Nov 3

Multiply two (large) integers

any constant size base enough

Assume: non negative integers expressed in bits

Ex: n=4

$a = 1101$ $\quad Dec(a) = 13$ $\quad Dec(a) \cdot Dec(b) = 39$

$b = 0011$ $\quad Dec(b) = 3$

```
  1101
x 0011
------
  1101
 1101
0000
0000
------
Dec(100111) = 39
  32168421
```

→ computing each row is $O(n)$

$\Rightarrow O(n^2)$ time for all n rows

→ Add up the n rows

$\Rightarrow O(n^2)$

$\Rightarrow$ Overall: $O(n^2) + O(n^2) = O(n^2)$

Goal: Do better than $O(n^2)$ time.

Input: $a = a_{n-1}, \ldots, a_0$ $\quad b = b_{n-1}, \ldots, b_0$

MSB ↗ ↖ LSB

$$Dec(a) = \sum_{i=0}^{n-1} a_i \cdot 2^i \qquad Dec(b) = \sum_{i=0}^{n-1} b_i \cdot 2^i$$

Output: $c = a \times b$ ($a \cdot b$ or ab)

To beat $O(n^2)$, we'll use a divide & conquer algo (Karatsuba's algo)

(Step 1:) $a = a_{n-1}, \ldots, a_0$

$a^0 = a_{\lceil \frac{n}{2} \rceil - 1}, \ldots, a_0$

$a^1 = a_{n-1}, \ldots, a_{\lceil \frac{n}{2} \rceil}$

$a = 11 : 01$

$a^1 : a^0$

$= 11 \quad = 01$

$Dec(a^1) = 3 \quad Dec(a^0) = 1$

$Dec(a^1) \cdot 2^{4/2} + Dec(a^0)$

$= 3 \cdot 2^2 + 1 = 3 \cdot 4 + 1 = 13$

Lemma: $Dec(a) = Dec(a^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + Dec(a^0)$

$Dec(a^0) = \sum_{j=0}^{\lceil \frac{n}{2} \rceil - 1} a_j \cdot 2^j$ ——— (1)

$a^0 = a_{\lceil \frac{n}{2} \rceil - 1}, \dots, a_0$

$a^1 = a_{n-1}, \dots, a_{\lceil \frac{n}{2} \rceil}$

$Dec(a^1) = a_{n-1} \cdot 2^{n-\lceil \frac{n}{2} \rceil - 1} + \dots + a_{\lceil \frac{n}{2} \rceil + 1} \cdot 2 + a_{\lceil \frac{n}{2} \rceil} \cdot 2^0$

$= \sum_{j=0}^{n-\lceil \frac{n}{2} \rceil - 1} a_{\lceil \frac{n}{2} \rceil + j} \cdot 2^j$

$\Rightarrow Dec(a^1) \cdot 2^{\lceil \frac{n}{2} \rceil} = 2^{\lceil \frac{n}{2} \rceil} \cdot \sum_{j=0}^{n-\lceil \frac{n}{2} \rceil - 1} a_{\lceil \frac{n}{2} \rceil + j} \cdot 2^j$

$= \sum_{j=0}^{n-\lceil \frac{n}{2} \rceil - 1} a_{\lceil \frac{n}{2} \rceil + j} \cdot 2^j \cdot 2^{\lceil \frac{n}{2} \rceil}$

$= \sum_{j=0}^{n-\lceil \frac{n}{2} \rceil - 1} a_{\lceil \frac{n}{2} \rceil + j} \cdot 2^{\lceil \frac{n}{2} \rceil + j}$

$i \leftarrow \lceil \frac{n}{2} \rceil + j$ →

$= \sum_{i=\lceil \frac{n}{2} \rceil}^{n-1} a_i \cdot 2^i$ ——— (2) =

$Dec(a) = \sum_{i=0}^{n-1} a_i \cdot 2^i$

$= \sum_{i=\lceil \frac{n}{2} \rceil}^{n-1} a_i \cdot 2^i + \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} a_i \cdot 2^i$

$= Dec(a^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + Dec(a^0)$ ∎

$Dec(b) = Dec(b^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + Dec(a^0)$.

$Dec(a) \cdot Dec(b) = (Dec(a^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + Dec(a^0)) \cdot (Dec(b^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + Dec(b^0))$

1 n bit mult

$= Dec(a^1) \cdot Dec(b^1) \cdot 2^{2\lceil \frac{n}{2} \rceil} + Dec(a^0) \cdot Dec(b^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + Dec(a^1) \cdot Dec(b^0) \cdot 2^{\lceil \frac{n}{2} \rceil} + Dec(a^0) \cdot Dec(b^0)$

$= Dec(a^1) \cdot Dec(b^1) \cdot 2^{2\lceil \frac{n}{2} \rceil} + (Dec(a^0) \cdot Dec(b^1) + Dec(a^1) \cdot Dec(b^0)) \cdot 2^{\lceil \frac{n}{2} \rceil} + Dec(a^0) \cdot Dec(b^0)$

4 $\frac{n}{2}$ bit mults.

1 n bit → 4 n bits → $O(n^2)$

1 n bit → 3 n bits → $O(n^{\log_2 3})$

mults

$O(n^{1.59...})$

~~$a^1 b^0 + a^0 b^1$~~ want: $a^1 b^0 + a^0 b^1$

$(a^1 + a^0) \cdot (b^1 + b^0)$

$\sim \frac{n}{2}$ bits $\sim \frac{n}{2}$ bits

$= a^1 \cdot b^1 + a^1 \cdot b^0 + a^0 \cdot b^1 + a^0 \cdot b^0$

$\Rightarrow a^1 \cdot b^0 + a^0 \cdot b^1 = (a^1 + a^0) \cdot (b^1 + b^0) - a^1 \cdot b^1 - a^0 \cdot b^0$