

Nov 9

Multiply two (large) numbers

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

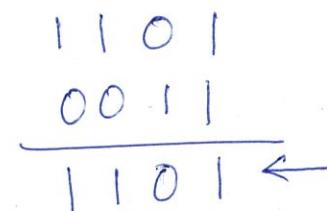
$$\text{Dec}(a) = \sum_{i=0}^{n-1} a_i \cdot 2^i$$

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

Output: $c = a \cdot b$

Ex: $a = 1101$ $\text{Dec}(a) = 13$
 $b = 0011$ $\text{Dec}(b) = 3$

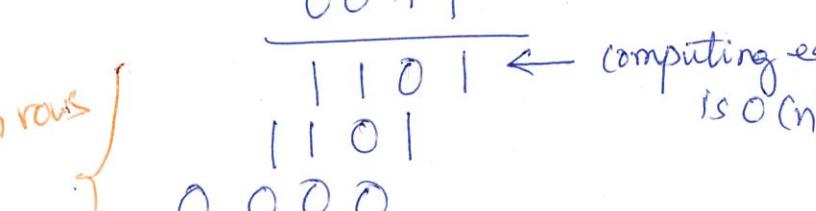
$O(n^2)$

Elementary school mult. algo =  time

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

Use Divide & Conquer algo

Step 1: Divide a and b into 2 equal halves

n rows } 

$$\begin{array}{r}
 1101 \\
 0011 \\
 \hline
 1101 \\
 1101 \\
 0000 \\
 0000 \\
 \hline
 \text{Dec}(100111) = 39
 \end{array}$$

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

$\xrightarrow{\lceil n/2 \rceil}$

a^1 a^0

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

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

Ex: $a = 1101$ $a^1 = 11$
 $\text{Dec}(a^1) = 3$ $a^0 = 01$
 $\text{Dec}(a^0) = 1$

Claim: $\text{Dec}(a) = \text{Dec}(a^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + \text{Dec}(a^0)$ LHS = 43

$\text{Dec}(a^0) = \sum_{j=0}^{\lceil \frac{n}{2} \rceil-1} a_j \cdot 2^j$ RHS = $3 \cdot 2^{\lceil \frac{n}{2} \rceil} + 1$

$\text{Dec}(a^1) = \sum_{j=0}^{n-\lceil \frac{n}{2} \rceil-1} a_{j+\lceil \frac{n}{2} \rceil} \cdot 2^j \equiv \sum_{i=\lceil \frac{n}{2} \rceil}^{n-1} a_i \cdot 2^{i-\lceil \frac{n}{2} \rceil}$ $= 3 \cdot 4 + 1 = 13 \checkmark$

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

$$\begin{aligned}
 \text{Dec}(a) &= \sum_{i=0}^{n-1} a_i \cdot 2^i \\
 &= \sum_{i=\lceil \frac{n}{2} \rceil}^{n-1} a_i \cdot 2^i + \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} a_i \cdot 2^i \\
 &= \text{Dec}(a^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + \text{Dec}(a^0)
 \end{aligned}$$

Similarly $b^0 = b_{\lceil \frac{n}{2} \rceil - 1}, \dots, b_0$ $\text{Dec}(b) = \text{Dec}(b^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + \text{Dec}(b^0)$

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

Let's expand out $a \circ b$

$$\begin{aligned}
 \text{Dec}(a) \circ \text{Dec}(b) &= (\text{Dec}(a^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + \text{Dec}(a^0)) (\text{Dec}(b^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + \text{Dec}(b^0)) \\
 &= \text{Dec}(a^1) \cdot \text{Dec}(b^1) \cdot 2^{2\lceil \frac{n}{2} \rceil} + \text{Dec}(a^1) \cdot \text{Dec}(b^0) \cdot 2^{\lceil \frac{n}{2} \rceil} \\
 &\quad + \text{Dec}(a^0) \cdot \text{Dec}(b^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + \text{Dec}(a^0) \cdot \text{Dec}(b^0)
 \end{aligned}$$

$$\stackrel{6}{=} a \circ b = a^1 \circ b^1 \cdot 2^{2\lceil \frac{n}{2} \rceil} + (a^1 \circ b^0 + a^0 \circ b^1) 2^{\lceil \frac{n}{2} \rceil} + a^0 \circ b^0$$

n-bit mult
 $\frac{n}{2}$ -bit mult

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

Key identity:

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

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