

Fast Fourier Transform

Быстрое преобразование Фурье

Конспект лекции: комплексные числа, БПФ, деление многочленов, интерполяция и multipoint evaluation

1 Комплексные числа

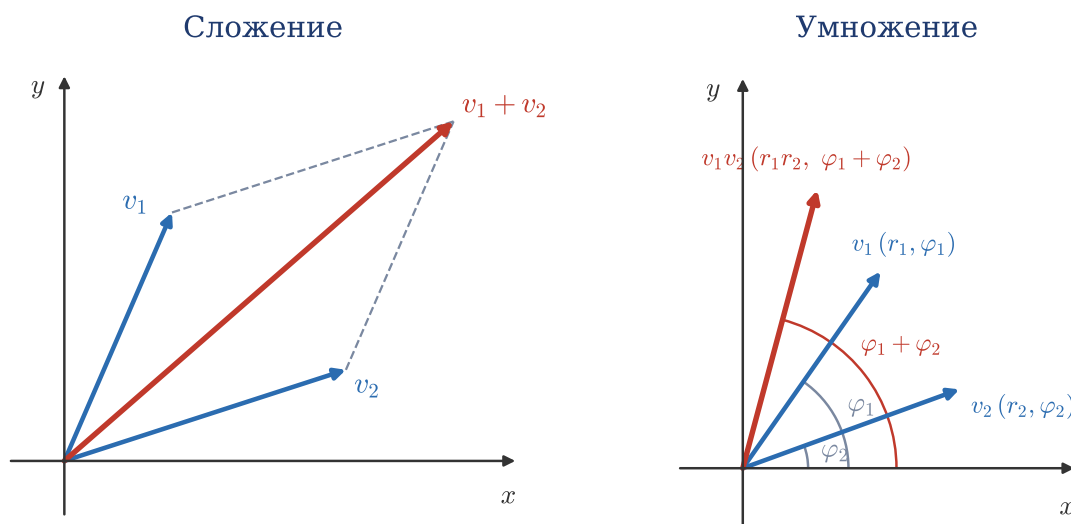
Комплексные числа удобно ввести как векторы плоскости $\mathbb{R}^2$, на которой заданы две операции. **Сложение** покоординатное:

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \end{pmatrix}.$$

1.1 Операция умножения

Зададим **умножение** геометрически: длины перемножаются, углы складываются. Если вектор v имеет длину r и угол φ , то

$$v_1 \cdot v_2 = (r_1 r_2, \varphi_1 + \varphi_2).$$



Сложение (слева) и умножение (справа): при умножении длины перемножаются, а углы, отсчитываемые от оси Ox , складываются.

Через координаты $x_i = r_i \cos \varphi_i$, $y_i = r_i \sin \varphi_i$:

$$\sin \varphi_i = \frac{y_i}{r_i}, \quad \cos \varphi_i = \frac{x_i}{r_i}.$$

Формулы сложения углов дают

$$\begin{aligned} \sin(\varphi_1 + \varphi_2) &= \sin \varphi_1 \cos \varphi_2 + \cos \varphi_1 \sin \varphi_2 = \frac{1}{r_1 r_2} (y_1 x_2 + x_1 y_2), \\ \cos(\varphi_1 + \varphi_2) &= \cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2 = \frac{1}{r_1 r_2} (x_1 x_2 - y_1 y_2). \end{aligned}$$

Поэтому координаты произведения $r_1 r_2 (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2))$ равны

$$x_{\text{res}} = x_1 x_2 - y_1 y_2, \quad y_{\text{res}} = x_1 y_2 + y_1 x_2.$$

Операция коммутативна, ассоциативна и дистрибутивна относительно сложения.

1.2 Мнимая единица и сопряжение

«Обычным» числам $\mathbb{R}$ соответствуют векторы $(x, 0)$; вектор $(0, y)$ обозначаем $y \cdot i$. Тогда

$$\alpha \cdot (1, 0) + \beta \cdot (0, 1) \text{ записывается как } \alpha + \beta i.$$

Сопряжённое к $z = \alpha + \beta i$ — это $\bar{z} = \alpha - \beta i$, и

$$z\bar{z} = (\alpha + \beta i)(\alpha - \beta i) = \alpha^2 + \beta^2 = \|z\|^2 \implies z^{-1} = \frac{\bar{z}}{\|z\|^2}.$$

2 Корни из единицы

Всякое z записывается в тригонометрической форме

$$z = a + bi, \quad \begin{cases} a = |z| \cos \varphi, \\ b = |z| \sin \varphi, \end{cases} \quad z = |z| (\cos \varphi + i \sin \varphi).$$

Рассмотрим уравнение $z^n = 1$. Возводя в степень,

$$z^n = |z|^n \underbrace{(\cos(n\varphi) + i \sin(n\varphi))}_{|\cdot|=1} = 1 \implies |z| = 1, \quad n\varphi = 2\pi k.$$

Существует ровно n корней n -й степени из единицы:

$$\omega_n^k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}, \quad k = 0, 1, \dots, n-1.$$

3 Преобразование Фурье: «разделяй и властвуй»

Пусть

$$P(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}.$$

Разобьём его на чётную и нечётную части:

$$P_1(x) = a_0 + a_2 x^2 + \dots + a_{n-2} x^{n-2}, \quad P_2(x) = a_1 x + a_3 x^3 + \dots + a_{n-1} x^{n-1}.$$

Введём многочлены половинной степени

$$q_1(x) = a_0 + a_2 x + \dots + a_{n-2} x^{\frac{n-2}{2}}, \quad q_2(x) = a_1 + a_3 x + \dots + a_{n-1} x^{\frac{n-2}{2}},$$

так что

$$P_1(x) = q_1(x^2), \quad P_2(x) = x q_2(x^2), \quad P(x) = P_1(x) + P_2(x).$$

Хотим вычислить $P(x)$ в точках $\omega_n^0, \dots, \omega_n^{n-1}$. Пользуясь $(\omega_n^k)^2 = \omega_{n/2}^k$:

$$P(\omega_n^k) = q_1(\omega_n^{2k}) + \omega_n^k q_2(\omega_n^{2k}) = q_1(\omega_{n/2}^k) + \omega_n^k q_2(\omega_{n/2}^k).$$

Обозначив через $q_1[k], q_2[k]$ значения половинных ДПФ, получаем «бабочку»:

$$k = 0, \dots, \frac{n}{2} - 1 : P[k] = q_1[k] + \omega_n^k q_2[k],$$

$$k = \frac{n}{2}, \dots, n - 1 : P[k] = q_1[k - \frac{n}{2}] - \omega_n^{k - \frac{n}{2}} q_2[k - \frac{n}{2}].$$

(во второй строке использовано $\omega_n^k = -\omega_n^{k-n/2}$).

4 Алгоритм FFT

Псевдокод

```

FFT(a,  $\omega_n$ ):
  if n == 1:
    return [a0]
  q1 = [a0, a2, ..., an-2]
  q2 = [a1, a3, ..., an-1]
  p1 = FFT(q1,  $\omega_n^2$ )
  p2 = FFT(q2,  $\omega_n^2$ )
  for i = 0 ... n/2 - 1:
    res[i] = p1[i] +  $\omega_n^i$  · p2[i]
    res[i + n/2] = p1[i] -  $\omega_n^i$  · p2[i]
  return res

```

Отсюда можем вычислять произведение многочленов, длинных чисел и т. д.

4.1 Матричная форма и обратное преобразование

Заметим, что ДПФ — это просто домножение вектора коэффициентов на матрицу:

$$\underbrace{\begin{pmatrix} \omega_n^{0 \cdot 0} & \omega_n^{0 \cdot 1} & \dots & \omega_n^{0 \cdot (n-1)} \\ \omega_n^{1 \cdot 0} & \omega_n^{1 \cdot 1} & \dots & \omega_n^{1 \cdot (n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_n^{(n-1) \cdot 0} & \omega_n^{(n-1) \cdot 1} & \dots & \omega_n^{(n-1) \cdot (n-1)} \end{pmatrix}}_W \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} P(\omega_n^0) \\ \vdots \\ P(\omega_n^{n-1}) \end{pmatrix}.$$

Вычислим W^2 . Элемент (i, j) равен

$$(W^2)_{i,j} = \sum_{k=0}^{n-1} \omega_n^{i \cdot k} \omega_n^{k \cdot j} = \sum_{k=0}^{n-1} \omega_n^{k(i+j)}.$$

Разбираем два случая:

- если $i + j \equiv 0 \pmod{n}$, то каждое слагаемое равно 1, и сумма равна n ;
- если $i + j \not\equiv 0, n$, это геометрическая прогрессия

$$\frac{\omega_n^0((\omega_n^{i+j})^n - 1)}{1 - \omega_n^{i+j}} = 0,$$

так как $(\omega_n^{i+j})^n = 1$.

$$W^2 = n \cdot \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

— это (с точностью до множителя n) перестановка, оставляющая индекс 0 на месте и переворачивающая остальные.

Отсюда **обратное преобразование**: применить прямое БПФ, перевернуть все элементы кроме нулевого и поделить на n .

iFFT

```
iFFT(a):
  a = FFT(a)
  reverse(a[1:])
  a = a / n
```

5 Обратный формальный степенной ряд

Задача деления. Даны $P(x)$ и $B(x)$; найти $Q(x), R(x)$ такие, что

$$P(x) = B(x)Q(x) + R(x) \implies P(x) - R(x) = B(x)Q(x).$$

Ключевой инструмент — обращение степенного ряда.

Рассмотрим формальный степенной ряд $A(x) = \sum_{k=0}^{\infty} a_k x^k$.

Для всякого ФСР с $a_0 \neq 0$ существует единственный обратный $A^{-1}(x)$, такой что $A^{-1}(x)A(x) = 1$.

Построение коэффициентов по одному. Пусть $A(x) = a_0 + a_1x + a_2x^2 + \dots$. Начинаем с $b_0 = 1/a_0$ и на каждом шаге подбираем очередной коэффициент так, чтобы обнулить соответствующий член произведения $A^{-1}A$:

$$b_0 = \frac{1}{a_0}, \quad b_k = -\frac{1}{a_0} \sum_{i=1}^k a_i b_{k-i} \quad (k \geq 1).$$

Так последовательно получаем $A^{-1}A = 1 + 0 \cdot x + 0 \cdot x^2 + \dots$, и т. д.

6 Обращение ряда методом Ньютона (удвоение точности)

Более быстрый способ — удваивать число верных коэффициентов за шаг. Пусть $B_k \equiv A^{-1} \pmod{x^{2^k}}$; стартуем с

$$B_0 = a_0^{-1} = A^{-1} \pmod{x^1}.$$

Индукция: пусть

$$AB_k \equiv 1 \pmod{x^{2^k}} \iff 1 - AB_k \equiv 0 \pmod{x^{2^k}}.$$

Значит, по модулю удвоенной точности $AB_k \equiv 1 + x^{2^k}C \pmod{x^{2^{k+1}}}$ для некоторого ряда C . Возведём разность в квадрат явно:

$$(1 - AB_k)^2 \equiv (1 - (1 + x^{2^k}C))^2 = (x^{2^k}C)^2 = x^{2^{k+1}}C^2 \equiv 0 \pmod{x^{2^{k+1}}}.$$

Раскрывая левую часть,

$$1 - 2AB_k + A^2B_k^2 \equiv 0 \implies 1 \equiv A(2B_k - AB_k^2) \pmod{x^{2^{k+1}}}.$$

$$B_{k+1} \equiv B_k (2 - AB_k) \pmod{x^{2^{k+1}}}.$$

7 Деление многочленов

Пусть $A(x), B(x)$ — многочлены, $\deg A = n$, $\deg B = m$, и

$$A(x) = B(x)Q(x) + R(x), \quad \deg R(x) < \deg B(x).$$

Введём **разворот** коэффициентов:

$$\text{rev}(P(x)) = x^{\deg P(x)} P\left(\frac{1}{x}\right).$$

Из $A(x) - R(x) = B(x)Q(x)$, применяя rev , получаем

$$\text{rev}(A(x)) - x^{n-\deg R} \text{rev}(R(x)) = \text{rev}(B(x)) \text{rev}(Q(x)).$$

Так как $\deg R < m$, старший (в развороте) вклад R уходит за модуль:

$$\begin{aligned} \text{rev}(A(x)) &\equiv \text{rev}(B(x)) \text{rev}(Q(x)) \pmod{x^{n-m+1}}, \\ \text{rev}(Q(x)) &\equiv \text{rev}(A(x)) \text{rev}(B(x))^{-1} \pmod{x^{n-m+1}}. \end{aligned}$$

Обратный ряд $\text{rev}(B)^{-1}$ считается методом Ньютона (см. выше). Остаток $R(x)$ вычисляется после нахождения $Q(x)$ как $R = A - BQ$.

8 Multipoint Evaluation

Дано: многочлен $A(x)$ и набор точек $x_1, \dots, x_m$.

Хотим: вычислить $A(x_1), \dots, A(x_m)$.

По теореме Безу

$$A(x_i) \equiv A(x) \pmod{x - x_i}.$$

Пусть

$$P_{l,r} = \prod_{i=l}^r (x - x_i).$$

Строим дерево отрезков: сначала для каждой вершины вычисляем $P_{l,r}$ (снизу вверх). Затем идём сверху вниз и для каждой вершины берём

$$P(x) \bmod P_{l,m} \quad \text{и} \quad P(x) \bmod P_{m,r}.$$

В листьях получаем ответ — значения $A(x_i)$.

9 Интерполяция (многочлен Лагранжа)

Многочлен степени n можно однозначно восстановить по значениям в $(n + 1)$ точке. Интерполяционный многочлен Лагранжа:

$$A(x) = \sum_{i=1}^n y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}.$$

Пусть

$$P(x) = \prod_{i=1}^n (x - x_i), \quad P'(x) = \sum_{i=1}^n \prod_{j \neq i} (x - x_j), \quad P'(x_i) = \prod_{j \neq i} (x_i - x_j).$$

При помощи multipoint evaluation (см. выше) получаем знаменатели $\prod_{j \neq i} (x_i - x_j)$, то есть коэффициенты

$$t_i = \frac{y_i}{\prod_{j \neq i} (x_i - x_j)}.$$

Остаётся вычислить числитель $\sum_{i=1}^n t_i \prod_{j \neq i} (x - x_j)$ методом «разделяй и властвуй»: на узле, покрывающем отрезок $[l, r]$ с серединой m ,

$$A_{lr} = A_{lm} P_{mr} + A_{mr} P_{lm},$$

где P — произведения $(x - x_i)$ по подотрезкам.