DESIGN AND ANALYSIS OF ALGORITHMS
UE19CS251

Shylaja S S
Department of Computer Science
& Engineering

DESIGN AND ANALYSIS OF ALGORITHMS

Multiplication of Large Integers and Strassen's Matrix Multiplication

Major Slides Content: Anany Levitin

Shylaja S S

Department of Computer Science & Engineering

Multiplication of large integers - Idea

- Let the two numbers being multiplied be a and b
- a and b are n–digit integers, where n is a positive even number
- Let the first half of a's digits be a_1 and second half be a_0
- Similarly, let the first half of b's digits be b_1 and second half be b_0
- In these notations, $a = a_1a_0$ implies $a = a_1*10^{n/2} + a_0$ and $b = b_1b_0$ implies $b = b_1*10^{n/2} + b_0$

Multiplication of large integers - Idea

$c = a*b = (a_1 10^{n/2} + a_0) * (b_1 10^{n/2} + b_0)$

$= (a_1 * b_1)10^n + (a_1 * b_0 + a_0 * b_1)10^{n/2} + (a_0 * b_0)$

$= c_2 10^n + c_1 10^{n/2} + c_0$

where

$c_2 = a_1 * b_1$ is the product of their first halves

$c_0 = a_0 * b_0$ is the product of their second halves

$c_1 = (a_1 + a_0) * (b_1 + b_0) - (c_2 + c_0)$ is the product of the sum of the a's halves and the sum of the b's halves minus the sum of c_2 and c_0

Multiplication of large integers - Analysis

- $M(n) = 3M(n/2)$ for $n > 1$, $M(1) = 1$
- Solving it by backward substitutions for $n = 2^k$ yields:

$M(2^k) = 3M(2^{k-1}) = 3[3M(2^{k-2})] = 3^2M(2^{k-2})$

$= \ldots = 3^i M(2^{k-i}) = \ldots = 3^kM(2^{k-k}) = 3^k$

- Since $k = \log_2 n$: $M(n) = 3^{\log_2 n} = n^{\log_2 3} = n^{1.585}$
- The number of additions is given by:

$$A(n) = 3A(n/2) + cn \text{ for } n > 1,\ A(1) = 1$$

$$A(n) \text{ belongs to } \Theta(n^{\log_2 3})$$

Multiplication of large integers - Example

2135 * 4014

$= (21*10^2 + 35) * (40*10^2 + 14)$

$= (21*40)*10^4 + c1*10^2 + 35*14$

where $c1 = (21+35)*(40+14) - 21*40 - 35*14$, and

$21*40 = (2*10 + 1) * (4*10 + 0)$

$= (2*4)*10^2 + c2*10 + 1*0$

where $c2 = (2+1)*(4+0) - 2*4 - 1*0$, etc.,

Strassen's Matrix Multiplication

- This algorithm was published by V Strassen in 1969
- The principal insight of the algorithm lies in the discovery that we can find product of two 2 – by – 2 matrices A and B with seven multiplications as opposed to the eight required by the Brute – Force algorithm
- This is accomplished by the following formulae:

$$\begin{bmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{bmatrix} = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} * \begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{bmatrix}$$

$$= \begin{bmatrix} m_1 + m_4 - m_5 + m_7 & m_3 + m_5 \\ m_2 + m_4 & m_1 + m_3 - m_2 + m_6 \end{bmatrix}$$

Strassen's Matrix Multiplication

$m_1 = (a_{00} + a_{11}) * (b_{00} + b_{11})$

$m_2 = (a_{10} + a_{11}) * b_{00}$

$m_3 = a_{00} * (b_{01} - b_{11})$

$m_4 = a_{11} * (b_{10} - b_{00})$

$m_5 = (a_{00} + a_{01}) * b_{11}$

$m_6 = (a_{10} - a_{00}) * (b_{00} + b_{01})$

$m_7 = (a_{01} - a_{11}) * (b_{10} + b_{11})$

Strassen's Matrix Multiplication – General Formula

For any two matrices A and B of size n – by – n, we can divide A, B and the product C as follows:

$$\left[\begin{array}{c|c} C_{00} & C_{01} \\ \hline C_{10} & C_{11} \end{array}\right] = \left[\begin{array}{c|c} A_{00} & A_{01} \\ \hline A_{10} & A_{11} \end{array}\right] * \left[\begin{array}{c|c} B_{00} & B_{01} \\ \hline B_{10} & B_{11} \end{array}\right]$$

The sub – matrices can be treated as numbers to get the correct product

Strassen's Matrix Multiplication – Analysis

- If $M(n)$ is the number of multiplications made by Strassen's algorithm in multiplying two matrices n – by – n, we get the following recurrence relation for it:

  $M(n) = 7M(n/2)$ for $n>1$, $M(1) = 1$

  Since $n = 2^k$,

  $$M(2^k) = 7M(2^{k-1}) = 7[7M(2^{k-2})] = 7^2M(2^{k-2}) = \ldots$$

  $$= 7^i M(2^{k-i}) \ldots = 7^k M(2^{k-k}) = 7^k$$

  Since $k = \log_2 n$,

  $$M(n) = 7^{\log_2 n} = n^{\log_2 7} \approx n^{2.807}$$

Strassen's Matrix Multiplication – Analysis

- The number of additions are given by the following recurrence:

  $A(n) = 7\,A(n/2) + 18(n/2)^2$ for $n>1$, $A(1) = 0$

- According to Master's Theorem, $A(n)$ belongs to $\Theta(n^{\log_2 7})$

THANK YOU

Shylaja S S

Department of Computer Science & Engineering

shylaja.sharath@pes.edu