473 L9 9/21/21

FFT Fast Fourier transform

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

$p(x)q(x) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j x^{i+j}$ — n^2 terms, $O(n^2)$

pq degree $2n-2$

convolution algorithm

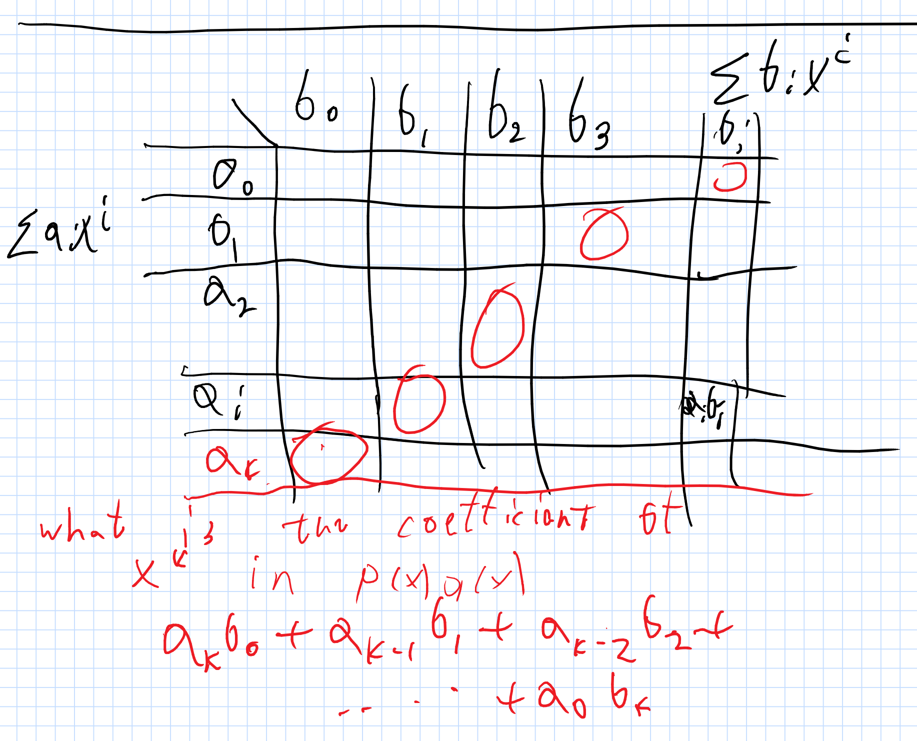
$u, v \in \mathbb{R}^n$

$\langle u, v\rangle = \sum u_i v_i$

$u \oplus i$ = shift u by i locations

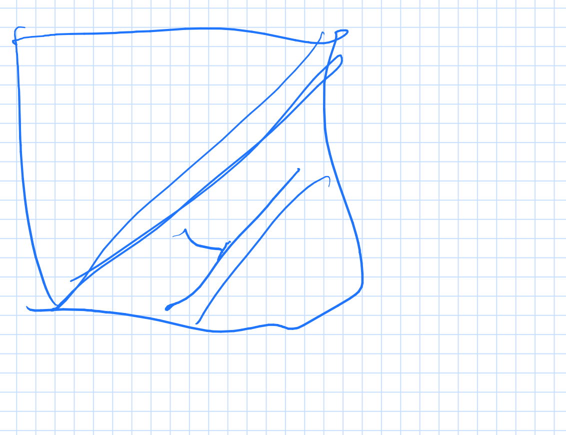
$\langle u \oplus i, v\rangle$ $i = 1, \dots, n$

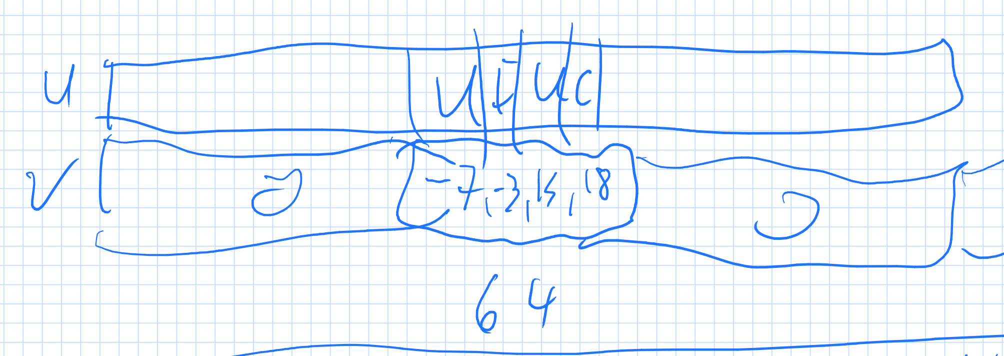
$\sum b_i x^i$, $\sum a_i x^i$



what is the coefficient of x^k in $p(x)q(x)$

$a_k b_0 + a_{k-1} b_1 + a_{k-2} b_2 + \dots + a_0 b_k$



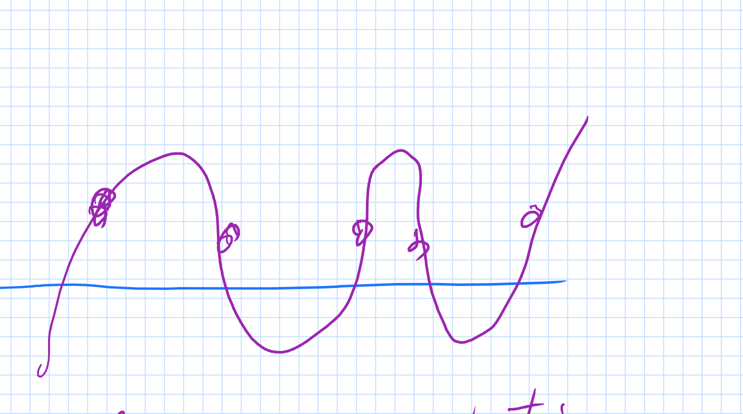


string

64

p polynomial of degree k (highest x^k)

If it is zero on $k+2$ different values $\Rightarrow p$ is the zero polynomial.



k $k+1$

point-value representation

$\{(x_1,y_1),(x_2,y_2),\dots,(x_{k+1},y_{k+1})\}$ $k+1$ points

$\Rightarrow$ define unique a polynomial of degree k.

$g(x) = \sum_{i=1}^{k+1} y_i \frac{\prod_{k \ne i}(x - x_k)}{\prod_{k \ne i}(x_i - x_k)}$ $g(x)$ polynomial of degree k

$g(x_i) = y_i \ \forall i$

$p(x) = \sum a_i x^i$

$x_1, x_2, \dots, x_{n+1}$ $(x_i, p(x_i))$ $i = 1, \dots n+1$

$(x_i, p(x_i))$, $(x_i, q(x_i))$ $i = 1 \dots 2n+2$

pq = point-value representation $(x_i, p(x_i) q(x_i))$ $\forall i$

$O(n)$ time

$p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \dots a_{n-1} x^{n-1}$

$s(x) = \sum_{i=0}^{n/2} a_{2i+1} x^{2i+1}$, $t(x) = \sum_{i=0}^{n/2} a_{2i} x^{2i}$

$p(x) = s(x) + t(x)$

$\tilde{s}(y) = \sum_{i=0}^{n/2} a_{2i+1} y^i$, $\tilde{t}(y) = \sum_{i=0}^{n/2} a_{2i} y^i$

$t(x) = \tilde{t}(x^2)$

$s(x) = \tilde{s}(x^2) \cdot x$

$\tilde{s}, \tilde{t}$ at degree $n/2$

$p(x) = \tilde{t}(x^2) + x \cdot \tilde{s}(x^2)$ X: n values

$O(n)$

$X \Rightarrow X^2 = \{x^2 \mid x \in X\}$

$\tilde{s}(X^2)$, $\tilde{t}(X^2)$ $\quad |X^2| = n$

$T(n, n) = O(n) + 2T(\frac{n}{2}, n)$ ($n/2$ = deg, # of values)

$= O(n^2)$

$|X| = n$ $\quad |X^2| = \frac{n}{2}$ $\quad |(X^2)^2| = \frac{n}{2}$

$X = \{-\frac{n}{2}, \frac{n}{2}\}$

$(-a)^2 = a^2$

$|X| = n = 2^l$

$X^{2^i} = \{x^{2^i} \mid x \in X\}$

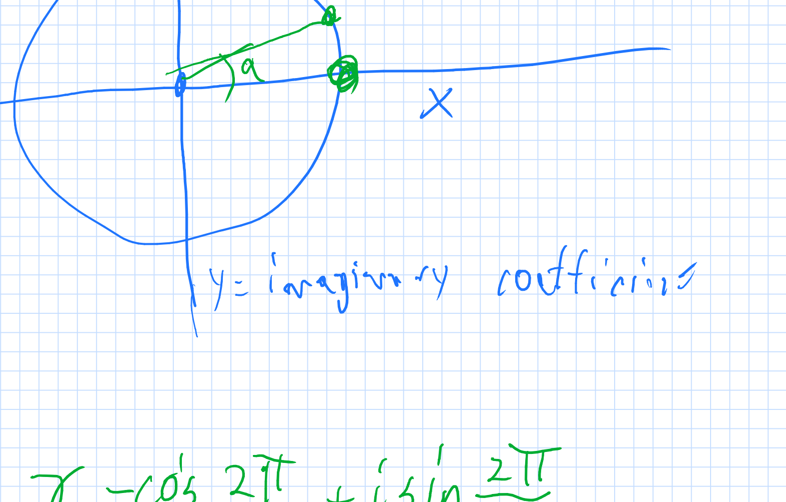
$|X^{2^i}| = \frac{n}{2^i}$ collapsible set

$T(n, n) = O(n) + 2T(\frac{n}{2}, \frac{n}{2})$

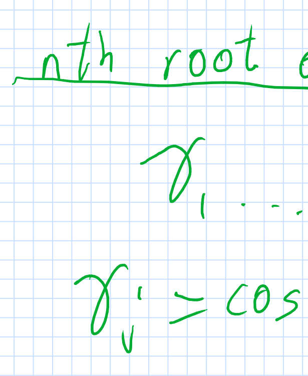
$= O(n \log n)$

n roots of unity

complex number



y: imaginary coefficient



$\gamma_i = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$

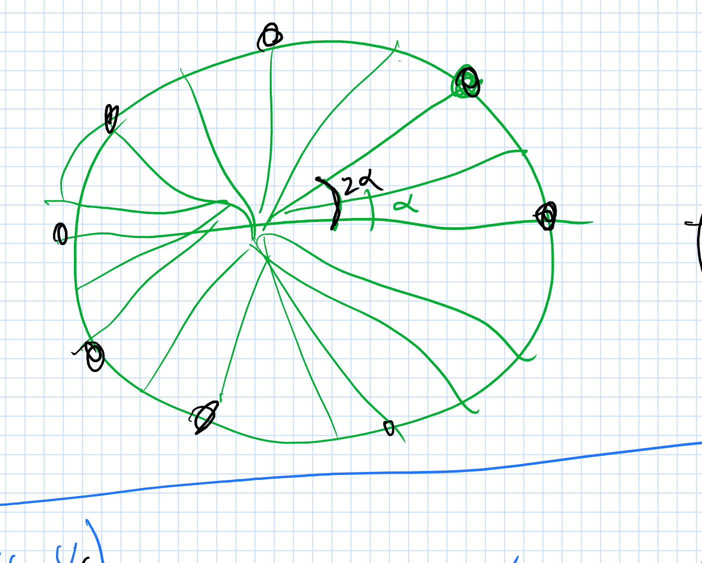
nth root of unity

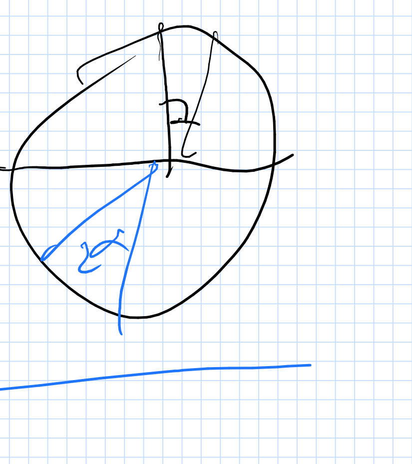
$\gamma_1, \dots, \gamma_j = (\gamma_1)^j$ $j = 0, \dots, n-1$

$\gamma_j = \cos\frac{2\pi}{n} j + i \sin\frac{2\pi}{n} j$

n is power of 2

collapsible set





(γ_i, y_i)

recover standard representation of polynomials

$y_i = p(\gamma_i) = \sum_{t=0}^{n-1} a_t (\gamma_i)^t$ $\forall i$

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & \gamma_1 & \gamma_1^2 & \cdots & \gamma_1^{n-1} \\ 1 & \gamma_2 & \gamma_2^2 & \cdots & \gamma_2^{n-1} \\ 1 & \gamma_3 & \gamma_3^2 & \cdots & \gamma_3^{n-1} \\ & & \vdots & & \\ 1 & \gamma_i & \gamma_i^2 & \cdots & \gamma_i^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

V Vandermonde matrix

$Y = V \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \text{FFT}$

$Y = V \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$

$V^{-1} Y = V^{-1} V \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix}$

$$V^{-1} = \frac{1}{n} \begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n-1} \\ & & \vdots & & \\ 1 & \beta_n & \beta_n^2 & \cdots & \beta_n^{n-1} \end{pmatrix}$$

$\beta_i = \frac{1}{\gamma_i} = \gamma_{-i}$

V_l