Длинная арифметика

Гусев Илья

Московский физико-технический институт

Москва, 2017

Содержание

Умножение Карацубы

$$x = \boxed{x_L}\boxed{x_R} = 2^{n/2}x_L + x_R$$
$$y = \boxed{y_L}\boxed{y_R} = 2^{n/2}y_L + y_R$$

Идея:

$x \cdot y = (2^{\frac{n}{2}} \cdot x_L + x_R)(2^{\frac{n}{2}} \cdot y_L + y_R) = 2^n \cdot x_L \cdot y_L + 2^{\frac{n}{2}}(x_L \cdot y_R + x_R \cdot y_L) + x_R \cdot y_R$

4 умножения $\rightarrow \mathrm{T(n)} = 4 \cdot T(\frac{n}{2}) + O(n) \rightarrow \mathrm{O(n^2)}$

$x \cdot y = 2^n \cdot x_L \cdot y_L + 2^{\frac{n}{2}}((x_L + x_R) \cdot (y_L + y_R) - x_R \cdot y_R - x_L \cdot y_L) + x_R \cdot y_R$

3 умножения $\rightarrow \mathrm{T(n)} = 3 \cdot T(\frac{n}{2}) + O(n) \rightarrow \mathrm{O(n^{log_2 3})}$

Дискретное преобразование Фурье

ДПФ для $\vec{x}$: $\vec{X} = \hat{A}\vec{x}$, где $\hat{A}$: $a_N^{mn} = e^{-\frac{2\pi i}{N} mn}$
Идея ДПФ для полинома: полином в степени n $\Leftrightarrow$ значения в n+1 точках
ДПФ для полинома $A(x) = a_0 x^0 + a_1 x^1 + \ldots + a_{n-1} x^{n-1}$:
$\mathrm{DFT}(a_0, a_1, \ldots, a_{n-1}) = (y_0, y_1, \ldots, y_{n-1}) = (A(w_n^0), A(w_n^1), \ldots, A(w_n^{n-1}))$
$w_n^k = e^{-i\frac{2\pi k}{n}}$

Дискретное преобразование Фурье

Пример для $13 \Leftrightarrow 3 + x, 24 \Leftrightarrow 4 + 2x$:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \times \begin{bmatrix} 3 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 4 \\ 3-i \\ 2 \\ 3+i \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \times \begin{bmatrix} 4 \\ 2 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 6 \\ 4-2i \\ 2 \\ 4+2i \end{bmatrix}$$

$$\begin{bmatrix} 4 & 3-i & 2 & 3+i \end{bmatrix} \times \begin{bmatrix} 6 \\ 4-2i \\ 2 \\ 4+2i \end{bmatrix} = \begin{bmatrix} 24 \\ 10-10i \\ 4 \\ 10+10i \end{bmatrix}$$

$$0.25 \times \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \times \begin{bmatrix} 24 \\ 10-10i \\ 4 \\ 10+10i \end{bmatrix} = \begin{bmatrix} 12 \\ 10 \\ 2 \\ 0 \end{bmatrix}$$

$12 + 10x + 2x^2 \Leftrightarrow 12 + 100 + 200 = 312$

Быстрое преобразование Фурье

Идея БПФ: разделяй и властвуй:

$A_0(x) = a_0x^0 + a_2x^1 + \ldots + a_{n-2}x^{n/2-1}$

$A_1(x) = a_1x^0 + a_3x^1 + \ldots + a_{n-1}x^{n/2-1}$

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

$y_k = y_k^0 + w_n^k y_k^1, \quad k = 0 \ldots n/2 - 1$

$y_{k+n/2} = y_k^0 - w_n^k y_k^1, \quad k = 0 \ldots n/2 - 1$

$y_{k+n/2} = A(w_n^{k+n/2}) = A_0(w_n^{2k+n}) + w_n^{k+n/2} A_1(w_n^{2k+n}) =$

$A_0(w_n^{2k}) - w_n^k A_1(w_n^{2k}) = y_k^0 - w_n^k y_k^1$

Быстрое преобразование Фурье

Обратное - через обратную матрицу к $\hat{A}$
$\mathrm{DFT}(A \times B) = \mathrm{DFT}(A) \times \mathrm{DFT}(B)$
$A \times B = \mathrm{InverseDFT}(\mathrm{DFT}(A) \times \mathrm{DFT}(B))$
Коэффициенты многочлена - числа в разрядах
Сложность: $O(n \cdot log(n))$

Полезные ссылки I

E-maxx: FFT

http://e-maxx.ru/algo/fft_multiply

Wiki: DFT

https://en.wikipedia.org/wiki/Discrete_Fourie_transform