СПбГУ · МКН · СП · 1 КУРС

Математические основы алгоритмов

Конспект лекций

Лектор: Косолобов Д. А.

Составители: ....

Санкт-Петербург, 2026

Вторая часть курса

1. Быстрое преобразование Фурье (FFT).

Свёртка и умножение многочленов

Определение 1

Пусть заданы последовательности чисел $a_0, \dots, a_{n-1}$ и $b_0, \dots, b_{n-1}$. Определим последовательность $c_0, \dots, c_{2n-2}$ по формуле

$$c_k = \sum_{t=0}^{n-1} a_t \, b_{k-t}, \qquad k = 0, \dots, 2n-2,$$

(считаем $a_i = b_i = 0$ при $i \notin [0, n-1]$). Эта операция называется **инволюцией (сверткой)**:

$$c = a * b.$$

Умножение многочленов

Рассмотрим многочлены:

$$A(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1},$$

$$B(x) = b_0 + b_1 x + \dots + b_{n-1} x^{n-1}.$$

Тогда их произведение:

$$C(x) = A(x)B(x) = c_0 + c_1 x + \dots + c_{2n-2} x^{2n-2},$$

где коэффициенты c_k задаются инволюцией.

Сложность

- Наивное умножение: $O(n^2)$.
- Карацуба: $O\left(n^{\log_2 3}\right)$.
- FFT (быстрое преобразование Фурье): $O(n \log n)$.

Идея FFT-умножения

Хотим быстро вычислить свёртку (а значит и произведение многочленов). Для этого:

1. Выбираем число точек N так, чтобы $N \geq 2n-1$ и обычно $N = 2^t$. Коэффициенты A, B дополняем нулями до длины N.
2. Быстро считаем значения в N точках:

   $$A(\omega^k), \quad B(\omega^k), \qquad k = 0, \dots, N-1,$$

   где ω — примитивный N-й корень из единицы.
3. Перемножаем покомпонентно:

   $$y_k = A(\omega^k)\, B(\omega^k).$$

4. По значениям y_k восстанавливаем коэффициенты C обратным FFT.

Ключевой факт: можно выбрать точки ω^k так, что и «вычисление значений», и «восстановление коэффициентов» делаются за $O(N \log N)$.

Реализация FFT

Далее считаем, что $N = 2^t$. Если исходная длина не степень двойки, дополняем нулями.

Прямое FFT: из коэффициентов в значения

Выбираем

$$\omega = e^{2\pi i/N} = \cos\frac{2\pi}{N} + i\sin\frac{2\pi}{N}, \qquad \omega_k = \omega^k.$$

Нужно вычислить

$$y_k = A(\omega^k) = \sum_{j=0}^{N-1} a_j(\omega^k)^j, \qquad k = 0, \dots, N-1.$$

Разобьём A на чётные и нечётные коэффициенты:

$$A_0(x) = a_0 + a_2x + \cdots + a_{N-2}x^{\frac{N}{2}-1}, \qquad A_1(x) = a_1 + a_3x + \cdots + a_{N-1}x^{\frac{N}{2}-1}.$$

Тогда

$$A(x) = A_0(x^2) + xA_1(x^2).$$

Подставим $x = \omega^k$:

$$A(\omega^k) = A_0(\omega^{2k}) + \omega^k A_1(\omega^{2k}).$$

Обозначим

$$y_k^{(0)} = A_0(\omega^{2k}), \qquad y_k^{(1)} = A_1(\omega^{2k}).$$

Так как значения ω^{2k} пробегают только $N/2$ различных точек, достаточно посчитать $y_k^{(0)}, y_k^{(1)}$ для $k = 0, \dots, \frac{N}{2} - 1$ (рекурсивно), а затем «склеить» ответы:

$$y_k = y_k^{(0)} + \omega^k\, y_k^{(1)}, \qquad y_{k+\frac{N}{2}} = y_k^{(0)} - \omega^k\, y_k^{(1)}.$$

(Здесь использовано $\omega^{k+N/2} = -\omega^k$.)

Оценка времени прямого FFT

На каждом уровне рекурсии решаем 2 подзадачи размера $N/2$ и делаем склейку за $O(N)$:

$$T(N) = 2T\left(\frac{N}{2}\right) + O(N) = O(N \log N).$$

Обратное FFT: из значений в коэффициенты

Прямое преобразование можно записать матрично:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^1 & (\omega^1)^2 & \cdots & (\omega^1)^{N-1} \\ 1 & \omega^2 & (\omega^2)^2 & \cdots & (\omega^2)^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & (\omega^{N-1})^2 & \cdots & (\omega^{N-1})^{N-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{pmatrix}.$$

Это матрица Вандермонда F_ω.

Утверждение 1

Выполнено

$$F_{\omega^{-1}}\, F_{\omega} = N \cdot \mathbf{I}.$$

Доказательство. Элемент в позиции (i, j) равен

$$\sum_{k=0}^{N-1} (\omega^i)^k (\omega^{-j})^k = \sum_{k=0}^{N-1} (\omega^{i-j})^k.$$

Если $i \neq j$, то $\omega^{i-j} \neq 1$ и сумма геометрической прогрессии даёт 0. Если $i = j$, то получаем сумму из N единиц, то есть N. ■

Следовательно, обратное преобразование — это прямое FFT с корнем ω^{-1}, после чего нужно поделить все коэффициенты на N:

$$a = \frac{1}{N}\, F_{\omega^{-1}}\, y.$$

Сложность умножения многочленов через FFT

Нужно:

- одно прямое FFT для A,
- одно прямое FFT для B,
- покомпонентное умножение ($O(N)$),
- одно обратное FFT.

Итого $O(N \log N)$, где N — ближайшая степень двойки, не меньшая $2n - 1$.

Обобщение: NTT (Number-Theoretic Transform)

Вместо $\mathbb{C}$ можно работать в кольце/поле R, если:

- в R существует элемент ω порядка N (примитивный N-й корень из единицы);
- число N обратимо в R (нужно для деления на N в обратном преобразовании).

Пример (поле $\mathbb{Z}_p$)

Пусть $R = \mathbb{Z}_p$, где p — простое, и

$$N = 2^k, \qquad p = c \cdot 2^k + 1.$$

Тогда $p - 1$ кратно N, и существует первообразный корень g по модулю p (порождает мультипликативную группу порядка $p - 1$). Можно взять

$$\omega \equiv g^c \pmod{p},$$

тогда ω имеет порядок N, и NTT работает полностью по модулю p.

Приложение: смысл коэффициентов ДПФ

Пусть дан сигнал (последовательность)

$$a_0, a_1, \ldots, a_{N-1}.$$

Определим дискретное преобразование Фурье:

$$y_k = \sum_{t=0}^{N-1} a_t \, \omega^{kt}, \qquad k = 0, \ldots, N-1, \quad \text{где } \omega = e^{2\pi i/N}.$$

Так как

$$\omega^{kt} = \cos\left(\frac{2\pi k}{N} t\right) + i \sin\left(\frac{2\pi k}{N} t\right),$$

то

$$\Re(y_k) = \sum_{t=0}^{N-1} a_t \cos\left(\frac{2\pi k}{N} t\right), \qquad \Im(y_k) = \sum_{t=0}^{N-1} a_t \sin\left(\frac{2\pi k}{N} t\right).$$

Эти суммы — скалярные произведения сигнала с косинусом и синусом частоты k. Если в сигнале сильно выражена гармоника частоты k, то вклады «складываются», и модуль $|y_k|$ получается большим; если такой частоты нет — вклады в основном взаимно компенсируются и $|y_k|$ близок к нулю.