Тема 3. Дискретное преобразование Фурье

С. Б. Гашков, И. С. Сергеев

Пусть $\mathbf{K}$ — коммутативное кольцо с единицей.

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

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

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

где ζ — примитивный корень степени N.

1 Основное свойство ДПФ

Фундаментальное свойство ДПФ формулируется следующим образом:

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

$$\text{ДПФ}_{N,\zeta^{-1}}(\gamma_0^*, \dots, \gamma_{N-1}^*) = (N\gamma_0, \dots, N\gamma_{N-1}),$$

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.

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 $m = \text{НОД}(l, N)$. По свойству наибольшего общего делителя, существуют целые q, s, такие, что $m = ql + sN$, 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 $\text{ДПФ}_{N,\zeta^{-1}}(\gamma_0^*, \ldots, \gamma_{N-1}^*)$ 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

$$\text{ДПФ}_{N,\zeta}^{-1} = N^{-1} \text{ДПФ}_{N,\zeta^{-1}}.$$

2 Полиномиальная интерпретация ДПФ

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

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

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

Доказательство. 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.

3 Вычисление ДПФ

Независимое вычисление компонент вектора ДПФ по формулам $(*)$ может быть выполнено за $O(N^2)$ операций в кольце. Для составного числа N можно предложить более эффективный способ.

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

Справедлива

Лемма 4 (Кули, Тьюки)**.** *ДПФ порядка PQ реализуется при помощи P ДПФ порядка Q, Q ДПФ порядка P и PQ операций умножения на степени ζ — примитивного корня степени PQ.*

Доказательство. Для $p = 0, \ldots, P-1$ и $q = 0, \ldots, Q-1$ запишем

$$\gamma^*_{pQ+q} = \sum_{I=0}^{PQ-1} \gamma_I \zeta^{I(pQ+q)} = \sum_{i=0}^{Q-1}\sum_{j=0}^{P-1} \gamma_{iP+j}\zeta^{(iP+j)(pQ+q)} = \sum_{i=0}^{Q-1}\sum_{j=0}^{P-1} \gamma_{iP+j}\zeta^{iqP+jpQ+jq} = \sum_{j=0}^{P-1} (\zeta^Q)^{jp} \cdot \zeta^{jq} \cdot \gamma^*_{(j),q},$$

где

$$\gamma^*_{(j),q} = \sum_{i=0}^{Q-1} \gamma_{iP+j}(\zeta^P)^{iq}.$$

Полученная формула позволяет произвести вычисления в следующем порядке:

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

$$\left(\gamma^*_{(j),0}, \gamma^*_{(j),1}, \ldots, \gamma^*_{(j),Q-1}\right) = \text{ДПФ}_{Q,\zeta^P}(\gamma_j, \gamma_{P+j}, \ldots, \gamma_{(Q-1)P+j}).$$

б) Вычисляются произведения $\omega_{(q),j} = \zeta^{jq} \cdot \gamma^*_{(j),q}$, $j = 0, \ldots, P-1$, $q = 0, \ldots, Q-1$.

в) Заметим, что

$$\gamma^*_{pQ+q} = \sum_{j=0}^{P-1} \omega_{(q),j}(\zeta^Q)^{jp}.$$

Это позволяет окончательно найти компоненты вектора ДПФ по формулам

$$\left(\gamma^*_q, \gamma^*_{Q+q}, \ldots, \gamma^*_{(P-1)Q+q}\right) = \text{ДПФ}_{P,\zeta^Q}(\omega_{(q),0}, \omega_{(q),1}, \ldots, \omega_{(q),P-1}),$$

где $q = 0, \ldots, Q-1$.

Утверждение леммы немедленно следует из вида действий, выполненных на шагах *а*–*в*.

Обозначим сложность ДПФ порядка N через $F(N)$. По индукции несложно проверяется

Следствие 1.

$$F(N_1 \cdot \ldots \cdot N_r) \leq N_1 \cdot \ldots \cdot N_r \left(\frac{F(N_1)}{N_1} + \ldots + \frac{F(N_r)}{N_r} + (r-1) \right).$$

В указанной оценке сложности слагаемое $(r-1)N_1 \cdot \ldots \cdot N_r$ отвечает операциям умножения на степени примитивного корня.

В случае, когда N — гладкое число, т.е. раскладывается в произведение относительно небольших сомножителей, метод леммы 4 также называется алгоритмом быстрого преобразования Фурье (БПФ). В наиболее важном случае $N = 2^k$ получаем

$$F(2^k) \leq N \left(\frac{k}{2} F(2) + k - 1 \right).$$

Очевидно, $F(2) \leq 3$ в силу соотношений

$$\gamma_0^* = \gamma_0 + \gamma_1, \qquad \gamma_1^* = \gamma_0 + \zeta\gamma_1.$$

Учитывая, что фактически $\zeta = -1$, при наличии операции вычитания указанные формулы переписываются как

$$\gamma_0^* = \gamma_0 + \gamma_1, \qquad \gamma_1^* = \gamma_0 - \gamma_1,$$

откуда вытекает $F(2) = 2$.

Окончательно получаем, что ДПФ порядка 2^k может быть вычислено за $2,5k2^k$ (или $2k2^k$ с использованием вычитаний) операций, из которых $k2^k$ — сложения (или вычитания), остальные — умножения на степени примитивного корня.

4 Умножение многочленов над кольцом K

Алгоритм БПФ подходящего порядка позволяет быстро выполнять умножение многочленов из $\mathbf{K}[x]$.

Теорема 1. *Пусть для любого $k \in \mathbb{N}$ существует ζ_k — примитивный корень степени 2^k в кольце $\mathbf{K}$, и элемент 2 обратим в $\mathbf{K}$. Тогда сложность $M(n)$ умножения многочленов степени $n-1$ над $\mathbf{K}$ не превосходит $O(n \log n)$.*

Доказательство. Обозначим перемножаемые многочлены через $A(x) = \sum_{i=0}^{n-1} a_i x^i$ и $B(x) = \sum_{i=0}^{n-1} b_i x^i$. Выберем такое k, что $2n-1 \le 2^k < 4n-1$. Согласно условиям теоремы, в кольце $\mathbf{K}$ определено ДПФ порядка 2^k и обратное к нему.

Быстрый способ умножения, основанный на БПФ, состоит в следующем: вычисляются вектора

$$(a_0^*, \ldots, a_{2^k-1}^*) = \text{ДПФ}_{2^k,\zeta_k}(a_0, \ldots, a_{n-1}, 0, \ldots, 0),$$

$$(b_0^*, \ldots, b_{2^k-1}^*) = \text{ДПФ}_{2^k,\zeta_k}(b_0, \ldots, b_{n-1}, 0, \ldots, 0).$$

Затем коэффициенты многочлена $C(x) = \sum c_i x^i = A(x)B(x)$ в силу $C(x) = C(x) \bmod (x^{2^k} - 1)$ могут быть найдены как

$$(c_0, \ldots, c_{2^k-1}) = 2^{-k}\text{ДПФ}_{2^k,\zeta_k^{-1}}(a_0^* b_0^*, \ldots, a_{2^k-1}^* b_{2^k-1}^*).$$

Таким образом, для умножения используется три ДПФ порядка 2^k, 2^k умножений на 2^{-k} и еще 2^k нетривиальных умножений, откуда получаем

$$M(n) \le 3F(2^k) + 2^{k+1} = O(n \log n).$$

Дополнительные вопросы

1. Показать, что любая степень ζ^m примитивного корня ζ степени N является примитивным корнем степени $N/\text{НОД}(m, N)$.
2. Уточнить оценку леммы Кули—Тьюки и, используя операцию вычитания, показать, что $F(2^k) \le 1,5k2^k$.
3. Пусть числа P и Q взаимно просты. Показать, что $F(PQ) \le PF(Q) + QF(P)$.