Oct 31

Multiply two (large) integers

Any constant base is fine

Assume: non-negative integers represented in bits

Ex. ($n=4$)

$a = 1101 \quad Dec(a) = 13$

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

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

```
    1101
  x 0011
  ------
    1101
   1101
  0000
 0000
```

n rows

$\leftarrow$ each row $O(n)$

$\Rightarrow O(n^2)$ to compute all n rows

$\Rightarrow$ Add all n rows

$\Rightarrow O(n^2)$ to add them

$Dec(\underset{32}{1}\ \underset{16}{0}\ \underset{8}{0}\ \underset{4}{1}\ \underset{2}{1}\ \underset{1}{1}) = 39$

Overall: $O(n^2) + O(n^2) = O(n^2)$.

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

Input: $a = a_{n-1}, \dots, a_0$ (MSB: a_{n-1}, LSB: a_0) $\qquad b = b_{n-1}, \dots, b_0$

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

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

Elementary school ~~al~~ algo: $O(n^2)$

To beat $O(n^2)$ we'll use Divide & Conquer algo (Karatsuba's algo)

Step 1: $a = a_{n-1}, \dots, a_0$

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

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

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

$a = 11 \,\vdots\, 01$ ($a^1 \mid a^0$)

$Dec(a^1) = 3$

$Dec(a^0) = 1$

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

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

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

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

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

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

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

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

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

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

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

② ①

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

∎

$b^0 = b_{\lceil \frac{n}{2} \rceil - 1}, \ldots, b_0 \qquad b^1 = b_{n-1}, \ldots, b_{\lceil \frac{n}{2} \rceil}$

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

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

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

$\equiv$

$$\underset{\substack{\uparrow \\ 1 \text{ n bit mult}}}{a \cdot b} = \underset{\substack{\uparrow \\ \frac{n}{2} \text{ bits mult}}}{\underline{a^1 \cdot b^1}} \cdot 2^{2\lceil \frac{n}{2} \rceil} + \boxed{(a^0 \cdot b^1 + a^1 \cdot b^0)} \cdot 2^{\lceil \frac{n}{2} \rceil} + \underline{a^0 \cdot b^0}$$

1 n bit $\rightarrow 4$ $\frac{n}{2}$ bit $\rightarrow O(n^2)$

$\rightarrow 3$ $\frac{n}{2}$ bit $\quad O(n^{\log_2 3})$ < 2

Key identity: $\underbrace{(a^1 + a^0)}_{\sim \frac{n}{2} \text{ bits}} \cdot \underbrace{(b^1 + b^0)}_{\sim \frac{n}{2} \text{ bits}}$

$$= a^1 \cdot b^1 + \boxed{a^1 \cdot b^0 + a^0 \cdot b^1} + a^0 \cdot b^0$$

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

3 $\frac{n}{2}$ bit mults