Algorithm & Data Structure Analysis

Lecture 4: Karatsuba Multiplication

Overview

- Last lecture:
  - Recursive multiplication

Overview

- Last lecture:
  - Recursive multiplication
- This lecture:
  - Karatsuba multiplication

Karatsuba multiplication

Let $a = a_1 B^k + a_0$ and $b = b_1 B^k + b_0$. Compute $a \times b$

Karatsuba multiplication

Let $a = a_1 B^k + a_0$ and $b = b_1 B^k + b_0$. Compute $a \times b$

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

Karatsuba multiplication

Let $a = a_1 B^k + a_0$ and $b = b_1 B^k + b_0$. Compute $a \times b$

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

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

Karatsuba multiplication

Let $a = a_1 B^k + a_0$ and $b = b_1 B^k + b_0$. Compute $a \times b$

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

Karatsuba multiplication (cont.)

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

Karatsuba multiplication (cont.)

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

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

$$= (a_1 \times b_1) B^{2k}$$

$$+ \Big((a_1 + a_0) \times (b_1 + b_0) - (a_1 \times b_1 + a_0 \times b_0) \Big) B^k$$

$$+ a_0 \times b_0$$

Karatsuba multiplication (cont.)

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

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

$$= \boxed{\begin{aligned} &(a_1 \times b_1) B^{2k} \\ &+ \Big((a_1 + a_0) \times (b_1 + b_0) - (a_1 \times b_1 + a_0 \times b_0) \Big) B^k \\ &+ a_0 \times b_0 \end{aligned}}$$ Karatsuba

Karatsuba multiplication (cont.)

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

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

$$= \boxed{\begin{aligned} &(a_1 \times b_1) B^{2k} \\ &+ \Big((a_1 + a_0) \times (b_1 + b_0) - (a_1 \times b_1 + a_0 \times b_0) \Big) B^k \\ &+ a_0 \times b_0 \end{aligned}}$$ Karatsuba

- # mul: $4 \rightarrow 3$

Karatsuba multiplication (cont.)

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

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

$$= \boxed{\begin{aligned} &(a_1 \times b_1) B^{2k} \\ &+ \Big((a_1 + a_0) \times (b_1 + b_0) - (a_1 \times b_1 + a_0 \times b_0) \Big) B^k \\ &+ a_0 \times b_0 \end{aligned}}$$ Karatsuba

- # mul: $4 \rightarrow 3$
- # add: $3 \rightarrow 6$

Karatsuba multiplication (cont.)

$$
\begin{aligned}
a \times b &= (a_1 B^k + a_0) \times (b_1 B^k b_0) && \text{Recursive Method} \\
&= \boxed{(a_1 \times b_1) B^{2k} + (a_1 \times b_0 + a_0 \times b_1) B^k + a_0 \times b_0} \\
&= \boxed{\begin{aligned}
&(a_1 \times b_1) B^{2k} \\
&+ \Big((a_1 + a_0) \times (b_1 + b_0) - (a_1 \times b_1 + a_0 \times b_0) \Big) B^k \\
&+ a_0 \times b_0 && \text{Karatsuba}
\end{aligned}}
\end{aligned}
$$

- # mul: $4 \rightarrow 3$
- # add: $3 \rightarrow 6$
- mul is more costly than add:

Karatsuba multiplication (cont.)

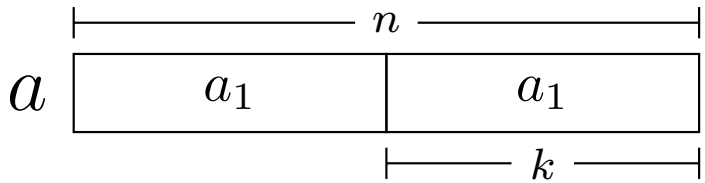
$$
\begin{aligned}
a \times b &= (a_1 B^k + a_0) \times (b_1 B^k b_0) && \text{Recursive Method} \\
&= \boxed{(a_1 \times b_1) B^{2k} + (a_1 \times b_0 + a_0 \times b_1) B^k + a_0 \times b_0} \\
&= \boxed{\begin{aligned} &(a_1 \times b_1) B^{2k} \\ &+ \Big((a_1 + a_0) \times (b_1 + b_0) - (a_1 \times b_1 + a_0 \times b_0) \Big) B^k \\ &+ a_0 \times b_0 \end{aligned}} && \text{Karatsuba}
\end{aligned}
$$

- # mul: $4 \rightarrow 3$
- # add: $3 \rightarrow 6$
- mul is more costly than add: $\Theta(n^2)$ vs $\Theta(n)$

Algorithm

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

$$a = a_1 B^k + a_0 \text{ and } b = b_1 B^k + b_0$$



$n < 4$: use school method

$n \geq 4$: use these steps

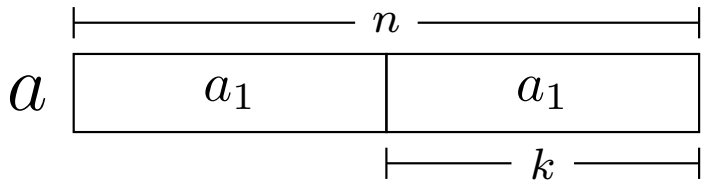
Algorithm

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

$$a = a_1 B^k + a_0 \text{ and } b = b_1 B^k + b_0$$

2. Compute the three products

$$p_2 = a_1 \times b_1, \quad p_1 = (a_1 + a_0) \times (b_1 + b_0), \quad p_0 = a_0 \times b_0$$

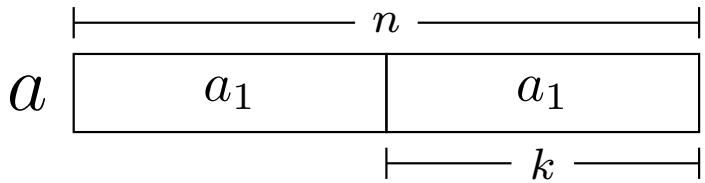


$n < 4$: use school method

$n \geq 4$: use these steps

Algorithm

1. Split a and b to obtain a_1, a_0, b_1 and b_0 where
$$a = a_1 B^k + a_0 \text{ and } b = b_1 B^k + b_0$$
2. Compute the three products
$$p_2 = a_1 \times b_1, \quad p_1 = (a_1 + a_0) \times (b_1 + b_0), \quad p_0 = a_0 \times b_0$$
3. Add aligned products to obtain
$$p = a \times b = p_2 B^{2k} + \big(p_1 - (p_2 + p_0)\big) B^k + p_0$$



$n < 4$: use school method

$n \geq 4$: use these steps

Runtime of Karatsuba multiplication

Theorem

Let $T_K(n)$ be the maximal number of primitive operations to multiply two n-digit integers using Karatsuba algorithm. Then

$$T_K(n) \leq \begin{cases} 3n^2 + 2n & \text{if } n < 4 \\ 3 \cdot T_K(\lceil n/2 \rceil + 1) + 6 \cdot 2 \cdot n & \text{if } n \geq 4 \end{cases}$$

Runtime of Karatsuba multiplication

Theorem

Let $T_K(n)$ be the maximal number of primitive operations to multiply two n-digit integers using Karatsuba algorithm. Then

$$T_K(n) \leq \begin{cases} 3n^2 + 2n & \text{if } n < 4 \\ 3 \cdot T_K(\lceil n/2 \rceil + 1) + 6 \cdot 2 \cdot n & \text{if } n \geq 4 \end{cases}$$

Proof:

Runtime of Karatsuba multiplication

Theorem

Let $T_K(n)$ be the maximal number of primitive operations to multiply two n-digit integers using Karatsuba algorithm. Then

$$T_K(n) \leq \begin{cases} 3n^2 + 2n & \text{if } n < 4 \\ 3 \cdot T_K(\lceil n/2 \rceil + 1) + 6 \cdot 2 \cdot n & \text{if } n \geq 4 \end{cases}$$

Proof:

1. $n < 4$: school method (lecture 2)

Runtime of Karatsuba multiplication

Theorem

Let $T_K(n)$ be the maximal number of primitive operations to multiply two n-digit integers using Karatsuba algorithm. Then

$$T_K(n) \leq \begin{cases} 3n^2 + 2n & \text{if } n < 4 \\ 3 \cdot T_K(\lceil n/2 \rceil + 1) + 6 \cdot 2 \cdot n & \text{if } n \geq 4 \end{cases}$$

Proof:

1. $n < 4$: school method (lecture 2)
2. Each subproblem has at most $\lceil n/2 \rceil + 1$ digits
   - 3 subproblems $\rightarrow$ at most $3 \cdot T_K(\lceil n/2 \rceil + 1)$ operations

Runtime of Karatsuba multiplication

Theorem

Let $T_K(n)$ be the maximal number of primitive operations to multiply two n-digit integers using Karatsuba algorithm. Then

$$T_K(n) \leq \begin{cases} 3n^2 + 2n & \text{if } n < 4 \\ 3 \cdot T_K(\lceil n/2 \rceil + 1) + 6 \cdot 2 \cdot n & \text{if } n \geq 4 \end{cases}$$

Proof:

1. $n < 4$: school method (lecture 2)
2. Each subproblem has at most $\lceil n/2 \rceil + 1$ digits
   - 3 subproblems $\rightarrow$ at most $3 \cdot T_K(\lceil n/2 \rceil + 1)$ operations
3. Another 6 additions of 2n-digit integers

Solving recursion

$$T_K(n) \leq \begin{cases} 3n^2 + 2n & \text{if } n < 4 \\ 3 \cdot T_K(\lceil n/2 \rceil + 1) + 6 \cdot 2 \cdot n & \text{if } n \geq 4 \end{cases}$$

Solving recursion

$$T_K(n) \leq \begin{cases} 3n^2 + 2n & \text{if } n < 4 \\ 3 \cdot T_K(\lceil n/2 \rceil + 1) + 6 \cdot 2 \cdot n & \text{if } n \geq 4 \end{cases}$$

Claim : $T_K(n) \leq 207 \cdot n^{\log 3}$

Solving recursion

$$T_K(n) \leq \begin{cases} 3n^2 + 2n & \text{if } n < 4 \\ 3 \cdot T_K(\lceil n/2 \rceil + 1) + 6 \cdot 2 \cdot n & \text{if } n \geq 4 \end{cases}$$

Claim : $T_K(n) \leq 207 \cdot n^{\log 3}$

Consider : $n = (2^k + 2)$ for $k \geq 0$

Solving recursion

$$T_K(n) \leq \begin{cases} 3n^2 + 2n & \text{if } n < 4 \\ 3 \cdot T_K(\lceil n/2 \rceil + 1) + 6 \cdot 2 \cdot n & \text{if } n \geq 4 \end{cases}$$

Claim : $T_K(n) \leq 207 \cdot n^{\log 3}$

Consider : $n = (2^k + 2)$ for $k \geq 0$

$$\lceil n/2 \rceil + 1 = \lceil (2^k + 2)/2 \rceil + 1 = 2^{k-1} + 1 + 1 = 2^{k-1} + 2$$

Proof: induction

Claim: $T_K(2^k + 2) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$

Proof: induction

Claim: $T_K(2^k + 2) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$

Proof:

Proof: induction

Claim: $T_K(2^k + 2) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$

Proof:

(base case) $k = 0$:

Proof: induction

Claim: $T_K(2^k + 2) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$

Proof:

$T_K(n) \leq 3n^2 + 2n$ if $n < 4$

(base case) $k = 0$:

$$T_K(2^0+2) = T_K(3) \leq 3 \cdot 3^2 + 2 \cdot 3 = 33 = 69 \cdot 3^0 - 24 \cdot 2^0 - 12$$

Proof: induction

Claim: $T_K(2^k + 2) \leq 69{\cdot}3^k - 24{\cdot}2^k - 12$

Proof:

$T_K(n) \leq 3n^2{+}2n$	if $n{<}4$

(base case) $k = 0$:

$$T_K(2^0{+}2) = T_K(3) \leq 3{\cdot}3^2{+}2{\cdot}3 = 33 = 69{\cdot}3^0{-}24{\cdot}2^0{-}12$$

(inductive step) assume claim is true for $k{-}1$ then for k:

Proof: induction

Claim: $T_K(2^k+2) \leq 69{\cdot}3^k - 24{\cdot}2^k - 12$

Proof:

$$\boxed{\begin{array}{ll} T_K(n) \leq 3n^2{+}2n & \text{if } n{<}4 \\ T_K(n) \leq 3{\cdot}T_K(\lceil n/2 \rceil{+}1){+}6{\cdot}2{\cdot}n & \text{if } n{\geq}4 \end{array}}$$

(base case) $k = 0$:

$$T_K(2^0{+}2) = T_K(3) \leq 3{\cdot}3^2{+}2{\cdot}3 = 33 = 69{\cdot}3^0{-}24{\cdot}2^0{-}12$$

(inductive step) assume claim is true for $k{-}1$ then for k:

$$T_K(2^k+2) \leq 3{\cdot}T_K(2^{k-1}+2) + 12{\cdot}(2^k+2)$$

Proof: induction

Claim: $T_K(2^k+2) \leq 69{\cdot}3^k - 24{\cdot}2^k - 12$

Proof:

$$\boxed{\begin{array}{ll} T_K(n) \leq 3n^2{+}2n & \text{if } n{<}4 \\ T_K(n) \leq 3{\cdot}T_K(\lceil n/2 \rceil{+}1){+}6{\cdot}2{\cdot}n & \text{if } n{\geq}4 \end{array}}$$

(base case) $k = 0$:

$$T_K(2^0{+}2) = T_K(3) \leq 3{\cdot}3^2{+}2{\cdot}3 = 33 = 69{\cdot}3^0{-}24{\cdot}2^0{-}12$$

(inductive step) assume claim is true for $k{-}1$ then for k:

$$\begin{aligned} T_K(2^k+2) &\leq 3{\cdot}T_K(2^{k-1}+2) + 12{\cdot}(2^k+2) \\ &\leq 3{\cdot}(69{\cdot}3^{k-1} - 24{\cdot}2^{k-1} - 12) + 12{\cdot}(2^k+2) \end{aligned}$$

Proof: induction

Claim: $T_K(2^k+2) \leq 69{\cdot}3^k - 24{\cdot}2^k - 12$

Proof:

$$\boxed{\begin{array}{ll} T_K(n) \leq 3n^2{+}2n & \text{if } n{<}4 \\ T_K(n) \leq 3{\cdot}T_K(\lceil n/2 \rceil{+}1){+}6{\cdot}2{\cdot}n & \text{if } n{\geq}4 \end{array}}$$

(base case) $k = 0$:

$$T_K(2^0{+}2) = T_K(3) \leq 3{\cdot}3^2{+}2{\cdot}3 = 33 = 69{\cdot}3^0{-}24{\cdot}2^0{-}12$$

(inductive step) assume claim is true for $k{-}1$ then for k:

$$\begin{aligned} T_K(2^k+2) &\leq 3{\cdot}T_K(2^{k-1}+2) + 12{\cdot}(2^k+2) \\ &\leq 3{\cdot}(69{\cdot}3^{k-1} - 24{\cdot}2^{k-1} - 12) + 12{\cdot}(2^k+2) \\ &\leq 69{\cdot}3^k - 24{\cdot}2^k - 12 \end{aligned}$$

Proof: repeated substitution

Claim: $T_K(2^k + 2) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$

$$T_K(2^k + 2) \leq 3T_K(2^{k-1} + 2) + 12(2^k + 2)$$

Proof: repeated substitution

Claim: $T_K(2^k + 2) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$

$$T_K(2^k + 2) \leq 3T_K(2^{k-1} + 2) + 12(2^k + 2)$$

$$\leq 3\big(3T_K(2^{k-2} + 2) + 12(2^{k-1} + 2)\big) + 12(2^k + 2)$$

Proof: repeated substitution

Claim: $T_K(2^k + 2) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$

$$
\begin{aligned}
T_K(2^k + 2) &\leq 3T_K(2^{k-1} + 2) + 12(2^k + 2) \\
&\leq 3\big(3T_K(2^{k-2} + 2) + 12(2^{k-1} + 2)\big) + 12(2^k + 2) \\
&\leq 3^2 T_K(2^{k-2} + 2) + 12\big(3^1(2^{k-1} + 2) + 3^0(2^k + 2)\big)
\end{aligned}
$$

Proof: repeated substitution

Claim: $T_K(2^k+2) \leq 69{\cdot}3^k - 24{\cdot}2^k - 12$

$$T_K(2^k+2) \leq 3T_K(2^{k-1}+2) + 12(2^k+2)$$

$$\leq 3\big(3T_K(2^{k-2}+2) + 12(2^{k-1}+2)\big) + 12(2^k+2)$$

$$\leq 3^2T_K(2^{k-2}+2) + 12\big(3^1(2^{k-1}+2) + 3^0(2^k+2)\big)$$

$$\leq 3^kT_K(2^0+2)+12\big(3^{k-1}(2^1+2)+\cdots 3^1(2^{k-1}+2)+3^0(2^k+2)\big)$$

Proof: repeated substitution

Claim: $T_K(2^k+2) \leq 69{\cdot}3^k - 24{\cdot}2^k - 12$

$$
\begin{aligned}
T_K(2^k+2) &\leq 3T_K(2^{k-1}+2) + 12(2^k+2) \\
&\leq 3\big(3T_K(2^{k-2}+2) + 12(2^{k-1}+2)\big) + 12(2^k+2) \\
&\leq 3^2 T_K(2^{k-2}+2) + 12\big(3^1(2^{k-1}+2) + 3^0(2^k+2)\big) \\
&\leq 3^k T_K(2^0+2) + 12\big(3^{k-1}(2^1+2) + \cdots 3^1(2^{k-1}+2) + 3^0(2^k+2)\big) \\
&\leq 33{\cdot}3^k + 12{\cdot}(3^{k-1}{\cdot}2^1 + \cdots + 3^0{\cdot}2^k) + 12{\cdot}2{\cdot}(3^{k-1} + \cdots + 3^0)
\end{aligned}
$$

Proof: repeated substitution

Claim: $T_K(2^k+2) \leq 69{\cdot}3^k - 24{\cdot}2^k - 12$

$$
\begin{aligned}
T_K(2^k+2) &\leq 3T_K(2^{k-1}+2) + 12(2^k+2) \\
&\leq 3\big(3T_K(2^{k-2}+2) + 12(2^{k-1}+2)\big) + 12(2^k+2) \\
&\leq 3^2 T_K(2^{k-2}+2) + 12\big(3^1(2^{k-1}+2) + 3^0(2^k+2)\big) \\
&\leq 3^k T_K(2^0+2) + 12\big(3^{k-1}(2^1+2) + \cdots 3^1(2^{k-1}+2) + 3^0(2^k+2)\big) \\
&\leq 33{\cdot}3^k + 12{\cdot}(3^{k-1}{\cdot}2^1 + \cdots + 3^0{\cdot}2^k) + 12{\cdot}2{\cdot}(3^{k-1} + \cdots + 3^0) \\
&\leq 33{\cdot}3^k + 12{\cdot}2^k\left(\left(\frac{3}{2}\right)^{k-1} + \cdots + \left(\frac{3}{2}\right)^0\right) + 12{\cdot}2(3^{k-1} + \cdots + 3^0)
\end{aligned}
$$

Proof: repeated substitution

Claim: $T_K(2^k+2) \le 69{\cdot}3^k - 24{\cdot}2^k - 12$

$$
\begin{aligned}
T_K(2^k+2) &\le 3T_K(2^{k-1}+2) + 12(2^k+2) \\
&\le 3\big(3T_K(2^{k-2}+2) + 12(2^{k-1}+2)\big) + 12(2^k+2) \\
&\le 3^2 T_K(2^{k-2}+2) + 12\big(3^1(2^{k-1}+2) + 3^0(2^k+2)\big) \\
&\le 3^k T_K(2^0+2) + 12\big(3^{k-1}(2^1+2) + \cdots 3^1(2^{k-1}+2) + 3^0(2^k+2)\big) \\
&\le 33{\cdot}3^k + 12{\cdot}(3^{k-1}{\cdot}2^1 + \cdots + 3^0{\cdot}2^k) + 12{\cdot}2{\cdot}(3^{k-1} + \cdots + 3^0) \\
&\le 33{\cdot}3^k + 12{\cdot}2^k\left(\left(\frac{3}{2}\right)^{k-1} + \cdots + \left(\frac{3}{2}\right)^0\right) + 12{\cdot}2(3^{k-1} + \cdots + 3^0) \\
&\le 33{\cdot}3^k + 12{\cdot}2^k\frac{(3/2)^k - 1}{3/2 - 1} + 12{\cdot}2\frac{3^k - 1}{3 - 1}
\end{aligned}
$$

Proof: repeated substitution

Claim: $T_K(2^k+2) \le 69{\cdot}3^k - 24{\cdot}2^k - 12$

$$
\begin{aligned}
T_K(2^k+2) &\le 3T_K(2^{k-1}+2) + 12(2^k+2) \\
&\le 3\big(3T_K(2^{k-2}+2) + 12(2^{k-1}+2)\big) + 12(2^k+2) \\
&\le 3^2 T_K(2^{k-2}+2) + 12\big(3^1(2^{k-1}+2) + 3^0(2^k+2)\big) \\
&\le 3^k T_K(2^0+2) + 12\big(3^{k-1}(2^1+2) + \cdots 3^1(2^{k-1}+2) + 3^0(2^k+2)\big) \\
&\le 33{\cdot}3^k + 12{\cdot}(3^{k-1}{\cdot}2^1 + \cdots + 3^0{\cdot}2^k) + 12{\cdot}2{\cdot}(3^{k-1} + \cdots + 3^0) \\
&\le 33{\cdot}3^k + 12{\cdot}2^k\left(\left(\frac{3}{2}\right)^{k-1} + \cdots + \left(\frac{3}{2}\right)^0\right) + 12{\cdot}2(3^{k-1} + \cdots + 3^0) \\
&\le 33{\cdot}3^k + 12{\cdot}2^k\frac{(3/2)^k - 1}{3/2 - 1} + 12{\cdot}2\frac{3^k - 1}{3 - 1} \\
&\le 69{\cdot}3^k - 24{\cdot}2^k - 12
\end{aligned}
$$

Proof: extend to general n

Let k be a minimal integer such that $n \leq 2^k + 2$

Proof: extend to general n

Let k be a minimal integer such that $n \leq 2^k + 2$

Claim: $T_K(n) \leq 207 \cdot n^{\log 3}$

Proof: extend to general n

Let k be a minimal integer such that $n \leq 2^k + 2$

Claim: $T_K(n) \leq 207 \cdot n^{\log 3}$

Proof: Multiplying n-digit integers does not cost more than multiplying $(2^k + 2)$-digit integers

Proof: extend to general n

Let k be a minimal integer such that $n \leq 2^k + 2$

Claim: $T_K(n) \leq 207 \cdot n^{\log 3}$

Proof: Multiplying n-digit integers does not cost more than multiplying $(2^k + 2)$-digit integers

This implies $T_K(n) \leq T_K(2^k + 2)$

Proof: extend to general n (cont.)

Since $T_K(2^k + 2) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$ and $T_K(n) \leq T_K(2^k + 2)$

Proof: extend to general n (cont.)

Since $T_K(2^k + 2) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$ and $T_K(n) \leq T_K(2^k + 2)$

We have

$$T_K(n) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$$

Proof: extend to general n (cont.)

Since $T_K(2^k + 2) \leq 69 \cdot 3^k - 24 \cdot 2^k - 12$ and $T_K(n) \leq T_K(2^k + 2)$

We have

$$\begin{aligned} T_K(n) &\leq 69 \cdot 3^k - 24 \cdot 2^k - 12 \\ &\leq 69 \cdot 3^k \end{aligned}$$

Proof: extend to general n (cont.)

Since $T_K(2^k+2) \leq 69{\cdot}3^k - 24{\cdot}2^k - 12$ and $T_K(n) \leq T_K(2^k+2)$

We have

$$\begin{aligned} T_K(n) &\leq 69{\cdot}3^k - 24{\cdot}2^k - 12 \\ &\leq 69{\cdot}3^k \\ &\leq 69{\cdot}3^{\log n+1} \end{aligned}$$

min k s.t. $n \leq 2^k + 2$

$2^{k-1} \leq 2^{k-1} + 2 \leq n \leq 2^k + 2$

$k \leq \log n + 1$

Proof: extend to general n (cont.)

Since $T_K(2^k+2) \leq 69{\cdot}3^k - 24{\cdot}2^k - 12$ and $T_K(n) \leq T_K(2^k+2)$

We have

$$\begin{aligned} T_K(n) &\leq 69{\cdot}3^k - 24{\cdot}2^k - 12 \\ &\leq 69{\cdot}3^k \\ &\leq 69{\cdot}3^{\log n+1} \\ &\leq 207{\cdot}3^{\log n} \end{aligned}$$

min k s.t. $n \leq 2^k + 2$

$2^{k-1} \leq 2^{k-1} + 2 \leq n \leq 2^k + 2$

$k \leq \log n + 1$

Proof: extend to general n (cont.)

Since $T_K(2^k+2) \leq 69{\cdot}3^k - 24{\cdot}2^k - 12$ and $T_K(n) \leq T_K(2^k+2)$

We have

$$
\begin{aligned}
T_K(n) &\leq 69{\cdot}3^k - 24{\cdot}2^k - 12 \\
&\leq 69{\cdot}3^k \\
&\leq 69{\cdot}3^{\log n+1} \\
&\leq 207{\cdot}3^{\log n} \\
&\leq 207{\cdot}n^{\log 3}
\end{aligned}
$$

min k s.t. $n \leq 2^k + 2$

$2^{k-1} \leq 2^{k-1} + 2 \leq n \leq 2^k + 2$

$k \leq \log n + 1$

$3^{\log n} = 2^{(\log 3)\cdot(\log n)} = n^{\log 3}$

Comparison of multiplication algorithms

- Karatsuba multiplication is asymptotically faster than the school multiplication
- Leading constant of Karatsuba multiplication is large
- Karatsuba multiplication is preferable for a large enough n

Master theorem

Simple form of the Master theorem

For constants $a \geq 1, b \geq 2, d \geq 0$ and $f(n) \in \Theta(n^d)$, consider the recurrence relation:

$$T(n) = aT\left(\frac{n}{b}\right) + f(n)$$

then

$$T(n) \in \begin{cases} \Theta(n^d) & \text{if } a < b^d \\ \Theta(n^d \log n) & \text{if } a = b^d \\ \Theta(n^{\log_b a}) & \text{if } a > b^d \end{cases}$$

Example of Master theorem

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

Example of Master theorem

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

Recall: $T(n) = aT\left(\frac{n}{b}\right) + f(n)$

Example of Master theorem

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

Recall: $T(n) = aT\left(\frac{n}{b}\right) + f(n)$

Consider $n = 2^k$:

Example of Master theorem

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

Recall: $T(n) = aT\left(\frac{n}{b}\right) + f(n)$

Consider $n = 2^k$: $a = 4, b = 2$ and $d = 1$

Example of Master theorem

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

Recall: $T(n) = aT\left(\frac{n}{b}\right) + f(n)$

Consider $n = 2^k$: $a = 4, b = 2$ and $d = 1$

$a > b^d : \Theta(n^{\log_b a}) = \Theta(n^{\log_2 4}) = \Theta(n^2)$

Summary

- Different multiplication algorithms
- Divide-and-conquer and recursive multiplications
- Comparison of school and Karatsuba multiplications
- Master theorem and recursive formulas
- Reading: Algorithms and Data Structures
  - Chapter 1.5: Karatsuba Multiplication
  - Chapter 2.6: Basic Algorithm Analysis

Advance reading

- https://eprint.iacr.org/2014/526.pdf
- https://eprint.iacr.org/2018/230.pdf
- http://ntruprime.cr.yp.to/ntruprime-20170816.pdf

Advance reading

- https://eprint.iacr.org/2014/526.pdf
- https://eprint.iacr.org/2018/230.pdf
- http://ntruprime.cr.yp.to/ntruprime-20170816.pdf