Problem Given 2 polynomials $P(x)$, $Q(x)$
in one var x of deg $n-1$
compute new polynomial $P(x)\cdot Q(x)$

e.g. $(x^2+x+5)\cdot(3x^2+x+4)$

$$= 3x^4 + \underbrace{(1\cdot1+1\cdot3)}_{4}x^3 + \underbrace{\boxed{(1\cdot4+1\cdot1+5\cdot3)}}_{20}x^2 + \underbrace{(1\cdot4+5\cdot1)}_{9}x + 20$$

$$= 3x^4 + 4x^3 + 20x^2 + 9x + 20$$

in general, $P(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0$

$Q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_0$

$P(x)\cdot Q(x) = c_{2n-2}x^{2n-2} + c_{2n-3}x^{2n-3} + \dots + c_0$

a_{n-1}	a_{n-2}	...	a_0
b_{n-1}	b_{n-2}	...	b_0

$\Rightarrow$

c_{2n-2}	c_{2n-3}	..	...	c_0

where $\boxed{c_k = \sum_{j=0}^{k} a_j b_{k-j}}$ $\quad k = 0 \,..\, 2n-2$

called convolution of two sequences

obvious alg'm - $O(n)$ time per c_k
$\Rightarrow$ $O(n^2)$ time
better?

Karatsuba's Alg'm (1960)

P

P_1	P_2

Karatsuba's Alg'm (1960)

P: $P_1 \mid P_2$

1st idea - divide each polynomial into 2 of deg $\frac{n}{2}-1$.

Q: $Q_1 \mid Q_2$

e.g. $P(x) = 3x^3 + 2x^2 + 4x + 1$

$$(\underbrace{3x+2}_{P_1(x)})x^2 + (\underbrace{4x+1}_{P_2(x)})$$

write $P(x) = P_1(x)\, x^{n/2} + P_2(x)$

$Q(x) = Q_1(x)\, x^{n/2} + Q_2(x)$.

recursive call

$$P(x)\,Q(x) = \boxed{P_1(x)\,Q_1(x)}\, x^n + \left(\boxed{P_1(x)\,Q_2(x)} + \boxed{P_2(x)\,Q_1(x)}\right) x^{n/2} + \boxed{P_2(x)\,Q_2(x)}.$$

4 recursive calls

$$\Rightarrow \quad T(n) = 4\,T\left(\frac{n}{2}\right) + \underbrace{O(n)}_{\text{additions \& shifts}}$$

$$\Rightarrow \quad T(n) = \boxed{O(n^2)}$$

$\log_2 4 = 2$

$T(n) = aT\left(\frac{n}{b}\right) + f(n)$

$\Rightarrow \ldots$ "master thm"

$$\begin{cases} n^{\log_b a} & \text{if } f(n) \ll n^{\log_b a} \\ f(n) & \text{if } f(n) \gg n^{\log_b a} \\ f(n)\log n & \text{if } f(n) = n^{\log_b a} \end{cases}$$

more clever idea -

recurse

rewrite $P_1(x)\,Q_2(x) + P_2(x)\,Q_1(x)$

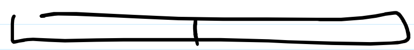
$$= \boxed{(P_1(x) + P_2(x)) \cdot (Q_1(x) + Q_2(x))} - \underbrace{P_1(x) \cdot Q_1(x)}_{\text{reuse}} - \underbrace{P_2(x) \cdot Q_2(x)}_{\text{reuse}}$$

$$- \underbrace{P_1(x)\cdot Q_1(x)}_{\text{reuse}} - \underbrace{P_2(x)\cdot Q_2(x)}_{\text{reuse}}$$

\# recursive calls = 3

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

$$\Rightarrow \quad O\left(n^{\log_2 3}\right) \le \boxed{O\left(n^{1.59}\right)}$$

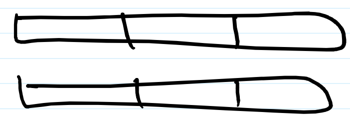


(alternatively - divide by even/odd

e.g. $P(x) = \left(3\underline{x^2} + 4\right)x + 2x^2 + 1$

$= P_1(x^2)\,x + P_2(x^2)$)

Toom and Cook (1963)



$$T(n) = \underline{5}\,T\left(\frac{n}{3}\right) + O(n)$$

$$\Rightarrow \quad O\left(n^{\log_3 5}\right) \le O\left(n^{1.47}\right)$$

$$T(n) = \underline{7}\,T\left(\frac{n}{4}\right) + O(n)$$

$$\Rightarrow \quad O\left(n^{\log_4 7}\right) \le O\left(n^{1.41}\right)$$

$\vdots$

$(2r-1)\,T\left(\frac{n}{r}\right) + O(n)$

$\log_r(2r-1)$

$$\Rightarrow \quad O\left(n^{1+\varepsilon}\right)$$ for any const $\varepsilon > 0$.

Cooley & Tukey's Alg'm (1965)

Problem A (Multi-Point Evaluation)

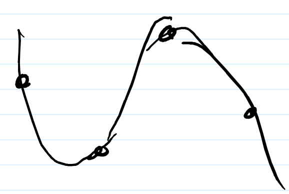
Given polynomial P of deg $N-1$
& N distinct values $\alpha_0, \alpha_1, \ldots, \alpha_{N-1}$
compute $P(\alpha_0), \ldots, P(\alpha_{N-1})$.

[trivial algm: $O(N)$ per α_k
$\Rightarrow O(N^2)$ time].

Problem B (Interpolation)

(inverse problem)

Given $P(\alpha_0), \ldots, P(\alpha_{N-1})$,
reconstruct polynomial P.



[Lagrange's interpolation formula: at least N^2 time].

To solve polynomial mult. problem: set $N = 2n-2$

1. compute $P(\alpha_0), \ldots P(\alpha_{N-1})$ by A
   $Q(\alpha_0) \ldots, Q(\alpha_{N-1})$
2. compute $P(\alpha_0) \cdot Q(\alpha_0), \ldots, P(\alpha_{N-1}) \cdot Q(\alpha_{N-1})$ in $O(N)$ time
3. reconstruct $P \cdot Q$ by B.

this works for any $\alpha_0, \ldots, \alpha_{N-1}$

this works for any $\alpha_0, \dots, \alpha_{N-1}$

~~f~~ find good choice of $\alpha_0, \dots, \alpha_{N-1}$
s.t. I can solve Probs A & B.