Winter 2016 COMP-250: Introduction to Computer Science Lecture 12, February 18, 2016

Master Theorem (CLRS 4.3)

Used for many divide-and-conquer recurrences

T(n) = aT(n/b) + f(n) ,

where $a \ge 1, b > 1$, and f(n) > 0.

a = (constant) number of sub-instances, b = (constant) size ration of sub-instances, f(n) = time used for dividing and recombining.

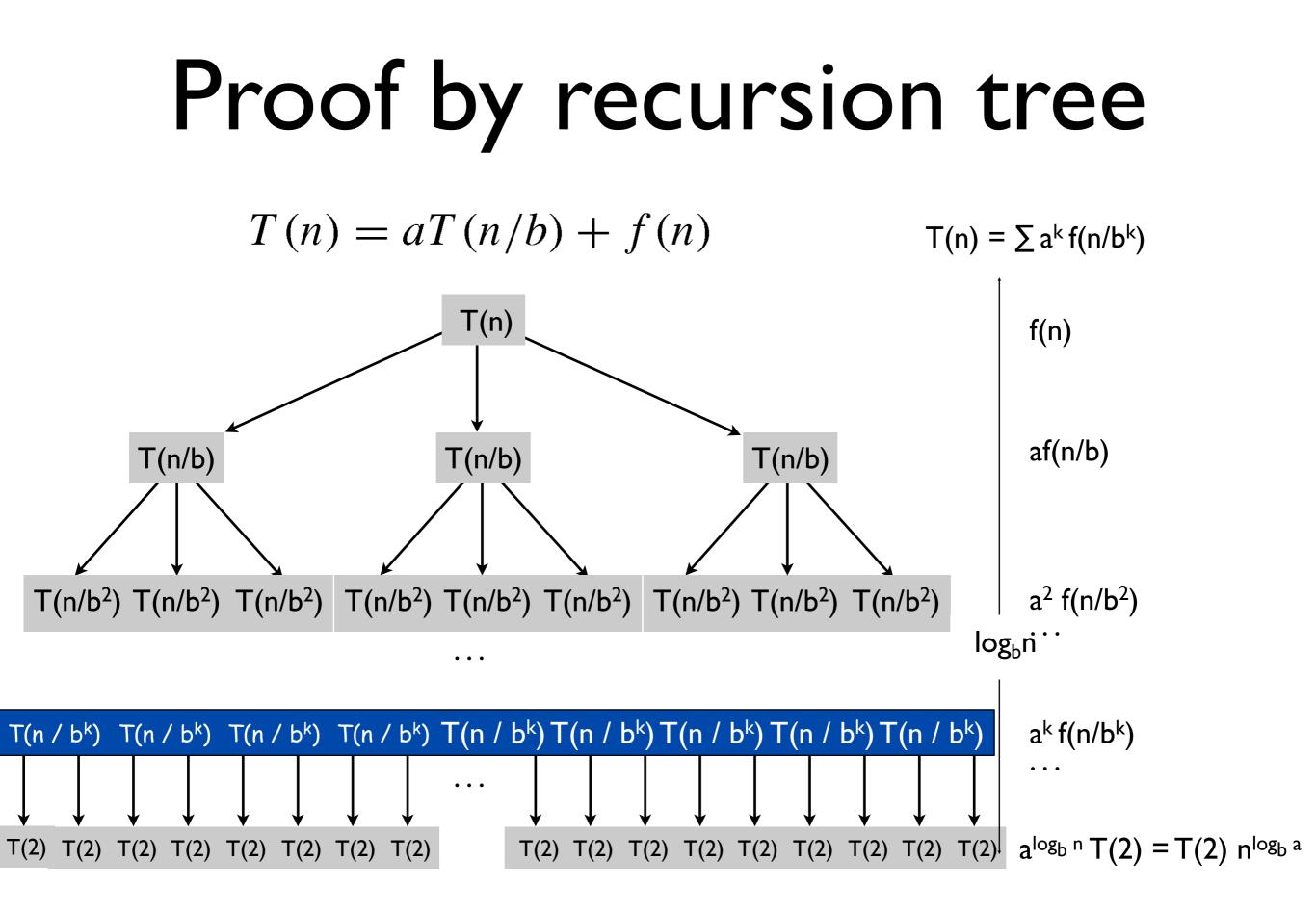
Used for many divide-and-conquer recurrences

T(n) = aT(n/b) + f(n) ,

where $a \ge 1, b > 1$, and f(n) > 0.

a = (constant) number of sub-instances, b = (constant) size ration of sub-instances, f(n) = time used for dividing and recombining.

Based on the *master theorem* (Theorem 4.1). Compare $n^{\log_b a}$ vs. f(n):



Master Theorem T(n) = aT(n/b) + f(n)**<u>Case 1</u>**: f(n) is $O(n^L)$ for some constant $L < \log_b a$. **Solution:** T(n) is $\Theta(n^{\log_b a})$

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. <u>Solution:</u> T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

<u>**Case 3:**</u> f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$

Master Theorem T(n) = aT(n/b) + f(n),where $a \ge 1, b > 1$, and f(n) > 0.

<u>Case 1</u>: f(n) is $O(n^L)$ for some constant $L < \log_b a$.

Solution: T(n) is $O(n^{\log_b a})$ (Intuitively: cost is dominated by leaves.)

Master Theorem T(n) = aT(n/b) + f(n),where $a \ge 1, b > 1$, and f(n) > 0.

<u>**Case 1:**</u> f(n) is $O(n^L)$ for some constant $L < \log_b a$. (f(n) is polynomially smaller than $n^{\log_b a}$.)

Solution: T(n) is $O(n^{\log_b a})$ (Intuitively: cost is dominated by leaves.)

$$T(n) = 5T(n/2) + \Theta(n^2)$$

$$T(n) = 5T(n/2) + \Theta(n^2)$$

$$T(n) = 5T(n/2) + \Theta(n^2)$$

Compare $n^{\log_2 5}$ vs. n^2 .

$$T(n) = 5T(n/2) + \Theta(n^2)$$

Compare $n^{\log_2 5}$ vs. n^2 .

$$T(n) = 5T(n/2) + \Theta(n^2)$$

Compare $n^{\log_2 5}$ vs. n^2 .
Since 2 < log₂ 5 use Case 1

$$T(n) = 5T(n/2) + \Theta(n^2)$$

Compare $n^{\log_2 5}$ vs. n^2 .
Since 2 < log₂ 5 use Case 1

<u>Case 1</u>: f(n) is $O(n^L)$ for some constant $L < \log_b a$. <u>Solution:</u> T(n) is $O(n^{\log_b a})$

> $T(n) = 5T(n/2) + \Theta(n^2)$ Compare $n^{\log_2 5}$ vs. n^2 . Since 2 < log₂ 5 use <u>Case 1</u> <u>Solution:</u> T(n) is $\Theta(n^{\log_2 5})$

T(n) = aT(n/b) + f(n), where $a \ge 1, b > 1$, and f(n) > 0.

<u>Simple Case 2</u>: f(n) is $\Theta(n^{\log_b a})$.

Solution: T(n) is $\Theta(n^{\log_b a} \log n)$

T(n) = aT(n/b) + f(n), where $a \ge 1, b > 1$, and f(n) > 0.

<u>**Case 2</u>**: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$.</u>

Solution: T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

(Intuitively: cost is $n^{\log_b a} \lg^k n$ at each level, and there are $\Theta(\lg n)$ levels.)

$$T(n) = 27T(n/3) + \mathcal{O}(n^3 \log n)$$

$$T(n) = 27T(n/3) + \mathcal{O}(n^3 \log n)$$

$$T(n) = 27T(n/3) + \Theta(n^3 \log n)$$

Compare $n^{\log_3 27}$ vs. n^3 .

$$T(n) = 27T(n/3) + \Theta(n^3 \log n)$$

Compare $n^{\log_3 27}$ vs. n^3 .

$$T(n) = 27T(n/3) + \Theta(n^3 \log n)$$

Compare $n^{\log_3 27}$ vs. n^3 .
Since $3 = \log_3 27$ use Case 2

$$T(n) = 27T(n/3) + \Theta(n^3 \log n)$$

Compare $n^{\log_3 27}$ vs. n^3 .
Since $3 = \log_3 27$ use Case 2

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. Solution: T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

> $T(n) = 27T(n/3) + \Theta(n^3 \log n)$ Compare $n^{\log_3 27}$ vs. n^3 . Since $3 = \log_3 27$ use <u>Case 2</u> Solution: T(n) is $\Theta(n^3 \log^2 n)$

T(n) = aT(n/b) + f(n), where $a \ge 1, b > 1$, and f(n) > 0.

<u>Case 3</u>: f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. (f(n) is polynomially greater than $n^{\log_b a}$.)

Solution: T(n) is $\Theta(f(n))$ (Intuitively: cost is dominated by root.)

<u>**Case 3</u>**: f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$ </u>

<u>**Case 3</u>**: f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$ </u>

What's with the Case 3 regularity condition?

- Generally not a problem.
- It always holds whenever $f(n) = n^k$ and f(n) is $\Omega(n^{\log_b a + \epsilon})$ for constant $\epsilon > 0$.

<u>**Case 3:**</u> f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$

<u>**Case 3:**</u> f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$

 $T(n) = 5T(n/2) + \Theta(n^3)$

<u>**Case 3:**</u> f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$

 $T(n) = 5T(n/2) + \Theta(n^3)$

<u>**Case 3:**</u> f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$

> $T(n) = 5T(n/2) + \Theta(n^3)$ Compare $n^{\log_2 5}$ vs. n^3 .

<u>**Case 3:**</u> f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$

> $T(n) = 5T(n/2) + \Theta(n^3)$ Compare $n^{\log_2 5}$ vs. n^3 .

<u>**Case 3:**</u> f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$

> $T(n) = 5T(n/2) + \Theta(n^3)$ Compare $n^{\log_2 5}$ vs. n^3 . Since $3 > \log_2 5$ use <u>Case 3</u>

<u>**Case 3:**</u> f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$

> $T(n) = 5T(n/2) + \Theta(n^3)$ Compare $n^{\log_2 5}$ vs. n^3 . Since $3 > \log_2 5$ use <u>Case 3</u>

<u>**Case 3:**</u> f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$

> $T(n) = 5T(n/2) + \Theta(n^3)$ Compare $n^{\log_2 5}$ vs. n^3 . Since $3 > \log_2 5$ use <u>Case 3</u> $af(n/b) = 5(n/2)^3 = 5/8 \ n^3 \le cn^3$, for c = 5/8

<u>**Case 3:**</u> f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$

> $T(n) = 5T(n/2) + \Theta(n^3)$ Compare $n^{\log_2 5}$ vs. n^3 . Since $3 > \log_2 5$ use <u>Case 3</u> $af(n/b) = 5(n/2)^3 = 5/8 \ n^3 \le cn^3$, for c = 5/8

<u>**Case 3</u>**: f(n) is $\Omega(n^L)$ for some constant $L > \log_b a$ and f(n) satisfies the regularity condition $af(n/b) \le cf(n)$ for some c < 1 and all large n. <u>**Solution:**</u> T(n) is $\Theta(f(n))$ </u>

> $T(n) = 5T(n/2) + \Theta(n^3)$ Compare $n^{\log_2 5}$ vs. n^3 . Since $3 > \log_2 5$ use <u>Case 3</u> $af(n/b) = 5(n/2)^3 = 5/8 \ n^3 \le cn^3$, for c = 5/8Solution: T(n) is $\Theta(n^3)$

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. <u>Solution:</u> T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. <u>Solution:</u> T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

 $T(n) = 27T(n/3) + \Theta(n^3/\log n)$

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. <u>Solution:</u> T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

 $T(n) = 27T(n/3) + \Theta(n^3/\log n)$

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. <u>Solution:</u> T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

> $T(n) = 27T(n/3) + \Theta(n^3/\log n)$ Compare $n^{\log_3 27}$ vs. n^3 .

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. <u>Solution:</u> T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

> $T(n) = 27T(n/3) + \Theta(n^3/\log n)$ Compare $n^{\log_3 27}$ vs. n^3 .

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. <u>Solution:</u> T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

> $T(n) = 27T(n/3) + \Theta(n^3/\log n)$ Compare $n^{\log_3 27}$ vs. n^3 . Since $3 = \log_3 27$ use <u>Case 2</u>

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. <u>Solution:</u> T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

> $T(n) = 27T(n/3) + \Theta(n^3/\log n)$ Compare $n^{\log_3 27}$ vs. n^3 . Since $3 = \log_3 27$ use <u>Case 2</u>

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. <u>Solution:</u> T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

> $T(n) = 27T(n/3) + \Theta(n^3/\log n)$ Compare $n^{\log_3 27}$ vs. n^3 . Since $3 = \log_3 27$ use <u>Case 2</u> <u>but</u> $n^3/\log n$ is not $\Theta(n^3 \log^k n)$ for $k \ge 0$

<u>Case 2</u>: f(n) is $\Theta(n^{\log_b a} \log^k n)$, for some $k \ge 0$. Solution: T(n) is $\Theta(n^{\log_b a} \log^{k+1} n)$

> $T(n) = 27T(n/3) + \Theta(n^3/\log n)$ Compare $n^{\log_3 27}$ vs. n^3 . Since $3 = \log_3 27$ use <u>Case 2</u> <u>but</u> $n^3/\log n$ is not $\Theta(n^3 \log^k n)$ for $k \ge 0$ Cannot use Master Method.

Divide-and-Conquer Paradigm

Divide-and-conquer.

Divide-and-conquer.

Break up problem into several parts.

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Most common usage.

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Most common usage.

Break up problem of size n into two equal parts of size n/2.

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Most common usage.

- Break up problem of size n into two equal parts of size n/2.
- Solve two parts recursively.

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Most common usage.

- Break up problem of size n into two equal parts of size n/2.
- Solve two parts recursively.
- Combine two solutions into overall solution in linear time.

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Most common usage.

- Break up problem of size n into two equal parts of size n/2.
- Solve two parts recursively.
- Combine two solutions into overall solution in linear time.

Divide et impera. Veni, vidi, vici. - Julius Caesar

 $T(n) = \begin{cases} 0 & \text{if } n = 1\\ \underline{2T(n/2)} + \underline{n} & \text{otherwise}\\ \text{sorting both halves merging} \end{cases}$

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Most common usage.

- Break up problem of size n into two equal parts of size n/2.
- Solve two parts recursively.
- Combine two solutions into overall solution in linear time.

Divide et impera. Veni, vidi, vici. - Julius Caesar

 $T(n) = \begin{cases} 0 & \text{if } n = 1\\ \underline{2T(n/2)} + \underline{n} & \text{otherwise}\\ \text{sorting both halves merging} \end{cases}$

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Most common usage.

- Break up problem of size n into two equal parts of size n/2.
- Solve two parts recursively.
- Combine two solutions into overall solution in linear time.

Consequence.

Divide et impera. Veni, vidi, vici. - Julius Caesar

 $T(n) = \begin{cases} 2T(n/2) \\ \text{sorting both halves} & \text{merging} \end{cases} \text{ otherwise}$

if n = 1

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Most common usage.

- Break up problem of size n into two equal parts of size n/2.
- Solve two parts recursively.
- Combine two solutions into overall solution in linear time.

Consequence.

Straightforward: n².

Divide et impera. Veni, vidi, vici. - Julius Caesar

 $T(n) = \begin{cases} 0 & \text{if } n = 1\\ 2T(n/2) + n & \text{otherwise} \\ \text{sorting both halves merging} \end{cases}$

Divide-and-conquer.

- Break up problem into several parts.
- Solve each part recursively.
- Combine solutions to sub-problems into overall solution.

Most common usage.

- Break up problem of size n into two equal parts of size n/2.
- Solve two parts recursively.
- Combine two solutions into overall solution in linear time.

Consequence.

- Straightforward: n².
- Divide-and-conquer: n log n.

Divide et impera. Veni, vidi, vici. - Julius Caesar

 $T(n) = \begin{cases} 2T(n/2) + n \\ \text{sorting both halves merging} \end{cases} \text{ otherwise}$

if n = 1

Divide-and-Conquer: Binary Search

Binary Search

Find a value v in a sorted array of elements.

$[a_0 \leq a_1 \leq \dots \leq a_{\text{Size}-1}]$

Size = number of elements.

Binary Search

Algorithm: binarySearch(a, v, low, high)

Input: array *a*, value *v*, lower and upper bound indices *low*, *high* (*low* = 0, *high* = n - 1 initially) **Output:** the index *i* of element *v* (if it is present), -1 (if *v* is not present)

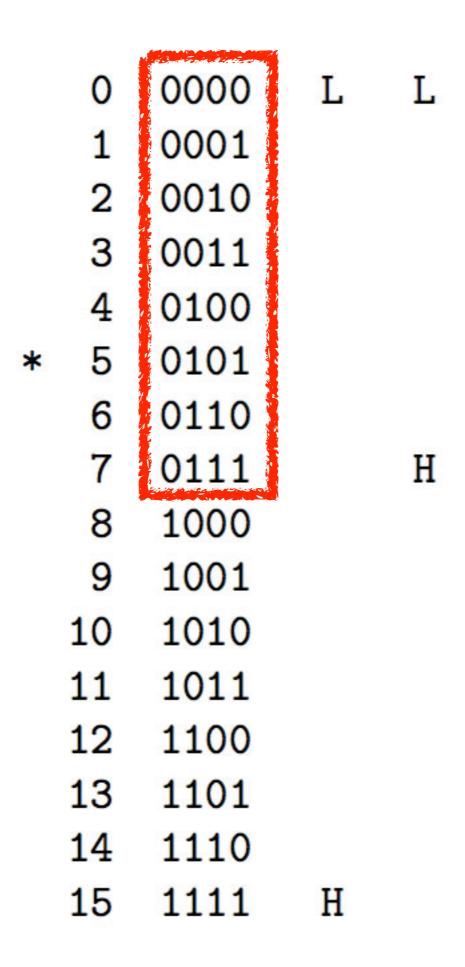
```
if low == high then
  if a[low] == v then
    return low
  else
    return -1
  end if
else
  mid \leftarrow (low + high)/2
  if v \leq a[mid] then
    return binarySearch(a, v, low, mid)
  else
    return binarySearch(a, v, mid + 1, high)
  end if
end if
```

	0	0000	L	L		
	1	0001				
	2	0010				
	3	0011				
	4	0100			L	L
*	5	0101				Н
	6	0110				
	7	0111		Н	H	
	8	1000				
	9	1001				
	10	1010				
	11	1011				
	12	1100				
	13	1101				
	14	1110				
	15	1111	Н			

			1		
	0	0000	L	L	
	1	0001			
	2	0010			
	3	0011			
	4	0100			L
*	5	0101			
	6	0110			
	7	0111		Н	Н
	8	1000	,) 4		
	9	1001			
	10	1010			
	11	1011			
	12	1100			
	13	1101			
	14	1110	•		
	15	1111	Н		

L L H L=H

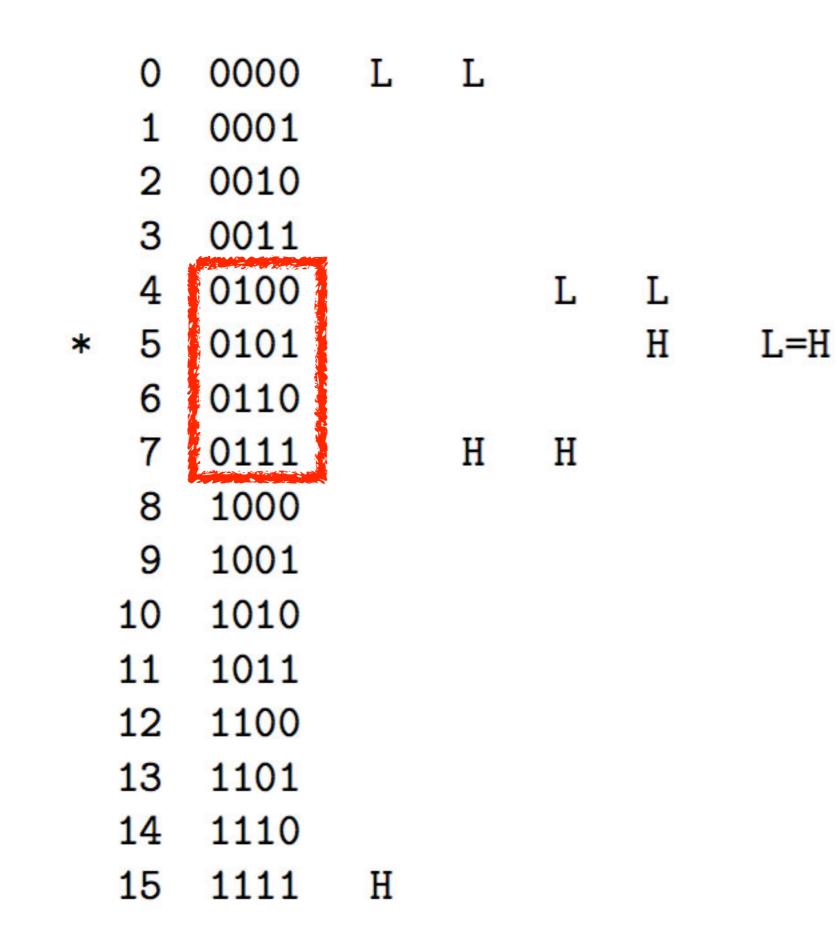
	0	0000	L	L		
	1	0001				
	2	0010				
	3	0011				
	4	0100			L	L
*	5	0101				Н
	6	0110				
	7	0111		Н	H	
	8	1000				
	9	1001				
	10	1010				
	11	1011				
	12	1100				
	13	1101				
	14	1110				
	15	1111	Н			



L L H

Η

	0	0000	L	L		
	1	0001				
	2	0010				
	3	0011				
	4	0100			L	L
*	5	0101				Н
	6	0110				
	7	0111		Н	H	
	8	1000				
	9	1001				
	10	1010				
	11	1011				
	12	1100				
	13	1101				
	14	1110				
	15	1111	Н			



	0	0000	L	L		
	1	0001				
	2	0010				
	3	0011				
	4	0100			L	L
*	5	0101				Н
	6	0110				
	7	0111		Н	H	
	8	1000				
	9	1001				
	10	1010				
	11	1011				
	12	1100				
	13	1101				
	14	1110				
	15	1111	Н			

	0	0000	L	L		
	1	0001				
	2	0010				
	3	0011				
	4	0100			L	L
*	5	0101				Н
	6	0110				
	7	0111		Н	Η	
	8	1000				
	9	1001				
	10	1010				
	11	1011				
	12	1100				
	13	1101				
	14	1110				
	15	1111	Η			

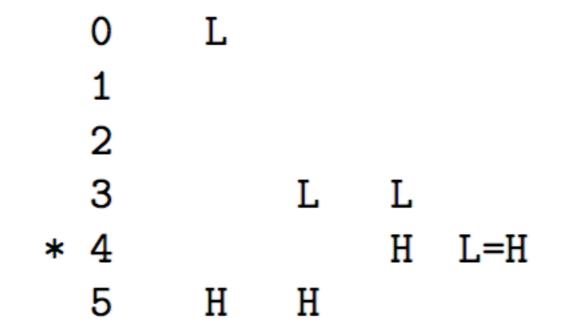
	0	0000	L	L		
	1	0001				
	2	0010				
	3	0011				
	4	0100			L	L
*	5	0101				Н
	6	0110				
	7	0111		Н	H	
	8	1000				
	9	1001				
	10	1010				
	11	1011				
	12	1100				
	13	1101				
	14	1110				
	15	1111	Н			

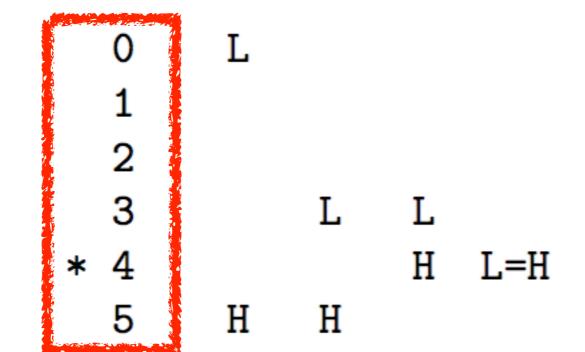
	0	0000	L	L	
	1	0001			
	2	0010			
	3	0011			
	4	0100			
*	5	0101			
	6	0110			
	7	0111		Н	
	8	1000			
	9	1001			
	10	1010			
	11	1011			
	12	1100			
	13	1101			
	14	1110			
	15	1111	Η		

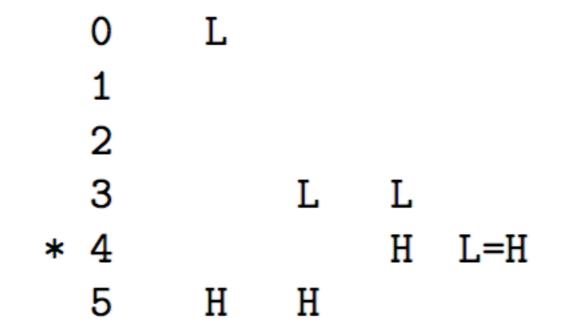
L L H L=H

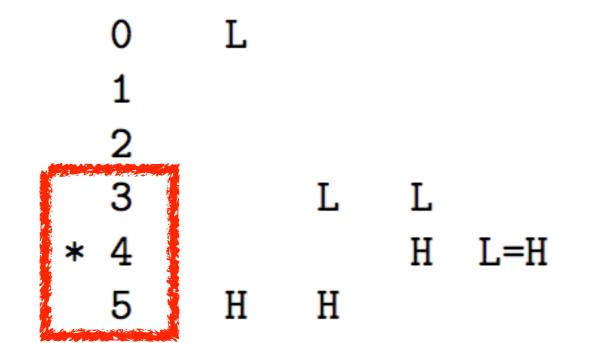
Η

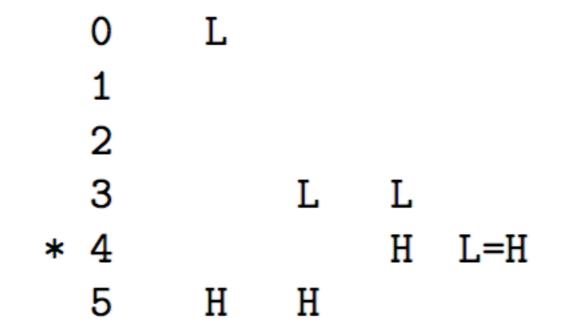
	0	0000	L	L		
	1	0001				
	2	0010				
	3	0011				
	4	0100			L	L
*	5	0101				Н
	6	0110				
	7	0111		Н	H	
	8	1000				
	9	1001				
	10	1010				
	11	1011				
	12	1100				
	13	1101				
	14	1110				
	15	1111	Н			

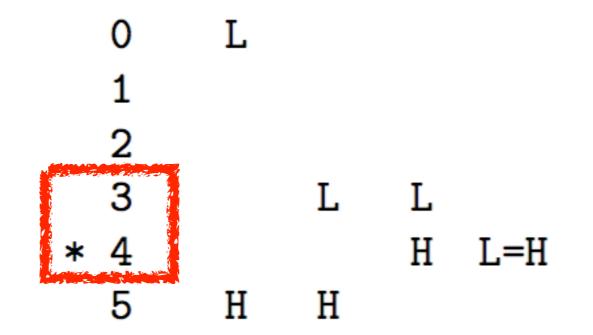


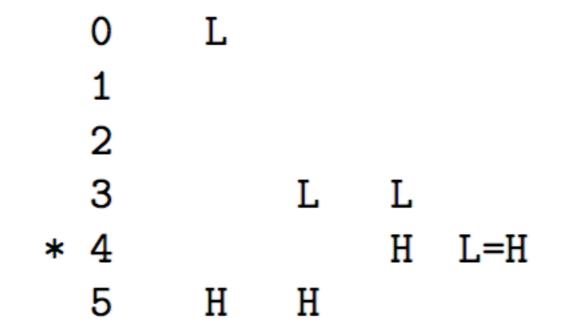


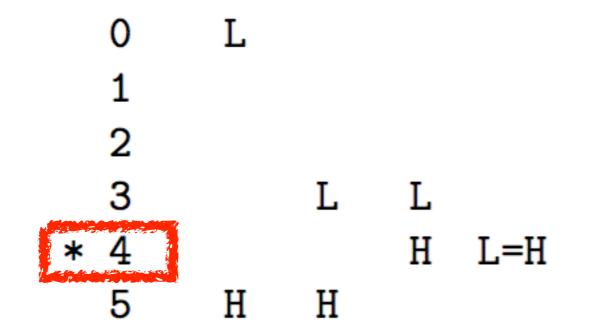


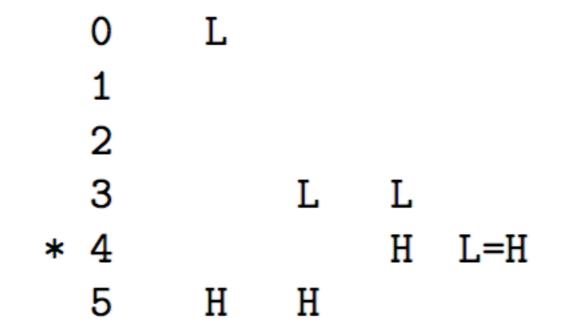












Recurrence Relation

Def. T(n) = number of comparisons to find v among n sorted elements.

Binary Search recurrence.

$$T(n) = \begin{cases} 1 & \text{if } n = 1 \\ T(n/2) + 1 & \text{if } n > 1 \end{cases}$$

Solution. T(n) is O(log n) (Master Theorem Case 2).

Divide-and-Conquer Multiplication

Integer Multiplication

1 1 0 1 0 1 0 1 0 Multiply. Given two n-digit integers a and b, compute a × b. × 0 1 1 1 1 1 0 1 • Grade School solution: $\Theta(n^2)$ bit operations. 1 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 Multiply 1 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 + 0 1 1 0

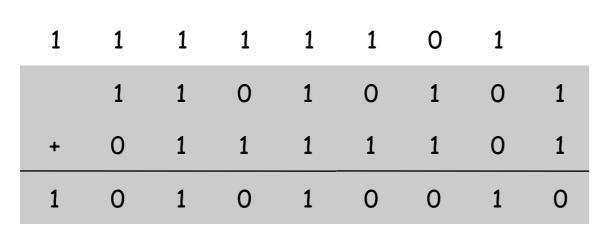
Integer Multiplication

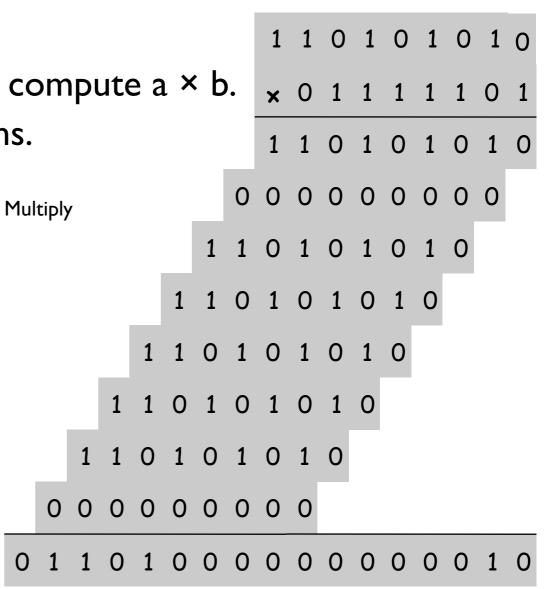
Add. Given two n-digit integers a and b, compute a + b.

Θ(n) bit operations.

Multiply. Given two n-digit integers a and b, compute a × b.

• Grade School solution: $\Theta(n^2)$ bit operations.





D&C Multiplication

To multiply two n-digit integers:

- Multiply four ⁿ/₂-digit integers.
- Add two ⁿ/₂-digit integers, and shift to obtain result.

$$\begin{aligned} x &= 2^{n/2} \cdot x_1 + x_0 \\ y &= 2^{n/2} \cdot y_1 + y_0 \\ xy &= \left(2^{n/2} \cdot x_1 + x_0\right) \left(2^{n/2} \cdot y_1 + y_0\right) = 2^n \cdot x_1 y_1 + 2^{n/2} \cdot \left(x_1 y_0 + x_0 y_1\right) + x_0 y_0 \end{aligned}$$

$$T(n) = \underbrace{4T(n/2)}_{\text{recursive calls}} + \underbrace{\Theta(n)}_{\text{add, shift}} \Rightarrow T(n) \operatorname{is} \Theta(n^2)$$

assumes n is a power of 2

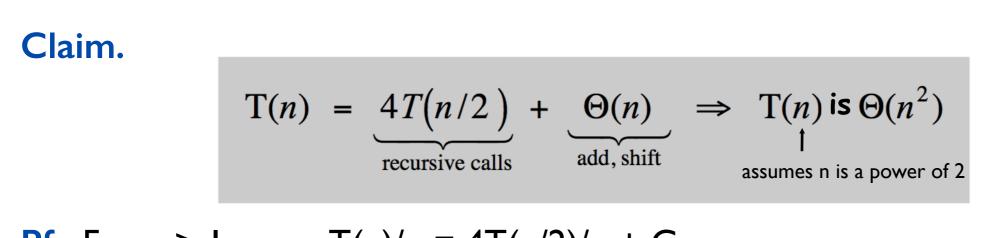
$$T(n) = \underbrace{4T(n/2)}_{\text{recursive calls}} + \underbrace{\Theta(n)}_{\text{add, shift}} \Rightarrow \underbrace{T(n) \text{ is } \Theta(n^2)}_{\text{t assumes n is a power of 2}}$$

$$T(n) = \underbrace{4T(n/2)}_{\text{recursive calls}} + \underbrace{\Theta(n)}_{\text{add, shift}} \Rightarrow \underbrace{T(n) \text{ is } \Theta(n^2)}_{\text{1}}$$

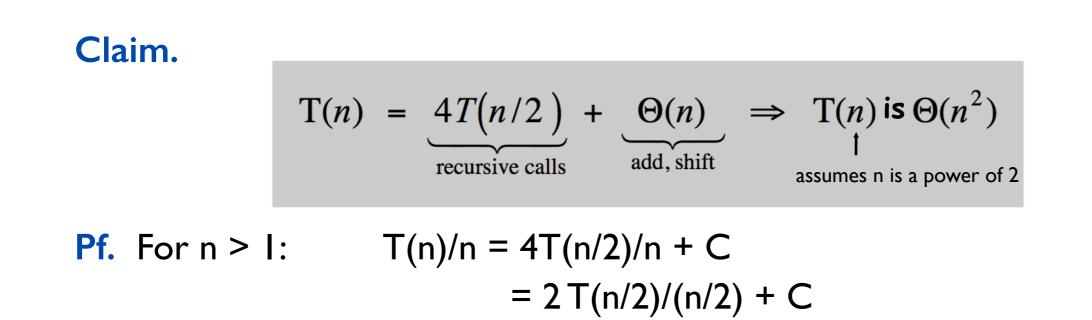
$$T(n) = \underbrace{4T(n/2)}_{\text{recursive calls}} + \underbrace{\Theta(n)}_{\text{add, shift}} \Rightarrow \underbrace{T(n) \text{ is } \Theta(n^2)}_{\text{1}}$$

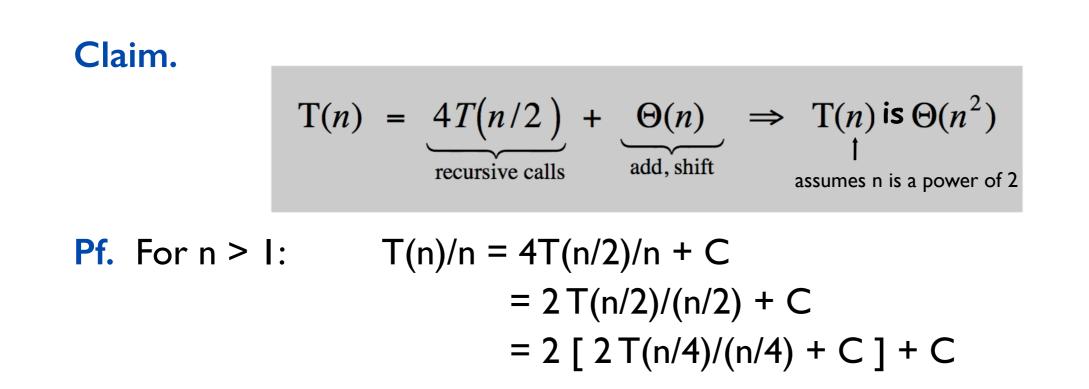
$$T(n) = \underbrace{4T(n/2)}_{\text{recursive calls}} + \underbrace{\Theta(n)}_{\text{add, shift}} \Rightarrow \underbrace{T(n) \text{ is } \Theta(n^2)}_{\text{1}}$$

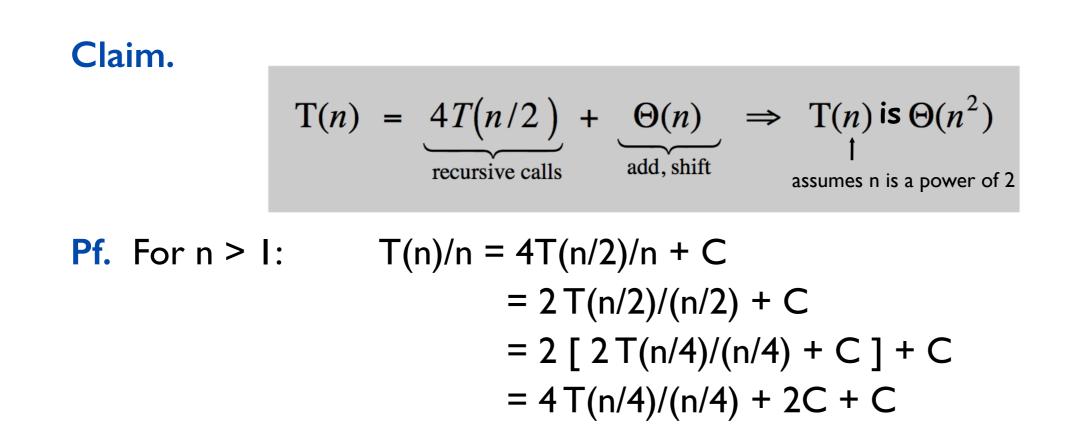
$$T(n) = \underbrace{4T(n/2)}_{\text{recursive calls}} + \underbrace{\Theta(n)}_{\text{add, shift}} \Rightarrow \underbrace{T(n) \text{ is } \Theta(n^2)}_{\text{1}}$$

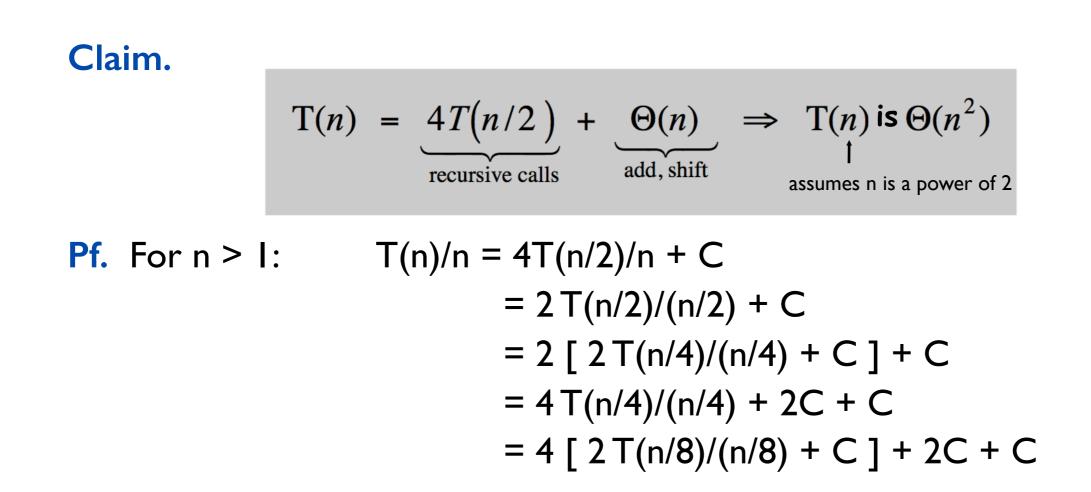


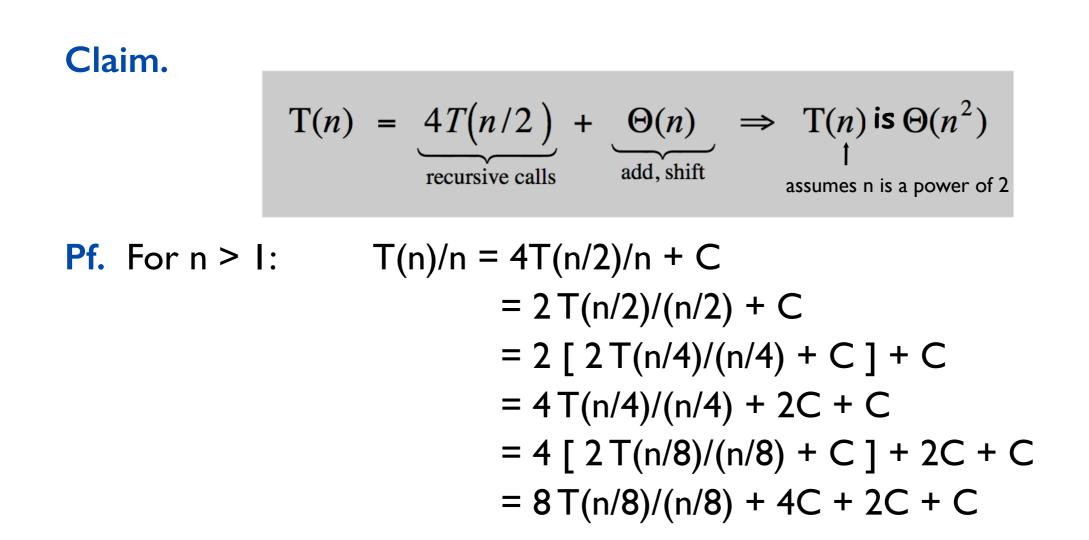
Pf. For n > I: T(n)/n = 4T(n/2)/n + C

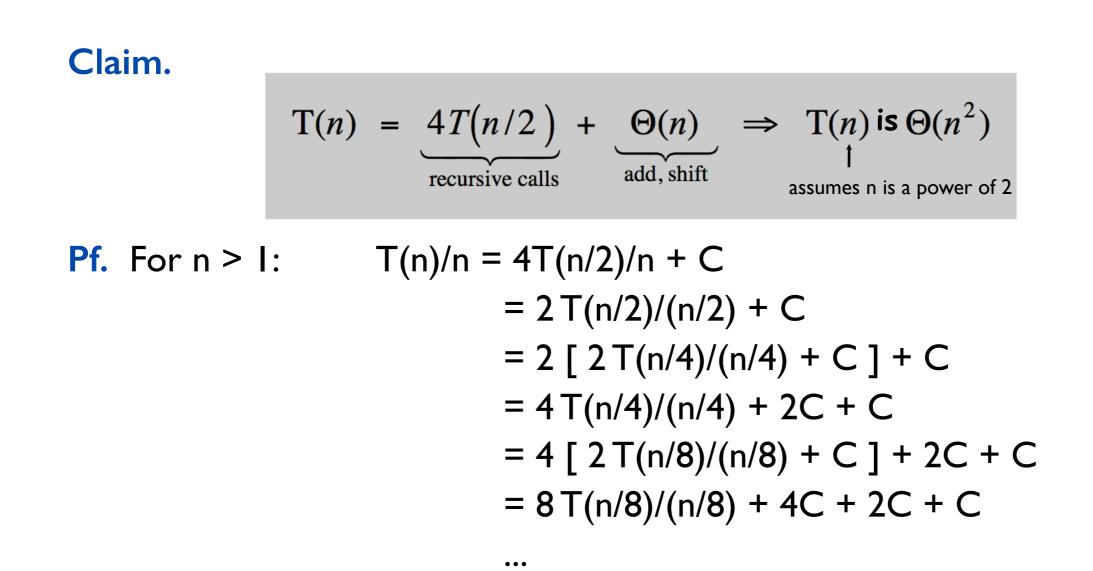


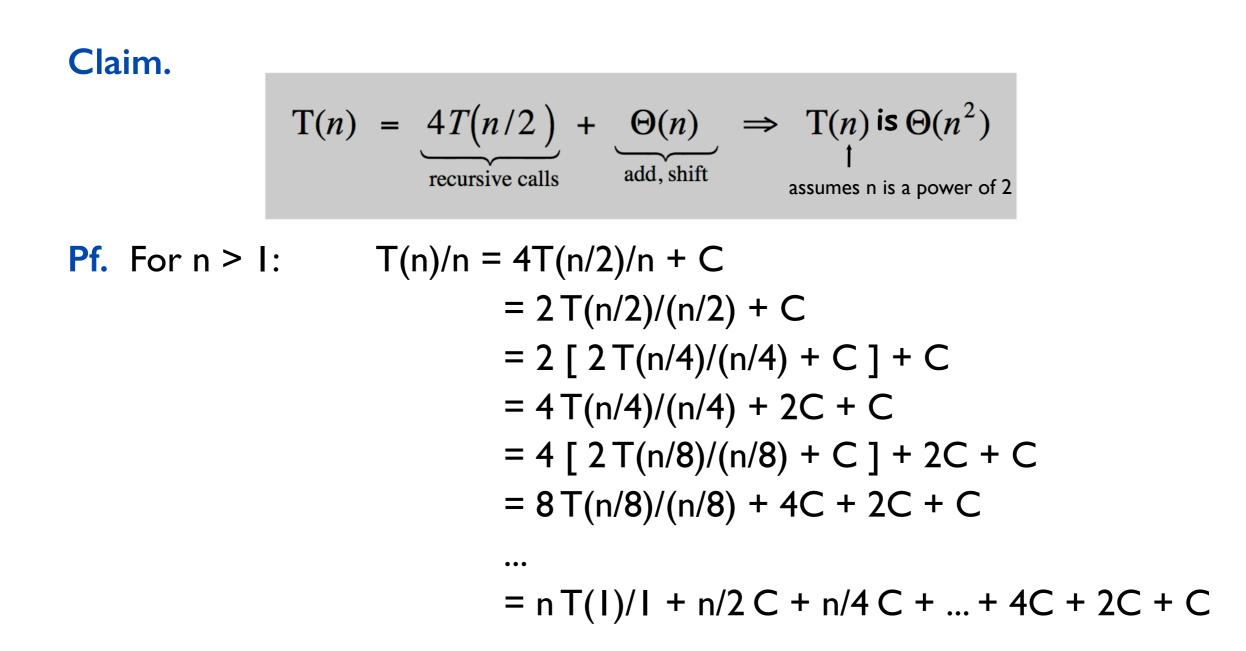


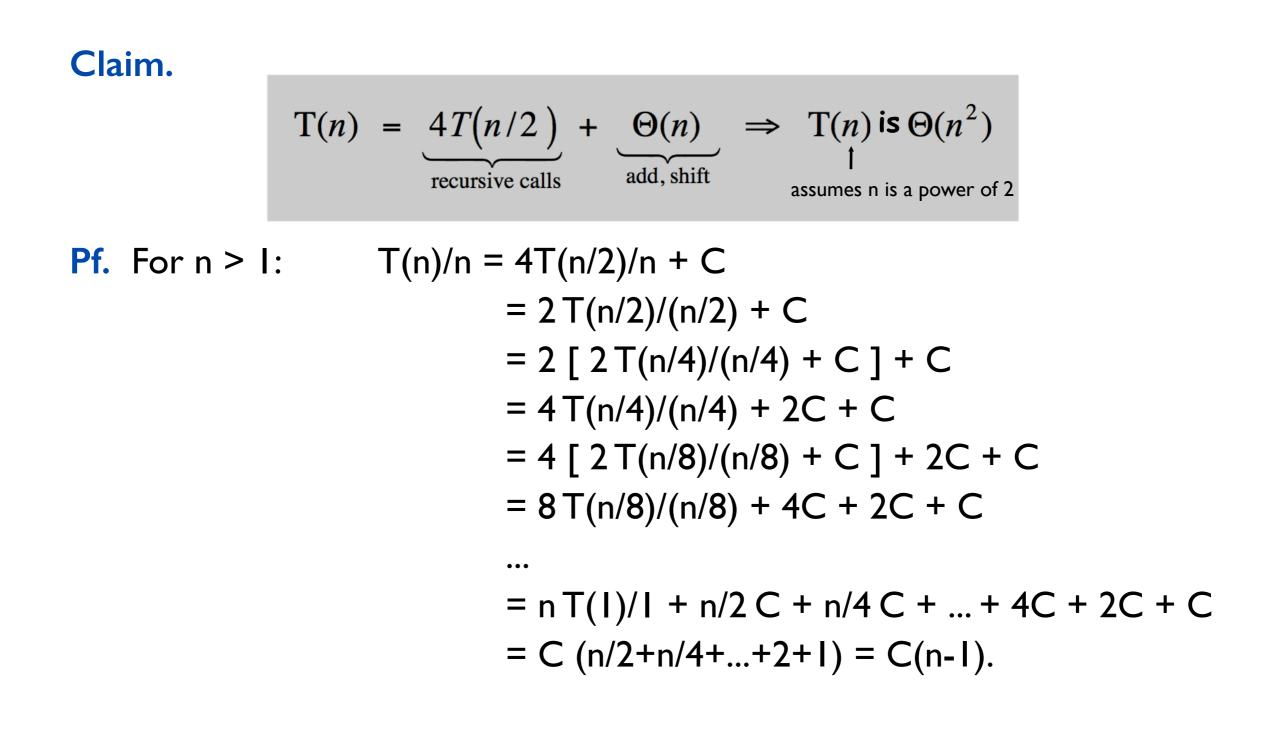












Karatsuba Multiplication

To multiply two n-digit integers:

- Add two ⁿ/₂ digit integers.
- Multiply three ⁿ/₂-digit integers.
- Add, subtract, and shift ⁿ/₂-digit integers to obtain result.

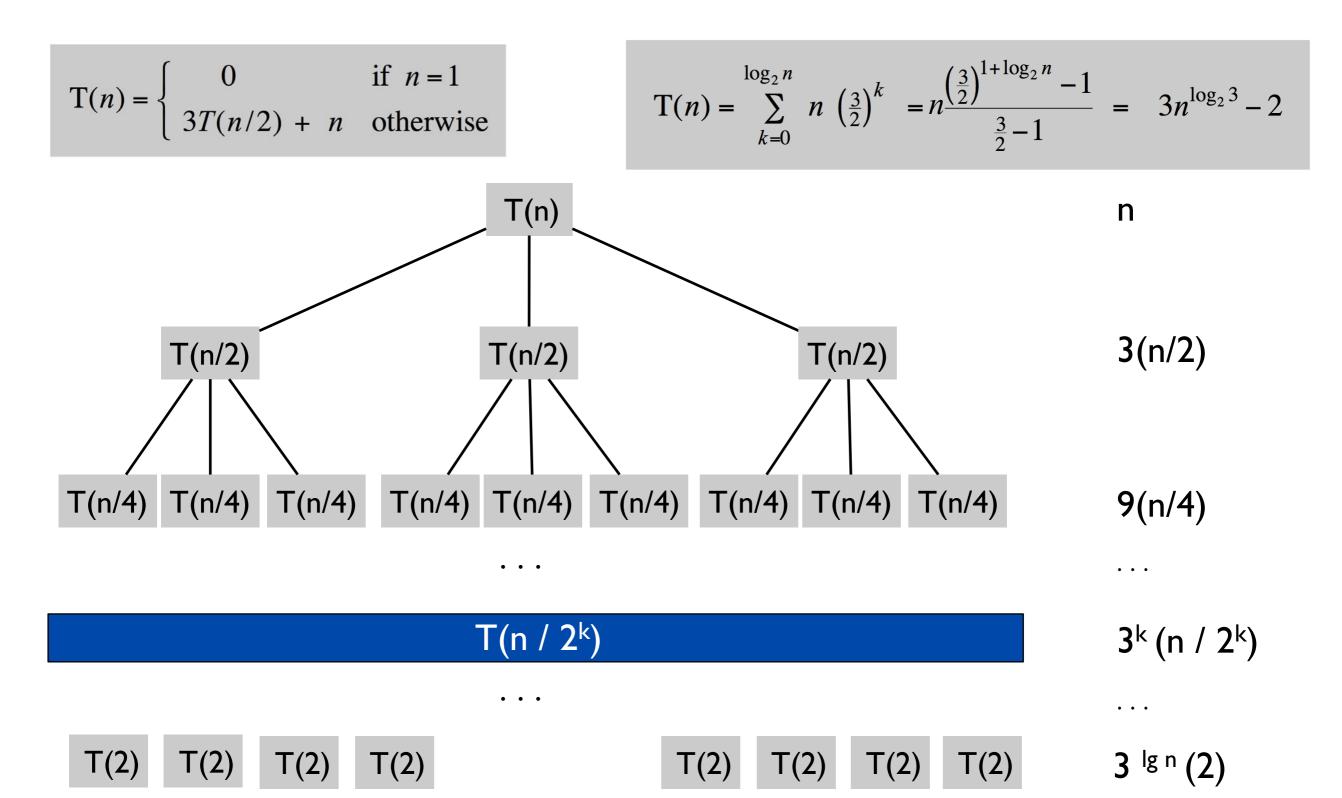
$$\begin{array}{rcl} x & = & 2^{n/2} \cdot x_1 \, + \, x_0 \\ y & = & 2^{n/2} \cdot y_1 \, + \, y_0 \\ xy & = & 2^n \cdot x_1 y_1 \, + \, 2^{n/2} \cdot \left(x_1 y_0 + x_0 y_1 \right) \, + \, x_0 y_0 \\ & = & 2^n \cdot x_1 y_1 \, + \, 2^{n/2} \cdot \left(\, (x_1 + x_0) \, (y_1 + y_0) \, - \, x_1 y_1 \, - \, x_0 y_0 \right) \, + \, x_0 y_0 \\ & & & \mathsf{A} & & \mathsf{B} & & \mathsf{A} & \mathsf{C} & \mathsf{C} \end{array}$$

Theorem. [Karatsuba-Ofman, 1962] Can multiply two n-digit integers in $O(n^{1.585})$ bit operations.

$$T(n) \leq \underbrace{T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + T(1 + \lceil n/2 \rceil)}_{\text{recursive calls}} + \underbrace{\Theta(n)}_{\text{add, subtract, shift}}$$

$$\Rightarrow T(n) \text{ is } O(n^{\log_2 3}) \text{ is } O(n^{1.585})$$

$\sum_{k=0}^{n-1} ar^{k} = a \frac{1-r^{n}}{1-r}$ Karatsuba Recursion Tree



Karatsuba Multiplication

Generalization: $O(n^{1+\epsilon})$ for any $\epsilon > 0$.

Best known: n log n 2^{O(log* n)}

where
$$\log^*(x) = \begin{cases} 0 & \text{if } x \le 1 \\ 1 + \log^*(\log x) & \text{if } x > 1 \end{cases}$$

Conjecture: $\Omega(n \log n)$ but not proven yet.

Winter 2016 COMP-250: Introduction to Computer Science Lecture 12, February 18, 2016