Nov 9

Multiply two (large) numbers

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

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

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

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

Output: $c = a \cdot b$

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

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

Elementary school mult. algo:

```
      1101
      0011
    ------
      1101   <- computing each row is O(n)
     1101
    0000
   0000
  --------
  Dec(100111) = 39
```

n rows

$O(n^2)$ time

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

Use Divide & Conquer algo

Step 1: Divide a and b into 2 equal halves

$a = \underbrace{a_{n-1}, \ldots}_{a^1} \mid \underbrace{\ldots, a_0}_{a^0}$

$\leftarrow n - \lceil \frac{n}{2} \rceil \rightarrow \quad \leftarrow \lceil \frac{n}{2} \rceil \rightarrow$

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

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

Ex: $a = 1101$ $\quad a^1 = 11$

$a^0 = 01$

$\mathrm{Dec}(a^1) = 3$

$\mathrm{Dec}(a^0) = 1$

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

LHS $= 13$

RHS $= 3 \cdot 2^{4/2} + 1$

$= 3 \cdot 4 + 1 = 13$ ✓

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

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

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

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

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

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

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

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

Let's expand out $\quad a \cdot b$

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

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

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

$$\equiv \underbrace{a \cdot b}_{n \text{ bit mult}} = a^1 \underbrace{\cdot}_{\frac{n}{2}\text{-bit mult}} b^1 \cdot 2^{2\lceil \frac{n}{2} \rceil} + (\boxed{a^1 \cdot b^0 + a^0 \cdot b^1})\, 2^{\lceil \frac{n}{2} \rceil} + a^0 \cdot b^0$$

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

3

Key identity:

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

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