

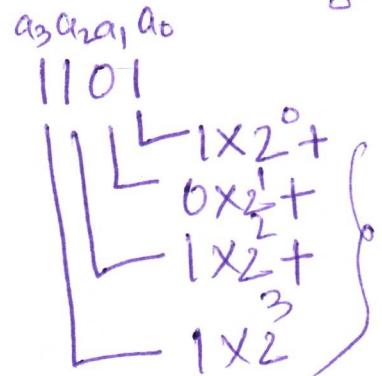
April 10Multiplying two (large) numbers

Assume: Integers are represented in binary.

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

$b = 0011 \quad \text{Dec}(b) = 3$

$\text{Dec}(a) \cdot \text{Dec}(b) = 13 \cdot 3 = 39$



$\begin{array}{r} 1101 \\ 0011 \\ \hline 1101 \\ 0000 \\ 0000 \\ \hline 10100111 \end{array}$

$\rightarrow O(n)$ time for each row;
 $O(n^2)$ to compute n rows. $= \sum_{i=0}^{n-1} a_i \cdot 2^i$
 Adding n rows is $O(n^2)$
 Overall: $O(n^2)$

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

$\uparrow \text{MSB}$ $\uparrow \text{LSB}$

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

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

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

Elementary school mult alg.: $O(n^2)$

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

Idea: Use divide & conquer approach (Karatsuba algo.)

Step 1° Divide $a \in b$ each into 2 roughly $\frac{n}{2}$ -bit numbers.

Ex:

$$\begin{array}{c|c|c} & 1 & 1 \\ & \hline a^1 & | & 0 \\ & a^0 & \end{array}$$

$$\begin{aligned} \text{Dec}(a^1) &= 3 \\ \text{Dec}(a^0) &= 1 \end{aligned} \quad \left. \begin{aligned} &\text{Dec}(a^1) \cdot 2^{\frac{n}{2}} + \text{Dec}(a^0) \\ &= 3 \cdot 2^{\frac{n}{2}} + 1 = 13 \\ &= \text{Dec}(a) \end{aligned} \right\}$$

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

$$\begin{aligned} \overset{\# \text{bits}}{=} n - \lceil \frac{n}{2} \rceil & \quad a^0 = a_{\lceil \frac{n}{2} \rceil - 1} \dots a_0 \\ a^1 = a_{\lceil \frac{n}{2} \rceil} \dots a_{\lceil \frac{n}{2} \rceil} & \end{aligned}$$

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

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

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

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

$$\Rightarrow \begin{aligned} i &= \lceil \frac{n}{2} \rceil + j \\ &= \sum_{i=\lceil \frac{n}{2} \rceil}^{n-1} a_i \cdot 2^i \end{aligned}$$

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

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

$$= \text{Dec}(a^l) \cdot 2^{\lceil n/2 \rceil} + \text{Dec}(a^o)$$

□

$$b = b_{n-1} \dots b_0$$

$$\text{Dec}(b) = \text{Dec}(b^l) \cdot 2^{\lceil n/2 \rceil} + \text{Dec}(b^o)$$

$$b^l = b_{\lceil n/2 \rceil - 1} \dots b_0$$

$$b^o = b_{n-1} \dots b_{\lceil n/2 \rceil}$$

$$\text{Dec}(a) \cdot \text{Dec}(b) = (\text{Dec}(a^l) \cdot 2^{\lceil n/2 \rceil} + \text{Dec}(a^o)) \cdot$$

$$(\text{Dec}(b^l) \cdot 2^{\lceil n/2 \rceil} + \text{Dec}(b^o))$$