August 26, 2022 10:34 AM

I. Basic Algorithmic Tools

Convolution Problem

Given 2 sequences $\langle a_0, \ldots, a_{n-1} \rangle$
$\langle b_0, \ldots, b_{n-1} \rangle$,

compute $\langle c_0, \ldots, c_{2n-2} \rangle$ where

$$c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0$$
$$= \sum_{k=0}^{i} a_k b_{i-k}.$$

(e.g. $\langle 1,2,3 \rangle$, $\langle 4,5,6 \rangle$ $\rightarrow$ $\langle 1\cdot4,\ 1\cdot5+2\cdot4,\ 1\cdot6+2\cdot5+3\cdot4,\ 2\cdot6+3\cdot5,\ 3\cdot6 \rangle$
$= \langle 4, 13, \ldots \rangle$)

Equiv.: given 2 polynomials
$$A(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0$$
$$B(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_0$$
compute $A(x)B(x) = c_{2n-2}x^{2n-2} + \ldots + c_0$

Trivial Alg'm: each c_i in $O(n)$ time
$\Rightarrow$ total $\boxed{O(n^2)}$

better?

Karatsuba's Alg'm ('60):

Warm-up: $n=2$

Given a_0, a_1, b_0, b_1, to compute
$c_0 = a_0 b_0$
$c_1 = a_1 b_0 + a_0 b_1$
$c_2 = a_1 b_1$

trivial: 4 mults.

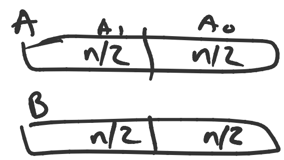
But can do with 3!

Sol'n: just rewrite $c_1 = (a_1 + a_0)(b_1 + b_0) - a_0 b_0 - a_1 b_1$

power of subtraction!

General n:

idea - binary divide & conquer



write $A(x) = A_1(x)\, x^{n/2} + A_0(x)$

$B(x) = B_1(x)\, x^{n/2} + B_0(x)$

$\Rightarrow A(x)B(x) = A_1(x)B_1(x)\, x^n +$
$\left(A_1(x)B_0(x) + A_0(x)B_1(x)\right) x^{n/2} +$
$A_0(x)B_0(x)$

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

$\Rightarrow O(n^2)$

$T(n) = a\,T\left(\frac{n}{b}\right) + \bigcirc$

$n^{\log_b a}$

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

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

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

Toom & Cook's Alg'm ('63):

Warm-up: $n=3$.

given $a_0, a_1, a_2, b_0, b_1, b_2$, to compute

$c_0 = a_0 b_0$

$c_1 = a_0 b_1 + a_1 b_0$

$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$

$c_3 = a_1 b_2 + a_2 b_1$

$c_4 = a_2 b_2$

trivial: 9 mults

better sol'n: compute

$d_0 = a_0 b_0$

$d_1 = (a_2 + a_1 + a_0)(b_2 + b_1 + b_0)$

$d_2 = (4a_2 + 2a_1 + a_0)(4b_2 + 2b_1 + b_0)$

$d_3 = (9a_2 + 3a_1 + a_0)(9b_2 + 3b_1 + b_0)$

$d_4 = (16a_2 + 4a_1 + a_0)(16b_2 + 4b_1 + b_0)$

can then recover $c_0, \ldots, c_4$ from $d_0, \ldots, d_4$

R(b)

$d_4 = (\ldots$

can then recover $c_0, \ldots, c_4$ from $d_0, \ldots, d_4$

(why? $d_k = (\underbrace{a_2k^2 + a_1k + a_0}_{= A(k)}) \, (\underbrace{b_2k^2 + b_1k + b_0}_{= B(k)})$

$\Rightarrow d_k = c_4k^4 + c_3k^3 + c_2k^2 + c_1k + c_0, \quad k = 0, \ldots, 4$

5 linear eq'ns, 5 vars)

$\Rightarrow$ 5 mults.

General n: 3-way D&C

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

$$\Rightarrow O\left(n^{\log_3 5}\right) = \boxed{O\left(n^{1.41}\right)}$$

r-way D&C

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

$$\Rightarrow O\left(n^{\log_r(2r-1)}\right)$$

$$\leq O\left(n^{\frac{\log(2r)}{\log r}}\right)$$

$$\leq O\left(n^{1+\frac{1}{\log r}}\right)$$

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

Cooley & Tukey's Alg'm ('65)

$N = 2n-1$

previous idea - compute $d_k = A(k) \cdot B(k) \quad k = 0, \ldots, N-1$

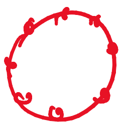
$= C(k)$

new idea - compute $d_k = \underbrace{A\left(e^{-\frac{2\pi i}{N}k}\right)}_{\hat{a}_k} \cdot \overbrace{B\left(e^{-\frac{2\pi i}{N}k}\right)}^{\hat{b}_k}$

$k = 0, \ldots, N-1$

here, $e^{-\frac{2\pi i}{N}k}$ are called roots of unity

i.e. roots of $z^N = 1$.



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

Soln: compute $\hat{a}_k = \sum_{j=0}^{n-1} a_j e^{-\frac{2\pi i k}{N} j}$ $\quad k = 0, .., N-1$

$$\hat{b}_k = \sum_{j=0}^{n-1} b_j e^{-\frac{2\pi i k}{N} j}$$

called Discrete Fourier Transform (DFT)

$$d_k = \hat{a}_k \cdot \hat{b}_k \qquad k = 0, .., N-1$$

$$c_j = \frac{1}{N} \sum_{k=0}^{N-1} d_k e^{\frac{2\pi i j}{N} k}$$

called inverse DFT

(similar to continuous Fourier transform:

$$\hat{f}(t) = \int_{x=-\infty}^{\infty} f(x) e^{-2\pi i t x} dx$$

Known: $\widehat{f \circ g} = \hat{f} \cdot \hat{g}$

inverse transform $\quad f(x) = \int_{t=-\infty}^{\infty} \hat{f}(t) e^{2\pi i x t} dt$)

New Problem (DFT) Given $\langle a_0, .., a_{N-1} \rangle$,

compute $\langle \hat{a}_0, .., \hat{a}_{N-1} \rangle$ where

$$\hat{a}_k = \sum_{j=0}^{N-1} a_j e^{-\frac{2\pi i k}{N} j}$$