

Алгоритмы и структуры данных

Лекция 3: Быстрое преобразование Фурье

А. Куликов

Академия современного программирования

План лекции

- 1 Быстрое вычисление значений в точках

План лекции

- 1 Быстрое вычисление значений в точках
- 2 Комплексные корни из единицы

План лекции

- 1 Быстрое вычисление значений в точках
- 2 Комплексные корни из единицы
- 3 Быстрое преобразование Фурье

План лекции

- 1 Быстрое вычисление значений в точках
- 2 Комплексные корни из единицы
- 3 Быстрое преобразование Фурье
- 4 Интерполяция

Умножение многочленов

Умножение многочленов

Умножение многочленов

Умножение многочленов

- Итак, мы научились быстро перемножать числа и матрицы. Теперь будем учиться эффективно перемножать многочлены.

Умножение многочленов

Умножение многочленов

- Итак, мы научились быстро перемножать числа и матрицы. Теперь будем учиться эффективно перемножать многочлены.
- Произведение двух многочленов $A(x) = \sum_{i=0}^d a_i x^i$ и $B(x) = \sum_{i=0}^d b_i x^i$ степени d может быть вычислено за время $O(d^2)$: если

$$C(x) = A(x) \cdot B(x) = \sum_{i=0}^{2d} c_i x^i,$$

то

$$c_k = \sum_{i=0}^k a_i b_{k-i}.$$

Альтернативное представление многочленов

Факт

Многочлен степени d однозначно задается значениями в любых $d + 1$ различных точках.

Альтернативное представление многочленов

Факт

Многочлен степени d однозначно задается значениями в любых $d + 1$ различных точках.

Задание многочлена значениями

Альтернативное представление многочленов

Факт

Многочлен степени d однозначно задается значениями в любых $d + 1$ различных точках.

Задание многочлена значениями

- Выберем произвольные $(d + 1)$ точку x_0, \dots, x_d .

Альтернативное представление многочленов

Факт

Многочлен степени d однозначно задается значениями в любых $d + 1$ различных точках.

Задание многочлена значениями

- Выберем произвольные $(d + 1)$ точку x_0, \dots, x_d .
- Многочлен $A(x) = a_0 + a_1x + \dots + a_dx^d$ может быть задан одним из двух способов:

Альтернативное представление многочленов

Факт

Многочлен степени d однозначно задается значениями в любых $d + 1$ различных точках.

Задание многочлена значениями

- Выберем произвольные $(d + 1)$ точку x_0, \dots, x_d .
- Многочлен $A(x) = a_0 + a_1x + \dots + a_dx^d$ может быть задан одним из двух способов:
 - 1 коэффициентами a_0, \dots, a_d

Альтернативное представление многочленов

Факт

Многочлен степени d однозначно задается значениями в любых $d + 1$ различных точках.

Задание многочлена значениями

- Выберем произвольные $(d + 1)$ точку x_0, \dots, x_d .
- Многочлен $A(x) = a_0 + a_1x + \dots + a_dx^d$ может быть задан одним из двух способов:
 - 1 коэффициентами a_0, \dots, a_d
 - 2 значениями $A(x_0), \dots, A(x_d)$

Альтернативное представление многочленов

Факт

Многочлен степени d однозначно задается значениями в любых $d + 1$ различных точках.

Задание многочлена значениями

- Выберем произвольные $(d + 1)$ точку x_0, \dots, x_d .
- Многочлен $A(x) = a_0 + a_1x + \dots + a_dx^d$ может быть задан одним из двух способов:
 - 1 коэффициентами a_0, \dots, a_d
 - 2 значениями $A(x_0), \dots, A(x_d)$
- Второе представление более удобно для вычисления произведения, однако обычно многочлены даны нам в виде списка коэффициентов и произведение необходимо вычислить в таком же виде.

Общая идея

Общая идея

Общая идея

Общая идея

- Выберем несколько точек x_0, \dots, x_{n-1} , где $n \geq 2d + 1$, в каждой из них вычислим $C(x_i) = A(x_i)B(x_i)$ и по полученному набору точек восстановим многочлен C (данная операция называется интерполяцией).

Общая идея

Общая идея

- Выберем несколько точек x_0, \dots, x_{n-1} , где $n \geq 2d + 1$, в каждой из них вычислим $C(x_i) = A(x_i)B(x_i)$ и по полученному набору точек восстановим многочлен C (данная операция называется интерполяцией).
- Ясно, что произведения мы вычислим за линейное время.

Общая идея

Общая идея

- Выберем несколько точек x_0, \dots, x_{n-1} , где $n \geq 2d + 1$, в каждой из них вычислим $C(x_i) = A(x_i)B(x_i)$ и по полученному набору точек восстановим многочлен C (данная операция называется интерполяцией).
- Ясно, что произведения мы вычислим за линейное время.
- Но сколько потребуется для вычисления всех значений $A(x_i), B(x_i)$?

Общая идея

Общая идея

- Выберем несколько точек x_0, \dots, x_{n-1} , где $n \geq 2d + 1$, в каждой из них вычислим $C(x_i) = A(x_i)B(x_i)$ и по полученному набору точек восстановим многочлен C (данная операция называется интерполяцией).
- Ясно, что произведения мы вычислим за линейное время.
- Но сколько потребуется для вычисления всех значений $A(x_i), B(x_i)$?
- Потребуется $\Theta(d^2)$ операций.

Общая идея

Общая идея

- Выберем несколько точек x_0, \dots, x_{n-1} , где $n \geq 2d + 1$, в каждой из них вычислим $C(x_i) = A(x_i)B(x_i)$ и по полученному набору точек восстановим многочлен C (данная операция называется интерполяцией).
- Ясно, что произведения мы вычислим за линейное время.
- Но сколько потребуется для вычисления всех значений $A(x_i), B(x_i)$?
- Потребуется $\Theta(d^2)$ операций.
- Мы покажем, что для некоторых специально выбранных точек x_i вычисление всех значений $A(x_i), B(x_i)$ можно провести за время $\Theta(d \log d)$, после чего по полученным значениям восстановить многочлен, опять же, за время $\Theta(d \log d)$.

План лекции

- 1 Быстрое вычисление значений в точках
- 2 Комплексные корни из единицы
- 3 Быстрое преобразование Фурье
- 4 Интерполяция

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

- Рассмотрим набор точек $\pm x_0, \pm x_1, \dots, \pm x_{n/2-1}$ и многочлен A степени не более $n - 1$.

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

- Рассмотрим набор точек $\pm x_0, \pm x_1, \dots, \pm x_{n/2-1}$ и многочлен A степени не более $n - 1$.
- Интуитивно ясно, что вычисление значений многочлена на таком наборе точек должно быть проще, поскольку $A(x_i)$ и $A(-x_i)$ содержат много одинаковых мономов.

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

- Рассмотрим набор точек $\pm x_0, \pm x_1, \dots, \pm x_{n/2-1}$ и многочлен A степени не более $n - 1$.
- Интуитивно ясно, что вычисление значений многочлена на таком наборе точек должно быть проще, поскольку $A(x_i)$ и $A(-x_i)$ содержат много одинаковых мономов.
- Разложим мономы A по чётности степени:
 $A(x) = A_0(x^2) + xA_1(x^2)$, где многочлены A_0 и A_1 имеют степень не более $n/2 - 1$.

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

- Рассмотрим набор точек $\pm x_0, \pm x_1, \dots, \pm x_{n/2-1}$ и многочлен A степени не более $n - 1$.
- Интуитивно ясно, что вычисление значений многочлена на таком наборе точек должно быть проще, поскольку $A(x_i)$ и $A(-x_i)$ содержат много одинаковых мономов.
- Разложим мономы A по чётности степени:
 $A(x) = A_0(x^2) + xA_1(x^2)$, где многочлены A_0 и A_1 имеют степень не более $n/2 - 1$.
- Нетрудно видеть, что

$$\begin{aligned}A(x_i) &= A_0(x_i^2) + x_i A_1(x_i^2) \\A(-x_i) &= A_0(x_i^2) - x_i A_1(x_i^2)\end{aligned}$$

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

- Таким образом, мы свели задачу вычисления значений многочлена A степени не более $n - 1$ в n точках $\pm x_0, \dots, \pm x_{n/2-1}$ к задаче вычисления значений двух многочленов A_0 и A_1 степени не более $n/2 - 1$ в $n/2$ точках $x_0^2, \dots, x_{n/2-1}^2$.

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

- Таким образом, мы свели задачу вычисления значений многочлена A степени не более $n - 1$ в n точках $\pm x_0, \dots, \pm x_{n/2-1}$ к задаче вычисления значений двух многочленов A_0 и A_1 степени не более $n/2 - 1$ в $n/2$ точках $x_0^2, \dots, x_{n/2-1}^2$.
- Соответствующее рекуррентное соотношение:
$$T(n) = 2T(n/2) + O(n).$$

Быстрое вычисление значений в точках

Быстрое вычисление значений в точках

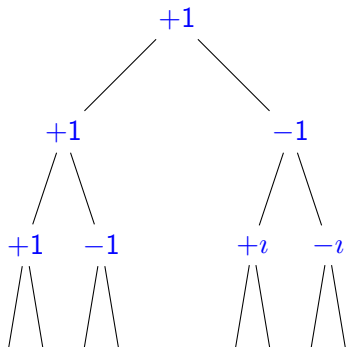
- Таким образом, мы свели задачу вычисления значений многочлена A степени не более $n - 1$ в n точках $\pm x_0, \dots, \pm x_{n/2-1}$ к задаче вычисления значений двух многочленов A_0 и A_1 степени не более $n/2 - 1$ в $n/2$ точках $x_0^2, \dots, x_{n/2-1}^2$.
- Соответствующее рекуррентное соотношение:
$$T(n) = 2T(n/2) + O(n).$$
- Но к полученному набору значений рекурсия не применима, поскольку он не является набором вида $\pm y_0, \dots, \pm y_k!$

Быстрое вычисление значений в точках

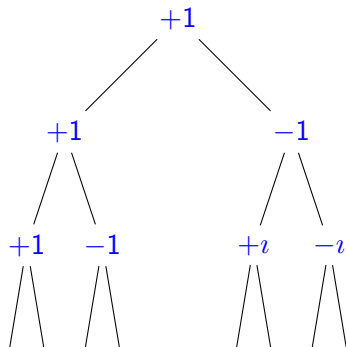
Быстрое вычисление значений в точках

- Таким образом, мы свели задачу вычисления значений многочлена A степени не более $n - 1$ в n точках $\pm x_0, \dots, \pm x_{n/2-1}$ к задаче вычисления значений двух многочленов A_0 и A_1 степени не более $n/2 - 1$ в $n/2$ точках $x_0^2, \dots, x_{n/2-1}^2$.
- Соответствующее рекуррентное соотношение:
$$T(n) = 2T(n/2) + O(n).$$
- Но к полученному набору значений рекурсия не применима, поскольку он не является набором вида $\pm y_0, \dots, \pm y_k!$
- Идея: брать в качестве x_j комплексные числа.

Пример идеи



Пример идеи



Итак, нас интересуют комплексные корни из единицы.

План лекции

- 1 Быстрое вычисление значений в точках
- 2 **Комплексные корни из единицы**
- 3 Быстрое преобразование Фурье
- 4 Интерполяция

Комплексные корни из единицы

Определение

Комплексным корнем степени n из единицы называется такое комплексное число ω , что $\omega^n = 1$.

Комплексные корни из единицы

Определение

Комплексным корнем степени n из единицы называется такое комплексное число ω , что $\omega^n = 1$.

Факты

Комплексные корни из единицы

Определение

Комплексным корнем степени n из единицы называется такое комплексное число ω , что $\omega^n = 1$.

Факты

- Имеется ровно n комплексных корней из 1: $e^{2\pi i k/n}$ для $k = 0, 1, \dots, n-1$.

Комплексные корни из единицы

Определение

Комплексным корнем степени n из единицы называется такое комплексное число ω , что $\omega^n = 1$.

Факты

- Имеется ровно n комплексных корней из 1: $e^{2\pi i k/n}$ для $k = 0, 1, \dots, n-1$.
- Корни равномерно распределены на окружности единичного радиуса с центром в нуле.

Комплексные корни из единицы

Определение

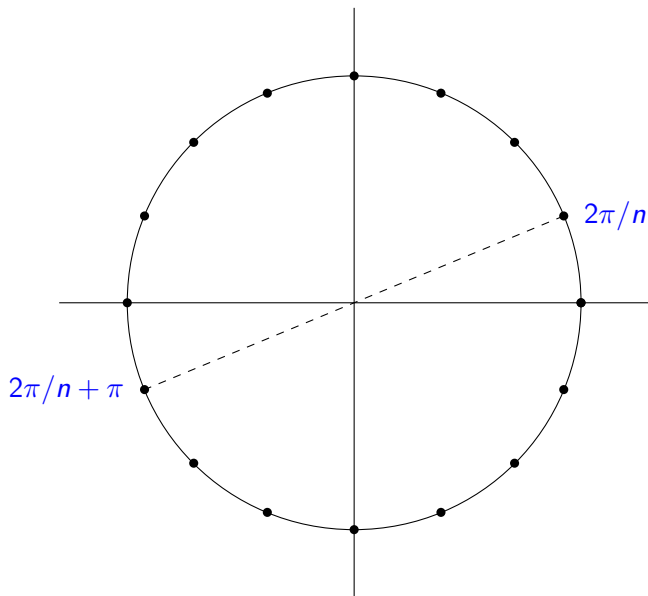
Комплексным корнем степени n из единицы называется такое комплексное число ω , что $\omega^n = 1$.

Факты

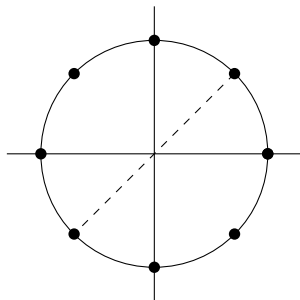
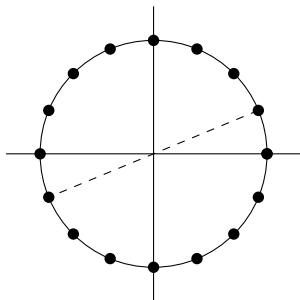
- Имеется ровно n комплексных корней из 1: $e^{2\pi i k/n}$ для $k = 0, 1, \dots, n-1$.
- Корни равномерно распределены на окружности единичного радиуса с центром в нуле.
- Все корни являются степенями **главного значения корня степени n из единицы**:

$$\omega_n = e^{2\pi i/n}.$$

Комплексные корни из единицы



Комплексные корни из единицы



Сводим задачу вычисления значений многочлена A в корнях n -й степени из единицы к задаче вычисления значений многочленов A_0 и A_1 в корнях $n/2$ -й степени из единицы. Рассматриваемые точки при этом остаются разбитыми на пары.

План лекции

- 1 Быстрое вычисление значений в точках
- 2 Комплексные корни из единицы
- 3 Быстрое преобразование Фурье
- 4 Интерполяция

Дискретное преобразование Фурье

Определение

Дискретным преобразованием Фурье вектора (a_0, \dots, a_{n-1}) называется вектор (y_0, \dots, y_{n-1}) , где

$$y_k = A(\omega_n^k) = \sum_{i=0}^{n-1} a_i w_n^{ki}.$$

Быстрым преобразованием Фурье называется метод быстрого вычисления дискретного преобразования Фурье.

Быстрое преобразование Фурье

FFT(A, ω_n)

- 1 ▷ Вход: коэффициенты многочлена A степени не более $n - 1$,
где n — степень двойки; корень из единицы n -й степени ω_n .
- 2 ▷ Выход: значения $A(\omega_n^0), \dots, A(\omega_n^{n-1})$.
- 3 **if** $\omega = 1$
- 4 **then return** $A(1)$
- 5 представить $A(x)$ в виде $A_0(x^2) + xA_1(x^2)$
- 6 FFT($A_0(\omega_n^2)$)
- 7 FFT($A_1(\omega_n^2)$)
- 8 **for** $j \leftarrow 0$ **to** $n - 1$
- 9 **do** $A(\omega_n^j) = A_0(\omega_n^{2j}) + \omega_n^j A_1(\omega_n^{2j})$
- 10 **return** $A(\omega_n^0), \dots, A(\omega_n^{n-1})$

План лекции

- 1 Быстрое вычисление значений в точках
- 2 Комплексные корни из единицы
- 3 Быстрое преобразование Фурье
- 4 Интерполяция

Интерполяция в терминах матриц

Интерполяция в терминах матриц

$$\begin{bmatrix} A(x_0) \\ A(x_1) \\ \vdots \\ A(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

Интерполяция в терминах матриц

Интерполяция в терминах матриц

$$\begin{bmatrix} A(x_0) \\ A(x_1) \\ \vdots \\ A(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

- Матрица M в центре называется **матрицей Вандермонда** и обладает важным свойством: если x_0, \dots, x_{n-1} попарно различны, то M обратима.

Интерполяция в терминах матриц

Интерполяция в терминах матриц

$$\begin{bmatrix} A(x_0) \\ A(x_1) \\ \vdots \\ A(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

- Матрица M в центре называется **матрицей Вандермонда** и обладает важным свойством: если x_0, \dots, x_{n-1} попарно различны, то M обратима.
- Таким образом, вычисление значений есть домножение на M , в то время как интерполяция — домножение на M^{-1} .

Быстрое преобразование Фурье

$$\text{FFT}(A, \omega_n) = \underbrace{\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_n & \omega_n^2 & \dots & \omega_n^{n-1} \\ 1 & \omega_n^2 & \omega_n^4 & \dots & \omega_n^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega_n^j & \omega_n^{2j} & \dots & \omega_n^{(n-1)j} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{n-1} & \omega_n^{2(n-1)} & \dots & \omega_n^{(n-1)(n-1)} \end{bmatrix}}_{M_n} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_j \\ \vdots \\ a_{n-1} \end{bmatrix}$$

Обратная матрица

Обратная матрица

Обратная матрица

Обратная матрица

- Итак, для восстановления коэффициентов многочлена по его значениям в точках $\omega_n^0, \dots, \omega_n^{n-1}$ необходимо построить матрицу M_n^{-1} .

Обратная матрица

Обратная матрица

- Итак, для восстановления коэффициентов многочлена по его значениям в точках $\omega_n^0, \dots, \omega_n^{n-1}$ необходимо построить матрицу M_n^{-1} .
- (k, j) -й элемент матрицы M_n равен ω_n^{jk} .

Обратная матрица

Обратная матрица

- Итак, для восстановления коэффициентов многочлена по его значениям в точках $\omega_n^0, \dots, \omega_n^{n-1}$ необходимо построить матрицу M_n^{-1} .
- (k, j) -й элемент матрицы M_n равен ω_n^{jk} .
- Покажем, что (k, j) -й элемент матрицы M_n^{-1} равен ω_n^{-jk} / n .

Обратная матрица

Обратная матрица

- Итак, для восстановления коэффициентов многочлена по его значениям в точках $\omega_n^0, \dots, \omega_n^{n-1}$ необходимо построить матрицу M_n^{-1} .
- (k, j) -й элемент матрицы M_n равен ω_n^{jk} .
- Покажем, что (k, j) -й элемент матрицы M_n^{-1} равен ω_n^{-jk} / n .
- Необходимо показать, что для заданной таким образом матрицы M_n^{-1} выполнено равенство

$$M_n^{-1} M_n = I_n.$$

Доказательство

Доказательство

$$M_n^{-1} M_n[j, k] = \sum_{i=0}^{n-1} (\omega_n^{-ij} / n) (\omega_n^{ik}) = \sum_{i=0}^{n-1} \omega_n^{i(k-j)} / n$$

Доказательство

Доказательство

$$M_n^{-1} M_n[j, k] = \sum_{i=0}^{n-1} (\omega_n^{-ij} / n) (\omega_n^{ik}) = \sum_{i=0}^{n-1} \omega_n^{i(k-j)} / n$$

- если $j \neq k$, то

$$\sum_{i=0}^{n-1} \omega_n^{i(k-j)} / n = \frac{1^{k-j} - 1}{(\omega_n^{k-j} - 1)n} = 0$$

(знаменатель не равен нулю)

Доказательство

Доказательство

$$M_n^{-1}M_n[j, k] = \sum_{i=0}^{n-1} (\omega_n^{-ij}/n)(\omega_n^{ik}) = \sum_{i=0}^{n-1} \omega_n^{i(k-j)}/n$$

- если $j \neq k$, то

$$\sum_{i=0}^{n-1} \omega_n^{i(k-j)}/n = \frac{1^{k-j} - 1}{(\omega_n^{k-j} - 1)n} = 0$$

(знаменатель не равен нулю)

- если $j = k$, то $M_n^{-1}M_n[j, k] = 1$



Резюме

Резюме

Таким образом, для восстановления многочлена по его значениям в точках $\omega_n^0, \dots, \omega_n^{n-1}$ достаточно применить быстрое преобразование Фурье к набору этих значений в точке ω_n^{-1} и поделить полученные коэффициенты на n .

Общая схема: еще раз

Общая схема: еще раз

Общая схема: еще раз

Общая схема: еще раз

- Даны два многочлена A и B степени d с коэффициентами a_0, \dots, a_d и b_0, \dots, b_d . Требуется найти коэффициенты многочлена $C = AB$.

Общая схема: еще раз

Общая схема: еще раз

- Даны два многочлена A и B степени d с коэффициентами a_0, \dots, a_d и b_0, \dots, b_d . Требуется найти коэффициенты многочлена $C = AB$.
- Пусть $n = 2d + 1$, ω_n — комплексный корень степени n из единицы.

Общая схема: еще раз

Общая схема: еще раз

- Даны два многочлена A и B степени d с коэффициентами a_0, \dots, a_d и b_0, \dots, b_d . Требуется найти коэффициенты многочлена $C = AB$.
- Пусть $n = 2d + 1$, ω_n — комплексный корень степени n из единицы.
- При помощи быстрого преобразования Фурье вычислить $A(\omega_n^0), \dots, A(\omega_n^{n-1})$ и $B(\omega_n^0), \dots, B(\omega_n^{n-1})$.

Общая схема: еще раз

Общая схема: еще раз

- Даны два многочлена A и B степени d с коэффициентами a_0, \dots, a_d и b_0, \dots, b_d . Требуется найти коэффициенты многочлена $C = AB$.
- Пусть $n = 2d + 1$, ω_n — комплексный корень степени n из единицы.
- При помощи быстрого преобразования Фурье вычислить $A(\omega_n^0), \dots, A(\omega_n^{n-1})$ и $B(\omega_n^0), \dots, B(\omega_n^{n-1})$.
- Вычислить $C(\omega_n^0), \dots, C(\omega_n^{n-1})$ ($C(\omega_n^i) = A(\omega_n^i)B(\omega_n^i)$).

Общая схема: еще раз

Общая схема: еще раз

- Даны два многочлена A и B степени d с коэффициентами a_0, \dots, a_d и b_0, \dots, b_d . Требуется найти коэффициенты многочлена $C = AB$.
- Пусть $n = 2d + 1$, ω_n — комплексный корень степени n из единицы.
- При помощи быстрого преобразования Фурье вычислить $A(\omega_n^0), \dots, A(\omega_n^{n-1})$ и $B(\omega_n^0), \dots, B(\omega_n^{n-1})$.
- Вычислить $C(\omega_n^0), \dots, C(\omega_n^{n-1})$ ($C(\omega_n^i) = A(\omega_n^i)B(\omega_n^i)$).
- Применив быстрое преобразование Фурье к набору значений $C(\omega_n^0), \dots, C(\omega_n^{n-1})$ и корню ω_n^{-1} и поделив все полученные значения на n , получим коэффициенты многочлена C .

Спасибо за внимание!