April 11

# Multiplying two (large) integers/numbers

Assume integers are represented in binary.

$a = 1001$ $\quad Dec(a) = 9 \quad Dec(a) \cdot Dec(b)$

$b = 0011$ $\quad Dec(b) = 3 \quad = 9 \cdot 3 = 27$

$$\begin{array}{r} 1001 \\ 0011 \\ \hline 1001 \\ 1001\phantom{0} \\ 0000\phantom{00} \\ 0000\phantom{000} \\ \hline \end{array}$$

n rows

$Dec(0011011) = 27$

Computation of n rows: $O(n^2)$

Adding n rows: $O(n^2)$

Total cost: $O(n^2)$

$a = 1001$

$1 \times 2^0 +$
$0 \times 2^1 +$
$0 \times 2^2 +$
$1 \times 2^3$

$= \sum_{i=0}^{4-1} a_i \times 2^i$

---

Input: $a = a_{n-1} \cdots a_0$ (MSB: $a_{n-1}$, LSB: $a_0$) $\quad b = b_{n-1} \cdots b_0$

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

Naive integer mult algo: $O(n^2)$

Goal: Beat $O(n^2)$ algo.

Idea: Use Divide & conquer.

Divide the n-bit a & b to two roughly $\frac{n}{2}$-bit numbers.

n=4 $\quad a = 10 \mid 01$ ($a^1 \mid a^0$) $\quad Dec(a^0) = 1 \quad Dec(a^1) = 2$

$Dec(a) = 9$
$= 2 \cdot 2^2 + 1$
$= Dec(a^1) \cdot 2^{4/2} + Dec(a^0)$

$a^1 = 10$

$a = a_{n-1} \cdots a_0$

$a^1 = a_{n-1} \cdots a_{\lceil \frac{n}{2} \rceil}$ ← # bits $n - \lceil \frac{n}{2} \rceil$

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

<u>lemma</u> : $\mathrm{Dec}(a) = \mathrm{Dec}(a^1) \cdot 2^{\lceil \frac{n}{2} \rceil} + \mathrm{Dec}(a^0)$

$$\mathrm{Dec}(a^0) = a_{\lceil \frac{n}{2} \rceil - 1} \cdot 2^{\lceil \frac{n}{2} \rceil - 1} + \cdots + a_1 \cdot 2^1 + a_0 \cdot 2^0 = \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} a_i \cdot 2^i$$

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

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

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

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

$i = n - \cancel{\lceil \frac{n}{2} \rceil} - 1 + \cancel{\lceil \frac{n}{2} \rceil} = n-1$

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

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

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

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

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

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

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

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

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

$$\underset{\substack{\uparrow \\ \text{1 mult} \\ \text{of } n\text{-bit} \\ \text{number}}}{a \cdot b} = \underbrace{\underline{a^1} \cdot b^1 \cdot 2^{\lceil \frac{n}{2} \rceil} + (\underline{a^1} \cdot b^0 + b^1 \cdot \underline{a^0}) \cdot 2^{\lceil \frac{n}{2} \rceil} + \underline{a^0} \cdot b^0}_{\text{4 mults of } \frac{n}{2}\text{-bit numbers.}}$$