April 10

Multiplying two (large) numbers

Assume: Integers are represented in binary. ← Any constant size done in time.

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

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

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

$a_3 a_2 a_1 a_0$

1101

$1 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 + 1 \times 2^3 = 13 = \sum_{i=0}^{n-1} a_i \cdot 2^i$

```
   1101
   0011
  -----
   1101   -> O(n) time for each row;
  1101       O(n^2) to compute n rows.
 0000        Adding n rows is O(n^2)
0000         overall: O(n^2)
```

n rows

$Dec(0100111) = 39$

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

a_{n-1} ← MSB, a_0 ← LSB

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

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

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

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

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

Step 1: Divide a & b each into 2 roughly $n/2$-bit numbers.

Ex: $1\,1 \mid 0\,1$; $a^1 \mid a^0$

$Dec(a^1) = 3$, $Dec(a^0) = 1$

$Dec(a^1) \cdot 2^{4/2} + Dec(a^0) = 3 \cdot 2^2 + 1 = 13 = Dec(a)$

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

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

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

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

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

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

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

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

$\Rightarrow i = \lceil n/2 \rceil + j$

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

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

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

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

$\square$

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

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

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

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

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