Nov 1

Multiply two (large) numbers

Assume: integer represented in binary

any constant sized base is fine.

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

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

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

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

n rows

$\leftarrow O(n)$ for each row $\quad O(n^2)$ to compute all n rows

Adding all n rows is $O(n^2)$

overall: $O(n^2)$

$Dec(100111) = 39$

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

MSB LSB

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

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

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

Goal: Beat the $\Theta(n^2)$ time algo.

Idea: Use divide & conquer algo (Karatsuba's algo)

Step 1: Divide a & b ~~in~~ each into 2 roughly $\frac{n}{2}$-bit numbers

$a = 11 \mid 01$ $\qquad Dec(a^1) = 3 \rightarrow Dec(a^1) \cdot 2^{4/2} + Dec(a^0)$

$\quad\; a^1 \mid a^0$ $\qquad Dec(a^0) = 1 \qquad = 3 \cdot 4 + 1$

$= 12 + 1 = 13 = Dec(a)$

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

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

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

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

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

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

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

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

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

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

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

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

$$\mathrm{Dec}(b) = \mathrm{Dec}(b^1)\cdot 2^{\lceil \frac{n}{2}\rceil} + \mathrm{Dec}(b^0) \quad \Big| \quad b^0 = b_{\lceil \frac{n}{2}\rceil - 1}, \ldots, b_0$$

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

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

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

$\equiv$

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

1 mult of n bit numbers

rewrite:

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

4 mults of $\frac{n}{2}$-bit numbers

Key identity: $(a^1 + a^0)(b^1 + b^0)$

$$= \underbrace{a^1 b^1}_{1} + (a^1 b^0 + a^0 b^1) + \underbrace{a^0 b^0}_{2}$$

$$a^1 b^0 + a^0 b^1 = \underbrace{(a^1 + a^0)\cdot (b^1 + b^0)}_{3} - a^1 b^1 - a^0 b^0$$