31/03/2022

FFT and Polynomials

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

Given P as $(a_0, a_1, a_2, \ldots, a_{n-1})$

Given Q as $(b_0, b_1, b_2, \ldots, b_{n-1})$

coefficient representation

Addition: $P+Q = (a_0+b_0, a_1+b_1, \ldots, a_{n-1}+b_{n-1})$

Evaluation: Evaluate P at a given point

$$P(x) = a_0 + x(a_1 + a_2 x^1 + a_3 x^2 + \cdots + a_{n-1} x^{n-2}) \checkmark$$

$$= a_0 + x(a_1 + x(a_2 + a_3 x + \cdots + a_{n-1} x^{n-3}))$$

$$\vdots$$

$$= a_0 + x(a_1 + x(a_2 + x(a_3 + \cdots + x(a_{n-2} + x a_{n-1}))))$$

Horner's Rule

now evaluation becomes $O(n)$

Multiplication: Given $P(x)$ and $Q(x)$.

$$R(x) = P(x) \cdot Q(x)$$

$$= (a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1})\ (b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1})$$

Total time := $a_i b_j \quad \forall\ i$ and j

$$O(n^2)$$

$\Rightarrow \quad P(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$

How many complex roots $P(x)$ have?

exactly $n-1$ roots.

$$\underbrace{(\alpha_1, P(\alpha_1)), \ldots, (\alpha_n, P(\alpha_n))}_{n \text{ evaluations. at distinct points.}}$$

There exists a unique polynomial of degree $\leq n-1$ that passes through the above n distinct points.

Point-Value representation

Represent a polynomial of deg $n-1$ with evaluations at n distinct points.

$$P(x) := \left((\alpha_1, P(\alpha_1)), \ldots, (\alpha_n, P(\alpha_n)) \right).$$

Addition: $P(x)$ and $Q(x)$

$$R(x) = P(x) + Q(x)$$
$$= \left((\alpha_1, P(\alpha_1) + Q(\alpha_1)), \ldots, (\alpha_n, P(\alpha_n) + Q(\alpha_n)) \right)$$

Multiplication: $R(x) = P(x) \cdot Q(x)$

$\leftarrow \deg \leq 2n-2$

$$\left((\alpha_1, P(\alpha_1) \cdot Q(\alpha_1)), \ldots, (\alpha_n, P(\alpha_n) \cdot Q(\alpha_n)) \right)$$

Start with point-value rep. of P and Q at $(2n-1)$ distinct points.

Total time: $O(n)$ time.

Evaluation:

$$P(x) = \left((\alpha_1, P(\alpha_1)), (\alpha_2, P(\alpha_2)), \ldots, (\alpha_n, P(\alpha_n)) \right)$$

given a point β.

Find $P(\beta)$. ?

$$P(x) = \sum_{i=1}^{n} P(\alpha_i) \frac{\prod_{j \neq i}(x-\alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)}$$ ← Lagrange's Form

Total time := $O(n^2)$

	Eval	Multiply
Coeff.	$O(n)$	$O(n^2)$
Point-value	$O(n^2)$	$O(n)$
FFT	$O(n \log n)$	$O(n \log n)$

Question: Multiply two given polynomials in Coeff-form in $O(n \log n)$ time?

$P(x) = (a_0, \ldots, a_{n-1})$ $\quad Q(x) = (b_0, \ldots, b_{n-1})$

$R(x) = (c_0, \ldots, c_{2n-2})$

Overall Strategy:

(1) Evaluate P and Q at $2n$ points. (to obtain point-value rep.)

Evaluation

$(\alpha_1, \ldots, \alpha_{2n})$

(2) Multiply in point-value form.

$$R(\alpha_1) = P(\alpha_1) \cdot Q(\alpha_1).$$

to obtain point-value representation of R.

(3) Interpolate R using $2n$ evaluations.

Interpolation

Step 1: Evaluation (Assume n is power of 2)

Main idea: evaluate at $(2n)^{th}$ roots of unity. $(e^{i\theta} = \cos\theta + i \sin\theta)$

$$\omega_{2n} = e^{\frac{2\pi i}{2n}} \qquad i = \sqrt{-1}$$

$$\{\omega_{2n}^{0}, \omega_{2n}^{1}, \ldots, \omega_{2n}^{2n-1}\}$$

where $\omega_{2n}^{j} = e^{\frac{2\pi i j}{2n}}$

$$x^{2n} = 1.$$

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

$$\left[T(n) \leq 2 \cdot T\left(\frac{n}{2}\right) + O(n) \right]$$

$$P_{even}(x) = a_0 + a_2 x + a_4 x^2 + \cdots + a_{n-2} x^{\frac{n-2}{2}}$$

$$P_{odd}(x) = a_1 + a_3 x + a_5 x^2 + \cdots + a_{n-1} x^{\frac{n-2}{2}}$$

$$P(x) = P_{even}(x^2) + x \cdot P_{odd}(x^2).$$

$$P(\omega_{2n}^{j}) = P_{even}\left(\left(\omega_{2n}^{j}\right)^2\right) + \omega_{2n}^{j} \cdot P_{odd}(\omega_{2n}^{2j})$$

But what is $\omega_{2n}^{2j} = e^{\frac{2\pi i \cdot 2j}{2n}}$

$= \underline{e^{\frac{2\pi i \cdot j}{n}}}$

one of the n^{th} roots of unity.

P_{even} and P_{odd} has $\deg \leq \frac{n-2}{2}$

and we need to evaluate them at n^{th} roots of unity.

$T(n)$:= no. of operations required to evaluate deg $n-1$ polynomial at all of $(2n)^{th}$ roots of Unity.

$$T(n) \leq 2 \cdot T\left(\frac{n}{2}\right) + O(n).$$

$$\Rightarrow \quad T(n) = O(n \log n).$$

Step 3 : Interpolation

Evaluations of R at 2n points.

where R is of degree $(2n-2)$.

and 2n points are $(2n)^{th}$ roots of unity.

$$R(x) = \underbrace{c_0 + c_1 x + c_2 x^2 + \cdots + c_{2n-2}}_{\text{unknowns}} x^{2n-2}$$

$$R(\omega_{2n}^0) = c_0 + c_1 \omega_{2n}^0 + c_2 (\omega_{2n}^0)^2 + \cdots + c_{2n-2} (\omega_{2n}^0)^{2n-2}$$

$$\vdots$$

$$R(\omega_{2n}^{2n-1}) = c_0 + c_1 \omega_{2n}^{2n-1} + c_2 (\omega_{2n}^{2n-1})^2 + \cdots + c_{2n-2} (\omega_{2n}^{2n-1})^{2n-2}$$

you have got $2n$ equations in $(2n-1)$ variables.

$$\overset{R}{\begin{bmatrix} R(\omega_{2n}^0) \\ \vdots \\ R(\omega_{2n}^{2n-2}) \end{bmatrix}} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_{2n} & \omega_{2n}^2 & \cdots & \omega_{2n}^{2n-2} \\ 1 & (\omega_{2n}^2) & (\omega_{2n}^2)^2 & \cdots & \\ \vdots & \vdots & & & \\ 1 & (\omega_{2n}^{2n-2}) & (\omega_{2n}^{2n-2})^2 & \cdots & (\omega_{2n}^{2n-2})^{2n-2} \end{bmatrix} \begin{bmatrix} c_0 \\ \vdots \\ c_{2n-2} \end{bmatrix}$$

$$\Updownarrow$$

denote $z_j := \omega_{2n}^j$

$z_0, \dots, z_{2n-2}$

$$\begin{bmatrix} 1 & z_0 & z_0^2 & \cdots & z_0^{2n-2} \\ 1 & z_1 & z_1^2 & \cdots & z_1^{2n-2} \\ 1 & - & - & - & - \\ \vdots & & & & \\ 1 & z_{2n-2} & z_{2n-2}^2 & \cdots & z_{2n-2}^{2n-2} \end{bmatrix}$$

Vandermonde matrix

determinant $:= \prod_{0 \le i < j \le 2n-2} (z_j - z_i)$

$$R = V[c]$$

$$[c] = V^{-1} R.$$

$$[V^{-1}]_{jk} = \frac{1}{2n} \omega_{2n}^{-jk}$$

$0 \leq j \leq 2n-1$

$0 \leq k \leq 2n-1$

$$c_j = \sum_{0 \leq k \leq 2n-1} \frac{1}{2n} \omega_{2n}^{-jk} \cdot R(\omega_{2n}^{k})$$

$$c_j = \sum_{0 \leq k \leq 2n-1} \left[\frac{1}{2n} \cdot R(\omega_{2n}^{k})\right] \cdot (\omega_{2n}^{-j})^{k}$$

we have reduce interpolation to

evaluations at roots of unity.

In particular to Step 1.