Nov 1

Multiply two (large) integers

any $O(1)$ size base.

Assume: non-negative expressed in bits

EX: $n=4$

$$\overset{\cdots 8\,4\,2\,1}{}$$

$a = 1101$ $\quad Dec(a) = 13$ $\quad Dec(a) \cdot Dec(b) = 13 \cdot 3 = 39$

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

```
    1101
  x 0011
  ------
    1101    -> computing each row is O(n)
   1101          -> over all rows : O(n^2)
  0000      -> Add up all the n rows
 0000            => ~~overall~~ adding takes O(n^2)
 ------
Dec(100111) = 39  => OVERALL: O(n^2) + O(n^2) = O(n^2)
   32 16 8 4 2 1
```

n rows

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

Input: $a = a_{n-1}, \overset{2^i}{a_i}, a_0$ $\quad b = b_{n-1}, \ldots, b_0$

MSB LSB

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

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

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

Step 1: $a = \underbrace{a_{n-1},}_{a^L} \mid \underbrace{\ldots, a_0}_{a^R}$

$2^{\lceil \frac{n}{2} \rceil - 1}$ $\quad \lceil \frac{n}{2} \rceil$ bits $\quad 1$

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

$2^{\lceil \frac{n}{2} \rceil - 1} \ldots 2 \quad 1$

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

$a = 11 \mid 01$

$a^L = 11 \mid a^R = 01$

$Dec(a^L) = 3$ $\quad Dec(a^R) = 1$

$Dec(a^L) \times 2^{4/2} + Dec(a^R) \cdot 1$

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

$= Dec(a)$

Lemma: For any $a = a_{n-1}, \dots, a_0$

$$\mathrm{Dec}(a) = \mathrm{Dec}(a^L) \cdot 2^{\lceil \frac{n}{2} \rceil} + \mathrm{Dec}(a^R)$$

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

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

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

$$\mathrm{Dec}(a^L) \cdot 2^{\lceil \frac{n}{2} \rceil} = 2^{\lceil \frac{n}{2} \rceil} \cdot \mathrm{Dec}(a^L)$$

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

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

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

$$i \leftarrow \lceil \tfrac{n}{2} \rceil + j \;\longrightarrow\; = \sum_{i=\lceil \frac{n}{2} \rceil}^{n-1} a_i \cdot 2^i$$

$$\mathrm{Dec}(a^L) \cdot 2^{\lceil \frac{n}{2} \rceil} + \mathrm{Dec}(a^R)$$

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

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

$$\mathrm{Dec}(a) = \mathrm{Dec}(a^L) \cdot 2^{\lceil \frac{n}{2} \rceil} + \mathrm{Dec}(a^R)$$

$$\mathrm{Dec}(b) = \mathrm{Dec}(b^L) \cdot 2^{\lceil \frac{n}{2} \rceil} + \mathrm{Dec}(b^R)$$

$$\mathrm{Dec}(a) \cdot \mathrm{Dec}(b) = \left(\mathrm{Dec}(a^L) \cdot 2^{\lceil \frac{n}{2} \rceil} + \mathrm{Dec}(a^R)\right) \cdot \left(\mathrm{Dec}(b^L) \cdot 2^{\lceil \frac{n}{2} \rceil} + \mathrm{Dec}(b^R)\right)$$

1 n-bit mult

$$= \mathrm{Dec}(a^L) \cdot \mathrm{Dec}(b^L) \cdot 2^{2\lceil \frac{n}{2} \rceil} + \mathrm{Dec}(a^L) \cdot \mathrm{Dec}(b^R) \cdot 2^{\lceil \frac{n}{2} \rceil} + \mathrm{Dec}(a^R) \cdot \mathrm{Dec}(b^L) \cdot 2^{\lceil \frac{n}{2} \rceil} + \mathrm{Dec}(a^R) \cdot \mathrm{Dec}(b^R$$

$$= \mathrm{Dec}(a^L) \cdot \mathrm{Dec}(b^L) \cdot 2^{2\lceil \frac{n}{2} \rceil} + \left(\mathrm{Dec}(a^L) \cdot \mathrm{Dec}(b^R) + \mathrm{Dec}(a^R) \cdot \mathrm{Dec}(b^L)\right) \cdot 2^{\lceil \frac{n}{2}} + \mathrm{Dec}(a^R) \cdot \mathrm{Dec}(b^R)$$

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

1 n-bit mult $\Rightarrow$ 4 $\frac{n}{2}$ bit mult $\Rightarrow O(n^2)$

1 ———— $\Rightarrow$ 3 $\frac{n}{2}$ bit mults $\Rightarrow O(n^{\log_2 3})$

$\leq O(n^{1.59})$

Karatsuba's algo

~~Ga~~ Want: $\mathrm{Dec}(a^L) \cdot \mathrm{Dec}(b^R) + \mathrm{Dec}(a^R) \cdot \mathrm{Dec}(b^L)$

$$\underbrace{(a^L + a^R)}_{\sim \frac{n}{2} \text{ bits}} \cdot \underbrace{(b^L + b^R)} = a^L \cdot b^L + \underbrace{a^L \cdot b^R + a^R \cdot b^L} + a^R \cdot b^R$$

$$a^L \cdot b^R + a^R \cdot b^L = (a^L + a^R) \cdot (b^L + b^R) - a^L \cdot b^L - a^R \cdot b^R$$