# Lec 4

## Fast Fourier Transform

Multiply two polynomials $p(z) \cdot q(z)$.

**prop.** A degree-$d$ polynomial is determined by the value at $d+1$ distinct points.

**Pf.** $p(z) = \sum_{i=0}^{d} a_i z^i$.

$d+1$ points. $z_0, z_1, \dots, z_d$

$$\Rightarrow \begin{bmatrix} p(z_0) \\ p(z_1) \\ \vdots \\ p(z_d) \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & z_0 & z_0^2 & \cdots & z_0^d \\ 1 & z_1 & z_1^2 & \cdots & z_1^d \\ & & \vdots & & \\ 1 & z_d & z_d^2 & \cdots & z_d^d \end{bmatrix}}_{A} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{bmatrix} = A^{-1} \begin{bmatrix} p(z_0) \\ \vdots \\ p(z_d) \end{bmatrix}.$$

$A$ : Vandermonde Matrix.

$$|A| = \prod_{0 \le i < j \le d} (z_i - z_j).$$

**Corollary.** Determining $p(z) \cdot q(z)$

$\Longleftrightarrow$ Computing $p(z_0)q(z_0), p(z_1)q(z_1), \ldots, p(z_d)q(z_d)$

## Divide and Conquer

$$p(z) = \sum_{i=0}^{d-1} a_i \cdot z^i$$

Choose $\alpha_0, \ldots, \alpha_{d-1}$.

each $p(\alpha_i)$ costs $O(d)$.

total $O(d^2)$.

$$p(z) = \sum_{i=0}^{d/2-1} a_{2i} \cdot z^{2i} + \sum_{i=0}^{d/2-1} a_{2i+1} \cdot z^{2i+1}$$

[Assume $d$ even]

$$= P_e(z^2) + z \cdot P_o(z^2).$$

Then $P_e(\alpha) = P_e(-\alpha)$

$P_o(\alpha) = P_o(-\alpha)$.

Only two recursives calls required to compute $p(\alpha)$ and $p(-\alpha)$.

Evaluate $p(\alpha)$ at $\begin{matrix} \alpha_0, & \alpha_1, & \ldots & \alpha_{d/2-1} \\ -\alpha_0 & -\alpha_1 & & -\alpha_{d/2-1} \end{matrix}$ > $d$ points

$\leq$ Evaluate $P_e, P_o$ at $\alpha_0^2, \alpha_1^2, \ldots \alpha_{d/2-1}^2$. $d/2$ points

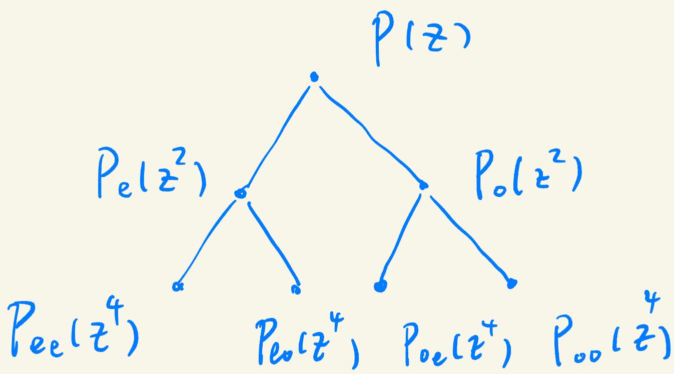
$$T(d) = 2T(d/2) + O(d) = O(d \log d).$$

How to apply this recursively?

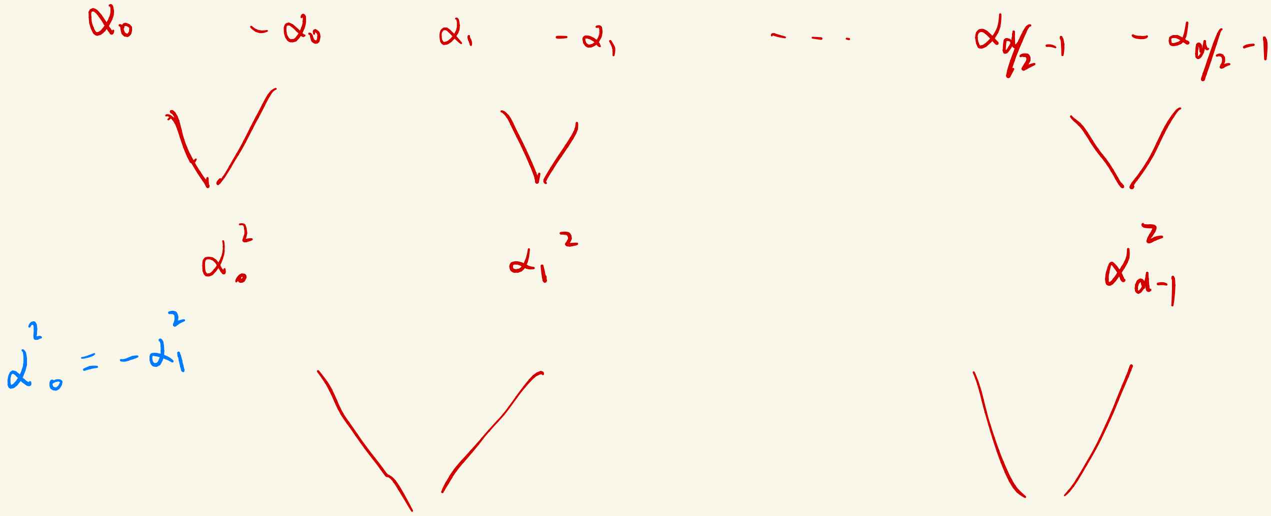
In $P_e(z^2)$, there are only even terms.

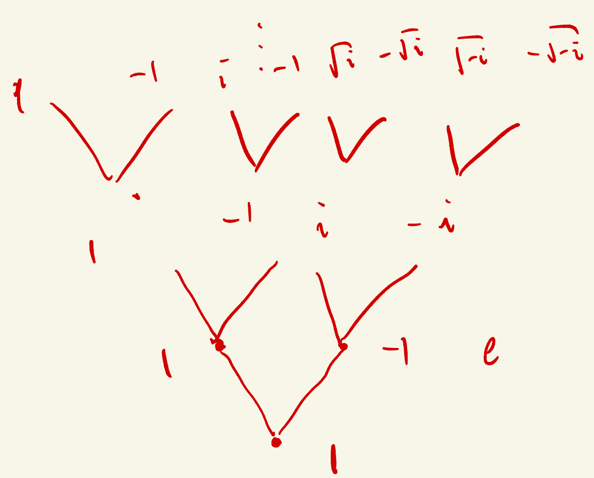
$$P_e(z^2) = \sum_{i=0}^{d/2-1} b_i \cdot (z^2)^i = \sum_{i=0}^{d/4-1} b_{2i} \cdot (z^2)^{2i} + \sum_{i=0}^{d/4-1} b_{2i+1} (z^2)^{2i+1}$$

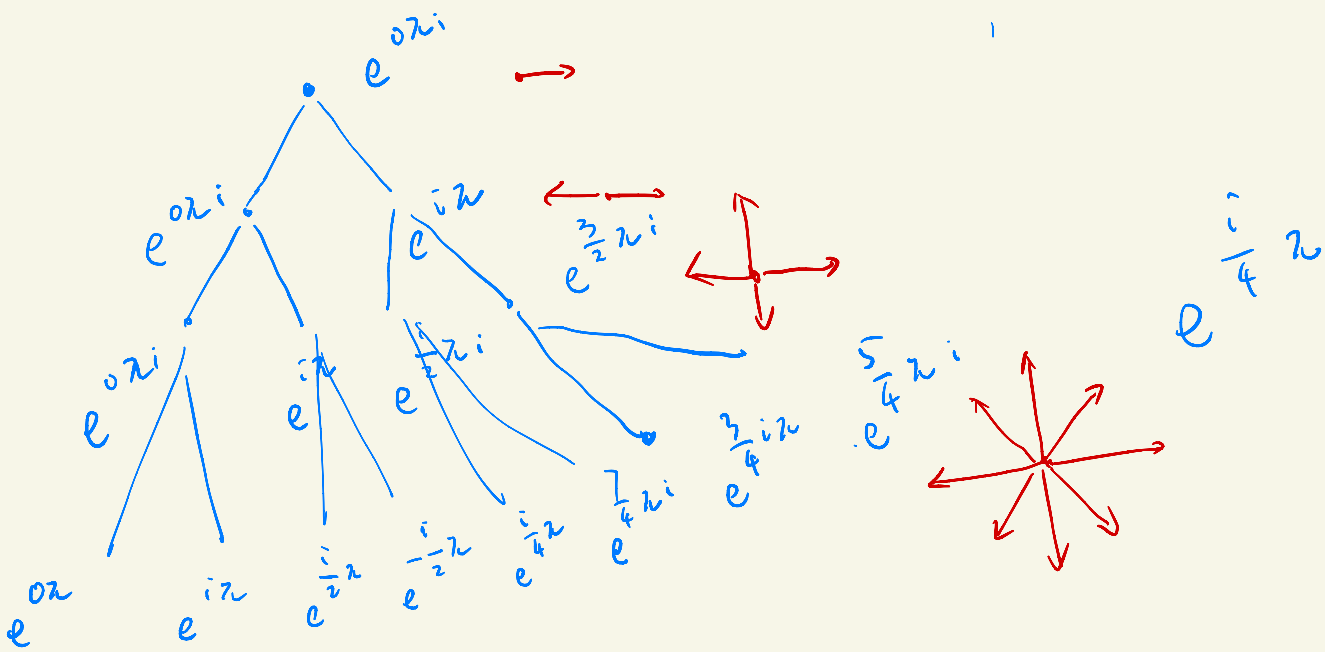
$$= P_{ee}(z^4) + z^2 P_{eo}(z^4)$$




$\sqrt{i}$





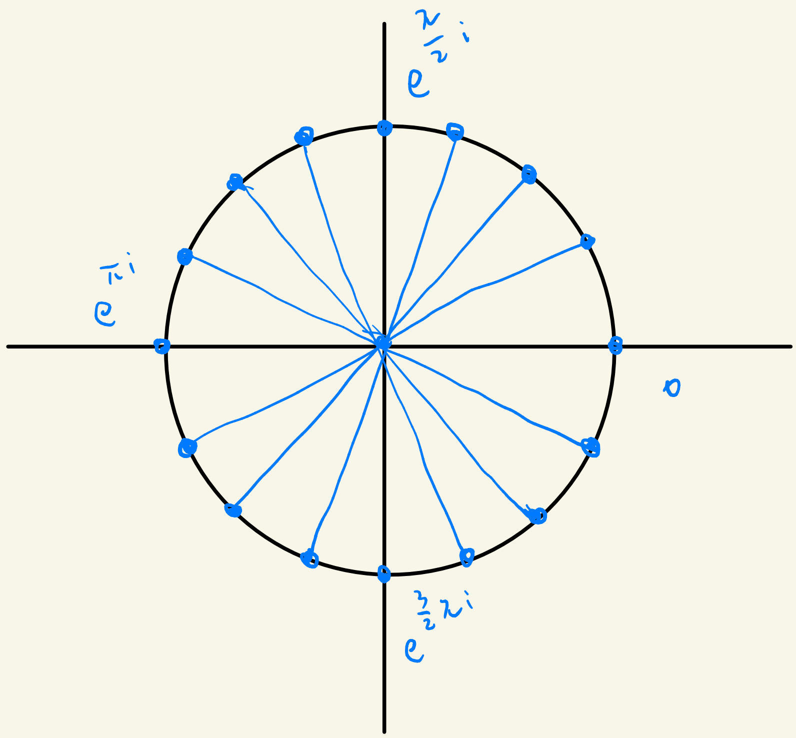

⋮

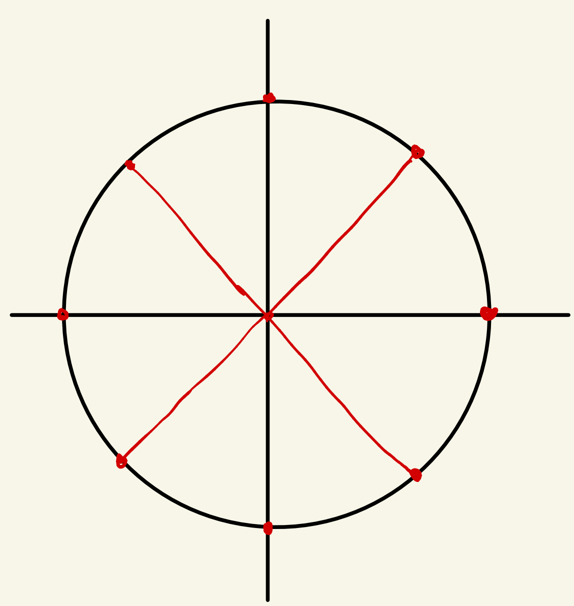
n - th level.

$$w = e^{\frac{2\pi}{n} i}$$

$$\{ w^i \}_{i=0,\dots,2^n-1}$$

$p(x)$. → $p_e(x)$, $p_o(x)$



$w = e^{\frac{2\pi}{n} i}$.

FFT $(P, w)$.

if $w = 1$ return $P(1)$

Compute $P_e$, $P_o$

FFT $(P_e, w^2)$

FFT $(P_o, w^2)$.

for $j = 0 \to d-1$

$$p(w^j) = P_e(w^{2j}) + w^j P_o(w^{2j}).$$

return $p(w^0), p(w^1), \dots p(w^{d-1})$.

Interpolation

$$a_0, \dots a_{d-1} \underset{\text{interpolation}}{\overset{\text{evaluation}}{\rightleftarrows}} p(\alpha_0), \dots p(\alpha_{d-1})$$

The matrix

$$A = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{d-1} \\ \vdots & & \vdots & & \\ 1 & w^j & w^{2j} & \cdots & w^{(n-1)j} \\ \vdots & & & & \\ 1 & w^{(n-1)} & w^{2(n-1)} & \cdots & w^{(n-1)(n-1)} \end{bmatrix} = \left[ c^{(0)}, \dots c^{(n-1)} \right].$$

$$A(i,j) = w^{(i-1)(j-1)}$$

<u>Prop.</u> $A$ is orthogonal.

if. $$\langle c^{(i)}, c^{(j)} \rangle = \sum_{k=0}^{n-1} w^{(i-j)k}$$

$$= \begin{cases} n & \text{if } i = j \\ \dfrac{1 - w^{(i-j)d}}{1 - w^{i-j}} = 0 & \text{if } i \neq j. \end{cases}$$

Therefor $\frac{1}{n} A$ is orthonormal

$$A^{-1} = \frac{1}{n} A^{*}. \qquad A^{*}(i,j) = \overline{A(j,i)}$$

$$= w^{-(i-1)(j-1)}$$

$$= A(i,j)^{-1}.$$

Evaluation

Compute multiplication in nlogn.

$$\begin{bmatrix} p(w^0) \\ p(w^1) \\ \vdots \\ p(w^{d-1}) \end{bmatrix} = A \begin{bmatrix} a_0 \\ \vdots \\ a_d \end{bmatrix}$$

for $w$.

Interpolation. $A^{-1}$. for $w^{-1}$.

FFT $(p(w), w^{-1})$.

---

<u>Graphs</u>.

Representation

DFS.

SCC.