

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 $N \rightarrow \infty$ оценка вещественной мультипликативной сложности $M(N)$ алгоритмов имеет вид:

$$M(N) = CN \log_2 N + O(N). \quad (1)$$

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]:

$$M(N) = 4,4N \log_5 N - 3N + 3. \quad (2)$$

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 \mathbb{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 (2×2) -МАТРИЦ

Отметим ряд известных или легко доказываемых свойств алгебры (2×2) -матриц $M_2(\mathbb{R})$. Автор счел возможным опустить доказательства, сводящиеся к непосредственной проверке матричных тождеств.

Предложение 1.1. Алгебра $M_2(\mathbb{R})$ является четырехмерной ассоциативной \mathbb{R} -алгеброй.

Матрицы

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

образуют базис $M_2(\mathbb{R})$ над \mathbb{R} , то есть любая матрица A из $M_2(\mathbb{R})$ представима в виде

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

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

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

$$E = T^2 = R^2 = I^4.$$

Отображения θ, ρ, ι алгебры $M_2(\mathbb{R})$ на себя:

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

являются (внутренними) автоморфизмами алгебры $M_2(\mathbb{R})$.

Предложение 1.3. Автоморфизмы θ, ρ, ι действуют на базисные элементы T, R, I следующим образом:

$$\begin{aligned} \theta(T) &= T, & \rho(T) &= -T, & \iota(T) &= -T; \\ \theta(R) &= -R, & \rho(R) &= R, & \iota(R) &= -R; \\ \theta(I) &= -I, & \rho(I) &= -I, & \iota(I) &= I. \end{aligned}$$

Предложение 1.4. Пусть $A \in M_2(\mathbb{R})$:

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

тогда справедливы соотношения:

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

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 $c = \cos 2\pi/5$, $s = \sin 2\pi/5$, $\beta = 2c$,

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

Тогда существует невырожденная матрица C такая, что

$$B = C^{-1}S C.$$

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

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

Предложение 1.6. Матрица B имеет мультипликативный порядок, равный пяти, причем:

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

Пусть α и β являются корнями уравнения

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

$\mathbb{Q}(\alpha)$ и $\mathbb{Q}(\beta)$ — алгебраические расширения поля рациональных чисел с примитивными элементами α и β соответственно:

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

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

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

$$\langle u_1, v_1 \rangle + \langle u_2, v_2 \rangle = \langle (u_1 + u_2), (v_1 + v_2) \rangle, \quad (5)$$

$$(u_1, v_1) \times (u_2, v_2) = ((u_1 u_2 + v_1 v_2), (u_1 v_2 + u_2 v_1 - v_1 v_2)). \quad (6)$$

Распространим правила сложения и умножения (5)–(6) пар на $\mathbb{R} \times \mathbb{R}$, задав тем самым структуру кольца, которое обозначим J . Кольцо матриц с коэффициентами из кольца J обозначим $M_2(J)$; матрицы X , компоненты которых заданы кодами, будем обозначать $\langle X \rangle$.

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

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

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

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

$$V = q_0 E + q_1 B. \quad (7)$$

Доказательство. В самом деле, так как

$$(c_N E + s_N I)^K = S,$$

то

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

а так как из предложения 1.5 следует, что

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

то, полагая

$$q_1 = \frac{s_N}{s}, \quad q_0 = c_N - \frac{c s_N}{s},$$

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

Непосредственное умножение матрицы из $M_2(J)$ на степени матрицы $\langle V \rangle$ требует шестнадцати вещественных умножений. Но, в силу предложения 1.8, матрица $\langle V^m \rangle$ имеет специфический вид:

$$\langle V^m \rangle = \begin{pmatrix} (x, y) & (y, 0) \\ (-y, 0) & (x, 0) \end{pmatrix}$$

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

Предложение 1.9. Умножение матрицы из $M_2(J)$ на степени матрицы $\langle V \rangle$ требует четырнадцати вещественных умножений.

Доказательство. Действительно, так как

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

то при

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

имеем

$$\begin{aligned} X = a_4 + a_5, \quad Y = a_1 - a_3 + a_2, \\ Z = a_1 + a_4 + a_6, \quad T = a_4 + a_6 + a_7. \end{aligned} \quad (10)$$

Поэтому вычисление левой части (8) требует, согласно (9) и (10), семи вещественных умножений, а умножение матрицы из $M_2(J)$ на степени матрицы $\langle V \rangle$ – четырнадцать вещественных умножений.

Пусть далее $\langle x \rangle = (x_1, x_2) \in J$,

$$\langle x \rangle_\alpha = x_1 + x_2\alpha, \quad \langle x \rangle_\beta = x_1 + x_2\beta;$$

аналогичный смысл имеют обозначения $\langle V \rangle_\alpha$ и $\langle V \rangle_\beta$ для матриц.

Предложение 1.10. Существуют невырожденная матрица $F \in M_2(\mathbb{R})$ и целое число d , такие что справедливо соотношение

$$\langle V^d \rangle_\alpha = F^{-1} W F.$$

Доказательство. Достаточно показать, что $\langle V \rangle_\alpha$ является первообразным матричным корнем степени N из E . А это следует из предложения 1.7 и непосредственно проверяемых равенств:

$$[\langle V \rangle_\alpha]^N = [\langle V^K \rangle_\alpha]^5 = [\langle B \rangle_\alpha]^5 = [\langle A \rangle_\alpha]^5 = [\langle A \rangle_\alpha]^5 = A^5 = E.$$

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 $\langle h(n) \rangle$ – последовательность матриц периода $N = 5^k$ с коэффициентами из J . Пусть $\langle H(m) \rangle$ – “матричный спектр” последовательности $\{h(n)\}$:

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

где V – матрица, определенная в предложении 1.8. Тогда для вычисления $\langle H(m) \rangle$ достаточно

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

вещественных умножений.

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

$$\langle H(m) \rangle = \sum_{a=0}^4 \left[\sum_{n=0}^{N/5-1} \langle h(5n+a) \rangle \langle V^{5mn} \rangle \right] \langle V^{am} \rangle = \sum_{a=0}^4 \langle H_a(m) \rangle \langle V^{am} \rangle. \quad (13)$$

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

$$\Delta_0 = \{0, 1, \dots, N/5 - 1\}.$$

Действительно, значения $\langle H_a(m) V^{am} \rangle$ для m , лежащих в областях Δ_b , полученных из Δ_0 аддитивным сдвигом на $Nb/5$ ($b = 1, 2, 3, 4$), отличаются от соответствующих значений $\langle H_a(m) V^{am} \rangle$ только умножениями на степени матрицы $\langle V \rangle$, 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 $\langle V^{am} \rangle$ для $m \in \Delta_0$. Считая, что умножения матриц на степени $\langle V \rangle$ реализованы согласно предложению 1.9, получаем для $M^*(N)$ рекуррентное соотношение:

$$M^*(N) = 5M^*(N/5) + 4 \times 14 \times N/5$$

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:

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

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

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

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

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

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

$$\langle \mathbf{h}(n) \rangle = \begin{pmatrix} \langle z_1(n) \rangle & \langle z_2(n) \rangle \\ \langle z_3(n) \rangle & \langle z_4(n) \rangle \end{pmatrix}, \quad \text{где } \langle z_s(n) \rangle = (x_s(n), y_s(n)).$$

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

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

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

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

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

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

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

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

$$\mathbf{C} \langle \mathbf{H}_a(m) \rangle_\beta \mathbf{C}^{-1} = \sum_{n=0}^{T/5-1} \langle z_a(n) \rangle_\beta \mathbf{W}^{mn}, \quad (18)$$

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

$$\mathbf{F} \langle \mathbf{H}_a(dm) \rangle_\alpha \mathbf{F}^{-1} = \sum_{n=0}^{T/5-1} \langle z_a(n) \rangle_\alpha \mathbf{W}^{mn}. \quad (19)$$

Поэтому для

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

справедливы равенства:

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

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:

$$Z_a(m) = e_1 X_a(m) e_1^\tau + i e_2 Y_a(m) e_2^\tau$$

и (16) (здесь $e_1 = (1, 0)$, $e_2 = (0, 1)$ – вектор–строки; τ – знак транспонирования).

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

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

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

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

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} :

$$\langle g_s(n) \rangle = \left(\begin{array}{cc} (f_{1+8s}(n), f_{2+8s}(n)) & (f_{3+8s}(n), f_{4+8s}(n)) \\ (f_{5+8s}(n), f_{6+8s}(n)) & (f_{7+8s}(n), f_{8+8s}(n)) \end{array} \right), \quad (s = 0, 1, 2),$$

понимая компоненты матриц $\langle g_s(n) \rangle$ как элементы кольца \mathbb{J} .

Производя вычисления матричных спектров $\langle G_s(m) \rangle$ и выделяя, как в предыдущем разделе, "частичные спектры" $F_a(m)$, получаем в этом случае для $M_1(T)$ рекуррентное соотношение:

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

откуда следует (21).

ЗАКЛЮЧЕНИЕ

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

Для рассмотренного случая ($N = 5^k$, (2×2) -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 В. В частности, возможен синтез аналогичного алгоритма для $p = 7$ с совмещением в кольце (3×3) — 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.

Л и т е р а т у р а

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