Linear Transformations

$M \in R^{n \times n}$
$\uparrow$ Ring
(Simply, a domain with $+, \times, 0, 1$)

Given $\vec{a} \in R^n$, what is the complexity of computing $M \cdot \vec{a}$?

$$\vec{a} \longrightarrow \vec{b} = M \cdot \vec{a}$$

$(a_0, a_1, \ldots, a_{n-1}) \quad (b_0, b_1, \ldots, b_{n-1})$

$\underline{O(n^2)}$

$$\underbrace{b_i = \sum_{j=0}^{n-1} M_{i,j} \cdot a_j}$$

$M_{i,j} = \omega^{ij}$ ← n^{th} primitive root of unity.

$i \in [0, n-1]$
$j \in [0, n-1]$

↳ $\omega^n = 1$ but for all $k \in [1, n-1]$ $\omega^k \neq 1$.

$x^n = 1$

Solutions to $x^n = 1$ are n^{th} roots of unity.

$$\begin{array}{c|c}
 & \begin{matrix} 0 & & & & & n-1 \end{matrix} \\
\begin{matrix} 0 \\ \\ \\ \\ \\ n-1 \end{matrix} & \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & & & & & \\ 1 & & & \omega^{ij} & & \\ 1 & & & & & \\ 1 & & & & & \end{bmatrix}
\end{array}$$

$d = n-1$

$\alpha_i = \omega^i$
$i \in [0, n-1]$

Ex: Compute primitive 3rd root of unity.

$$\boxed{\text{Given a univariate polynomial's eval at } d+1 \text{ points, they strictly determine the poly.}}$$

$$\begin{bmatrix} \alpha_1^0 & \alpha_1 & \cdots & \alpha_1^d \\ \alpha_2^0 & \alpha_2 & \cdots & \alpha_2^d \\ & & & \\ \alpha_{d+1}^0 & \alpha_{d+1} & \cdots & \alpha_{d+1}^d \end{bmatrix} \begin{bmatrix} a_0 \\ \vdots \\ a_d \end{bmatrix} = \begin{bmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \vdots \\ f(\alpha_{d+1}) \end{bmatrix}$$

(Vandermonde matrices.

Ex: Show that Vandermonde matrices are full rank

$f(z) = a_0 + a_1 z + \cdots + a_d z^d$

$\underbrace{f(\alpha_1), \ldots, f(\alpha_{d+1})}$ ↳ $\sum_{i=0}^{d} a_i \cdot (\alpha_j)^i = f(\alpha_j) \quad \forall j \in [1, d+1]$

$$(M^{-1})_{i,j} = \frac{\omega^{-i \cdot j}}{n} = \frac{\omega^{n - i \cdot j}}{n}$$

Rephrase: We want to understand the complexity of a linear transform whose entries are $\{w^{ij}\}_{i,j\in[0,n-1]}$

$(a_0,\cdots,a_{n-1})$

$$f(z)=a_0+a_1\underline{\underline{z}}+\cdots+a_{n-1}z^{n-1}.\Big\}\to\underbrace{\sum_{i=0}^{n-1}a_i\cdot(w^j)^i=f(w^j)}_{\forall j\in[0,n-1]}$$

Suppose $a_0,\cdots,a_{n-1}$ are known.

then $\underbrace{M\cdot\vec{a}}$ is giving us $f(w^0),f(w^1),\ldots,f(w^{n-1})$.

$$\boxed{\vec{b}=M\cdot\vec{a}}$$

$$\left[\;w^{ij}\;\right]\begin{bmatrix}a_0\\ \vdots\\ a_{n-1}\end{bmatrix}=\begin{bmatrix}\cancel{f(w^0)}\;b_0\\ \vdots\\ \cancel{f(w^{n-1})}\;b_{n-1}\end{bmatrix}$$

$$f(z)=f_0(z)+z^{n/2}\cdot f_1(z)\cdot\Big\}$$

$$b_i=\sum_{j=0}^{n-1}(w^{ij})\cdot a_j=\sum_{j=0}^{n/2-1}(w^i)^j\cdot a_j+\sum_{j=\frac{n}{2}}^{n-1}(w^i)^j\cdot a_j$$

Need primitive $\frac{n}{2}$th root of unity.

$$=\sum_{j=0}^{n/2-1}(w^i)^j\cdot a_j+(w^i)^{n/2}\cdot\sum_{j'=0}^{n/2-1}(w^i)^{j'}\cdot \underbrace{a_{j'+\frac{n}{2}}}_{j'+\frac{n}{2}=j}$$

Claim: w^2

If w is primitive nth root of unity $\Big\}\Rightarrow$ w^2 is $\frac{n}{2}$th primitive root.

$$(w^2)^k\neq 1\quad\forall\ k\in[1,\tfrac{n}{2}-1]$$

$$b_i=\sum_{j=0}^{n/2-1}(w^i)^j\cdot a_j+(w^i)^{\frac{n}{2}}\sum_{j'=0}^{n/2-1}(w^i)^{j'}\cdot a_{j'+\frac{n}{2}}\quad\Bigg|\quad\forall\ i\in[0,n-1]$$

$\underline{i=2p}\Big\}$ $i\in[0,n-1]\to 2p=n-2\Rightarrow p\leq\frac{n}{2}-1$

$$b_{i=2p}=\sum_{j=0}^{n/2-1}(w^2)^{p\cdot j}\cdot a_j+\underbrace{(w^{2p})^{\frac{n}{2}}}\cdot\sum_{j'=0}^{n/2-1}(w^2)^{p\cdot j'}\cdot a_{j'+\frac{n}{2}}.$$

$$= \sum_{j=0}^{n/2-1} (w^2)^{p \cdot j} \left[a_j + a_{j+\frac{n}{2}} \right] \longrightarrow \begin{array}{cc} & \downarrow j \\ p \to & \left[(w^2)^{pj} \right] \end{array} \begin{bmatrix} a_0 + a_{\frac{n}{2}} \\ a_1 + a_{\frac{n}{2}+1} \\ \vdots \\ a_{\frac{n}{2}-1} + a_{n-1} \end{bmatrix},$$

$i = 2q+1$

$$b_{2q+1} = \left(\sum_{j=0}^{n/2-1} \underbrace{(w^2)^{p \cdot j}}_{} \cdot a_j \; w^j \right) + w^{(2p+1)\frac{n}{2}} \cdot \sum_{j'=0}^{n/2-1} \left((w^2)^{p \cdot j'} \cdot a_{j'+\frac{n}{2}} \cdot w^{j'} \right)$$

$$(w^{2p+1})^j = (w^{2p})^j \cdot w^j$$

$$w^{\cancel{2}p \cdot \frac{n}{\cancel{2}}} \cdot w^{\frac{n}{2}} = (w^n)^p \, \underbrace{w^{n/2}}_{\to -1}$$

$$= \sum_{j=0}^{n/2-1} (w^2)^{p \cdot j} \cdot \left[a_j - a_{j+\frac{n}{2}} \right] \cdot w^j$$

$$\begin{bmatrix} b_0 \\ \\ \\ b_{n-1} \end{bmatrix}$$

even i's $\to$ Linear transformation of size $\frac{n}{2}$ of vector $\left(a_0 + a_{\frac{n}{2}},\ a_1 + a_{\frac{n}{2}+1},\ \dots,\ a_{\frac{n}{2}-1} + a_{n-1} \right)$

odd i's $\to$ Linear transformation of size $\frac{n}{2}$ of $\left((a_0 - a_{\frac{n}{2}}) \cdot w^0,\ (a_1 - a_{\frac{n}{2}+1}) \cdot w,\ \dots,\ (a_{\frac{n}{2}-1} - a_{n-1}) w^{\frac{n}{2}-1} \right)$

$$\begin{array}{cc} & \downarrow j \\ p \to & \left[(w^2)^{pj} \right] \end{array} \begin{bmatrix} a_0 + a_{\frac{n}{2}} \\ a_1 + a_{\frac{n}{2}+1} \\ \vdots \\ a_{\frac{n}{2}-1} + a_{n-1} \end{bmatrix} \qquad \begin{array}{cc} & \downarrow j \\ p \to & \left[(w^2)^{pj} \right] \end{array} \begin{bmatrix} (a_0 - a_{\frac{n}{2}}) \cdot 1 \\ (a_1 - a_{\frac{n}{2}+1}) w \\ \vdots \\ (a_{\frac{n}{2}-1} - a_{n-1}) w^{\frac{n}{2}-1} \end{bmatrix}$$

even $\qquad\qquad$ Odd

$$\left[w^{ij} \right] \begin{bmatrix} a_0 \\ a_{n-1} \end{bmatrix}$$

$$T(n) = 2 \cdot T\left(\tfrac{n}{2}\right) + O(n)$$

$$= O(n \log n).$$

"Discrete Fourier Transform" (DFT)

$\hookrightarrow \left[w^{ij} \right] \cdot \begin{bmatrix} a_0 \\ a_{n-1} \end{bmatrix}$

# of arithmetic operation.

Modular arithmetic

n = prime

"Fast Fourier Transform" (FFT)

$\hookrightarrow$ Divide and Conquer algo for DFT

$\hookrightarrow$ Inverse Discrete Fourier Transform

$$\left[\frac{w^{n-i \cdot j}}{n} \right] \begin{bmatrix} a_0 \\ a_{n-1} \end{bmatrix}$$

Ex: Work this out and obtain smaller instances.

$$\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \underset{\xleftarrow{\text{inv. DFT}}}{\xrightarrow{\text{DFT}}} \begin{bmatrix} f(w^0) \\ \vdots \\ f(w^{n-1}) \end{bmatrix}$$

Coefficient space

Evaluation space.

{Reed Solomon codes