

CS5800 – ALGORITHMS

MODULE 3. DIVIDE & CONQUER - I

Lesson 3: Integer Multiplication

Ravi Sundaram

Topics

- Integer multiplication – grade school
- Naïve Divide & Conquer
- Karatsuba's algorithm
- Summary

3. Multiplication over the integers

$$\begin{array}{r} 36185027886661311069865932815214971104 \quad A \\ \times \quad \underline{5932020762686101} \quad B \\ \hline 214650336722050463946651358202698404452609868137425504 \quad C \end{array}$$

The diagram illustrates the grade school multiplication algorithm. It shows two large numbers, A and B, being multiplied. Number A is 36185027886661311069865932815214971104 and number B is 5932020762686101. The result of the multiplication is C, which is 214650336722050463946651358202698404452609868137425504. The multiplication is performed by writing A above B, drawing a line under B, and then performing successive additions of shifted versions of A. The result is then written below the line.

- Naïve (grade school) multiplication is quadratic time $\Theta(\lg A * \lg B)$
- If both A and B are n-bit numbers then (naïve) multiplication is $\Theta(n^2)$

Naïve Divide & Conquer

- Let $X = \boxed{A} \boxed{B}$ and $Y = \boxed{C} \boxed{D}$ where A,B,C and D are $n/2$ bit integers
- Simple Method: $XY = (2^{n/2}A+B)(2^{n/2}C+D)$
 $= 2^nA*C + 2^{n/2}(A*D+B*C) + B*D$
- Running Time Recurrence
 $T(n) < 4T(n/2) + 100n$
- Solution $T(n) = \theta(n^2)$

Karatsuba's Algorithm

- Famous Russian mathematician Andrey Kolmogorov conjectured that the grade school algorithm was asymptotically optimal
- Posed it as a conjecture in his seminar at Moscow State Univ in 1960
- 23 yr old Karatsuba solved it within a week and the seminar was terminated!

Karatsuba's Algorithm

- Let $X = \boxed{A} \boxed{B}$ and $Y = \boxed{C} \boxed{D}$ where A,B,C and D are $n/2$ bit integers
- Karatsuba:
Compute A^*C , B^*D and use $AD + BC = (A+B)^*(C+D) - AC - BD$

$$XY = 2^nAC + 2^{n/2}(AD + BC) + BD$$

Reduced from 4 to 3 multiplications.

Remember - addition and subtraction are linear

Karatsuba's Algorithm

- Running Time Recurrence

$$T(n) < 3T(n/2) + 100n$$

- Solution: $T(n) = O(n^{\lg 3}) = O(n^{1.58})$

Summary

- Divide & Conquer is only an approach.
- Cleverness continues to play a very important role in how to realize the Divide and Conquer steps
- In a recent breakthrough (Harvey, van der Hoeven 2019) the complexity of integer multiplication and division of n-bit numbers is now at $O(n \log n)$
- Main takeaway: An understanding of recurrence equations (Master Theorem) is crucial for designing fast algorithms.