KARATSUBA multiplication algorithm for polynomials

f, g : degree n

trivial algor. requires n^2 scalar multiplications

KARATSUBA Divide & Conquer

$n^{\log_2 3} \approx n^{1.58}$

---

count multiplications
additions / subtraction
of scalars
reals

bookkeeping
pushing links

Claim: Total cost $O(n^{\alpha})$ $\alpha = \log_2 3 \approx 1.58$

DEF big-Oh notation

a_n, b_n sequences of reals

$$a_n \overset{\text{"is"}}{=} O(b_n) \qquad a_n \text{ is big-Oh of } b_n$$

if $(\exists C)$(for all sufficiently large n)$\left(|a_n| \le C|b_n|\right)$

Example:

$$10n^2 + 10^6 = O(n^2)$$

$$C = 10$$

$$10n^2 + 10^6 \not\le 10n^2$$

$$C = 10.001 \checkmark$$

$\forall \varepsilon > 0$ $\quad C = 10 + \varepsilon$

$\forall C > 10$ works

big-Omega notation

$$a_n = \Omega(b_n) \text{ if}$$
$$b_n = O(a_n)$$

Do

$$a_n \overset{\text{"is"}}{=} \Omega(b_n) \iff$$
$$(\exists\, c>0)(\text{for all suff. large } n)$$
$$|a_n| \geq c|b_n|$$

$$a_n = O(b_n)$$
$$|a_n| \leq O(b_n)$$

Do

$$a_n \overset{C}{=} O(b_n), \quad b_n \overset{D}{=} O(c_n)$$
$$\implies a_n = \underset{\text{const.} = CD}{O}(c_n)$$

multiplying polynomials
of degree $\underline{n-1}$

$n = \#$ coefficients

$f \quad g \quad f \cdot g$

assumption: $n = 2^k$

$M(n)$: # scalar multiplications

trivial: $M(n) \leq 4 \cdot M\left(\frac{n}{2}\right)$

KARATSUBA: $\boxed{M(n) \leq 3 \cdot M\left(\frac{n}{2}\right)}$

$T(n)$ total # operations: mult $\pm$ scalars

bookkeeping

$$\boxed{T(n) \leq 3 \cdot T\left(\frac{n}{2}\right) + O(n)}$$

$T(1) = 1$

METHOD OF REVERSE INEQUALITIES

$$T(n) \le 3T\left(\frac{n}{2}\right) + Cn \qquad (1)$$

Guess $g(n)$ s.t.

$$g(1) \ge T(1) \qquad (*) \ (2)$$

$$g(n) \ge 3g\left(\frac{n}{2}\right) + Cn \qquad (3)$$

Claim $(\forall n)\big(\underbrace{g(n) \ge T(n)}_{(**)}\big)$

Pf: true for $n=1$ $(*)$

inductive step

Ind. Hyp: $(**)$ true for $\frac{n}{2}$ $(n>1)$

$\Downarrow$

Desired conclusion $(**)$ true for n

Proof

$$g(n) \underset{\text{Eq}(3)}{\ge} 3g\left(\frac{n}{2}\right) + Cn \underset{\text{I.H.}}{\ge} 3\cdot T\left(\frac{n}{2}\right) + Cn \underset{\text{by Eq}(1)}{\ge} T(n)$$

Guess $g(n) = n^\alpha$ $\alpha = \log_2 3$

$n=1$ $g(1) = 1 = T(1)$ ✓

$n \geq 2$

need to check

$$g(n) \overset{?}{\geq} 3g\left(\frac{n}{2}\right) + Cn$$

$$\underline{n^\alpha} \overset{?}{\geq} \underline{3\cdot\left(\frac{n}{2}\right)^\alpha} + Cn$$

NO, always $<$

$$\boxed{n^\alpha = 3\left(\frac{n}{2}\right)^\alpha \quad \text{b/c} \quad 2^\alpha = 3}$$

Next guess

$$\underline{g(n) = A\cdot n^\alpha + Bn}$$

$$g(1) = \underline{A+B} \overset{?}{\geq} T(1) = \underline{1}$$

$$g(n) = An^\alpha + Bn \overset{?}{\geq} 3\cdot\left(A\left(\frac{n}{2}\right)^\alpha + B\cdot\frac{n}{2}\right) + Cn$$

Next guess

$$g(n) = A\cdot n^{\alpha} + Bn$$

$$g(1) = \boxed{A+B} \overset{?}{\geq} T(1) = \boxed{1}$$

$$g(n) = An^{\alpha} + Bn \overset{?}{\geq} 3\cdot\left(A\left(\tfrac{n}{2}\right)^{\alpha} + B\cdot\tfrac{n}{2}\right) + Cn$$

$$An^{\alpha} + Bn \overset{?}{\geq} 3A\left(\tfrac{n}{2}\right)^{\alpha} + 3B\tfrac{n}{2} + Cn$$

$$Bn \overset{?}{\geq} B\cdot 3\tfrac{n}{2} + Cn$$

$$B \overset{?}{\geq} \tfrac{3}{2}B + C$$

$$-\tfrac{B}{2} \overset{?}{\geq} C$$

$$\boxed{B \leq -2C}$$

Choose $\boxed{B := -2C}$

need $A + B \geq 1$

$A - 2C \geq 1$

$A \geq 2C+1$

Choose $\boxed{A = 2C+1}$

$$(\forall n)\ \left(T(n) \leq (2C+1)n^{\alpha} - 2Cn\right) \quad O(n^{\alpha})$$