January 19, 2023 1:17 PM

Announcement: I'll be away next Tue (1/24)
Please watch a pre-recorded video

Polynomial Multiplication / Convolution

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

$$= 3x^4 + (1\cdot1+1\cdot3)x^3 + (1\cdot4+1\cdot1+5\cdot3)x^2 + (1\cdot4+5\cdot1)x + 5\cdot4$$

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

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

$Q(x) = b_{n-1}x^{n-1} + \dots + b_1x + b_0$

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

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

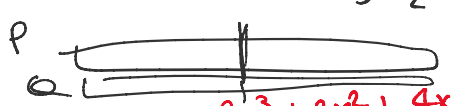
$\langle c_0,\dots,c_{2n-2}\rangle$ called convolution of sequences $\langle a_0,\dots,a_{n-1}\rangle$, $\langle b_0,\dots,b_{n-1}\rangle$

Obvious alg'm: $\boxed{O(n^2)}$ time

better?

Karatsuba's Alg'm (1960)

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



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

$= \boxed{3x+2}\,x^2 + \boxed{4x+1}$

In general, write
$$\begin{cases} P(x) = P_1(x)\,x^{n/2} + P_2(x) \\ Q(x) = Q_1(x)\,x^{n/2} + Q_2(x) \end{cases}$$

P_1, P_2, Q_1, Q_2 deg $\frac{n}{2}-1$

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

use recursion

$$T(n) = 4T\left(\frac{n}{2}\right) + O(n)$$

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

$aT\left(\frac{n}{b}\right)$

$n^{\log_b a}$

more clever idea - $P_1(x)Q_2(x) + P_2(x)Q_1(x)$

$$= (P_1(x) + P_2(x))(Q_1(x) + Q_2(x)) - \boxed{P_1(x)Q_1(x)} - \boxed{P_2(x)Q_2(x)}$$

reuse reuse

$\Rightarrow$ 3 recursive calls

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

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

[alternative - divide by even-odd

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

$= (3x^2+4)x + (2x^2+1)$

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

P_1, P_2 deg $\frac{n}{2}-1$]

Toom-Cook '63:

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

$$\Rightarrow O(n^{\log_3 5}) \leq O(n^{1.47})$$

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

$$\Rightarrow O(n^{1.41})$$

$\vdots$

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

better?

Cooley and 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]

Problem B (Interpolation) (inverse)

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

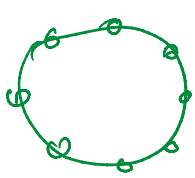
[alg'm/formula by Lagrange (17??)]
$\Rightarrow \geq N^2$ time

To Solve orig. polynomial mult. Problem: $(N = 2n-1)$

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

Note - this works for any $\alpha_0, \ldots, \alpha_{N-1}$
pick some nice values . . .

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



called roots of unity
because they satisfy $z^N = 1$

because they satisfy $z^N = 1$

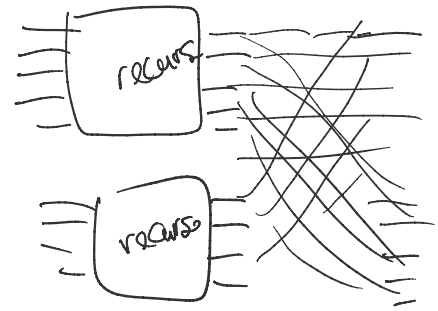
$$\left(\left(e^{-\frac{2\pi i k}{N}}\right)^N = e^{-2\pi i} = 1 \right)$$

Alg'm for Problem A:

1. divide by odd-even:

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

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



2. recursively compute

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

$$P_2\left(e^{-\frac{2\pi i k}{N/2}}\right), \quad k = 0, 1, \ldots, \frac{N}{2}-1$$

2 recursive calls

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

output $$P\left(e^{-\frac{2\pi i k}{N}}\right) = \underbrace{P_1\left(e^{-\frac{4\pi i k}{N}}\right)}_{\text{known from step 2}} e^{-\frac{2\pi i k}{N}} + \underbrace{P_2\left(e^{-\frac{4\pi i k}{N}}\right)}_{\text{known from step 2}}$$

note: if $k > \frac{N}{2}$,

$$e^{-\frac{4\pi i k}{N}} = e^{-\frac{4\pi i}{N}(k - N/2)}$$

because $e^{+\frac{4\pi i}{\cancel{N}} \cdot \frac{\cancel{N}}{2}} = e^{2\pi i} = 1$

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

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