ рекуррентное соотношение:

$$M^{*}(N)=5M^{*}\left(N/5\right)+4\times 14\times N/5$$

с начальным условием $M^{*}(5)=0$, решение которого дает (12).

## 3. БЫСТРЫЙ АЛГОРИТМ ВЫЧИСЛЕНИЯ ПРЕОБРАЗОВАНИЯ ФУРЬЕ КОМПЛЕКСНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Пусть z(n) = x(n) + y(n)i − комплексная T−периодическая последовательность, Z(m) − спектр Фурье:

$$Z(m)=\sum_{n=0}^{T-1}z(n)\omega^{mn},\quad \left(m=0,1,\ldots,T-1,\quad \omega=\exp\left\{2\pi i/T\right\},\quad T=5^t\right). \tag{14}$$

Предложение 3.1. Для вычисления Z(m) достаточно M(T) вещественных умножений, где

$$M(T)=\frac{14}{5}T\log_5 T+O(T). \tag{15}$$

Доказательство. Представим Z(m) в форме:

$$Z(m)=\sum_{n=0}^{T/5-1}z(n)\omega^{5mn}+\sum_{a=1}^{4}Z_a(m)\omega^{am},$$

где

$$Z_a(m) = \sum_{n=0}^{T/5-1} z(5n+a)\omega^{5mn} = \sum_{n=0}^{T/5-1} z_a(n)\omega^{5mn}. \qquad (16)$$

Для вычисления $Z_a(m)$ образуем матричную последовательность периода T/5 с коэффициентами из $\mathbf{J}$:

$$< \mathbf{h}(n) >= \begin{pmatrix} < z_1(n) > < z_2(n) > \\ < z_3(n) > < z_4(n) > \end{pmatrix}, \qquad \text{где } < z_s(n) >= \left(x_s(n), y_s(n)\right).$$

Для вычисления кодов матричного спектра $< \mathbf{H}(m) >$ последовательности $< \mathbf{h}(n) >$ достаточно, согласно предложению 2.1,

$$M^*\left(\frac{T}{5}\right) = \frac{56}{25}T\left(\log_5 T - 2\right)$$

вещественных умножений. Далее, реконструкция $Z_a(m)$ и Z(m) проводится по следующей схеме.

**Шаг 1.** Решая систему уравнений (3) для каждого m, находим

$$< \mathbf{H}_a(m) >= \sum_{n=0}^{T/5-1} z_a(n) < \mathbf{V}^{mn} >, \qquad (17)$$

что требует умножений только на степени двойки, которые мы не учитываем при анализе вычислительной сложности алгоритма.

**Шаг 2.** По известным кодам $< \mathbf{H}_a(m) >$ находим $< \mathbf{H}_a(m) >_\alpha$ и $< \mathbf{H}_a(m) >_\beta$, что требует 8T/5 вещественных умножений.

**Шаг 3.** В соответствии с предложением 1.5, имеем из (17):

$$\mathbf{C} < \mathbf{H}_a(m) >_\beta \mathbf{C}^{-1} = \sum_{n=0}^{T/5-1} < z_a(n) >_\beta \mathbf{W}^{mn}, \qquad (18)$$

а в соответствии с предложением 1.10, из (17) имеем:

$$\mathbf{F} < \mathbf{H}_a(dm) >_\alpha \mathbf{F}^{-1} = \sum_{n=0}^{T/5-1} < z_a(n) >_\alpha \mathbf{W}^{mn}. \qquad (19)$$

Поэтому для

$$\mathbf{X}_a(m) = \sum_{n=0}^{T/5-1} x_a(n)\,\mathbf{W}^{mn} \text{ и } \mathbf{Y}_a(m) = \sum_{n=0}^{T/5-1} y_a(n)\,\mathbf{W}^{mn}$$

справедливы равенства:

$$\begin{cases} 2\mathbf{X}_a(m) - \mathbf{Y}_a(m) = \mathbf{C} < \mathbf{H}_a(m) >_\beta \mathbf{C}^{-1} + \mathbf{F} < \mathbf{H}_a^\alpha(dm) >_\alpha \mathbf{F}^{-1}, \\ \sqrt{5}\mathbf{Y}_a(m) = \mathbf{C} < \mathbf{H}_a(m) >_\beta \mathbf{C}^{-1} - \mathbf{F} < \mathbf{H}_a^\alpha(dm) >_\alpha \mathbf{F}^{-1}. \end{cases} \qquad (20)$$

Отметим, что для нахождения левых частей равенств (18), (19) и решения системы (20) достаточно O(T) умножений.

**Шаг 4**. Окончательная реконструкция $Z_a(m)$ и $Z(m)$, как нетрудно проверить, сводится к вычислениям по формулам:

$$Z_a(m) = \mathbf{e}_1 \mathbf{X}_a(m) \mathbf{e}_1^\tau + i\mathbf{e}_2 \mathbf{Y}_a(m) \mathbf{e}_2^\tau$$

и (16) ( здесь $\mathbf{e}_1 = (1,0)$, $\mathbf{e}_2 = (0,1)$ – вектор–строки; $\tau$ – знак транспонирования ).

Таким образом, суммируя вышесказанное, для мультипликативной сложности $M(T)$ вычисления $Z(m)$ имеем рекуррентное соотношение:

$$M(T) = M\left(\frac{T}{5}\right) + \frac{56}{25} T\left(\log_5 T - 2\right) + O(T),$$

откуда следует оценка (15).

## 4. БЫСТРЫЙ АЛГОРИТМ ВЫЧИСЛЕНИЯ ПРЕОБРАЗОВАНИЯ ФУРЬЕ ВЕЩЕСТВЕННОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Пусть $f(n)$ – вещественная входная $T$–периодическая последовательность, $F(m)$ – спектр Фурье.

Предложение 4.1. Для вычисления $F(m)$ достаточно $M_1(T)$ вещественных умножений, где

$$M_1(T) = \frac{7}{5} T \log_5 T + O(T). \tag{21}$$

Доказательство. Представим $F(m)$ в форме:

$$F(m) = \sum_{n=0}^{K/25-1} f(n)\omega^{25mn} + \sum_{a=1}^{24} F_a(m)\omega^{am},$$

где

$$F_a(m) = \sum_{n=0}^{K/25-1} f(25n+a)\omega^{25mn} = \sum_{n=0}^{K/25-1} f_a(n)\omega^{25mn}.$$

Для вычисления $F_a(m)$ образуем три матричные последовательности периода $N/25$ с коэффициентами из $\mathbb{J}$:

$$<\mathbf{g}_s(n)> = \begin{pmatrix} \left(f_{1+8s}(n), f_{2+8s}(n)\right) & \left(f_{3+8s}(n), f_{4+8s}(n)\right) \\ \left(f_{5+8s}(n), f_{6+8s}(n)\right) & \left(f_{7+8s}(n), f_{8+8s}(n)\right) \end{pmatrix}, \qquad (s = 0, 1, 2),$$

понимая компоненты матриц $<\mathbf{g}_s(n)>$ как элементы кольца $\mathbb{J}$.

Производя вычисления матричных спектров $<\mathbf{G}_s(m)>$ и выделяя, как в предыдущем разделе, "частичные спектры" $F_a(m)$, получаем в этом случае для $M_1(T)$ рекуррентное соотношение:

$$M_1(T) = M\left(\frac{T}{25}\right) + 3\left(\frac{56}{125} T\left(\log_5 T - 3\right)\right) + O(T),$$

откуда следует (21).

## ЗАКЛЮЧЕНИЕ

Отметим ряд характерных особенностей предложенной методики синтеза БПФ с совмещением в матричных кольцах.

Для рассмотренного случая ($N = 5^k$, $(2 \times 2)$−матрицы ) основные идеи алгоритма реализуются в наиболее рафинированном виде. Их экстраполяция на общий случай $N = p^k$ (p − простое число) возможна при наличии тождеств со значительным числом "тривиальных" коэффициентов для матриц мультипликативного порядка p, аналогичных **B**. В частности, возможен синтез аналогичного алгоритма для $p = 7$ с совмещением в кольце $(3 \times 3)$ − матриц, для которого $C = \frac{30}{7}$ в оценке (1), что тоже несколько лучше оценки, приведенной в [2]. Нахождение таких тождеств (или доказательство их отсутствия) представляет собой весьма трудную математическую задачу, связанную с тонкими арифметическими свойствами значений базисных функций дискретного преобразования Фурье как элементов поля алгебраических чисел.

### Литература


1. *Крот А.М.* Дискретные модели динамических систем на основе полиномиальной алгебры. Минск: Навука і тэхника, 1990.

2. *Власенко В.А., Лаппа Ю.М., Ярославский Л.П.* Методы синтеза быстрых алгоритмов свертки и спектрального анализа сигналов. М.: Наука, 1990, 160с.

3. *Chernov V.M.* Arithmetic methods in the theory of discrete orthogonal transforms // Workshop on Digital Image Processing and Computer Graphics. Proceedings SPIE, V.2363, 1994.

4. *Чернов В.М.* Алгоритмы дискретного преобразования Фурье с представлением данных в полях алгебраических чисел // Автоматика и выч. техника. 1994, N 4. С.64−69.

5. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов. М.: Мир, 1987, 448с.

# New discrete Fourier transform algorithm to base five

*V.M. Chernov*

***Abstract***

When realizing the well-known and well-described [1,2] "combined" discrete Fourier transform (DFT) algorithms of real sequences with the even length N, the redundancy of input data in relation to the complex values of the basis transformation functions is used. More precisely, the transformation of a sequence with the length N reduces to the transformation of a complex sequence of length associated with the original one, and a certain (not very large) number of additional multiplications. Regardless of the matching scheme chosen, it is possible to apply this technique due to the presence of non-identical trivially realized automorphism in the field of complex numbers C. An attempt to synthesize fast multiple-matching DFT (FFT) algorithms realized in complex arithmetic encounters fundamental difficulties associated with the absence of a sufficient number of trivially realized automorphisms in field C. The synthesis of FFT with multiple matching in a different algebraic structure other than C was considered by the author in [3,4]. Compositional algebras [3] and cyclotomic extensions of the field of rational numbers we used as such structures.

*Citation*: Chernov VM. New discrete Fourier transform algorithm to base five. Computer Optics 1995; 14-15(2): 4-12.

***References***

[1] Krot AM. Discrete models of dynamical systems based on polynomial algebra; Minsk: Navuka i tekhnika; 1990.
[2] Vlasenko VA, Lappa YM, Yaroslavsky LP. Methods of synthesis of fast algorithms for signal convolution and spectral analysis; Moscow: Nauka Publisher; 1990; 160.
[3] Chernov VM. Arithmetic methods in the theory of discrete orthogonal transforms. Workshop on Digital Image Processing and Computer Graphics. Proceedings SPIE; 1994; V.2363.
[4] Chernov VM. The FFT algorithms with data representation in algebraic number fields. Automatic Control and Comp. Sci.; 1994; 4: 64-69.
[5] Blahut R. Fast algorithms of digital signal processing; Moscow: Mir Publisher; 1987; 448.