Oct 28

Multiply two (large) integers

Input: $a = a_{n-1}, \dots, a_0$ (MSB ↗, LSB ↖) $\quad Dec(a) = \sum_{i=0}^{n-1} a_i \cdot 2^i$

$b = b_{n-1}, \dots, b_0 \quad Dec(b) = \sum_{i=0}^{n-1} b_i \cdot 2^i$

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

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

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

$O(n^2)$ overall

```
  1101
 x0011
------
  1101   <- each row O(n)
  1101
  0000
 0000
------
 100111
```

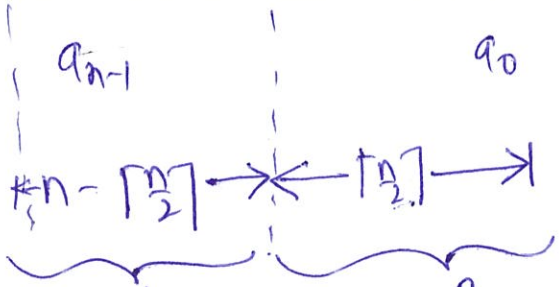
$Dec(100111) = 39$

Elementary school mult. algo: n rows

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

Use Divide & Conquer algo

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



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

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

Ex: $a = 1101 \quad a^1 = 11 \quad Dec(a^1) = 3$

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

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

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

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

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

$i = j + \lceil \frac{n}{2} \rceil$ ↘

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

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

Ex: $a = 1101$, $Dec(a) = 13$, $Dec(a^1) = 3$, $Dec(a^0) = 1$

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

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

$$\rightarrow 2^{\lceil \frac{4}{2} \rceil} \cdot 3 + 1 = 2^2 \cdot 3 + 1 = 4 \cdot 3 + 1 = 13$$

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

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

Let's expand on $a \cdot b$

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

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

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

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

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

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