1/28/21

FFT 2

$p(x)\ a(x)$ $\le n$

$x_0, x_1, \dots, x_{n-1}$

$(x_i, p(x_i))$, $i = 0, \dots, n-1$

$\times\ (x_i, q(x_i))$

$(x_i, p(x_i)\,q(x_i))$ $O(n\log n)$

collapsible sets

$X \subseteq \mathbb{C}$
$X^{2^i} = |X|/2^i$

n roots of unity

$p(x) = \sum_{i=0}^{n-1} a_i x^i$

$\gamma_0, \gamma_1, \gamma_2, \dots, \gamma_{n-1}$ ~ n roots of unity

$y_i = p(\gamma_i)$

$p(x) = \langle (1, x, x^2, \dots, x^{n-1}), (a_0, a_1, \dots, a_{n-1}) \rangle$
$= \sum_i a_i x^i$

Vandermonde matrix

$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{pmatrix} = \qquad \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix} \sim \begin{pmatrix} p(\gamma_0) \\ \\ \\ \end{pmatrix}$

$\bar{Y}$

(γ_i, y_i)

$\bar{Y} = V \bar{A}$

$\bar{Y} = V \bar{B}$

$\bar{Y} = V \bar{B}$

V^{-1} = inverse of V

$B = V^{-1} \bar{Y}$ $\qquad V^{-1}$ $n \times n$ entries n^2

Lemma

$V^{-1} = \frac{1}{n} \begin{pmatrix} 1 & \beta_0 & \beta_0^2 & \cdots & \beta_0^{n-1} \\ 1 & \beta_1 & \beta_1^2 & & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & & \vdots \\ 1 & \vdots & & & \\ 1 & \beta_{n-1} & & & \beta_{n-1}^{n-1} \end{pmatrix}$

$\begin{pmatrix} 1 & \gamma_0 & \gamma_0^2 & \cdots & \gamma_0^{n-1} \\ 1 & \gamma_1 & \gamma_1^2 & \cdots & \gamma_1^{n-1} \\ 1 & \vdots & & & \\ 1 & \gamma_{n-1} & \gamma_{n-1}^2 & & \gamma_{n-1}^{n-1} \end{pmatrix}$

V

$\beta_i = 1/\gamma_i =$

$\beta_0 = 1$

$\beta_i = \gamma_{n-i}$

$\gamma_1 = \gamma_n = 1$

$\beta_i = \gamma_{n-i} = \gamma_1^{n-i}$

$\times\ \gamma_i = \gamma_1^i = \gamma_i^h$

$= \gamma_1^{n-i+i} = \gamma_1^n = 1.$

Lemma

Recovering the coefficients of the polynomial can be done with FFT + O(n) work.

$V^{-1} V = I$

$\bar{B} = V^{-1} \bar{Y}$

$\frac{1}{n} V \bar{Y}$ $\qquad$ reshuf the entries

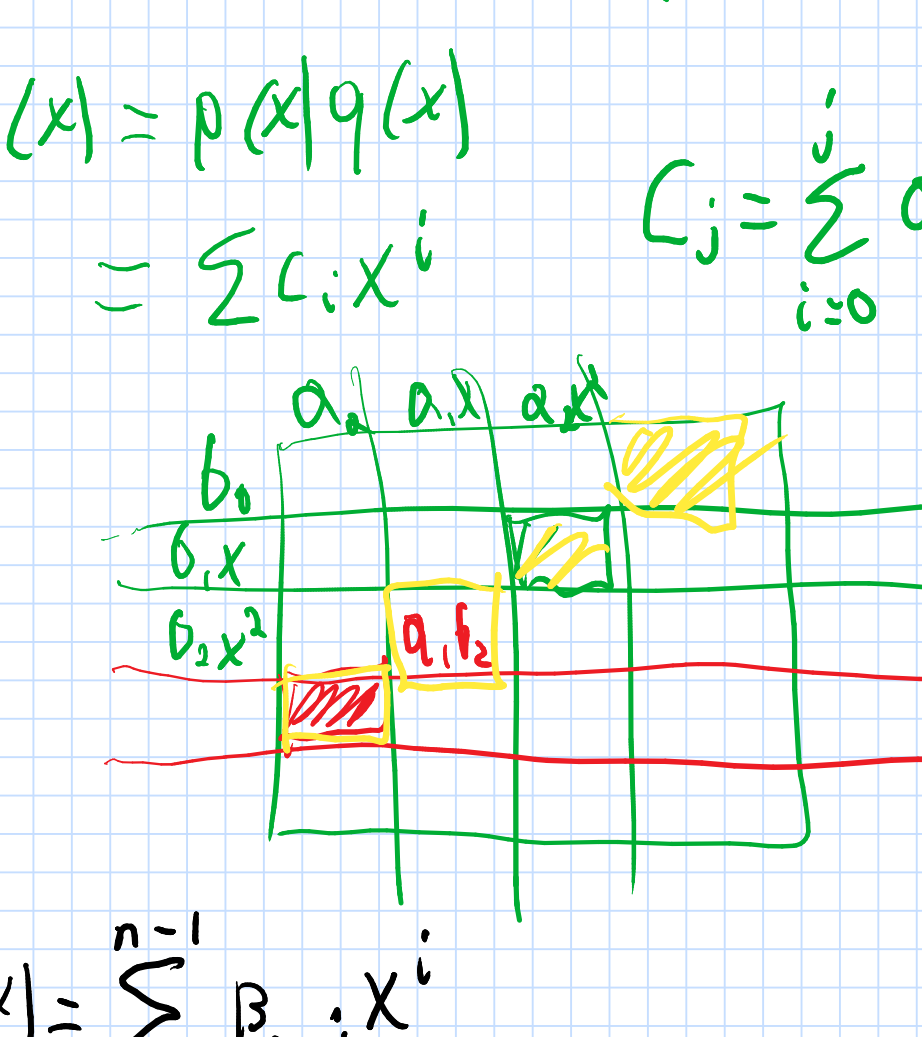
$V\bar{Y}$ $\qquad$ flip the

FFT transform

Convolution

$p(x) = \sum a_i x^i \qquad q(x) = \sum b_i x^i$

$c(x) = p(x)q(x)$
$= \sum c_i x^i \qquad c_j = \sum_{i=0}^{j} a_i b_{j-i}$

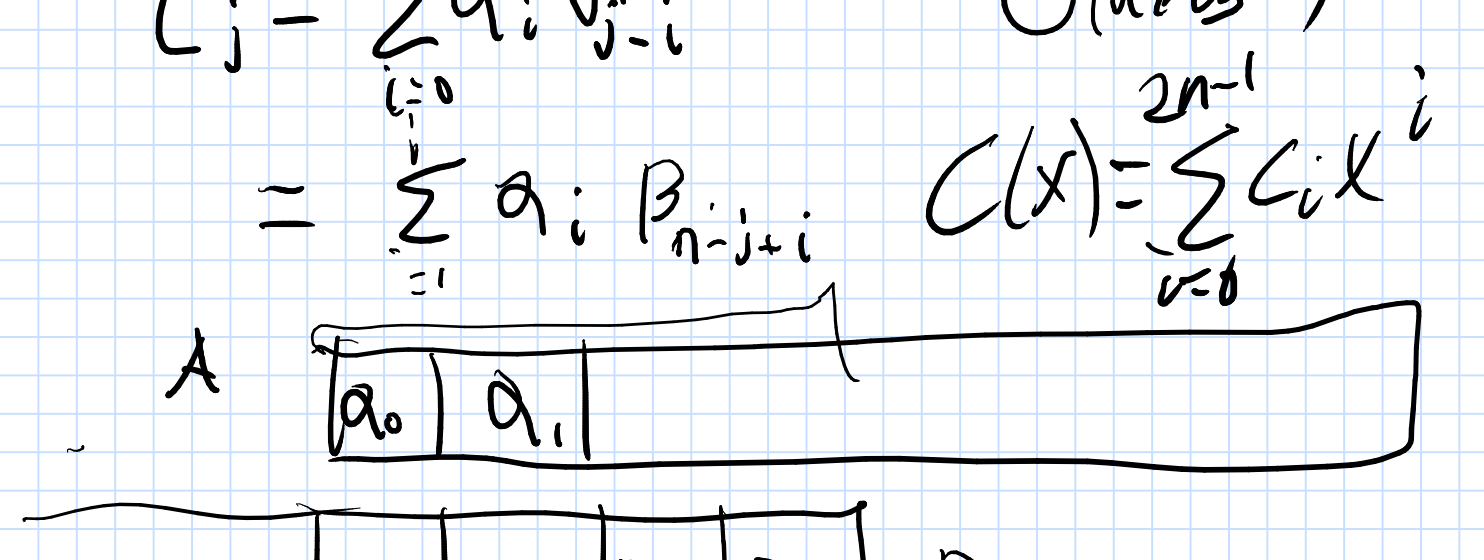


$q(x) = \sum_{i=0}^{n-1} \beta_{n-i} x^i$

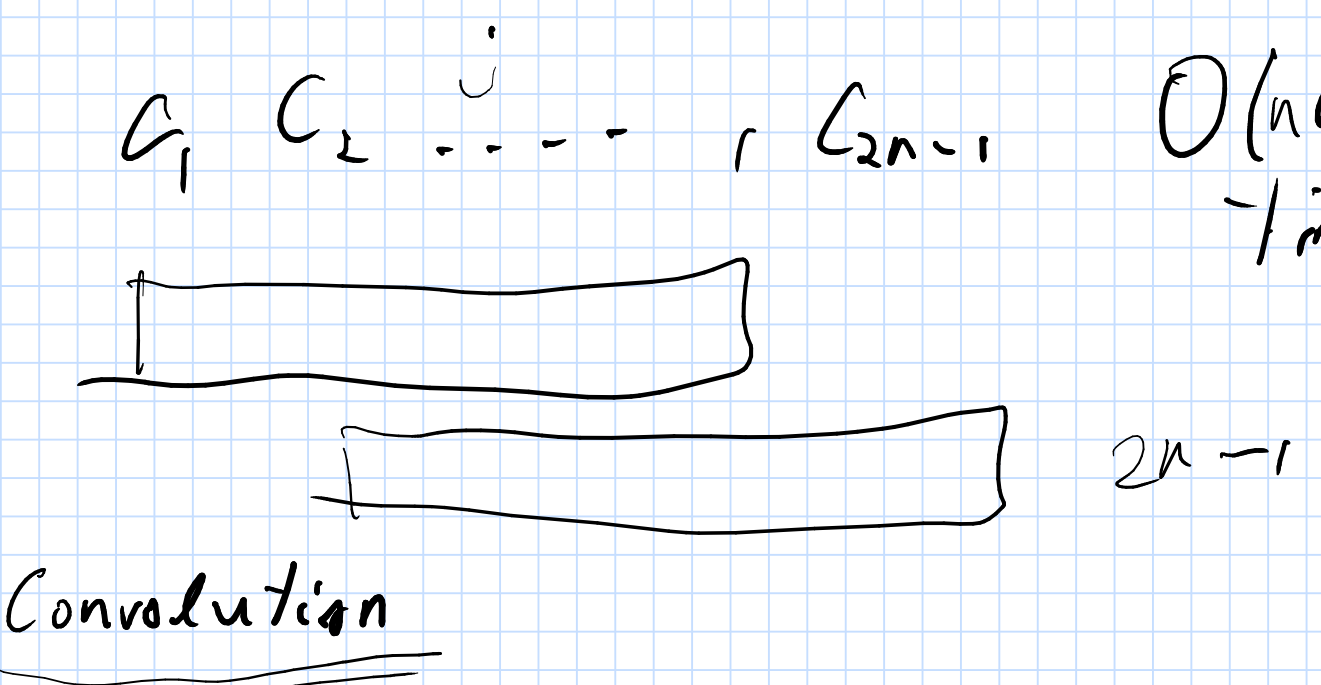
β_{n-j+i}

$c_j = \sum_{i=0}^{j} a_i b_{j-i}$ $\qquad O(n\log n)$

$= \sum_{i=1}^{j} a_i \beta_{n-j+i} \qquad c(x) = \sum_{i=0}^{2n-1} c_i x^i$



$c_1\ c_2\ \dots,\ c_{2n-1}$ $\qquad O(n\log n)$ time

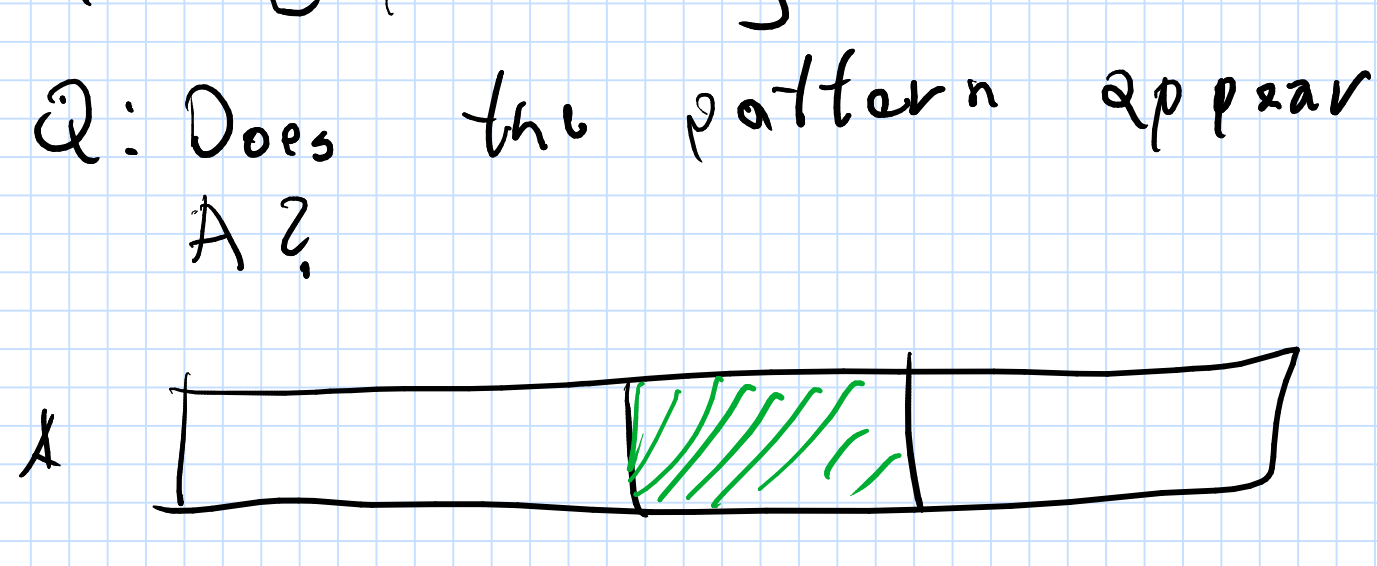


Convolution

$A = [a_1, a_2, \dots, a_n]$

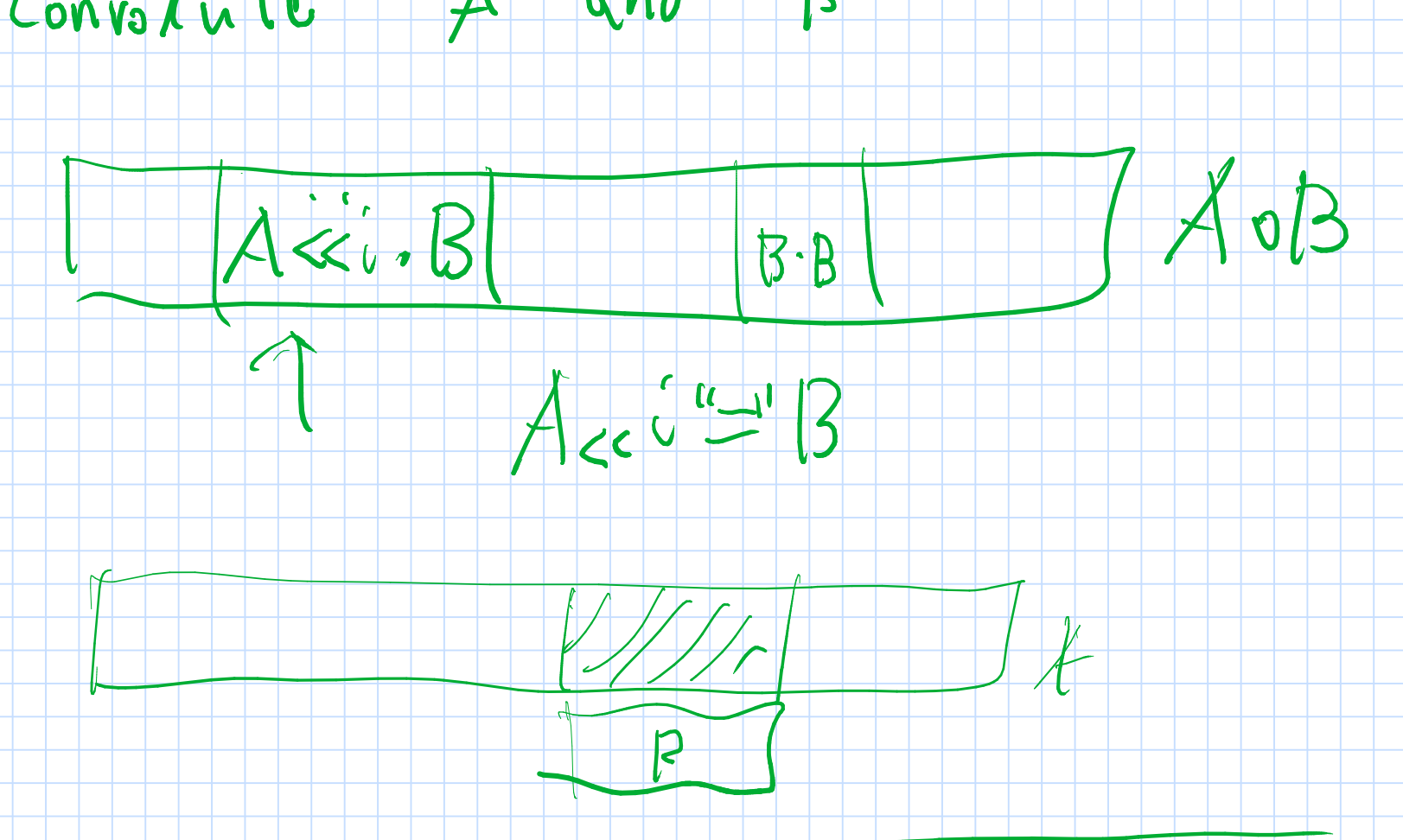
$P = [b_1, b_2, \dots, b_k]$

Q: Does the pattern appear in A?



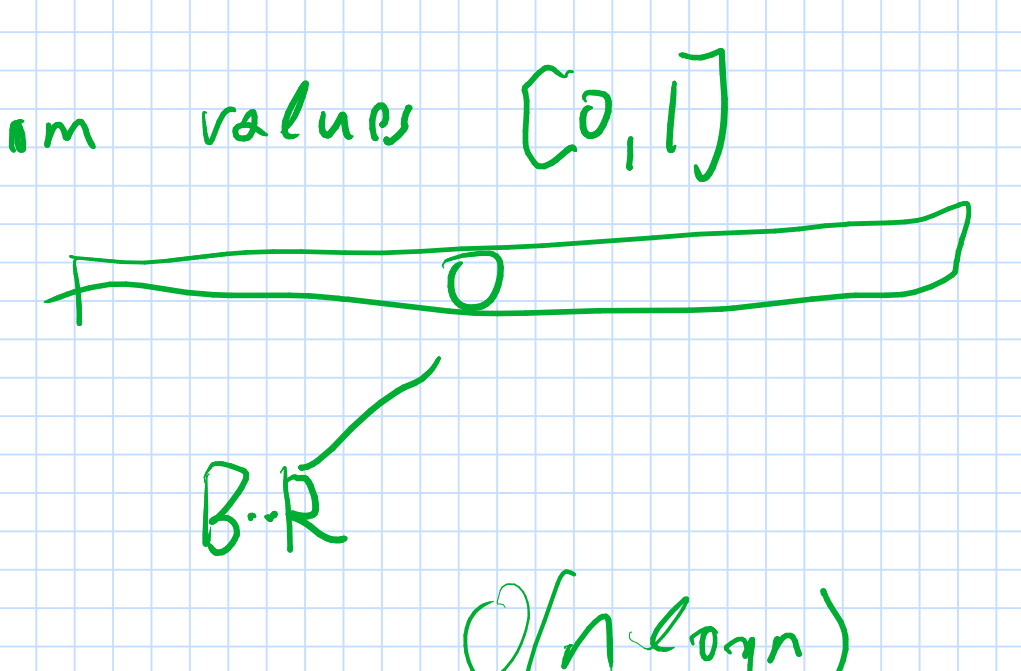
$O(nk)$

– Convolute A and B

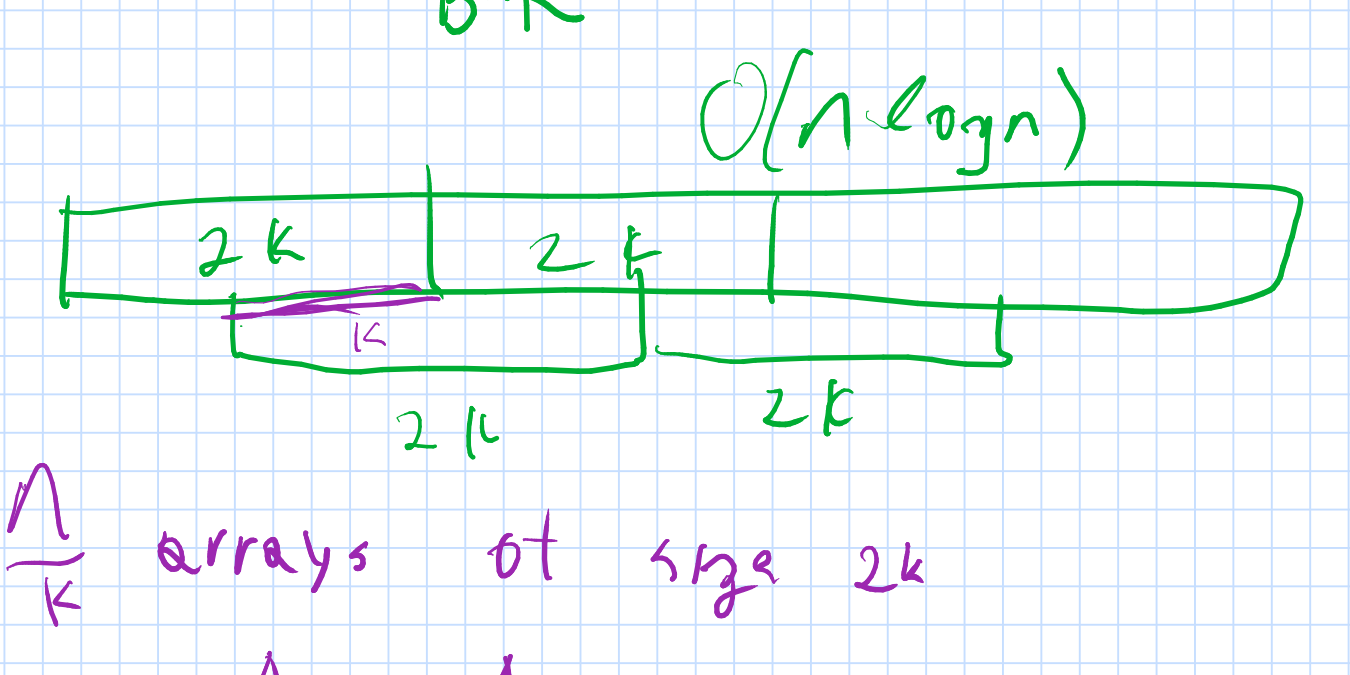


$|R| = |B|$
= random values [0, 1]

$A \circ R$



$O(n\log n)$



$\frac{n}{k}$ arrays of size 2k

$A_1, \dots, A_{\frac{n}{k}}$

$A_i \cdot B \qquad O(k\log k)$

$O\left(\frac{n}{k} k\log k\right) = O(n\log k)$

Schonhage–Strassen algorithm for multiplying large numbers

$b = b_{n-1} b_{n-2} \dots b_0$ $\qquad$ base 2

$c = c_{n-1} c_{n-2} \dots c_0$

$b \cdot c$ $\qquad$ 3500 years multiplication

$x \mid y$
$2x \mid y/2$
$x \mid y-1$

column
x
y is even
y is odd

$O(n)$

$b(x) = \sum_{i=0}^{n-1} b_i x_i$

$b(2)$

$b \cdot c \qquad b(x)\,c(x) = q(x)$
$q(2)$

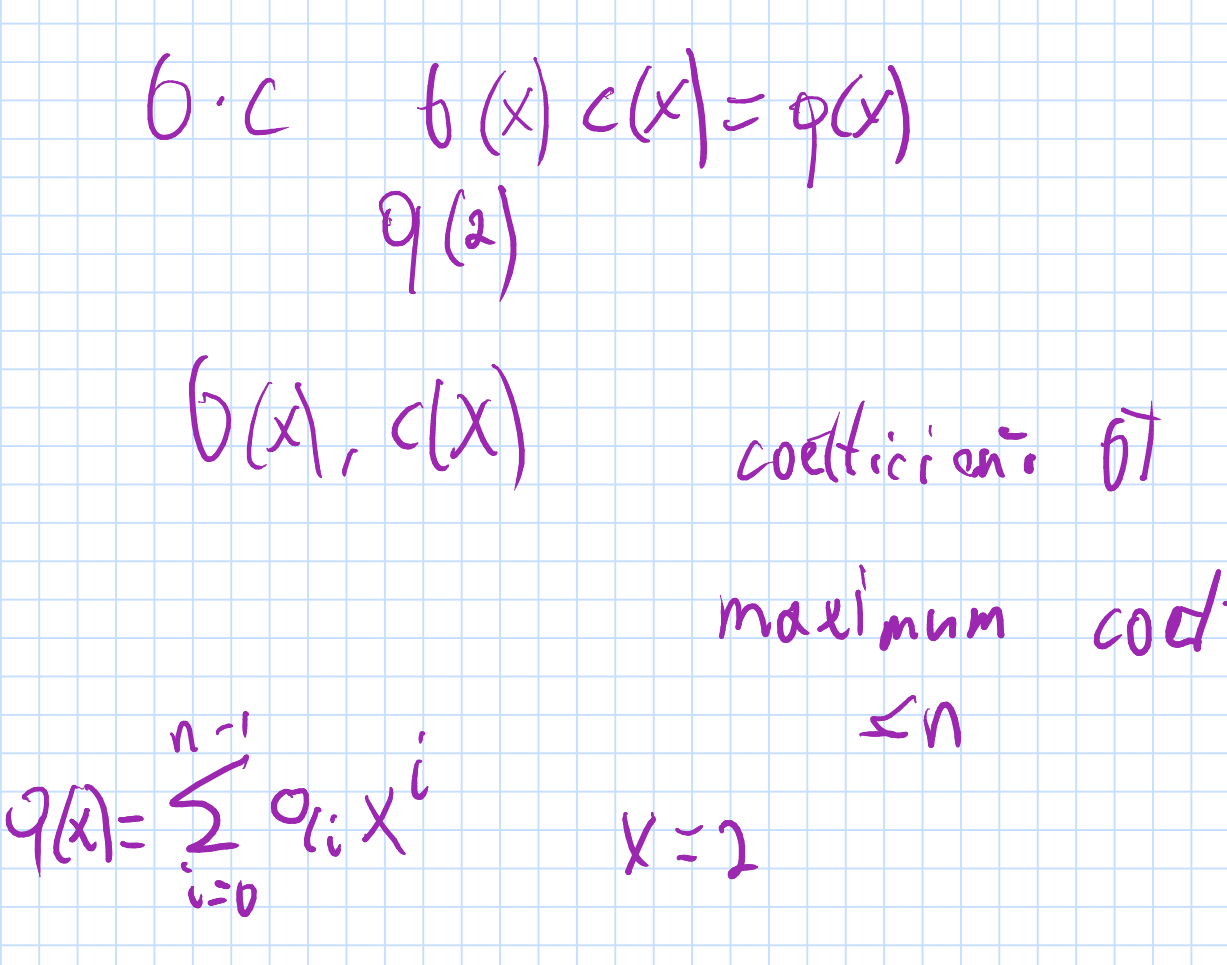
$b(x), c(x)$ $\qquad$ coefficients of q

maximum coeff $\le n$

$q(x) = \sum_{i=0}^{n-1} q_i x^i \qquad x = 2$

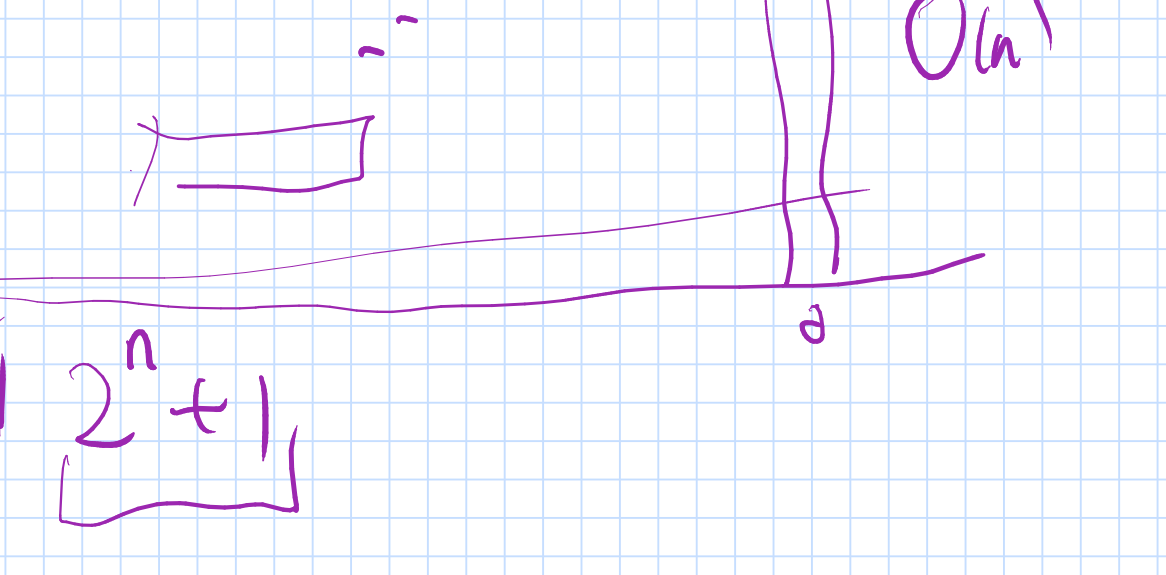
$q(2) = \sum q_i << i$

$O(n\log n)$ time



mod $2^n + 1$

$y = 2^{\sqrt{n}}$



$\sum b_{[i]} y^i$

$\sum c_{[i]} y^i$

$\sqrt{n}$

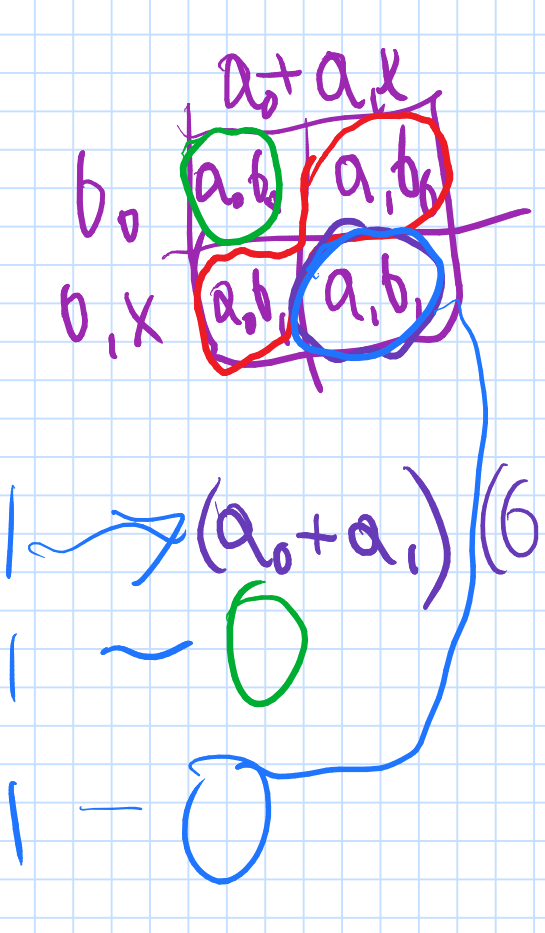
$O(n\log n)$

$O(\sqrt{n}\log n)$

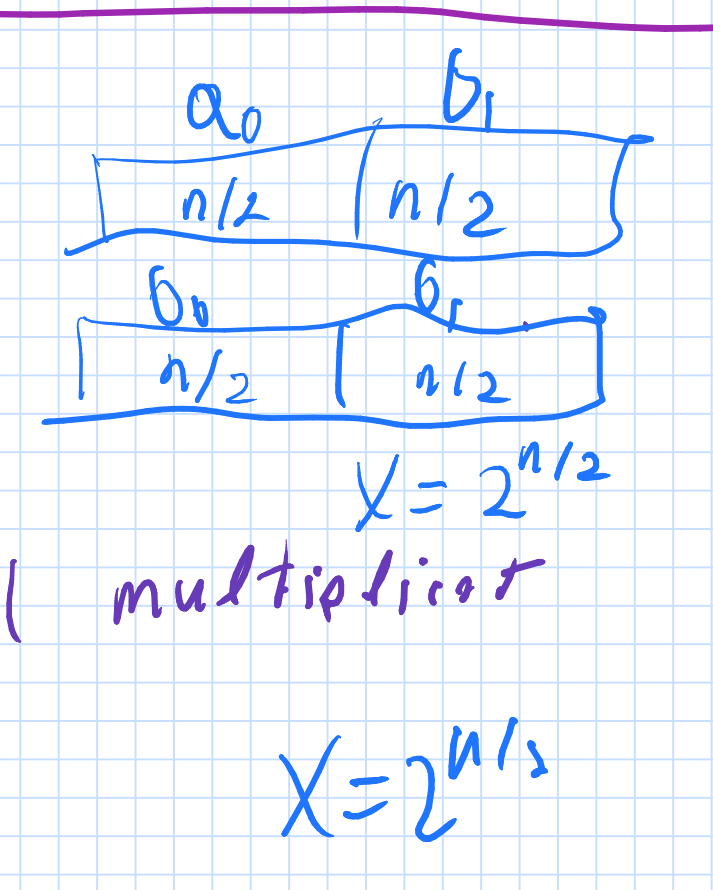
$T(n) = O(n\log n) + \sqrt{n}\log n \cdot T(\sqrt{n})$

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

Karatsuba n^{3}



4



$x = 2^{n/2}$

$1 \to (a_0 + a_1)(b_0 + b_1) = 1$ multiplication

$1 \sim O$

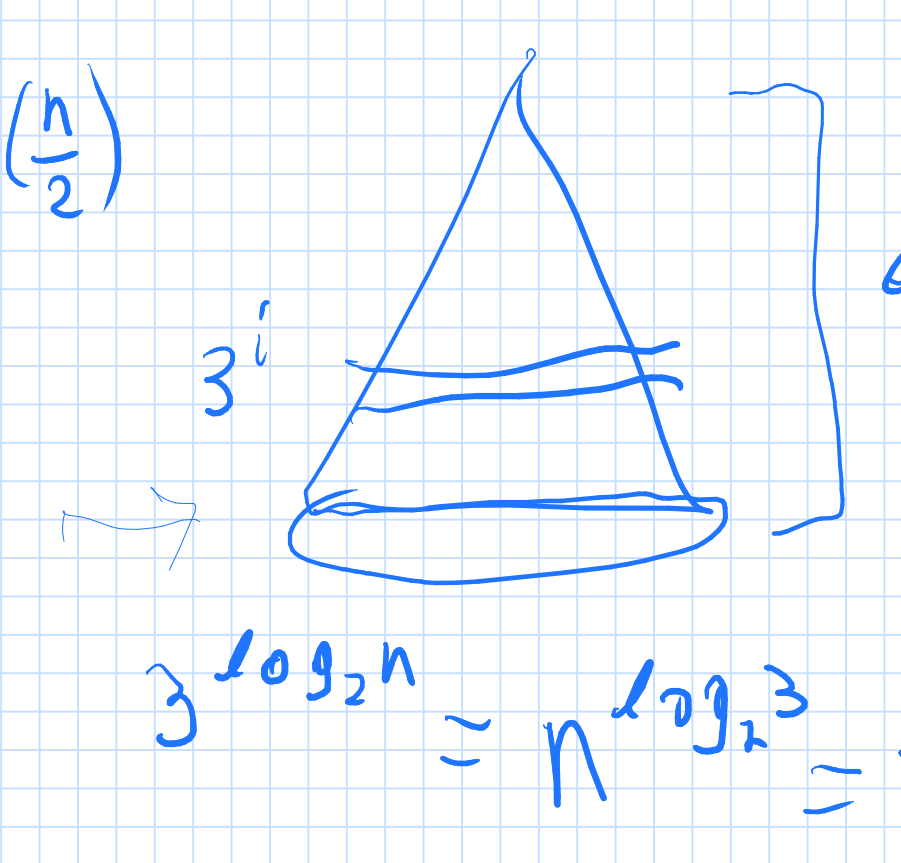
$1 - O$

T

$x = 2^{n/3}$

$c_0 + c_1 x + c_2 x^2$

$T(n) = O(n) + 3T\left(\frac{n}{2}\right)$



$3^{\log_2 n} = n^{\log_2 3} = n^{\text{something}}$ $\quad 2$ $\vee$