Apr 2

Multiplying two (large) integers

Input: $a = a_{n-1} \cdots\cdots a_0$ $\quad Dec(a) = \sum_{i=0}^{n-1} a_i \cdot 2^i$

MSB (a_{n-1}), LSB (a_0)

$b = b_{n-1} \cdots\cdots b_0$ $\quad Dec(b) = \sum_{i=0}^{n-1} b_i \cdot 2^i$

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

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

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

$$
\begin{array}{r}
1\;1\;0\;1 \\
\times\quad 0\;0\;1\;1 \\
\hline
1\;1\;0\;1 \\
1\;1\;0\;1 \\
0\;0\;0\;0 \\
+\;0\;0\;0\;0 \\
\hline
\end{array}
$$

each row is $O(n)$

n rows

Elementary school mult. alg.

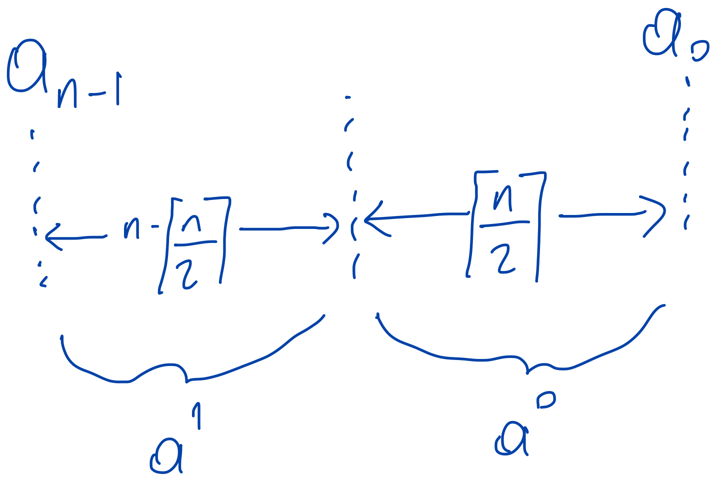
$Dec(1\;0\;0\;1\;1\;1) = 39$

$O(n^2)$ overall

Goal: Beat the $O(n^2)$ runtime.

Use Divide & Conquer.

Step 1: Divide a & b into 2 $\frac{n}{2}$ bit numbers



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

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

Ex. $a = 1001$

$a^1 = 10 \quad Dec(a^1) = 2$

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

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

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

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

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

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

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

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

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

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

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

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

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

Ex.

$a = 1001$

$Dec(a) = 9$

$Dec(a^1) = 2$

$Dec(a^0) = 1$

$2^{\lceil \frac{4}{2} \rceil} \cdot 2 + 1 = 2^2 \cdot 2 + 1$

$= 9$

Let's expand on a.b

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

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

$$\equiv$$

$$a.b = \underbrace{a^1.b^1}_{1}.2^{2\lceil \frac{n}{2} \rceil} + \underbrace{(a^1b^0 + a^0b^1)}_{2}.2^{\lceil \frac{n}{2} \rceil} + \underbrace{a^0b^0}_{3}$$

1 n-bit mult $\Rightarrow$ 4 $\frac{n}{2}$ bit mult.

Key identity: $(a^1 + a^0)(b^1 + b^0) = \underbrace{a^1b^1}_{1} + \underbrace{a^1b^0 + a^0b^1}_{2} + \underbrace{a^0b^0}_{3}$

$$\boxed{a^1b^0 + a^0b^1 = (a^1 + a^0)(b^1 + b^0) - a^1b^1 - a^0b^0}$$