Nov 6

Multiply two (large) integers

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

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

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

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

Output: $c = a \cdot b$

Ex. $a = 1101$, $b = 0011$

$\text{Dec}(a) = 13$, $\text{Dec}(b) = 3$

Overall $O(n^2)$

Elementary school mult. algo:

$$\begin{array}{r} 1\,1\,0\,1 \\ \times\ 0\,0\,1\,1 \\ \hline 1\,1\,0\,1 \\ 1\,1\,0\,1 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \\ \hline \text{Dec}(1\,0\,0\,1\,1\,1) = 39 \end{array}$$

↑ computing each row: $O(n)$

Goal: Beat $O(n^2)$

↳ Divide & Conquer

Step 1: Divide a & b into 2 equal halves

$a = a_{n-1} \ldots a_0$ (split: $n - \lceil \frac{n}{2} \rceil$ | $\lceil \frac{n}{2} \rceil$)

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

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

Ex. $a = 1101$, $a^1 = 11$, $\text{Dec}(a^1) = 3$

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

$a^0 = 01$ ↖ $\text{Dec}(a^0) = 1$

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

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

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

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

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

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

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

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

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

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

Expand the product $a \cdot b$

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

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

Equivalent:

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

$a \cdot b$: n bit mult

$a^0 \cdot b^0$: $\sim \frac{n}{2}$ bit mult.

Key Identity:

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

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