

CS 170 Lecture Notes, Fall 2020

Algorithms and Intractable Problems

Professors: Avishay Tal, Umesh Vazirani

Scribe: Vishal Raman

Contents

1 September 1st, 2020	3
1.1 Naive Multiplication	3
1.2 Divide and Conquer: Karatsuba's Algorithm	3

§1 September 1st, 2020

§1.1 Naive Multiplication

Recall the example of Fibonacci: we went from a complexity of $O(2^n) \rightarrow O(n^2) \rightarrow O(f(n))$, where $f(n)$ is the runtime for multiplying n -bit numbers. The naive algorithm is the usual multiplication algorithm for multiplying by hand.

$$\begin{array}{r} 17 \\ 21 \\ \hline 17 \\ 34x \\ \hline 357 \end{array}$$

Listing 1: Naive n -bit multiplication

```

1 function multiply(x, y):
2   Input: n-bit integers, x, y, y >= 0
3   Output: Product
4
5   if (y == 0) return 0;
6   s = multiply(x, floor(y/2))
7   if y is even:
8     return 2s
9   else
10    return x+2s

```

If we write $x = \sum_{i=0}^{n-1} x_j 2^i$, $y = \sum_{i=0}^{n-1} y_i 2^i$, so

$$xy = \left(\sum_{i=0}^{n-1} x_j 2^i \right) \left(\sum_{i=0}^{n-1} y_i 2^i \right) = \sum_{j,k=0}^n x_j y_k 2^{j+k}.$$

§1.2 Divide and Conquer: Karatsuba's Algorithm

For a Divide and Conquer problem, we do the following:

1. Break problem into pieces.
2. Solve pieces recursively.
3. Glue solutions of pieces to get solution of original problem.

We first have x an n -bit number that we break up into x_L, x_R , each $n/2$ bit numbers. Similarly, we break y into y_L, y_R .

$$x = \underbrace{\begin{array}{c} \xleftarrow{n/2} \quad \xrightarrow{n/2} \\ x_L \quad | \quad x_R \end{array}}_{n \text{ bit.}}$$

Note that $x = 2^{n/2}x_L + x_R$, $y = 2^{n/2}y_L + y_R$, so

$$xy = 2^n x_L x_L + 2^{n/2}(x_L y_R + x_R y + L) + x_R y_R.$$

We now have 4 multiplications, involving $n/2$ -bit numbers. Multiplication by 2^m can be shifting ($O(m)$ time), and addition is $O(1)$. Hence, we have a recurrence equation for the runtime,

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



Note that the depth of the recursion tree is $\log n$ and there are $4^{\log n} = n^2$ leaves. But this would have the same runtime as the naive algorithm, so more work is required to optimize.