# Lec14-Karatsuba-Strassen

Wednesday, September 27, 2023 10:41 AM

Examples of Divide & Conquer for numerics

(Anatoly) (1962)

Karatsuba's alg for integer multiplication

$$\begin{array}{r} 123 \\ \times\ 321 \\ \hline 123 \\ 246\phantom{0} \\ 369\phantom{00} \\ \hline 39483 \end{array} \qquad \begin{array}{r} 1010110 \\ \times\ 01011101 \\ \hline 1010110 \\ \cancel{00000000}\phantom{0} \\ 1010110\phantom{00} \\ 1010110\phantom{000} \\ 1010110\phantom{0000} \\ \cancel{00000000}\phantom{0} \\ 1010110\phantom{000000} \\ \hline 111110011010110 \end{array}$$

$n$ numbers of $n$ bits

$O(n^2)$ - time

Break items into half-sized blocks:

Say $x$ is $n$ bits, let $m = \frac{n}{2}$.

$$x = x_1 2^m + x_0$$

$$y = y_1 2^m + y_0$$

$$\text{Then} \quad xy = (x_1 2^m + x_0)(y_1 2^m + y_0) = x_1 y_1 \overbrace{2^{2m}}^{\substack{O(m) \\ \text{bit-shift}}} + (x_1 y_0 + x_0 y_1) \overbrace{2^m}^{\substack{O(m) \\ \text{bitshift}}} + x_0 y_0$$

4 mults of size $m$ bitstrings

$$\text{But,} \quad x_1 y_0 + x_0 y_1 = \underbrace{(x_1 + x_0)(y_1 + y_0)}_{\text{one mult}} - x_1 y_1 - x_0 y_0$$

reuse mults from above

Only 3 mults needed!

Let
$$p_0 = x_0 y_0$$
$$p_1 = x_1 y_1$$
$$p_2 = (x_1 + x_0)(y_1 + y_0) - p_0 - p_1$$

Then $xy = p_1 2^{2m} + p_2 2^m + p_0$

Analysis: Let $n = 2^k$ for some $k$.

$$\frac{T(2^k)}{3^k} = \frac{\cancel{3}\, T(2^{k-1})}{3^{k-1}} + \frac{c 2^k}{3^k}$$

By recursion $T(2^k)$ ... $c \sum^{k} 2^j < B$ for some constant v $B$

$3^k \qquad 3^{k-1} \qquad 3^{\cdots}$

By recursion, $\dfrac{T(2^k)}{3^k} = \underbrace{\gamma}_{\text{base case}} + \underbrace{c\sum_{j=1}^{k} \frac{2^j}{3^j}}_{\text{geom series}} \leq \beta$ for some constant $\gamma, \beta$

$$\Rightarrow \quad \frac{T(2^k)}{3^k} \leq \beta$$

$$T(2^k) \leq \beta 3^k = \beta\, 2^{\log_2 3^k} = \beta\, 2^{k \log_2 3}$$

$$T(n) \leq \beta (2^k)^{\log_2 3} = \beta n^{\log_2 3} = \beta n^{1.58\ldots} = O(n^{1.58\ldots}) \leq O(n^2)$$

---

**Matrix multiplication:**

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 5+2\cdot 7 & 6+2\cdot 8 \\ 5\cdot 3+4\cdot 7 & 3\cdot 6+4\cdot 8 \end{bmatrix} = \begin{bmatrix} 19 & 22 \\ 43 & 50 \end{bmatrix}$$

$$\begin{array}{r} \\ \\ \text{row } j \\ \\ \end{array} \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{bmatrix} = \begin{bmatrix} \sum_{k=1}^{n} a_{1k} b_{k1} & \cdots & \sum_{k=1}^{n} a_{1k} b_{kn} \\ \vdots & \sum_{k=1}^{n} a_{ik} b_{kj} & \\ & & \end{bmatrix}$$

col $j$

$n \times n$ matrix

each entry takes $\Theta(n)$ to compute

$n^2$ entries $\Rightarrow \Theta(n^3)$

**Notice:** Matrix addition is much cheaper than multiplication $\Theta(n^2)$

Let's try divide (conquering for later)

Assume matrix is of size $n = 2^m$ for some $m$, so we can break the matrix into quarters

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \cdot \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}$$

$A \in \mathbb{R}^{n \times n} \qquad B \in \mathbb{R}^{n \times n} \qquad C \in \mathbb{R}^{n \times n}$

$$C_{11} = A_{11}B_{11} + A_{12}B_{21} \qquad C_{12} = A_{11}B_{12} + A_{12}B_{22}$$

$$C_{21} = A_{21}B_{11} + A_{22}B_{21} \qquad C_{22} = A_{21}B_{12} + A_{22}B_{22}$$

8 matrix mults of half size matrices

**Intuition:** $\underbrace{(X+Y)(Z+W)}_{1 \text{ mult}} = \underbrace{XZ + YZ + XW + YW}_{4 \text{ mults}}$

Can we rewrite the formulas for $C_{11}, C_{12}, C_{21}, C_{22}$ to use fewer mults?

**Strassen:**

$$P_1 = (A_{11} + A_{22})(B_{11} + B_{22})$$
$$P_2 = (A_{21} + A_{22})B_{11}$$
$$P_3 = A_{11}(B_{12} - B_{22})$$
$$P_4 = A_{22}(B_{21} - B_{11})$$
$$P_5 = (A_{11} + A_{12})B_{22}$$
$$P_6 = (A_{21} - A_{11})(B_{11} + B_{22})$$
$$P_7 = (A_{12} - A_{22})(B_{21} + B_{22})$$

$$C_{11} = P_1 + P_4 - P_5 + P_7$$
$$C_{12} = P_3 + P_5$$
$$C_{21} = P_2 + P_4$$
$$C_{22} = P_1 - P_2 + P_3 + P_6$$

Only 7 mults instead of 8

Apply idea recursively to $P_1, P_2, \ldots, P_7$, which are square matrices half the size.

**Recurrence:** $T(n) = \underbrace{7T\left(\frac{n}{2}\right)}_{\text{recursion}} + \underbrace{cn^2}_{\text{additions}}$

Recall $n = 2^m$: $T(2^m) = 7T(2^{m-1}) + c4^m$

$$\frac{T(2^m)}{7^m} = \frac{7T(2^{m-1})}{7^m} + \frac{c4^m}{7^m}$$

$$\frac{T(2^m)}{7^m} = \frac{T(2^{m-1})}{7^{m-1}} + \frac{c4^m}{7^m} = \frac{c4^m}{7^m} + \frac{c4^{m-1}}{7^{m-1}} + \frac{T(2^{m-2})}{7^{m-2}}$$

recursively expand

$$= \sum_{k=1}^{m} \frac{c4^k}{7^k} + \frac{T(1)}{1}$$

$$\leq \sum_{k=1}^{\infty} \frac{c4^k}{7^k} + \gamma \quad \text{for some constant } \gamma$$

$$= c\sum_{k=1}^{\infty}\left(\frac{4}{7}\right)^k + \gamma = c \cdot \frac{\frac{4}{7}}{1 - \frac{4}{7}} + \gamma = \frac{4}{3}c + \gamma = \alpha \quad \text{for some constant } \alpha.$$

$\Rightarrow T(2^m)$ [illegible] $2^m$

$$\Rightarrow \frac{T(2^m)}{7^m} \le \alpha \Rightarrow T(2^m) \le \alpha\, 7^m$$
$$= \alpha\, 2^{m \log_2 7}$$
$$\Rightarrow T(n) = \alpha\, n^{\log_2 7} = \alpha\, n^{2.807\ldots} = O(n^{2.807\ldots})$$

Strassen first to show improvement over $O(n^3)$

Can we do better?

Volker Strassen, 1969, $O(n^{2.807})$

⋮

Coppersmith + Winograd, 1990, $O(n^{2.3754})$

Andrew Stothers, 2010, $O(n^{2.3736})$

Virginia Williams, 2013, $O(n^{2.3729})$ (CMU PhD 2008)

⋮

Williams, Xu, Xu, Zhou, 2023, $O(n^{2.371552})$