АЛГОРИТМЫ БЫСТРОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ[1]

С. Б. Гашков, И. С. Сергеев (Москва)

В работе рассматривается построение быстрых алгоритмов дискретного преобразования Фурье в некоторых кольцах и их применение к умножению многочленов. В качестве показателя быстродействия алгоритма используется его сложность, определяемая как число выполняемых двухвходовых операций сложения, вычитания, умножения, а также операций умножения на константы кольца.

1. Дискретное преобразование Фурье

Пусть $\mathbf{K}$ — коммутативное кольцо с единицей. Элемент $\zeta \in \mathbf{K}$ называется *примитивным* (*первообразным*) *корнем степени* $N \in \mathbb{N}$, если $\zeta^N = 1$, и никакой из элементов $\zeta^{N/p} - 1$, где p — простой делитель числа N, не является делителем нуля в $\mathbf{K}$. (Напомним, что элемент a называется делителем нуля, если существует ненулевой элемент b, такой, что $ab = 0$.)

Дискретным преобразованием Фурье (*ДПФ*) *порядка* N называется $(\mathbf{K}^N \to \mathbf{K}^N)$-преобразование

$$\text{ДПФ}_{N,\zeta}[\mathbf{K}](\gamma_0, \ldots, \gamma_{N-1}) = (\gamma_0^*, \ldots, \gamma_{N-1}^*), \qquad \gamma_j^* = \sum_{i=0}^{N-1} \gamma_i \zeta^{ij}. \qquad (1)$$

где ζ — примитивный корень степени N.

Фундаментальное свойство ДПФ формулируется следующим образом:

Лемма 1. *Пусть элементы* γ_j^* *определяются из* (1). *Тогда*

$$\text{ДПФ}_{N,\zeta^{-1}}[\mathbf{K}](\gamma_0^*, \ldots, \gamma_{N-1}^*) = (N\gamma_0, \ldots, N\gamma_{N-1}),$$

где под N *в правой части формулы понимается сумма* N *единиц кольца.*

Перед тем, как перейти к доказательству леммы, установим несколько вспомогательных фактов.

Заметим, что если элемент $a \in \mathbf{K}$ не является делителем нуля, и $a = cd$, то множители c и d также не являются делителями нуля. Действительно, если, скажем, $ce = 0$ и $e \neq 0$, то $ae = (ce)d = 0$, откуда следует, что a — делитель нуля.

[1] Сборник «Дискретная математика и ее приложения». Часть V. М.: Изд-во Института прикладной математики РАН, 2009, 3–23.

Лемма 2. *Если ζ — примитивный корень степени N, то при любом $l = 1, \ldots, N-1$*

$$\sum_{i=0}^{N-1} \zeta^{il} = 0.$$

Доказательство. Рассмотрим разложение

$$0 = \zeta^{lN} - 1 = (\zeta^l - 1) \sum_{i=0}^{N-1} \zeta^{il}.$$

Из определения примитивного корня следует, что N — это минимальный натуральный показатель степени n, при котором $\zeta^n = 1$, поэтому $\zeta^l - 1 \neq 0$. Следовательно, либо $\zeta^l - 1$ является делителем нуля, либо $\sum_{i=0}^{N-1} \zeta^{il} = 0$. Покажем, что первое невозможно.

Пусть $m = \text{НОД}(l, N)$. Как известно, существуют целые q, s, такие, что $m = ql + sN$ (числа q, s называются коэффициентами Безу), при этом можно считать, что q — положительно. В таком случае $\zeta^m - 1 = \zeta^{ql} - 1$ делится на $\zeta^l - 1$. С другой стороны, поскольку $m < N$, найдется простое p, такое, что $m \mid (N/p)$. Тогда $(\zeta^m - 1) \mid (\zeta^{N/p} - 1)$. Окончательно, имеем $(\zeta^l - 1) \mid (\zeta^{N/p} - 1)$. Поскольку элемент $\zeta^{N/p} - 1$ не является делителем нуля, то и $\zeta^l - 1$ не может быть делителем нуля. Следовательно, $\sum_{i=0}^{N-1} \zeta^{il} = 0$. Лемма доказана.

Доказательство леммы 1. В векторе $\text{ДПФ}_{N,\zeta^{-1}}[\mathbf{K}](\gamma_0^*, \ldots, \gamma_{N-1}^*)$ рассмотрим произвольную j-ю компоненту:

$$\sum_{i=0}^{N-1} \gamma_i^* \zeta^{-ij} = \sum_{i=0}^{N-1} \sum_{k=0}^{N-1} \gamma_k \zeta^{ki} \zeta^{-ij} = \sum_{k=0}^{N-1} \sum_{i=0}^{N-1} \gamma_k \zeta^{i(k-j)} = \sum_{k=0}^{N-1} \gamma_k \sum_{i=0}^{N-1} (\zeta^{k-j})^i.$$

Внутренняя сумма, как следует из леммы 2, равна нулю во всех случаях, за исключением случая $k - j = 0$, в котором эта сумма равна N. Поэтому, продолжая выкладку, получаем $N\gamma_j$, что и требовалось. Лемма 1 доказана.

Как следствие, получаем, что если элемент $N = 1 + \ldots + 1 \in \mathbf{K}$ обратим, то определено обратное к ДПФ преобразование

$$\text{ДПФ}_{N,\zeta}^{-1}[\mathbf{K}] = N^{-1} \text{ДПФ}_{N,\zeta^{-1}}[\mathbf{K}].$$

2. Полиномиальная интерпретация ДПФ

Рассмотрим многочлен $\Gamma(x) = \gamma_0 + \ldots + \gamma_{N-1}x^{N-1}$. Тогда, по определению,

$$\text{ДПФ}_{N,\zeta}[\mathbf{K}](\gamma_0, \ldots, \gamma_{N-1}) = \left(\Gamma(\zeta^0), \ldots, \Gamma(\zeta^{N-1})\right),$$

т.е. ДПФ вычисляет значения многочлена $\Gamma(x)$ в точках ζ^i. Смысл обратного преобразования $\text{ДПФ}^{-1}_{N,\zeta}[\mathbf{K}]$ заключается в восстановлении коэффициентов единственного многочлена степени, меньшей N, имеющего заданный набор значений в точках $\zeta^0, \ldots, \zeta^{N-1}$.

Формально, связь между ДПФ и интерполяцией описывается следующей леммой:

Лемма 3. *Преобразование* $\text{ДПФ}_{N,\zeta}[\mathbf{K}]$ *задает изоморфизм:* $\mathbf{K}[x]/(x^N - 1) \to \mathbf{K}^N$.

Доказательство. Биективность отображения следует из того, что многочлен степени не выше $N-1$ однозначно определяется своими значениями на наборе из N различных точек.

Проверим, что ДПФ сохраняет операции сложения и умножения: в кольце $\mathbf{K}[x]/(x^N-1)$ эти операции выполняются как с обычными многочленами, только с последующим приведением по модулю $x^N - 1$, в кольце $\mathbf{K}^N$ операции выполняются покомпонентно.

Действительно, значение суммы многочленов $\Gamma_1(x) + \Gamma_2(x)$ в некоторой точке совпадает с суммой значений каждого из многочленов в данной точке. Представляя произведение многочленов в форме $Q(x)(x^N - 1) + R(x)$, где $R(x)$ — остаток от деления на $x^N - 1$, убеждаемся, что произведение переходит в произведение в силу:

$$\Gamma_1(\zeta^j)\Gamma_2(\zeta^j) = Q(\zeta^j)(\zeta^{jN} - 1) + R(\zeta^j) = R(\zeta^j) = (\Gamma_1\Gamma_2 \bmod (x^N - 1))(\zeta^j).$$

Лемма доказана.

Рассмотренный изоморфизм приводит к эффективному способу умножения многочленов над $\mathbf{K}$.

Теорема 1. *Пусть в кольце* $\mathbf{K}$ *определено преобразование* $\text{ДПФ}_{N,\zeta}[\mathbf{K}]$ *и обратное к нему. Тогда умножение двух многочленов суммарной степени не выше* $N-1$ *над* $\mathbf{K}$ *можно выполнить при помощи двух преобразований* $\text{ДПФ}_{N,\zeta}[\mathbf{K}]$, *одного* $\text{ДПФ}^{-1}_{N,\zeta}[\mathbf{K}]$ *и* N *умножений в* $\mathbf{K}$.

Доказательство. Обозначим перемножаемые многочлены через $A(x) = \sum a_i x^i$ и $B(x) = \sum b_i x^i$. Вычислим вектора

$$(a^*_0, \ldots, a^*_{N-1}) = \text{ДПФ}_{N,\zeta}[\mathbf{K}](a_0, \ldots, a_{N-1}),$$

$$(b_0^*, \ldots, b_{N-1}^*) = \text{ДПФ}_{N,\zeta}[\mathbf{K}](b_0, \ldots, b_{N-1}).$$

Затем коэффициенты многочлена $C(x) = \sum c_i x^i = A(x)B(x)$ в силу $C(x) = C(x) \bmod (x^N - 1)$ могут быть найдены как

$$(c_0, \ldots, c_{N-1}) = \text{ДПФ}_{N,\zeta}^{-1}[\mathbf{K}](a_0^* b_0^*, \ldots, a_{N-1}^* b_{N-1}^*),$$

откуда следует утверждение теоремы. Теорема доказана.

3. Вычисление ДПФ

Независимое вычисление компонент вектора ДПФ по формулам (1) может быть выполнено за $O(N^2)$ операций сложения, вычитания и умножения на константы в кольце $\mathbf{K}$. Для составного числа N можно предложить следующий более эффективный способ.

Прежде заметим, что если ζ — примитивный корень степени ST, то ζ^S и ζ^T — примитивные корни степени T и S соответственно (это легко проверить непосредственно из определения).

Справедлива

Лемма 4 (Кули, Тьюки [5]). *ДПФ порядка ST реализуется при помощи S ДПФ порядка T, T ДПФ порядка S и $(S-1)(T-1)$ операций умножения на степени ζ — примитивного корня степени ST.*

Доказательство. Для $s = 0, \ldots, S-1$ и $t = 0, \ldots, T-1$ запишем

$$\gamma_{sT+t}^* = \sum_{I=0}^{ST-1} \gamma_I \zeta^{I(sT+t)} = \sum_{i=0}^{T-1} \sum_{j=0}^{S-1} \gamma_{iS+j} \zeta^{(iS+j)(sT+t)} =$$

$$= \sum_{i=0}^{T-1} \sum_{j=0}^{S-1} \gamma_{iS+j} \zeta^{itS+jsT+jt} = \sum_{j=0}^{S-1} (\zeta^T)^{js} \cdot \zeta^{jt} \cdot \gamma_{(j),t}, \quad (2)$$

где

$$\gamma_{(j),t} = \sum_{i=0}^{T-1} \gamma_{iS+j} (\zeta^S)^{it}.$$

Полученная формула позволяет произвести вычисления в следующем порядке:

а) Для $j = 0, \ldots, S-1$ вычисляются вектора

$$\left(\gamma_{(j),0}, \gamma_{(j),1}, \ldots, \gamma_{(j),T-1}\right) = \text{ДПФ}_{T,\zeta^S}[\mathbf{K}](\gamma_j, \gamma_{S+j}, \ldots, \gamma_{(T-1)S+j}).$$

б) Вычисляются произведения $\omega_{(t),j} = \zeta^{jt} \cdot \gamma_{(j),t}$, $j = 0, \ldots, S-1$, $t = 0, \ldots, T-1$.

в) Заметим, что

$$\gamma^*_{sT+t} = \sum_{j=0}^{S-1} \omega_{(t),j} (\zeta^T)^{js}.$$

Это позволяет окончательно найти компоненты вектора ДПФ по формулам

$$\left(\gamma^*_t, \gamma^*_{T+t}, \ldots, \gamma^*_{(S-1)T+t}\right) = \text{ДПФ}_{S,\zeta^T}[\mathbf{K}](\omega_{(t),0}, \omega_{(t),1}, \ldots, \omega_{(t),S-1}),$$

где $t = 0, \ldots, T-1$.

Утверждение леммы немедленно следует из вида действий, выполняемых на шагах *а*–*в*), если заметить, что среди ST умножений на шаге *б*) есть $S+T-1$ умножений на $\zeta^0 = 1$. Лемма доказана.

Замечание (Гуд, Томас [6]). *Если числа S и T взаимно просты, то для вычисления ДПФ порядка ST достаточно выполнить S ДПФ порядка T и T ДПФ порядка S, т.е. дополнительных умножений не требуется.*

Обозначим через $F(N) = F_A(N) + F_C(N)$ сложность схемы ДПФ порядка N, построенной методом леммы 4, где $F_A(N)$ — число аддитивных элементов (сложений и вычитаний) в схеме, а $F_C(N)$ — число скалярных умножений (т.е. умножений на константы кольца $\mathbf{K}$). При этом необходимые схемы ДПФ простых порядков должны быть построены отдельно.

Несложно построить схему для ДПФ порядка 2, если оно существует. Компоненты ДПФ определяются формулами

$$\gamma^*_0 = \gamma_0 + \gamma_1, \qquad \gamma^*_1 = \gamma_0 - \gamma_1,$$

т.к. в качестве примитивного корня степени 2 можно взять -1. Поэтому положим $F(2) = 2$, $F_A(2) = 2$, $F_C(2) = 0$.

Для вычисления сложности схемы ДПФ порядка 2^k, где $k > 1$, воспользуемся рекуррентными соотношениями, вытекающими из леммы 4 при значениях параметров $S = 2^{k-1}$ и $T = 2$:

$$F_A(2^k) = 2F_A(2^{k-1}) + 2^{k-1}F_A(2), \quad F_C(2^k) = 2F_C(2^{k-1}) + 2^{k-1}F_C(2) + 2^{k-1} - 1.$$

Легко проверить, что указанные соотношения разрешаются как

$$F_A(2^k) = k2^k, \qquad F_C(2^k) = (k-2)2^{k-1} + 1. \tag{3}$$

Доказана

Теорема 2. *ДПФ порядка 2^k может быть выполнено за $k2^k$ операций сложения-вычитания и $(k-2)2^{k-1}+1$ операций скалярного умножения.*

Эта оценка является асимптотически наилучшей из известных верхних оценок сложности ДПФ порядка 2^k.

Сложность схемы обратного ДПФ порядка 2^k с точностью до 2^k умножений на константы 2^{-k} совпадает со сложностью «прямого» ДПФ, причем при $k \geq 2$ умножения на 2^{-k} можно совместить с умножениями на шаге *б*).

Приведенный алгоритм является примером алгоритма *быстрого преобразования Фурье* (*БПФ*). Вообще, под алгоритмами БПФ понимаются такие алгоритмы, в которых используется прием сведения ДПФ составного порядка N к ДПФ порядка множителей числа N. Иногда термин БПФ прилагается к любым алгоритмам сложности $O(N \log N)$.

4. Вещественная сложность комплексного ДПФ

Ситуация, когда аддитивные и мультипликативные операции в кольце $\mathbf{K}$ нельзя считать равноценными, приводит к возникновению специальных алгоритмов БПФ. Проиллюстрируем это на примере поля комплексных чисел $\mathbb{C}$.

Комплексное число обычно представляется парой вещественных чисел — действительной и мнимой частью: $z = x + \mathbf{i}y$. Пересчитаем операции с комплексными числами на операции с вещественными. Комплексное сложение (вычитание) равноценно двум вещественным сложениям (вычитаниям). Комплексное умножение можно выполнить, используя четыре вещественных умножения и два сложения-вычитания. Кроме того, для умножения на константу достаточно трех вещественных умножений и трех сложений-вычитаний.

Для описанной выше схемы комплексного ДПФ порядка 2^k получаем оценки $F_A^{\mathbb{R}}(2^k) < 3,5k2^k$ для числа вещественных сложений-вычитаний и $F_C^{\mathbb{R}}(2^k) < 1,5k2^k$ — для числа вещественных скалярных умножений и суммарно $F^{\mathbb{R}}(2^k) < 5k2^k$.

Можно, однако, получить лучшую оценку, если заметить, что некоторые умножения в алгоритме леммы 4 выгодно не выполнять сразу, а перенести на следующий этап вычислений (реализация ДПФ порядка S). На этом наблюдении основан известный алгоритм БПФ «с расщепленным основанием».

Теорема 3. *ДПФ порядка 2^k над полем $\mathbb{C}$ можно реализовать, используя не более $3k2^k$ сложений-вычитаний и не более $k2^k$ умножений в поле $\mathbb{R}$.*

Доказательство. Вычислим по формуле (2), в которой $S = 2^{k-1}$ и $T = 2$, только компоненты ДПФ порядка 2^k с четными индексами, т.е.

при $t = 0$. Для этого достаточно вычислить по одной компоненте $\gamma_{(j),0} = \gamma_j + \gamma_{S+j}$ каждого из 2^{k-1} внутренних ДПФ порядка 2 и реализовать внешнее ДПФ порядка 2^{k-1}.

Для вычисления компонент с нечетными индексами положим $S = 2^{k-2}$ и $T = 4$ и вновь воспользуемся формулой (2). У каждого из 2^{k-2} внутренних ДПФ порядка 4 требуется вычислить по две компоненты $\gamma_{(j),1}$ и $\gamma_{(j),3}$. Каждая такая пара в силу $\zeta^S = \mathbf{i}$ может быть вычислена по формулам

$$\gamma_{(j),1} = (\gamma_j - \gamma_{2S+j}) + \mathbf{i}(\gamma_{S+j} - \gamma_{3S+j}),$$

$$\gamma_{(j),3} = (\gamma_j - \gamma_{2S+j}) - \mathbf{i}(\gamma_{S+j} - \gamma_{3S+j}).$$

Поскольку умножение на $\pm\mathbf{i}$ сводится к перестановке действительной и мнимой части со сменой знака у одной из них, вычисление одной пары $\gamma_{(j),1}$, $\gamma_{(j),3}$ по этим формулам выполняется за 8 вещественных сложений-вычитаний. Окончательно, выполняется 2^{k-1} умножений на степени ζ^{jt} и два ДПФ порядка 2^{k-2}.

Для числа сложений-вычитаний $F_A^{\mathbb{R}}(2^k)$ и числа скалярных умножений $F_C^{\mathbb{R}}(2^k)$ в построенной схеме имеем рекуррентные соотношения:

$$F_A^{\mathbb{R}}(2^k) \le F_A^{\mathbb{R}}(2^{k-1}) + 2F_A^{\mathbb{R}}(2^{k-2}) + 4,5 \cdot 2^k,$$

$$F_C^{\mathbb{R}}(2^k) \le F_C^{\mathbb{R}}(2^{k-1}) + 2F_C^{\mathbb{R}}(2^{k-2}) + 1,5 \cdot 2^k,$$

которые с учетом начальных данных

$$F_A^{\mathbb{R}}(2) = 4,\ F_C^{\mathbb{R}}(2) = 0,\ F_A^{\mathbb{R}}(4) = 16,\ F_C^{\mathbb{R}}(4) = 0,$$

разрешаются так, как заявлено в утверждении теоремы. Теорема доказана.

Более аккуратный учет позволяет получить оценки сложности метода в виде: $3k2^k - 3 \cdot 2^k + 4$ сложений-вычитаний и $k2^k - 3 \cdot 2^k + 4$ скалярных умножений над $\mathbb{R}$. Эта оценка была получена не позднее 1968 г., но только в 2004 г. ван Бускирк обнаружил, что она может быть улучшена (см. обзор [3]). Его метод учитывает, что умножение на константы вида $\pm 1 + a\mathbf{i}$ или $a \pm \mathbf{i}$ можно выполнить, используя по два вещественных сложения-вычитания и умножения.

Теорема 4. *ДПФ порядка 2^k над полем $\mathbb{C}$ можно реализовать, используя не более $(8/3)k2^k$ сложений-вычитаний и не более $(10/9)k2^k + 2^{k+1}$ умножений в поле $\mathbb{R}$.*

Доказательство. При $k \in \mathbb{N}$ и $j \in \mathbb{Z}$ определим вещественные коэффициенты

$$\sigma_{k,j} = \prod_{l \geq 0} \max\left\{\left|\cos\frac{4^l 2\pi j}{2^k}\right|, \left|\sin\frac{4^l 2\pi j}{2^k}\right|\right\}.$$

Эти коэффициенты обладают свойствами симметрии $\sigma_{k,j} = \sigma_{k,-j}$ и периодичности $\sigma_{k,j} = \sigma_{k,j+2^{k-2}}$, что вытекает из известных соотношений

$$\sin x = -\sin(-x), \quad \cos x = \cos(-x),$$

$$\left\{\left|\sin\left(x + \frac{\pi n}{2}\right)\right|, \left|\cos\left(x + \frac{\pi n}{2}\right)\right|\right\} = \{|\sin x|, |\cos x|\},$$

где $x \in \mathbb{R}$, $n \in \mathbb{Z}$. Кроме того, для примитивного корня $\zeta = e^{\frac{2\pi\mathbf{i}}{2^k}}$ степени 2^k справедливо: $(\sigma_{k-2,j}/\sigma_{k,j})\zeta^j$ имеет вид $\pm 1 + a\mathbf{i}$ или $a \pm \mathbf{i}$, поскольку

$$\zeta^j = \cos\frac{2\pi j}{2^k} + \mathbf{i}\sin\frac{2\pi j}{2^k}, \qquad \frac{\sigma_{k,j}}{\sigma_{k-2,j}} = \max\left\{\left|\cos\frac{2\pi j}{2^k}\right|, \left|\sin\frac{2\pi j}{2^k}\right|\right\}.$$

Будем строить схемы для преобразований

$$\Phi_{2^k}(\gamma_0, \ldots, \gamma_{2^k-1}) = \text{ДПФ}_{2^k,\zeta}[\mathbb{C}](\sigma_{k,0}^{-1}\gamma_0,\, \sigma_{k,1}^{-1}\gamma_1, \ldots, \sigma_{k,2^k-1}^{-1}\gamma_{2^k-1}).$$

Согласно формуле (2) с выбором параметров $S = 2^{k-2}$ и $T = 4$ и свойству периодичности коэффициентов $\sigma_{k,j}$ для компонент φ_i преобразования Φ_{2^k} выполнено:

$$\varphi_{4s+t} = \sum_{j=0}^{S-1} (\zeta^4)^{js} \cdot \zeta^{jt} \cdot \sigma_{k,j}^{-1}\gamma_{(j),t}, \qquad \gamma_{(j),t} = \sum_{l=0}^{3} \gamma_{lS+j} \cdot \mathbf{i}^{lt}.$$

Компоненты $\gamma_{(j),t}$, $t = 0, \ldots, 3$, каждого из 2^{k-2} ДПФ порядка 4 можно вычислить, используя 16 вещественных сложений-вычитаний. Последующие вычисления при $t = 0,\ 1,\ 3$ выполняются по формулам

$$\varphi_{4s} = \sum_{j=0}^{S-1} (\zeta^4)^{js} \sigma_{k-2,j}^{-1} \cdot (\sigma_{k-2,j}/\sigma_{k,j}) \cdot \gamma_{(j),0},$$

$$\varphi_{4s+1} = \sum_{j=0}^{S-1} (\zeta^4)^{js} \sigma_{k-2,j}^{-1} \cdot (\sigma_{k-2,j}/\sigma_{k,j})\zeta^j \cdot \gamma_{(j),1},$$

$$\varphi_{4s+3} = \sum_{j=0}^{S-1} (\zeta^4)^{j(s+1)} \sigma_{k-2,j}^{-1} \cdot (\sigma_{k-2,j}/\sigma_{k,j})\zeta^{-j} \cdot \gamma_{(j),3}.$$

Эти вычисления состоят в выполнении 2^{k-2} умножений на действительные константы, 2^{k-1} умножений на константы вида $\pm 1 + a\mathbf{i}$ или $a \pm \mathbf{i}$ и трех преобразований $\Phi_{2^{k-2}}$.

Для вычисления оставшихся компонент φ_{4s+2} используем формулу (2) с параметрами $S' = 2^{k-3}$ и $T' = 8$:

$$\varphi_{8s+2} = \sum_{j=0}^{S'-1} (\zeta^8)^{js} \sigma_{k-3,j}^{-1} \cdot (\sigma_{k-3,j}/\sigma_{k-1,j})(\zeta^2)^j \cdot \gamma'_{(j),2},$$

$$\varphi_{8s+6} = \sum_{j=0}^{S'-1} (\zeta^8)^{j(s+1)} \sigma_{k-3,j}^{-1} \cdot (\sigma_{k-3,j}/\sigma_{k-1,j})(\zeta^2)^{-j} \cdot \gamma'_{(j),6},$$

где

$$\gamma'_{(j),2} = (\sigma_{k-1,j}/\sigma_{k,j})\gamma_{(j),2} + (\sigma_{k-1,j+S'}/\sigma_{k,j+S'})\mathbf{i}\gamma_{(j+S'),2},$$
$$\gamma'_{(j),6} = (\sigma_{k-1,j}/\sigma_{k,j})\gamma_{(j),2} - (\sigma_{k-1,j+S'}/\sigma_{k,j+S'})\mathbf{i}\gamma_{(j+S'),2}.$$

Заметим, что $\sigma_{k-1,j} = \sigma_{k-1,j+S'}$. Эти вычисления выполняются при помощи 2^{k-2} умножений на действительные или мнимые константы, 2^{k-2} умножений на константы вида $\pm 1 + a\mathbf{i}$ или $a \pm \mathbf{i}$ и двух преобразований $\Phi_{2^{k-3}}$.

Итого, для чисел $\hat{F}_A^{\mathbb{R}}(2^k)$ аддитивных вещественных операций и $\hat{F}_C^{\mathbb{R}}(2^k)$ вещественных скалярных умножений имеем рекуррентные соотношения:

$$\hat{F}_A^{\mathbb{R}}(2^k) \le 3\hat{F}_A^{\mathbb{R}}(2^{k-2}) + 2\hat{F}_A^{\mathbb{R}}(2^{k-3}) + 6 \cdot 2^k,$$

$$\hat{F}_C^{\mathbb{R}}(2^k) \le 3\hat{F}_C^{\mathbb{R}}(2^{k-2}) + 2\hat{F}_C^{\mathbb{R}}(2^{k-3}) + 2,5 \cdot 2^k,$$

которые в согласии с начальными данными для $k \le 3$, полученными предыдущим методом, разрешаются как

$$\hat{F}_A^{\mathbb{R}}(2^k) \le (8/3)k2^k, \qquad \hat{F}_C^{\mathbb{R}}(2^k) \le (10/9)k2^k.$$

Осталось учесть, что схема для ДПФ порядка 2^k достраивается из схемы для Φ_{2^k} при помощи 2^k умножений на вещественные константы $\sigma_{k,j}$. Теорема доказана.

Более аккуратный подсчет операций позволяет уточнить оценки теоремы 4 в остаточном члене (см., например, [2]).

Сложность обратного ДПФ (с точностью до умножений на 2^{-k}, которые могут быть совмещены со внутренними умножениями) в обоих рассмотренных алгоритмах оценивается так же, как и сложность «прямого», поскольку примитивный корень ζ^{-1} является комплексно-сопряженным к ζ числом.

Рассмотрим случай, когда ДПФ применяется к вектору с действительными компонентами γ_j — этот случай представляет интерес при умножении многочленов над $\mathbb{R}$. Оказывается, сложность ДПФ (будем называть его действительным ДПФ) в данном случае может быть понижена примерно вдвое по сравнению с общим случаем.

Заметим, что если все $\gamma_j \in \mathbb{R}$, то $\gamma^*_{N-j} = \overline{\gamma^*_j}$ для любого j, где γ^*_j определяются из (1), а $^-$ обозначает операцию комплексного сопряжения.

Лемма 5. *Действительное ДПФ порядка $4N$ может быть реализовано при помощи действительного ДПФ порядка $2N$, комплексного ДПФ порядка N, $7N$ операций сложения-вычитания и $3N$ операций скалярного умножения в $\mathbb{R}$.*

Доказательство. Для определения компонент γ^*_k с четными индексами $k = 2s$ воспользуемся формулой (2), полагая $S = 2N$ и $T = 2$:

$$\gamma^*_{2s} = \sum_{j=0}^{2N-1} (\zeta^2)^{js} \cdot (\gamma_j + \gamma_{2N+j}).$$

Эти вычисления сводятся к реализации ДПФ порядка $2N$ с вещественными аргументами и $2N$ сложениям в $\mathbb{R}$.

Среди компонент с нечетными индексами достаточно вычислить только γ^*_{4s+1}, т.к. $\gamma^*_{4s+3} = \overline{\gamma^*_{4(N-s-1)+1}}$. Для этого применяется (2) с параметрами $S = N$ и $T = 4$:

$$\gamma^*_{4s+1} = \sum_{j=0}^{N-1} (\zeta^4)^{js} \cdot \zeta^j \cdot (\gamma_j - \gamma_{2N+j} + \mathbf{i}(\gamma_{N+j} - \gamma_{3N+j})).$$

Для вычисления указанных компонент достаточно одного ДПФ порядка N, не более $2N$ вычитаний в $\mathbb{R}$ и N скалярных умножений в $\mathbb{C}$. Лемма доказана.

Другой способ сведения действительного ДПФ к комплексному ДПФ вдвое меньшего порядка можно посмотреть в [1].

Аналогичное утверждение можно доказать про сложность обратного к действительному ДПФ преобразования — его входом является вектор $(\gamma_0, \ldots, \gamma_{N-1})$ такой, что $\gamma_0 \in \mathbb{R}$ и $\gamma_{N-j} = \overline{\gamma_j}$ для любого $j = 1, \ldots, N-1$. Такое преобразование назовем действительнозначным ДПФ. В отношении этого ДПФ справедлив результат, аналогичный доказанному выше.

Лемма 6. *Действительнозначное ДПФ порядка $4N$ может быть реализовано при помощи действительнозначного ДПФ порядка $2N$, комплексного ДПФ порядка N, $7N$ операций сложения-вычитания и $3N$ операций скалярного умножения в $\mathbb{R}$.*

Доказательство. Используя формулу (2) и обозначения из леммы 4 с выбором параметров $S = 2$ и $T = 2N$, можно записать

$$\gamma^*_{2Ns+t} = \omega_{(t),0} + (-1)^s \omega_{(t),1} = \gamma_{(0),t} + (-1)^s \zeta^t \gamma_{(1),t},$$

где $s = 0,\ 1$ и $t = 0, \ldots, 2N-1$,

$$\gamma_{(0),t} = \sum_{i=0}^{2N-1} \gamma_{2i} (\zeta^2)^{it}, \qquad \gamma_{(1),t} = \sum_{i=0}^{2N-1} \gamma_{2i+1} (\zeta^2)^{it}.$$

При условии, что компоненты $\omega_{(t),i}$ вычислены, γ^*_j определяются за $4N$ вещественных сложений-вычитаний.

Вектор с компонентами $\omega_{(t),0} = \gamma_{(0),t}$ является образом действительнозначного ДПФ порядка $2N$, т.к. оно применяется к вектору $(\gamma_0, \gamma_2, \ldots, \gamma_{2(2N-1)})$. Для вычисления $\omega_{(t),1}$ представим $\gamma_{(1),t}$ в форме (2) с выбором параметров $S = 2$ и $T = N$:

$$\gamma_{(1),Ns'+t'} = \gamma'_{(0),t'} + (-1)^{s'} \zeta^{2t'} \gamma'_{(1),t'},$$

где $s' = 0,\ 1$ и $t' = 0, \ldots, N-1$,

$$\gamma'_{(0),t'} = \sum_{i=0}^{N-1} \gamma_{4i+1} (\zeta^4)^{it'}, \qquad \gamma'_{(1),t'} = \sum_{i=0}^{N-1} \gamma_{4i+3} (\zeta^4)^{it'}.$$

В силу $\gamma_{4N-j} = \overline{\gamma_j}$ справедливо:

$$\gamma'_{(1),t'} = \sum_{i=0}^{N-1} \overline{\gamma_{4(N-i-1)+1}} (\zeta^4)^{it'} = \sum_{i'=0}^{N-1} \overline{\gamma_{4i'+1}} (\zeta^4)^{(N-1-i')t'} =$$

$$= \zeta^{-4t'} \overline{\sum_{i'=0}^{N-1} \gamma_{4i'+1} (\zeta^4)^{i't'}} = \zeta^{-4t'} \overline{\gamma'_{(0),t'}}.$$

Таким образом, компоненты $\omega_{(t),1}$ могут быть определены по формулам:

$$\omega_{(Ns'+t'),1} = \mathbf{i}^{s'} (\zeta^{t'} \gamma'_{(0),t'} + (-1)^{s'} \zeta^{-t'} \overline{\gamma'_{(0),t'}}),$$

т.е.

$$\omega_{(t'),1} = \mathrm{Re}(2\zeta^{t'} \gamma'_{(0),t'}), \qquad \omega_{(N+t'),1} = -\mathrm{Im}(2\zeta^{t'} \gamma'_{(0),t'}).$$

Для вычисления всех $\omega_{(t),1}$ достаточно одного ДПФ порядка N и N операций умножения в $\mathbb{C}$. Лемма доказана.

Разрешая рекуррентные соотношения, вытекающие из доказанных лемм, с использованием теоремы 4 заключаем:

Следствие 1. *Как действительное, так и действительнозначное ДПФ порядка 2^k можно выполнить за $(4/3)k2^k + O(2^k)$ операций сложения-вычитания и $(5/9)k2^k + O(2^k)$ операций скалярного умножения в $\mathbb{R}$.*

5. ДПФ в кольце-расширении

Если кольцо $\mathbf{K}$ не содержит корней из единицы подходящей степени, то для умножения многочленов над $\mathbf{K}$ непосредственно использовать способ теоремы 1 невозможно. В алгоритме Шёнхаге—Штрассена [7, 8] и ему подобных в таком случае предлагается использовать расширение $\mathbf{K}_{2,n}(x) = \mathbf{K}[x]/(x^{2^n} + 1)$, при этом двойка должна быть обратима в $\mathbf{K}$.

В кольце $\mathbf{K}_{2,n}(x)$ определено ДПФ порядка 2^{n+1} с примитивным корнем x (здесь и далее вместо элементов фактор-кольца $\mathbf{K}_{2,n}(x)$, которыми являются классы эквивалентных по модулю $x^{2^n} + 1$ многочленов, будут фигурировать многочлены-представители классов).

Лемма 7. *ДПФ порядка 2^k над кольцом $\mathbf{K}_{2,n}(x)$, $k \le n+1$, может быть выполнено за $k2^{k+n}$ операций сложения-вычитания в $\mathbf{K}$.*

Доказательство. Представляя элементы кольца $\mathbf{K}_{2,n}(x)$ многочленами степени не выше $2^n - 1$, легко видеть, что сложение или вычитание в $\mathbf{K}_{2,n}(x)$ соответствует 2^n сложениям-вычитаниям в кольце $\mathbf{K}$, а умножение на x^m — к циклическому сдвигу коэффициентов со сменой знака у некоторых из них. Таким образом, если смена знака может быть учтена в последующих вычислениях, умножение на степени примитивного корня x реализуется «бесплатно». Для завершения доказательства теперь остается воспользоваться оценками (3). Лемма доказана.

Для реализации умножения в $\mathbf{K}_{2,n}(x)$ это кольцо удобно рассмотреть как расширение некоторого кольца $\mathbf{K}_{2,m}(y)$: справедлива

Лемма 8. *Пусть $m < n$. Имеет место изоморфизм*

$$\mathbf{K}_{2,n}(x) \cong \mathbf{K}_{2,m}(y)[x]/(x^{2^{n-m}} - y), \tag{4}$$

порождаемый подстановкой $x^{2^{n-m}} = y$.

Доказательство. Многочлен $f(x) \in \mathbf{K}_{2,n}(x)$ можно записать в виде $f(x) = \sum_{i=0}^{2^{n-m}-1} f_i(x^{2^{n-m}})x^i$, где $\deg f_i < 2^m$. Подстановка $x^{2^{n-m}} = y$ переводит $f(x)$ в многочлен $\sum_{i=0}^{2^{n-m}-1} f_i(y)x^i$. Положим $f_i(y) \in \mathbf{K}_{2,m}(y)$.

Очевидно, что подстановка порождает линейное взаимно однозначное отображение. Остается проверить, что это отображение сохраняет произведение, причем в силу линейности проверку можно ограничить нормированными одночленами. В кольце $\mathbf{K}_{2,n}(x)$ выполнено

$$x^{j_1 2^{n-m}+i_1} \cdot x^{j_2 2^{n-m}+i_2} = x^{j_3 2^{n-m}+i_3} = (-1)^k x^{j_4 2^{n-m}+i_3},$$

где

$$i_3 = (i_1 + i_2) \bmod 2^{n-m}, \qquad j_3 = j_1 + j_2 + (i_1 + i_2 - i_3)/2^{n-m},$$

$$j_4 = j_3 \bmod 2^m, \qquad k = (j_3 - j_4)/2^m.$$

С другой стороны, в кольце $\mathbf{K}_{2,m}(y)[x]/(x^{2^{n-m}} - y)$ также верно

$$y^{j_1} x^{i_1} \cdot y^{j_2} x^{i_2} = y^{j_3} x^{i_3} = (-1)^k y^{j_4} x^{i_3}.$$

Видно, что результаты обоих умножений переходят друг в друга при подстановке $y = x^{2^{n-m}}$. Лемма доказана.

Важно заметить, что рассматриваемое отображение реализуется простой перестановкой коэффициентов. Например, многочлену $x^3 + 2x^2 - 1 \in \mathbf{K}_{2,2}(x)$ соответствует многочлен $yx + (2y - 1) \in \mathbf{K}_{2,1}(y)[x]/(x^2 - y)$. Для реализации умножения можно использовать и другие изоморфизмы, см. [3].

Теорема 5. *Умножение в кольце $\mathbf{K}_{2,n}(x)$ может быть выполнено при помощи $3 \cdot 2^n n(\log_2 n + O(1))$ операций сложения-вычитания, $3 \cdot 2^{n+\lceil \log_2 n \rceil - 1}$ операций умножения и 2^n операций скалярного умножения в $\mathbf{K}$.*

Доказательство. Воспользуемся (4) с выбором параметра $m = \lceil n/2 \rceil$. Умножение многочленов над $\mathbf{K}_{2,m}(y)$ по модулю $x^{2^{n-m}} - y$ выполним как обычное умножение многочленов степени не выше $2^{n-m} - 1$ с последующим приведением по модулю.

Умножение выполняется при помощи трех ДПФ порядка $2^{n-m+1} = 2^{\lfloor n/2 \rfloor + 1}$ и $2^{\lfloor n/2 \rfloor + 1}$ умножений в кольце $\mathbf{K}_{2,m}(y)$, при этом обратное ДПФ реализуется с точностью до постоянного множителя. Приведение по модулю $x^{2^{n-m}} - y$ реализуется за 2^n сложений-вычитаний в $\mathbf{K}$. Окончательно результат умножается на подходящую степень 2^{-1}.

Для чисел $\mu_A(n)$ сложений-вычитаний и $\mu_M(n)$ нескалярных умножений в предложенной схеме при $n \geq 2$ имеем рекуррентные соотношения:

$$\mu_A(n) \leq 2^{\lfloor n/2 \rfloor + 1} \mu_A(\lceil n/2 \rceil) + 3(\lfloor n/2 \rfloor + 1) 2^{n+1} + 2^n,$$

$$\mu_M(n) \le 2^{\lfloor n/2 \rfloor + 1} \mu_M(\lceil n/2 \rceil),$$

которые разрешаются так, как заявлено в утверждении теоремы, если при $n = 1$ воспользоваться оценками $\mu_A(1) = 5$ и $\mu_M(1) = 3$. Иначе, можно положить $\mu_A(1) = 2$ и $\mu_M(1) = 4$ — в этом случае схема будет содержать $2^{n+\lceil \log_2 n \rceil + 1}$ умножений, но общее число операций будет несколько меньше. Теорема доказана.

Доказанная оценка сложности является асимптотически наилучшей из известных. Умножение многочленов над $\mathbf{K}$ теперь можно выполнить при помощи подходящей схемы умножения в $\mathbf{K}_{2,n}(x)$.

6. Применение ДПФ порядка 3^k

В кольце характеристики 2 нельзя определить ДПФ четного порядка, поэтому актуальной является задача построения и эффективной реализации (в самом кольце или в расширении) ДПФ нечетного порядка, предпочтительно порядка 3^k. Эта задача также является актуальной для колец, в которых есть примитивные корни степени 3^k, либо двойка необратима.

Компоненты ДПФ порядка 3 вычисляются по формулам

$$\gamma_0^* = \gamma_0 + \gamma_1 + \gamma_2, \quad \gamma_1^* = \gamma_0 - \gamma_2 + \zeta(\gamma_1 - \gamma_2), \quad \gamma_2^* = \gamma_0 - \gamma_1 - \zeta(\gamma_1 - \gamma_2), \quad (5)$$

где ζ — примитивный корень степени 3 в $\mathbf{K}$. Эти вычисления можно выполнить, используя семь операций сложения-вычитания и одно скалярное умножение (или шесть сложений-вычитаний и два умножения). Если $\operatorname{char} \mathbf{K} = 2$, то достаточно пяти сложений и одного умножения.

Из леммы 4 следует

Теорема 6. *ДПФ порядка 3^k можно реализовать, используя не более $(7/3)k3^k$ операций сложения-вычитания и $(k-1)3^k + 1$ операций скалярного умножения. В кольце характеристики 2 число аддитивных операций оценивается как $(5/3)k3^k$.*

Доказательство. Указанные оценки следуют из рекуррентных соотношений на числа $F_A(3^k)$ аддитивных операций и $F_C(3^k)$ операций скалярного умножения в методе леммы 4:

$$F_A(3^k) = 3F_A(3^{k-1}) + 3^{k-1}F_A(3),$$

$$F_C(3^k) = 3F_C(3^{k-1}) + 3^{k-1}F_C(3) + 2 \cdot 3^{k-1} - 2$$

и начальных условий: $F_C(3) = 1$, $F_A(3) = 7$ в общем случае или $F_A(3) = 5$ для кольца характеристики 2. Теорема доказана.

Если в кольце $\mathbf{K}$ нет примитивных корней достаточно большой степени 3^k, но тройка обратима, то можно рассмотреть расширение $\mathbf{K}_{3,n}(x) = \mathbf{K}[x]/(x^{2\cdot 3^n} + x^{3^n} + 1)$, в котором x является примитивным корнем степени 3^{n+1}.

В кольце $\mathbf{K}_{3,n}(x)$ сложение (вычитание) выполняется за $2 \cdot 3^n$ операций сложения (вычитания) в $\mathbf{K}$, а сложность умножения на x^m зависит от m: справедлива

Лемма 9. *Сложность умножения на x^m с точностью до множителя ± 1 в кольце $\mathbf{K}_{3,n}(x)$ составляет $|m|$ операций вычитания в $\mathbf{K}$, если $-3^n \le m \le 3^n$, и 3^n операций вычитания, иначе (т.е. если $3^n < m < 2 \cdot 3^n$).*

Доказательство. Пусть $0 \le m \le 3^n$. Запишем многочлен $f(x) \in \mathbf{K}_{3,n}(x)$ в виде $a(x)x^{2\cdot 3^n - m} + b(x)$, где $\deg a < m$ и $\deg b < 2 \cdot 3^n - m$. В кольце $\mathbf{K}_{3,n}(x)$ выполняется равенство

$$f(x)x^m = b(x)x^m - a(x) - a(x)x^{3^n},$$

из которого видно, что, не считая умножений на -1, вычисление коэффициентов произведения требует m вычитаний в $\mathbf{K}$.

В случае $-3^n \le m < 0$ запишем $f(x) = b(x)x^{-m} + a(x)$. Тогда в силу

$$f(x)x^m = b(x) - a(x)x^{2\cdot 3^n} - a(x)x^{3^n}$$

для вычисления коэффициентов многочлена также требуется $|m|$ умножений.

Пусть $3^n < m < 2 \cdot 3^n$. Представим $f(x)$ в виде $a(x) + b(x)x^{2\cdot 3^n - m} + c(x)x^{-m}$, где $\deg a < 2 \cdot 3^n - m$, $\deg b < 3^n$ и $\deg c < m - 3^n$. Тогда для вычисления $f(x)x^m$ достаточно 3^n вычитаний, поскольку

$$f(x)x^m = a(x)x^m - b(x)x^{3^n} + c(x) - b(x).$$

Лемма доказана.

Лемма 10. *Любое из преобразований* $\text{ДПФ}_{3,\zeta}[\mathbf{K}_{3,n}(x)](\gamma_0, \zeta^{c_1}\gamma_1, \zeta^{c_2}\gamma_2)$, *где* $\zeta = x^{3^n}$, $c_1, c_2 \in \{0, 1, 2\}$, *может быть выполнено за* $13 \cdot 3^n$ *операций сложения-вычитания в* $\mathbf{K}$ *или за* $10 \cdot 3^n$ *операций сложения, если* $\operatorname{char} \mathbf{K} = 2$.

Доказательство. Несмотря на девять возможностей для выбора параметров c_1, c_2, в действительности достаточно рассмотреть три случая, например, $(c_1, c_2) \in \{(0, 0), (0, 1), (1, 1)\}$. Компоненты любого другого преобразования получаются перестановкой компонент одного из трех перечисленных.

Рассмотрим случай $c_1 = c_2 = 0$, в котором изучаемое преобразование является обычным ДПФ порядка 3. Запишем $\gamma_i \in \mathbf{K}_{3,n}(x)$ в виде $a_i(x) + x^{3^n} b_i(x)$, где a_i, b_i — многочлены степени меньше 3^n, $i = 0, 1, 2$. Тогда формулы (5) можно переписать как

$$\gamma_0^* = (a_0 + a_1 + a_2) + x^{3^n}(b_0 + b_1 + b_2),$$

$$\gamma_1^* = (a_0 - a_2 - (b_1 - b_2)) + x^{3^n}(b_0 - b_1 + a_1 - a_2),$$

$$\gamma_2^* = (a_0 - a_1 + b_1 - b_2) + x^{3^n}(b_0 - b_2 - (a_1 - a_2)).$$

Если представить γ_2^* в виде

$$\gamma_2^* = a_0 - a_2 + ((b_1 - b_2) - (a_1 - a_2)) + x^{3^n}(b_0 - b_1 + ((b_1 - b_2) - (a_1 - a_2))),$$

то станет ясно, что все три компоненты γ_i^* можно вычислить за 13 операций сложения-вычитания многочленов степени не выше $3^n - 1$.

В кольце характеристики 2 формулы для γ_i^* принимают вид

$$\gamma_0^* = (a_0 + a_1 + a_2) + x^{3^n}(b_0 + b_1 + b_2),$$

$$\gamma_1^* = (a_0 + a_2 + b_1 + b_2) + x^{3^n}(b_0 + b_1 + a_1 + a_2),$$

$$\gamma_2^* = (a_0 + a_1 + b_1 + b_2) + x^{3^n}(b_0 + b_2 + a_1 + a_2).$$

Если записать

$$\gamma_2^* = \gamma_1^* + (a_1 + a_2) + x^{3^n}(b_1 + b_2),$$

то несложно проверить, что для вычисления компонент γ_i^* можно ограничиться 10 сложениями многочленов степени не выше $3^n - 1$.

Другие два случая рассматриваются аналогично. Например, компоненты преобразования с параметрами $c_1 = c_2 = 1$ имеют вид

$$(a_0 - b_1 - b_2) + x^{3^n}(b_0 - (b_1 - a_2 + b_2 - a_1)),$$

$$(a_0 - a_1 + b_1 - a_2) + x^{3^n}(b_0 + b_2 - a_1),$$

$$(a_0 + a_1 - a_2 + b_2) + x^{3^n}(b_0 + b_1 - a_2),$$

откуда видно, что они могут быть вычислены за 13 операций сложения-вычитания многочленов степени не выше $3^n - 1$. Остальные пункты проверки предоставляются читателю. Лемма доказана.

Лемма 11. *ДПФ порядка 3^k над кольцом $\mathbf{K}_{3,n}(x)$, где $k \le n + 1$, может быть реализовано с использованием не более $4,5k3^{n+k}$ операций сложения-вычитания в $\mathbf{K}$, а в случае* $\operatorname{char} \mathbf{K} = 2$ *— не более $3,5k3^{n+k}$ операций сложения.*

Доказательство. Реализация ДПФ порядка 3^{k+1}, если воспользоваться леммой 4 с выбором параметров $S = 3$ и $T = 3^k$, сводится к выполнению 3^k ДПФ порядка 3, трех ДПФ порядка 3^k и умножениям на $x^{3^{n-k}jt}$, где $j = 1, 2$ и $t = 1, \ldots, 3^k - 1$.

Пусть $m = c3^n + m'$, где $c \in \mathbb{Z}$ и $|m'| < 3^n/2$. Тогда вместо умножения на x^m будем выполнять умножение на $x^{m'}$, перенося умножение на x^{c3^n} внутрь внешнего ДПФ порядка 3. Поскольку входы любого из внешних ДПФ имеют вид $\gamma_{(0),t}$, $x^l\gamma_{(1),t}$, $x^{2l}\gamma_{(2),t}$, где $l = 3^{n-k}t < 3^n$, то при сведении к умножениям на $x^{m'}$ внешнее ДПФ заменяется одним из преобразований леммы 10.

В рассматриваемой группе умножений умножения на каждую из степеней $x^{m'}$, $m' = 3^{n-k}t$, $t = -(3^k - 1)/2, \ldots, (3^k - 1)/2$, выполняются по два раза, поскольку

$$\{2t \bmod 3^k \mid t = 1, \ldots, 3^k - 1\} = \{1, \ldots, 3^k - 1\}.$$

Учитывая сложность каждого такого умножения как $|m'|$, сложность совокупности умножений оценивается величиной

$$4 \cdot 3^{n-k} \sum_{t=1}^{\frac{3^k-1}{2}} t = 3^{n-k}\frac{3^{2k} - 1}{2}$$

операций сложения-вычитания в $\mathbf{K}$.

Таким образом, для сложности $F_n(3^{k+1})$ построенной схемы имеем рекуррентное соотношение

$$F_n(3^{k+1}) \leq 3F_n(3^k) + 3^k F_n(3) + 3^{n+k}/2,$$

которое при начальных условиях $F_n(3) = 13 \cdot 3^n$ (или $F_n(3) = 10 \cdot 3^n$ для кольца характеристики 2) разрешается так, как заявлено в утверждении леммы. Лемма доказана.

Лемма 12. *Умножение в кольце $\mathbf{K}_{3,1}(x)$ может быть выполнено за* 30 *операций сложения-вычитания и* 27 *операций умножения в $\mathbf{K}$.*

Доказательство. Представим перемножаемые многочлены $A(x), B(x) \in \mathbf{K}_{3,1}(x)$ в виде $A(x) = A_1(x)x^3 + A_0$, $B(x) = B_1(x)x^3 + B_0$, где $\deg A_i, B_i \leq 2$. Их произведение вычислим методом Карацубы:

$$AB = A_1B_1x^6 + ((A_1 - A_0)(B_0 - B_1) + A_1B_1 + A_0B_0)x^3 + A_0B_0.$$

Обозначим $C = (A_1 - A_0)(B_0 - B_1) = C_1x^3 + C_0$, $D = A_0B_0 = D_1x^3 + D_0$, $E = A_1B_1 = E_1x^3 + E_0$, где $\deg C_0, D_0, E_0 \le 2$ и $\deg C_1, D_1, E_1 \le 1$. Тогда в кольце $\mathbf{K}_{3,1}(x)$, т.е. по модулю $x^6 + x^3 + 1$, справедливо соотношение

$$AB = Dx^6 + (C + D + E)x^3 + E = (C + D)x^3 + (D - E) =$$
$$= ((D_0 - C_1) + C_0 - E_1)x^3 + ((D_0 - C_1) - E_0 - D_1) = G_1x^3 + G_0.$$

Произведения C, D, E многочленов степени не выше 2 выполним прямолинейным способом за 9 умножений и 4 сложения каждое. Остальные действия выполняются за 18 операций сложения-вычитания: из них шесть используется для вычисления $A_1 - A_0$, $B_0 - B_1$ и 12 — для вычисления линейных комбинаций G_0, G_1. Лемма доказана.

Теорема 7. *Умножение в кольце* $\mathbf{K}_{3,n}(x)$ *может быть выполнено при помощи* $13,5 \cdot 3^n n(\log_2 n + O(1))$ *операций сложения-вычитания, не более* $3^{n+2} \cdot 2^{\lceil \log_2 n \rceil}$ *операций умножения и* $O(3^n)$ *операций скалярного умножения в* $\mathbf{K}$. *В случае кольца характеристики* 2 *аддитивная сложность составляет не более* $10,5 \cdot 3^n n(\log_2 n + O(1))$.

Доказательство. Теорема доказывается аналогично теореме 5. При $n \ge 2$ представим кольцо $\mathbf{K}_{3,n}(x)$ как расширение кольца $\mathbf{K}_{3,m}(y)$ (справедлив аналог леммы 8):

$$\mathbf{K}_{3,n}(x) \cong \mathbf{K}_{3,m}(y)[x]/(x^{3^{n-m}} - y)$$

и выберем $m = \lceil n/2 \rceil$. Как и в двоичном случае, умножение многочленов над $\mathbf{K}_{3,m}(y)$ по модулю $x^{3^{n-m}} - y$ будем выполнять как обычное умножение многочленов степени не выше $3^{n-m} - 1$ с последующим приведением по модулю.

В отличие от двоичного случая (ввиду отсутствия ДПФ порядка $2 \cdot 3^{n-m}$) для умножения используется шесть ДПФ порядка $3^{n-m} = 3^{\lfloor n/2 \rfloor}$: три ДПФ используются обычным образом для вычисления произведения по модулю $x^{3^{n-m}} - 1$, а три других — для вычисления произведения по модулю $x^{3^{n-m}} - \alpha^{3^{n-m}}$, где $\alpha = y^{3^{n \bmod 2}}$, которое сводится к подстановке $x = \alpha z$ и вычислению произведения по модулю $z^{3^{n-m}} - 1$. Действительно,

$$\big(f(x) \bmod (x^N - \alpha^N)\big) \mid_{x=\alpha z} = f(\alpha z) \bmod (z^N - 1).$$

Выполнение любого из преобразований $x = \alpha z$ и $z = x/\alpha$ выполняется в кольце $\mathbf{K}_{3,n}(x)$ посредством $O(3^{n-m})$ операций умножения на степени y в кольце $\mathbf{K}_{3,m}(y)$, т.е. всего за $O(3^n)$ аддитивных операций в $\mathbf{K}$, если проводить вычисления с точностью до множителя ± 1.

Восстановление многочлена $f(x) \in \mathbf{K}_{3,m}(y)[x]$ степени не выше $2N-2$ по остаткам f_1 и f_α от деления соответственно на x^N-1 и $x^N-\alpha^N$ можно выполнить по формуле

$$f(x) = \frac{1}{\alpha^N - 1}\left((x^N-1)f_\alpha - (x^N-\alpha^N)f_1\right),$$

причем при $N = 3^{n-m}$ в силу $\alpha^{2N}+\alpha^N+1=0$ множитель $(\alpha^N-1)^{-1}$ равен $-3^{-1}(\alpha^N+2)$. Ясно, что описанная процедура восстановления многочлена также может быть выполнена за $O(3^{n-m})$ сложений-вычитаний и умножения на степени y в кольце $\mathbf{K}_{3,m}(y)$, т.е. всего за $O(3^n)$ сложений-вычитаний в $\mathbf{K}$.

Приведение многочлена степени, меньшей $2\cdot 3^{n-m}$, по модулю $x^{3^{n-m}}-y$ также сводится к $O(3^{n-m})$ операций сложения-вычитания и умножения на степени y в кольце $\mathbf{K}_{3,m}(y)$ или к $O(3^n)$ аддитивных операций в $\mathbf{K}$.

Для чисел $\mu_A(n)$ сложений-вычитаний и $\mu_M(n)$ нескалярных умножений в данной схеме при $n \geq 2$ получаем рекуррентные соотношения:

$$\mu_A(n) \leq 2\cdot 3^{\lfloor n/2\rfloor}\mu_A(\lceil n/2\rceil) + 6F_{\lceil n/2\rceil}(3^{\lfloor n/2\rfloor}) + O(3^n),$$

$$\mu_M(n) \leq 2\cdot 3^{\lfloor n/2\rfloor}\mu_M(\lceil n/2\rceil),$$

где значение $F_{\lceil n/2\rceil}$ определяется из леммы 11. Эти соотношения разрешаются так, как заявлено в утверждении теоремы, если при $n=1$ воспользоваться оценками леммы 12. Теорема доказана.

Заметим, что метод теоремы 5 дает для сложности умножения многочленов суммарной степени не выше $N-1$, где $N=2^k$, асимптотическую оценку $3N\log_2 N\log_2\log_2 N$, а метод теоремы 7 в случае кольца характеристики 2 и $N = 2\cdot 3^k$ — близкую оценку $3,32N\log_2 N\log_2\log_2 N$.

Замечание. *Умножение двоичных трехчленов можно выполнить за* 6 *умножений и* 12 *сложений-вычитаний. Поэтому оценки числа умножений в лемме* 12 *и, как следствие, в теореме* 7 *могут быть уменьшены в* $1,5$ *раза ценой некоторого увеличения числа аддитивных операций.*

7. Заключение

Стратегию умножения в случае $2^{-1}, 3^{-1} \notin \mathbf{K}$ указывает метод Кантора—Калтофена [4]. Способом теорем 5 и 7, только заменяя обратные преобразования $\text{ДПФ}^{-1}_{N,\zeta}$ ненормированными преобразованиями $\text{ДПФ}_{N,\zeta^{-1}}$, вычисляются «почти произведения»

$$2^{N_1}fg = 2^{N_1}fg \bmod (x^{2^{n_1}}+1), \quad 3^{N_2}fg = 3^{N_2}fg \bmod (x^{2\cdot 3^{n_2}} + x^{3^{n_2}} + 1)$$

при подходящих $n_i, N_i \in \mathbb{N}$, где f, g — перемножаемые многочлены. Окончательно произведение fg можно вычислить как $q2^{N_1}fg + s3^{N_2}fg$, где q, s — коэффициенты Безу, т.е. $q2^{N_1} + s3^{N_2} = 1$.

Впрочем, актуальность разработки быстрых алгоритмов умножения над такими достаточно экзотическими кольцами представляется пока незначительной.

Работа выполнена при финансовой поддержке РФФИ, проекты 08–01–00863 и 08–01–00632–а, программы «Ведущие научные школы», проект НШ–4470.2008.1, и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

Список литературы

1. Гашков С. Б. Замечания о быстром умножении многочленов, преобразовании Фурье и Хартли // Дискретная математика. — 2000. — Вып. 12, №3. — С. 124–153.

2. Bernstein D. J. The tangent FFT // Proc. AAECC. LNCS. — 2007. — V. 4851. — P. 291–300.

3. Bernstein D. J. Fast multiplication and its applications // Algorithmic Number Theory, MSRI Publ. — 2008. — V. 44. — P. 325–384.

4. Cantor D., Kaltofen E. On fast multiplication of polynomials over arbitrary algebras // Acta Inf. — 1991. — V. 28, №7. — P. 693–701.

5. Cooley J., Tukew J. An algorithm for the machine calculation of complex Fourier series // Math. Comp. — 1965. — V. 19. — P. 297–301.

6. Good I. J. The interaction algorithm and practical Fourier analysis // J. R. Statist. Soc. B. — 1958. — V. 20, №2. — 361–372; 1960. — V. 22, №2. — 372–375.

7. Schönhage A. Schnelle multiplikation von polynomen über körpern der charakteristik 2 // Acta Inf. — 1977. — V. 7. — P. 395–398.

8. Schönhage A., Strassen V. Schnelle multiplikation großer zahlen // Computing. — 1971. — V. 7. — P. 271–282. [Русский перевод: Шёнхаге А., Штрассен В. Быстрое умножение больших чисел // Кибернетический сборник. Вып. 10. — М.: Мир, 1973. — С. 87–98].

Замечание от 01.11.2010. В доказательстве леммы 2 используется ассоциативность кольца $\mathbf{K}$. Поэтому везде по тексту кольцо следует считать еще и ассоциативным.

Замечание от 05.12.2010. В доказательстве леммы 9, 2 абзац, вместо «$|m|$ умножений» следует читать «$|m|$ вычитаний».

Замечание от 02.04.2012. В доказательстве леммы 12 вместо

$$AB = Dx^6 + (C + D + E)x^3 + E = \dots$$

следует читать

$$AB = Ex^6 + (C + D + E)x^3 + D = \dots$$