Integer Multiplication Algorithm

We start with addition. The time to add two integers is linear with the number of digits: Upper bound is elementary school algorithm, and lower bound is must examine every input digit. For the remainder of this discussion, assume that time to add two n digit numbers is $A(n) = \alpha n$.

Now ready for multiplication:

Elementary school algorithm: Every digit on bottom is multiplied with every digit on top. There are exactly n^2 atomic multiplies, and approximately $2n^2$ atomic additions if we do the additions "row-by-row" rather than by columns (see example below). Assume that the cost of an atomic muliply is μ. The algorithm would take time about $\mu n^2 + \alpha n^2$, which is quadratic.

Alternative algorithm: Use divide-and-conquer. Take two n digit numbers x, y and cut each in half to form:

$$x = a \circ b, \qquad y = c \circ d$$

where a is the $n/2$ leftmost digits of x, b is the $n/2$ rightmost digits of x, c is the $n/2$ leftmost digits of y, and d is the $n/2$ rightmost digits of y. Now,

$$xy = ac2^n + (ad + bc)2^{n/2} + bd$$

So we need the four products ac, ad, bc, and bd, which can be attained by calling the algorithm recursively four times (on $n/2$ digit numbers). The two values ac and bd can be concatenated, and ad can be added to bc in time αn. The final result is the sum of $ac \circ bd$ and $ad + bc$. Ignoring the rightmost $n/2$ digits of $ac \circ bd$, this sum can digit attained with and additional αn time plus the cost of potentially $n/2$ carries (which for simplicity we ignore). So the total time for the additions is $\alpha 2n$. The recursion ends when $n = 1$ and it multiplies two one digit numbers.

The recurrence for the time to multiply:

$$M(n) = 4T\left(\frac{n}{2}\right) + 2\alpha n$$

and $M(1) = \mu$. Using the tree method we find that

$$M(n) = \mu n^2 + 2\alpha n(n-1)$$

This is still quadratic and pretty much matches the elemtary school algorithm.

The next thing to note is that two two-digit numbers can be multiplied using only three multiplications: To form xy, let

$$\begin{aligned} u &= (a+b)(c+d) \\ v &= ac \\ w &= bd \end{aligned}$$

Then the product is

$$xy = v2^n + (u - v - w)2^{n/2} + w$$

We have reduced that number of multiplies from four to three, at the cost of increasing the number of additions. Multiplying by a power of 2 can be accomplished by shifts (this holds for any base). We can

estimate the addition time as $\alpha n/2$ to form $a+b$, $\alpha n/2$ to form $c+d$, αn to form $v+w$, αn to subtract that sum from u, and αn to add that to $v \circ w$. The total is $4\alpha n$. The recurrence for the time to multiply:

$$M(n) = 3T\left(\frac{n}{2}\right) + 4\alpha n$$

and $M(1) = \mu$. Using the tree method we find that

$$M(n) = (\mu + 8\alpha)n^{\log_3 2} - 8\alpha n$$

NOTE: $a+b$ and/or $c+d$ might have a carry making them $n/2+1$ digit numbers. For simplicity, we ignore this.

NOTE: In "real life" you would not recurse down to one digit, but down to the word size where the computer can do an atomic multiplication. (This comment holds for additions as well.) You can think of this as doing arithmetic in base 2^w, where w is the word size.

EXAMPLE of elementary school algorithm (with no additions until after all of the atomic multiplies):

```
  4352
  3748
    16
   40
  24
 32
    08
  20
 12
16
   14
 35
21
28
  06
 15
09
12
```

Concatenate the "even" and "odd" indexed values with each group.

```
  4352
  3748
  2416
 3240
  1208
1620
 2114
2835
 0906
1215
```

Now do the sum row-by-row. In general, this will take exactly n^2 atomic multiplications and $\sim 2n^2$ atomic additions.

EXAMPLE of alternative (recursive) algorithm.

```
 4352
 3748
```

Leaving out the recursion to produce the products of two 2-digit numbers:

$$ac = 37 \cdot 43 = 1591, \quad ad = 37 \cdot 52 = 1924, \quad bc = 48 \cdot 43 = 2064, \quad bd = 48 \cdot 52 = 2496, \quad ad + bc = 3988.$$

Concatenate ac with bd: 15912496.

The final sum is

```
15912496
  3988
```

EXAMPLE of full recursive algorithm.

```
 4352
 3748
```

$$\begin{aligned} u &= (a+b)(c+d) = (37+48)(43+52) = 85 \cdot 95 = 8075 \\ v &= ac = 37 \cdot 43 = 1591, \\ w &= bd = 48 \cdot 52 = 2496, \\ v+w &= ac + bd = 1591 + 2496 = 4087 \\ u-(v+w)) &= ad + bc = 8075 - 4087 = 3988 \end{aligned}$$

Now it is the same as the previous example.