January 24, 2025 12:10 PM

Polynomial Multiplication

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. $(1x^2+1x+5)(2x^2+1x+3)$

$= 2x^4 + (1\cdot1+1\cdot2)x^3 + (1\cdot3+1\cdot1+5\cdot2)x^2 + (1\cdot3+5\cdot1)x + 5\cdot3$

$= 2x^4 + 3x^3 + 14x^2 + 8x + 15$

in general, $P(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0$
$Q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1x + b_0$

$P(x)Q(x) = c_{2n-2}x^{2n-2} + c_{2n-3}x^{2n-3} + \dots + c_1x + c_0$.

where $c_k = \sum_{j=0}^{k} a_j b_{k-j}$ ← $O(n)$ time for each c_k

⇒ $O(n^2)$ time by brute force

can we do better?

$\langle a_{n-1}, \dots, a_0\rangle$
$\langle b_{n-1}, \dots, b_0\rangle$
↓
$\langle c_{2n-2}, \dots, c_0\rangle$

convolution

Karatsuba's Alg'm (1960)

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

e.g. $P(x) = 3x^3 + 2x^2 + 4x + 5$

$= (3x+2)x^2 + 4x+5$

in general, write $P(x) = P_1(x)\, x^{n/2} + P_2(x)$ P_1, P_2 deg $\frac{n}{2}-1$
$Q(x) = Q_1(x)\, x^{n/2} + Q_2(x)$ Q_1, Q_2

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

by recursion

by recursion

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

$$T(n) = aT\left(\tfrac{n}{b}\right) + f(n) \qquad \begin{cases} O(n^{\log_b a}) \\ O(n^{\log_b a}\log n) \\ O(f(n)) \end{cases}$$

$$T(n) = \underline{4}\,T\left(\tfrac{n}{2}\right) + O(\underbrace{n}_{\text{3 additions, 2 shifts}})$$

$$\Rightarrow O(n^{\log_2 4}) = O(n^2)$$

not better

more clever idea -

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

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

$$T(n) = \underbrace{3}\,T\left(\tfrac{n}{2}\right) + O(n)$$

$$\Rightarrow O(n^{\log_2 3}) \leq \boxed{O(n^{1.59})}$$

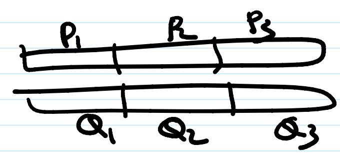
better?

(alternatively: divide by even-odd

$$P(x) = \underbrace{(3x^2+4)}x + \underbrace{2x^2+5}$$

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

Toom-Cook '63:



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

$$\Rightarrow O(n^{\log_3 5}) \leq O(n^{1.46})$$

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

$$\Rightarrow O(n^{\log_4 7}) \leq O(n^{1.41})$$

$\Rightarrow \quad O(n^{\log_4 7}) \le O(n^{[illegible]})$

$\vdots$

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

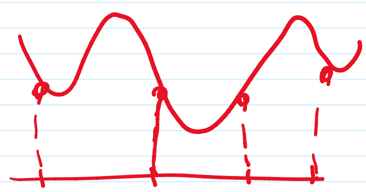
better?

Cooley-Tukey's Alg'm ('65).

Problem A (Multi-Point Evaluation)

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

[trivial alg'm: $O(N^2)$ time]
better?



Problem B (Interpolation)

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

[alg'm/formula by Lagrange (17..) ..]
$\hookrightarrow O(N^2)$ time

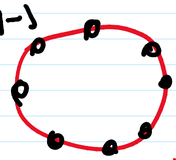
To solve orig. polynomial mult problem:
given P, Q, $N = 2n-1$

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

Note: works for any choice $\alpha_0, \ldots, \alpha_{N-1}$

Note: works for any choice $\alpha_0, .., \alpha_{N-1}$
pick good choice $\alpha_0, .., \alpha_{N-1}$

idea- choose $\alpha_k = e^{\frac{-2\pi i k}{N}}$ $k=0,..,N-1$



(called roots of unity
because they satisfy $z^N = 1$.
$\left(e^{\frac{-2\pi i k}{N}}\right)^N = \left(e^{2\pi i k}\right) = 1$)

Algm for Problem A: by divide & conquer

1. divide by odd-even:

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

P_1, P_2 of deg $\frac{N}{2} - 1$.

2. recursively compute

$$u_k = P_1\left(e^{\frac{-2\pi i k}{N/2}}\right) \quad \text{for } k = 0, \ldots, \tfrac{N}{2} - 1$$

$$v_k = P_2\left(e^{\frac{-2\pi i k}{N/2}}\right)$$

3. for $k = 0, .., N-1$,

$$z_k = P\left(e^{\frac{-2\pi i k}{N}}\right) = P_1\left(e^{-\frac{4\pi i k}{N}}\right) e^{-\frac{2\pi i k}{N}} + P_2\left(e^{-\frac{4\pi i k}{N}}\right)$$

$$e^{-\frac{4\pi i k}{N}} = \begin{cases} e^{-\frac{2\pi i k}{N/2}} & \text{if } k < N/2 \\ e^{-\frac{2\pi i}{N/2}\left(k - \frac{N}{2}\right)} & \text{if } k \geq \frac{N}{2} \end{cases}$$

$$\Rightarrow \quad z_k = \begin{cases} u_k\, e^{-\frac{2\pi i k}{N}} + v_k & \text{for } k = 0, .., \frac{N}{2} - 1 \\ u_{k - \frac{N}{2}}\, e^{-\frac{2\pi i k}{N}} + v_{k - N/2} & \text{for } k = \frac{N}{2}, .., N-1 \end{cases}$$

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

$$\Rightarrow \boxed{O(N \log N)}$$