FFT

We want efficient algoriths for these
Polynomial Operations (Multiplication, Addition, Evaluation)

Some reperesentations

$$2 + 3x + x^2 \rightarrow A = [2, 3, 1]$$

(-1,0),(0,2),(1,6)

Fact: A polynomial of degree d can be uniquely represented by its values in any $d+1$ points. (**at least** $d+1$)

Algorithms vs.	Representations		
	Coefficients	Roots	Samples
Evaluation	$O(n)$	$O(n)$	$O(n^2)$
Addition	$O(n)$	∞	$O(n)$
Multiplication	$O(n^2)$	$O(n)$	$O(n)$

So we want $Coef \to Value$ representation
Multiply
and then $Value \to Coef$.

NAINE APPROACH

$$\{(x_0, P(x_0)), (x_1, P(x_1)), \ldots, (x_d, P(x_d))\}$$

$$P(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_d x^d$$

$$\begin{aligned}
P(x_0) &= p_0 + p_1 x_0 + p_2 x_0^2 + \cdots + p_d x_0^d \\
P(x_1) &= p_0 + p_1 x_1 + p_2 x_1^2 + \cdots + p_d x_1^d \\
&\vdots \\
P(x_d) &= p_0 + p_1 x_d + p_2 x_d^2 + \cdots + p_d x_d^d
\end{aligned}$$

$$\begin{bmatrix} P(x_0) \\ P(x_1) \\ \vdots \\ P(x_d) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^d \\ 1 & x_1 & x_1^2 & \cdots & x_1^d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_d & x_d^2 & \cdots & x_d^d \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_d \end{bmatrix}$$

To find the values in $d+1$ point computation is $O(d^2)$

$$\begin{bmatrix} P(x_0) \\ P(x_1) \\ \vdots \\ P(x_d) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^d \\ 1 & x_1 & x_1^2 & \cdots & x_1^d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_d & x_d^2 & \cdots & x_d^d \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_d \end{bmatrix}$$

To find the values in $d+1$ point computation is $O(d^2)$

A nudge towards the Solution

What will happen when I compute $A(x_0)$ and $A(-x_0)$???

$$3 + 4x + 6x^2 + 2x^3 + x^4 + 10x^5 \;=\; (3 + 6x^2 + x^4) + x(4 + 2x^2 + 10x^4).$$

A nudge towards the Solution

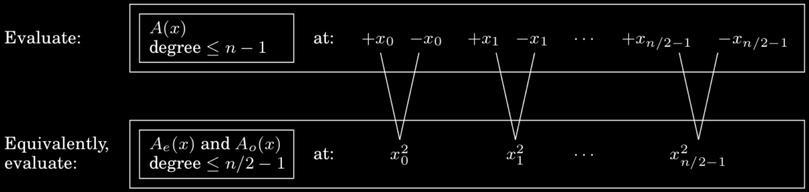
What will happen when I compute $P(x_0)$ and $P(-x_0)$???

$$3 + 4x + 6x^2 + 2x^3 + x^4 + 10x^5 \;=\; (3 + 6x^2 + x^4) + x(4 + 2x^2 + 10x^4).$$

$$P(x_i) = P_e(x_i^2) + x_i P_o(x_i^2)$$
$$P(-x_i) = P_e(x_i^2) - x_i P_o(x_i^2)$$

Evaluate only at squares of the original points $(n/2)$.

The degree of P_e and P_o also drops to half!!



Evaluate $P(x) : [p_0, p_1, \ldots, p_{n-1}]$ $[\pm x_1, \pm x_2, \ldots, \pm x_{n/2}]$

$$P(x) = P_e(x^2) + xP_o(x^2)$$

Evaluate $P_e(x^2) : [p_0, p_2, \ldots, p_{n-2}]$ $[x_1^2, x_2^2, \ldots, x_{n/2}^2]$

$[P_e(x_1^2), P_e(x_2^2), \ldots, P_e(x_{n/2}^2)]$

Evaluate $P_o(x^2) : [p_1, p_3, \ldots, p_{n-1}]$ $[x_1^2, x_2^2, \ldots, x_{n/2}^2]$

$[P_o(x_1^2), P_o(x_2^2), \ldots, P_o(x_{n/2}^2)]$

$$P(x_i) = P_e(x_i^2) + x_i P_o(x_i^2)$$
$$P(-x_i) = P_e(x_i^2) - x_i P_o(x_i^2)$$
$$i = \{1, 2, \ldots, n/2\}$$

It would be of a good complexity if there was no problem

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

X the set of all points stops geting halfed after step 1.

Solution: nth Roots of unity $z^n = 1$

Example 4th roots: $\{$1, -1, i, -i$\}$
Example 2nd roots: $\{$1, -1$\}$
Example 1st root: $\{$1$\}$

Expand the domain of the polynomials to $\mathbb{C}$ and everything still holds. With the help of some equations we denote the nth- roots by the complex numbers $1, \omega, \omega^2, \cdots, \omega^{n-1}$ where $\omega = e^{i2\pi/n}$. And pick $n = 2^l$.

Expand the domain of the polynomials to $\mathbb{C}$ and everything still holds. With the help of some equations we denote the nth- roots by the complex numbers $1, \omega, \omega^2, \cdots, \omega^{n-1}$ where $\omega = e^{i2\pi/n}$. And pick $n = 2^l$ for convinience.

$$\begin{bmatrix} P(x_0) \\ P(x_1) \\ P(x_2) \\ \vdots \\ P(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ \vdots \\ p_{n-1} \end{bmatrix}$$

$$\begin{bmatrix} P(\omega^0) \\ P(\omega^1) \\ P(\omega^2) \\ \vdots \\ P(\omega^{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ \vdots \\ p_{n-1} \end{bmatrix}$$

So in cases where V is as follows we have the FFT.

IFFT

Now given the values of a polynomial computed in the roots of unity how to go back to the coef representation ?

We solved $V * C_{oef} = Y$ now to solve $C_{oef} = V^{-1} * Y$. How V^{-1} looks like?

IFFT

$$x_k = \omega^k \text{ where } \omega = e^{\frac{2\pi i}{n}}$$

$$\begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ \vdots \\ p_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix}^{-1} \begin{bmatrix} P(\omega^0) \\ P(\omega^1) \\ P(\omega^2) \\ \vdots \\ P(\omega^{n-1}) \end{bmatrix}$$

$$\Downarrow$$

$$\begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ \vdots \\ p_{n-1} \end{bmatrix} = \frac{1}{n} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \cdots & \omega^{-(n-1)} \\ 1 & \omega^{-2} & \omega^{-4} & \cdots & \omega^{-2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \omega^{-2(n-1)} & \cdots & \omega^{-(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} P(\omega^0) \\ P(\omega^1) \\ P(\omega^2) \\ \vdots \\ P(\omega^{n-1}) \end{bmatrix}$$

IFFT

So if $V^{-1} = \frac{1}{n}\bar{V}$ we have that the the conjugates of the roots of unity ara also roots of unity of we can apply the FFT with $\omega = \omega^{-1}$ and then divide the resulting array by $1/n$.

Proof. We claim that $P = V \cdot \bar{V} = nI$:

$$\begin{aligned} p_{jk} &= (\text{row } j \text{ of } V) \cdot (\text{col. } k \text{ of } \bar{V}) \\ &= \sum_{m=0}^{n-1} e^{ij\tau m/n} \overline{e^{ik\tau m/n}} \\ &= \sum_{m=0}^{n-1} e^{ij\tau m/n} e^{-ik\tau m/n} \\ &= \sum_{m=0}^{n-1} e^{i(j-k)\tau m/n} \end{aligned}$$

Now if $j = k$, $p_{jk} = \sum_{m=0}^{n-1} = n$. Otherwise it forms a geometric series.

$$\begin{aligned} p_{jk} = &= \sum_{m=0}^{n-1} (e^{i(j-k)\tau/n})^m \\ &= \frac{(e^{i\tau(j-k)/n})^n - 1}{e^{i\tau(j-k)/n} - 1} \\ &= 0 \end{aligned}$$