Algorithm & Data Structure Analysis

Lecture 3: Recursive Multiplication

Overview

- Last week:
  - School method addition
  - School method multiplication

Overview

- Last week:
  - School method addition
  - School method multiplication
- This week:
  - Recursive multiplication
  - Karatsuba multiplication

Overview

- Last week:
  - School method addition
  - School method multiplication
- This week:
  - Recursive multiplication
  - Karatsuba multiplication Wednesday

Overview

- Last week:
  - School method addition
  - School method multiplication
- This week:
  - Recursive multiplication $\leftarrow$ Today
  - Karatsuba multiplication Wednesday

Examples of recursion

- Compute the sum of the first n positive integers

Examples of recursion

- Compute the sum of the first n positive integers

  procedure sum(n)

  if $n = 1$ **return** 1

  else return n + sum(n-1)

Examples of recursion

- Compute the sum of the first n positive integers

  procedure sum(n)

  if $n = 1$ **return** 1

  else return n + sum(n-1)

- Compute n factorial

  procedure factorial(n)

  if $n = 1$ **return** 1

  else return $n *$ factorial(n-1)

Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.

Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves

Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves

$$a = 1234 \qquad \times \qquad b = 5678$$

Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves

$$a = 1234 \qquad \times \qquad b = 5678$$

$$a_1 = 12 \qquad\qquad a_0 = 34$$

Ideas for recursive multiplication

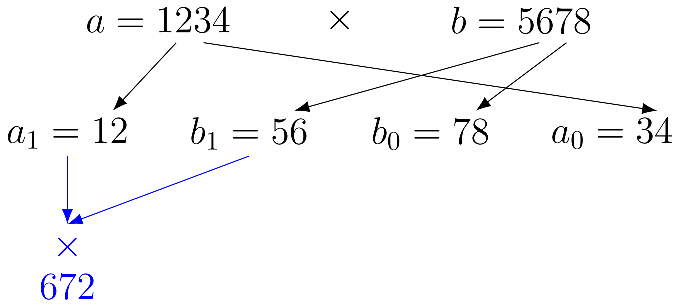
Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves

$$a = 1234 \qquad \times \qquad b = 5678$$

$$a_1 = 12 \qquad b_1 = 56 \qquad b_0 = 78 \qquad a_0 = 34$$

Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves



Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves

$$a = 1234 \qquad \times \qquad b = 5678$$

$$a_1 = 12 \qquad b_1 = 56 \qquad b_0 = 78 \qquad a_0 = 34$$

$$\times \qquad \times$$

$$672 \qquad 936$$

Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves

$$a = 1234 \qquad \times \qquad b = 5678$$

$$a_1 = 12 \qquad b_1 = 56 \qquad b_0 = 78 \qquad a_0 = 34$$

$$\times \qquad \times \qquad \times$$

$$672 \qquad 936 \qquad 1904$$

Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves

$$a = 1234 \qquad \times \qquad b = 5678$$

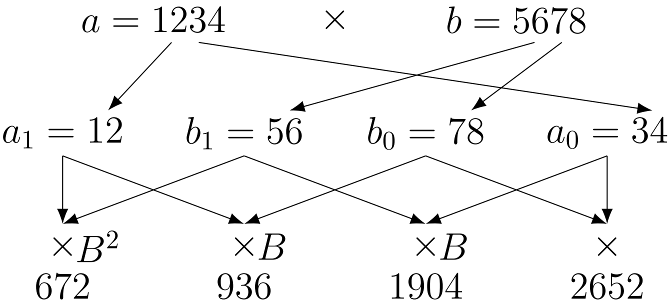
$$a_1 = 12 \qquad b_1 = 56 \qquad b_0 = 78 \qquad a_0 = 34$$

$$\times \qquad \times \qquad \times \qquad \times$$

$$672 \qquad 936 \qquad 1904 \qquad 2652$$

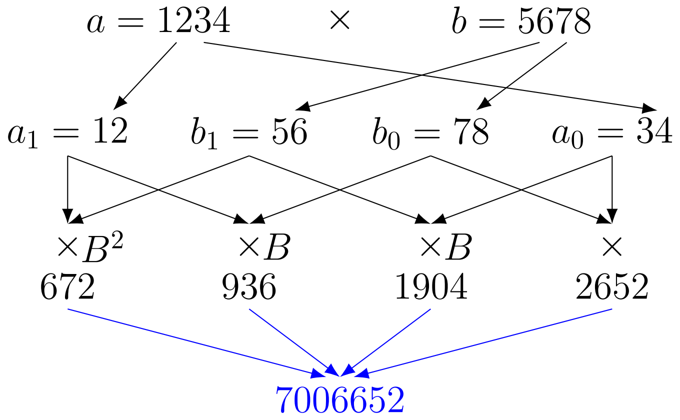
Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves



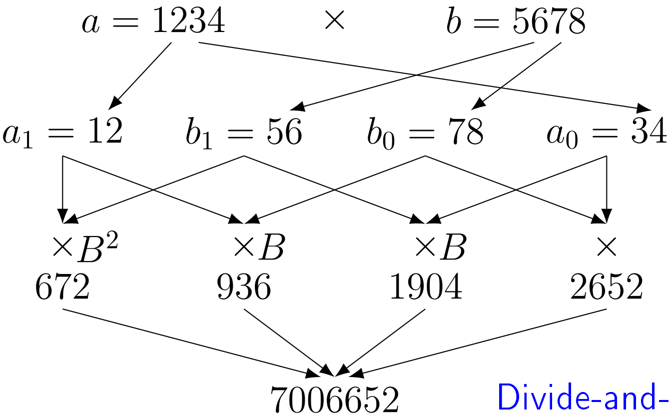
Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves



Ideas for recursive multiplication

Let $a = 1234$ and $b = 5678$. Compute $a \times b$.
Split a and b into halves



Divide-and-Conquer!

Recursion: divide

Let a and b be n-digit integers

Recursion: divide

Let a and b be n-digit integers

- Compute $k = \lfloor n/2 \rfloor$

Recursion: divide

Let a and b be n-digit integers

- Compute $k = \lfloor n/2 \rfloor$
- Split a into two integers a_0 and a_1 where
  - a_0 consists of the least k significant digits
  - a_1 consists of the most $n - k$ significant digits

Recursion: divide

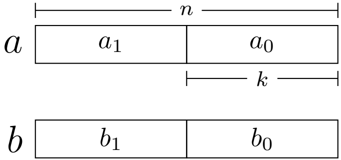
Let a and b be n-digit integers

- Compute $k = \lfloor n/2 \rfloor$
- Split a into two integers a_0 and a_1 where
  - a_0 consists of the least k significant digits
  - a_1 consists of the most $n - k$ significant digits
- Do the same for b to obtain b_0 and b_1

Recursion: divide

Let a and b be n-digit integers

- Compute $k = \lfloor n/2 \rfloor$
- Split a into two integers a_0 and a_1 where
  - a_0 consists of the least k significant digits
  - a_1 consists of the most $n - k$ significant digits
- Do the same for b to obtain b_0 and b_1



$$a = a_1 \cdot B^k + a_0$$

$$b = b_1 \cdot B^k + b_0$$

Recursion: conquer

$$a \times b = (a_1 \cdot B^k + a_0) \times (b_1 \cdot B^k + b_0)$$

Recursion: conquer

$$
\begin{aligned}
a \times b &= (a_1 \cdot B^k + a_0) \times (b_1 \cdot B^k + b_0) \\
&= a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0
\end{aligned}
$$

Recursion: conquer

$$
\begin{aligned}
a \times b &= (a_1 \cdot B^k + a_0) \times (b_1 \cdot B^k + b_0) \\
&= a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0
\end{aligned}
$$

Procedure:

Recursion: conquer

$$\begin{aligned} a \times b &= (a_1 \cdot B^k + a_0) \times (b_1 \cdot B^k + b_0) \\ &= a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0 \end{aligned}$$

Procedure:

1. Split a and b to obtain a_1, a_0, b_1 and b_0

Recursion: conquer

$$
\begin{aligned}
a \times b &= (a_1 \cdot B^k + a_0) \times (b_1 \cdot B^k + b_0) \\
&= a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0
\end{aligned}
$$

Procedure:

1. Split a and b to obtain a_1, a_0, b_1 and b_0
2. Compute $a_1 \cdot b_1, a_1 \cdot b_0, a_0 \cdot b_1$ and $a_0 \cdot b_0$

Recursion: conquer

$$
\begin{aligned}
a \times b &= (a_1 \cdot B^k + a_0) \times (b_1 \cdot B^k + b_0) \\
&= a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0
\end{aligned}
$$

Procedure:

1. Split a and b to obtain a_1, a_0, b_1 and b_0
2. Compute $a_1 \cdot b_1, a_1 \cdot b_0, a_0 \cdot b_1$ and $a_0 \cdot b_0$
3. Add the aligned products to obtain $a \times b$

Runtime of recursive multiplication

$$a \times b = a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0$$

Runtime of recursive multiplication

$$a \times b = a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0$$

Theorem

Let $T(n)$ be the maximal number of primitive operations to multiply two n-digit integers recursively. Then

$$T(n) \leq \begin{cases} 1 & \textit{if } n = 1 \\ 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \textit{if } n \geq 2 \end{cases}$$

Runtime of recursive multiplication

$$a \times b = a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0$$

Theorem

Let $T(n)$ be the maximal number of primitive operations to multiply two n-digit integers recursively. Then

$$T(n) \le \begin{cases} 1 & \text{if } n = 1 \\ 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \ge 2 \end{cases}$$

Proof:

Runtime of recursive multiplication

$$a \times b = a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0$$

Theorem

Let $T(n)$ be the maximal number of primitive operations to multiply two n-digit integers recursively. Then

$$T(n) \leq \begin{cases} 1 & \textit{if } n = 1 \\ 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \textit{if } n \geq 2 \end{cases}$$

Proof:

1. $n = 1$ requires 1 opeartion

Runtime of recursive multiplication

$$a \times b = a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0$$

Theorem

Let $T(n)$ be the maximal number of primitive operations to multiply two n-digit integers recursively. Then

$$T(n) \leq \begin{cases} 1 & \textit{if } n = 1 \\ 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \textit{if } n \geq 2 \end{cases}$$

Proof:

1. $n = 1$ requires 1 opeartion
2. Each subproblem has at most $\lceil n/2 \rceil$ digits
    - 4 subproblems $\rightarrow$ at most $4 \cdot T(\lceil n/2 \rceil)$ operations

Runtime of recursive multiplication

$$a \times b = a_1 b_1 \cdot B^{2k} + (a_1 b_0 + a_0 b_1) \cdot B^k + a_0 b_0$$

Theorem

Let $T(n)$ be the maximal number of primitive operations to multiply two n-digit integers recursively. Then

$$T(n) \leq \begin{cases} 1 & \text{if } n = 1 \\ 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \geq 2 \end{cases}$$

Proof:

1. $n = 1$ requires 1 opeartion
2. Each subproblem has at most $\lceil n/2 \rceil$ digits
   - 4 subproblems $\rightarrow$ at most $4 \cdot T(\lceil n/2 \rceil)$ operations
3. Another 3 additions of 2n-digit integers

Solving recursion

$$T(n) \le \begin{cases} 1 & \text{if } n = 1 \\ 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \ge 2 \end{cases}$$

Solving recursion

$$T(n) \leq \begin{cases} 1 & \text{if } n = 1 \\ 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \geq 2 \end{cases}$$

For n power of 2 : $T(n) \leq 7n^2 - 6n$

Solving recursion

$$T(n) \leq \begin{cases} 1 & \text{if } n = 1 \\ 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \geq 2 \end{cases}$$

For n power of 2 : $T(n) \leq 7n^2 - 6n$

For general n : $T(n) \leq 28n^2$

Proof: n power of 2

Claim: $T(n) \leq 7n^2 - 6n$ for $n = 2^k$

Proof: n power of 2

Claim: $T(n) \leq 7n^2 - 6n$ for $n = 2^k$

Proof:

Proof: n power of 2

Claim: $T(n) \le 7n^2 - 6n$ for $n = 2^k$

Proof:

$$\boxed{\begin{aligned} &T(n) \\ &\quad \le 1 && \text{if } n = 1 \\ &\quad \le 4{\cdot}T(\lceil n/2 \rceil) + 3{\cdot}2{\cdot}n && \text{if } n \ge 2 \end{aligned}}$$

Proof: n power of 2

Claim: $T(n) \leq 7n^2 - 6n$ for $n = 2^k$

Proof:

$$T(2^k) \leq 4 \cdot T(2^{k-1}) + 6 \cdot 2^k$$

$$\boxed{\begin{array}{ll} T(n) & \\ \quad \leq 1 & \text{if } n = 1 \\ \quad \leq 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \geq 2 \end{array}}$$

Proof: n power of 2

Claim: $T(n) \leq 7n^2 - 6n$ for $n = 2^k$

Proof:

$$T(n) \begin{cases} \leq 1 & \text{if } n = 1 \\ \leq 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \geq 2 \end{cases}$$

$$T(2^k) \leq 4 \cdot T(2^{k-1}) + 6 \cdot 2^k$$

$$\leq 4 \cdot \left(4 \cdot T(2^{k-2}) + 6 \cdot 2^{k-1}\right) + 6 \cdot 2^k$$

Proof: n power of 2

Claim: $T(n) \leq 7n^2 - 6n$ for $n = 2^k$

Proof:

$$\boxed{\begin{array}{ll} T(n) & \\ \quad \leq 1 & \text{if } n = 1 \\ \quad \leq 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \geq 2 \end{array}}$$

$$\begin{aligned} T(2^k) &\leq 4 \cdot T(2^{k-1}) + 6 \cdot 2^k \\ &\leq 4 \cdot \left(4 \cdot T(2^{k-2}) + 6 \cdot 2^{k-1}\right) + 6 \cdot 2^k \\ &\leq 4^2 \cdot T(2^{k-2}) + 6 \cdot (4^1 \cdot 2^{k-1} + 2^k) \end{aligned}$$

Proof: n power of 2

Claim: $T(n) \le 7n^2 - 6n$ for $n = 2^k$

Proof:

$$T(n) \begin{cases} \le 1 & \text{if } n = 1 \\ \le 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \ge 2 \end{cases}$$

$$\begin{aligned}
T(2^k) &\le 4 \cdot T(2^{k-1}) + 6 \cdot 2^k \\
&\le 4 \cdot \left(4 \cdot T(2^{k-2}) + 6 \cdot 2^{k-1}\right) + 6 \cdot 2^k \\
&\le 4^2 \cdot T(2^{k-2}) + 6 \cdot (4^1 \cdot 2^{k-1} + 2^k) \\
&\le 4^2 \cdot \left(4 \cdot T(2^{k-3}) + 6 \cdot 2^{k-2}\right) + 6 \cdot (4^1 \cdot 2^{k-1} + 2^k)
\end{aligned}$$

Proof: n power of 2

Claim: $T(n) \le 7n^2 - 6n$ for $n = 2^k$

Proof:

$$T(n) \begin{cases} \le 1 & \text{if } n = 1 \\ \le 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \ge 2 \end{cases}$$

$$\begin{aligned}
T(2^k) &\le 4 \cdot T(2^{k-1}) + 6 \cdot 2^k \\
&\le 4 \cdot \left(4 \cdot T(2^{k-2}) + 6 \cdot 2^{k-1}\right) + 6 \cdot 2^k \\
&\le 4^2 \cdot T(2^{k-2}) + 6 \cdot (4^1 \cdot 2^{k-1} + 2^k) \\
&\le 4^2 \cdot \left(4 \cdot T(2^{k-3}) + 6 \cdot 2^{k-2}\right) + 6 \cdot (4^1 \cdot 2^{k-1} + 2^k) \\
&\le 4^3 \cdot T(2^{k-3}) + 6 \cdot (4^2 \cdot 2^{k-2} + 4^1 \cdot 2^{k-1} + 2^k)
\end{aligned}$$

Proof: n power of 2

Claim: $T(n) \leq 7n^2 - 6n$ for $n = 2^k$

Proof:

$$T(n) \begin{cases} \leq 1 & \text{if } n = 1 \\ \leq 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \geq 2 \end{cases}$$

$$\begin{aligned}
T(2^k) &\leq 4 \cdot T(2^{k-1}) + 6 \cdot 2^k \\
&\leq 4 \cdot \left(4 \cdot T(2^{k-2}) + 6 \cdot 2^{k-1}\right) + 6 \cdot 2^k \\
&\leq 4^2 \cdot T(2^{k-2}) + 6 \cdot (4^1 \cdot 2^{k-1} + 2^k) \\
&\leq 4^2 \cdot \left(4 \cdot T(2^{k-3}) + 6 \cdot 2^{k-2}\right) + 6 \cdot (4^1 \cdot 2^{k-1} + 2^k) \\
&\leq 4^3 \cdot T(2^{k-3}) + 6 \cdot (4^2 \cdot 2^{k-2} + 4^1 \cdot 2^{k-1} + 2^k) \\
&\leq \dots
\end{aligned}$$

Proof: n power of 2

Claim: $T(n) \le 7n^2 - 6n$ for $n = 2^k$

Proof:

$$T(n) \begin{cases} \le 1 & \text{if } n = 1 \\ \le 4 \cdot T(\lceil n/2 \rceil) + 3 \cdot 2 \cdot n & \text{if } n \ge 2 \end{cases}$$

$$\begin{aligned}
T(2^k) &\le 4 \cdot T(2^{k-1}) + 6 \cdot 2^k \\
&\le 4 \cdot \left(4 \cdot T(2^{k-2}) + 6 \cdot 2^{k-1}\right) + 6 \cdot 2^k \\
&\le 4^2 \cdot T(2^{k-2}) + 6 \cdot (4^1 \cdot 2^{k-1} + 2^k) \\
&\le 4^2 \cdot \left(4 \cdot T(2^{k-3}) + 6 \cdot 2^{k-2}\right) + 6 \cdot (4^1 \cdot 2^{k-1} + 2^k) \\
&\le 4^3 \cdot T(2^{k-3}) + 6 \cdot (4^2 \cdot 2^{k-2} + 4^1 \cdot 2^{k-1} + 2^k) \\
&\le \ldots \\
&\le 4^k \cdot T(1) + 6 \sum_{i=0}^{k-1} 4^i \cdot 2^{k-i}
\end{aligned}$$

Proof: n power of 2 (cont.)

$$T(2^k) \leq 4^k \cdot T(1) + 6\sum_{i=0}^{k-1} 4^i \cdot 2^{k-i}$$

Proof: n power of 2 (cont.)

$$T(2^k) \leq 4^k \cdot T(1) + 6 \sum_{i=0}^{k-1} 4^i \cdot 2^{k-i}$$

$$\leq 4^k + 6 \cdot 2^k \sum_{i=0}^{k-1} 2^i$$

Proof: n power of 2 (cont.)

$$T(2^k) \leq 4^k \cdot T(1) + 6 \sum_{i=0}^{k-1} 4^i \cdot 2^{k-i}$$

$$\leq 4^k + 6 \cdot 2^k \sum_{i=0}^{k-1} 2^i$$

Geometric series:

$$\sum_{i=0}^{k-1} ar^i = a\left(\frac{a - r^k}{1 - r}\right)$$

Proof: n power of 2 (cont.)

$$T(2^k) \le 4^k \cdot T(1) + 6 \sum_{i=0}^{k-1} 4^i \cdot 2^{k-i}$$

$$\le 4^k + 6 \cdot 2^k \sum_{i=0}^{k-1} 2^i$$

$$\le 4^k + 6 \cdot 2^k (2^k - 1)$$

Geometric series:

$$\sum_{i=0}^{k-1} ar^i = a\left(\frac{a - r^k}{1 - r}\right)$$

Proof: n power of 2 (cont.)

$$T(2^k) \leq 4^k \cdot T(1) + 6 \sum_{i=0}^{k-1} 4^i \cdot 2^{k-i}$$

$$\leq 4^k + 6 \cdot 2^k \sum_{i=0}^{k-1} 2^i$$

$$\leq 4^k + 6 \cdot 2^k (2^k - 1)$$

$$= n^2 + 6 \cdot n(n-1)$$

Geometric series:

$$\sum_{i=0}^{k-1} ar^i = a\left(\frac{a - r^k}{1 - r}\right)$$

Proof: n power of 2 (cont.)

$$
\begin{aligned}
T(2^k) &\leq 4^k \cdot T(1) + 6 \sum_{i=0}^{k-1} 4^i \cdot 2^{k-i} \\
&\leq 4^k + 6 \cdot 2^k \sum_{i=0}^{k-1} 2^i \\
&\leq 4^k + 6 \cdot 2^k (2^k - 1) \\
&= n^2 + 6 \cdot n(n-1) \\
&= 7n^2 - 6 \cdot n
\end{aligned}
$$

$$\boxed{\text{Geometric series: } \sum_{i=0}^{k-1} ar^i = a\left(\frac{a - r^k}{1 - r}\right)}$$

Proof: general n

Claim: $T(n) \leq 28n^2$ for general n

Proof: general n

Claim: $T(n) \leq 28n^2$ for general n

Proof: Multiplying n-digit integers does not cost more than multiplying $2^{\lceil \log n \rceil}$-digit integers

Proof: general n

Claim: $T(n) \leq 28n^2$ for general n

Proof: Multiplying n-digit integers does not cost more than multiplying $2^{\lceil \log n \rceil}$-digit integers

This implies $T(n) \leq T(2^{\lceil \log n \rceil})$

Proof: general n

Claim: $T(n) \leq 28n^2$ for general n

Proof: Multiplying n-digit integers does not cost more than multiplying $2^{\lceil \log n \rceil}$-digit integers

This implies $T(n) \leq T(2^{\lceil \log n \rceil})$

Since $2^{\lceil \log n \rceil} \leq 2^{\log n + 1} \leq 2 \cdot 2^{\log n} = 2n$

Proof: general n

Claim: $T(n) \leq 28n^2$ for general n

Proof: Multiplying n-digit integers does not cost more than multiplying $2^{\lceil \log n \rceil}$-digit integers

This implies $T(n) \leq T(2^{\lceil \log n \rceil})$

Since $2^{\lceil \log n \rceil} \leq 2^{\log n + 1} \leq 2 \cdot 2^{\log n} = 2n$ and $T(n) \leq 7n^2 - 6n$ for $n = 2^k$

Proof: general n

Claim: $T(n) \le 28n^2$ for general n

Proof: Multiplying n-digit integers does not cost more than multiplying $2^{\lceil \log n \rceil}$-digit integers

This implies $T(n) \le T(2^{\lceil \log n \rceil})$

Since $2^{\lceil \log n \rceil} \le 2^{\log n + 1} \le 2 \cdot 2^{\log n} = 2n$ and $T(n) \le 7n^2 - 6n$ for $n = 2^k$

We have $T(n) \le 28n^2$ for all n

Summary

- Divide-and-conquer and recursive multplication
- Maximal primitive operations required
  - $7n^2 - 6n$ for n power of 2
  - $28n^2$ for general n
- Reading: Algorithms and Data Structures
  - Chapter 1.4: A Recursive Version of the School Method

Next lecture

- Karatsuba multiplication
- Reading: Algorithms and Data Structures
  - Chapter 1.5: Karatsuba Multiplication