Nov 7

Multiply two (large) integers

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

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

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

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

Output: $c = a \cdot b$

E.g.: $a = 1101$ $\quad Dec(1101) = 13$

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

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

$Dec(1\,0\,0\,1\,1\,1) = 32+4+2+1 = 39$

$\Rightarrow O(n^2)$ multiplication in general.

Goal: Beat $O(n^2)$

↳ Divide & Conquer.

Step 1: Divide a ($\& b$) in 2 equal halves

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

$n - \lceil \frac{n}{2} \rceil$ | $\lceil \frac{n}{2} \rceil$

a^1 | a^0

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

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

ex $a = 1101$

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

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

$Dec(a) = 13 = 3 \times 4 + 1 = 3 \times 2^2 + 1$

Claim:

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

Pf: $Dec(a^0) = \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} a_i \cdot 2^i$

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

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

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

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

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

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

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

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

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

$$\equiv$$

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

$a \cdot b$: n bits; $a^0 \cdot b^0$, $a^0 \cdot b^1$, $a^1 \cdot b^0$, $a^1 \cdot b^1$: $\sim \frac{n}{2}$ bits

Key identity:

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

$\sim \frac{n}{2}$ mult

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

$\sim n/2$ mult $\quad \sim \frac{n}{2}$ mult

$11 \cdot 2 \qquad 110$

$= 3 \qquad = 6$