Apr 3

Multiply two (large) integers

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

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

$b = b_{n-1}, \ldots, b_0$

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

Output: $c = a \times b$ $(a.b, ab)$

Ex: $a = 1101$ $Dec(a) = 13$

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

Elementary school mult. algo

$$\begin{array}{r} 1101 \\ \times\ 0011 \\ \hline 1101 \\ 1101\ \ \\ 0000\ \ \ \\ +\ 0000\ \ \ \ \\ \hline Dec(1001\,11) = 39 \end{array}$$

n rows

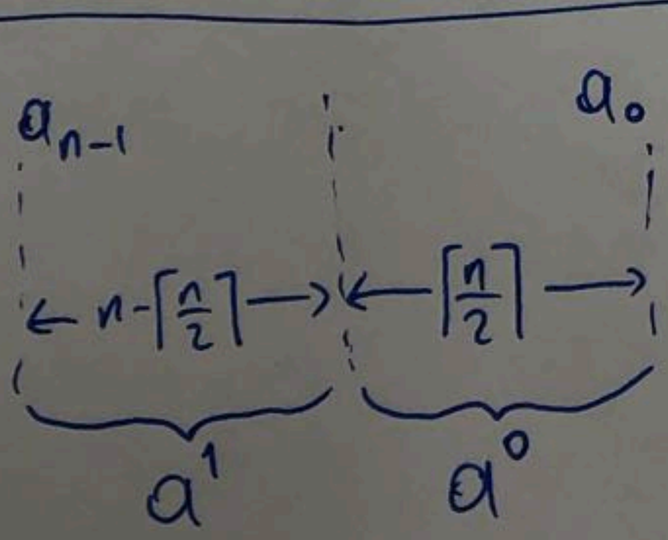
$O(n^2)$ overall

each row $O(n)$

Goal: Beat the $O(n^2)$ runtime

Use Divide & Conquer

Step 1: Divide a & b into 2 $\frac{n}{2}$-bit number each



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

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

Ex. $a = 1001$ $a^1 = 10$ $Dec(a^1) = 2$

$a^0 = 01$ $Dec(a^0) = 1$

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

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

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

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

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

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

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

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

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

Similarly $b' = b_{n-1} \dots b_{\lceil \frac{n}{2} \rceil}$

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

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

Ex: $a = 1001$

$Dec(a) = 9$

$Dec(a') = 2$

$Dec(a^0) = 1$

$$2^{\lceil \frac{4}{2} \rceil} \cdot 2 + 1 = 2^2 \cdot 2 + 1$$

$$= 9$$

Let's expand on $a.b$

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

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

$\equiv$

$$a.b = \underbrace{a^1.b^1}_{1}.2^{2\lceil \frac{n}{2} \rceil} + \underbrace{(a^1.b^0 + a^0.b^1)}_{2}.2^{\lceil \frac{n}{2} \rceil} + \underbrace{a^0.b^0}_{3}$$

1 n-bit mult $\Longrightarrow$ 4 $\frac{n}{2}$-bit mult.

Key identity: $(a^1+a^0)(b^1+b^0) = \underbrace{a^1b^1}_{1} + \underbrace{a^1b^0 + a^0b^1}_{2} + \underbrace{a^0b^0}_{3}$

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