

THOMAS H. CORMEN  
CHARLES E. LEISERSON  
RONALD L. RIVEST  
CLIFFORD STEIN

Over  
**1 MILLION**  
copies sold  
worldwide

INTRODUCTION TO

# ALGORITHMS

FOURTH EDITION



---

# **Introduction to Algorithms**

*Fourth Edition*



---

Thomas H. Cormen  
Charles E. Leiserson  
Ronald L. Rivest  
Clifford Stein

---

**Introduction to Algorithms**  
*Fourth Edition*

The MIT Press  
Cambridge, Massachusetts   London, England

© 2022 Massachusetts Institute of Technology

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher.

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in Times Roman and MathTime Professional II by the authors.

Names: Cormen, Thomas H., author. | Leiserson, Charles Eric, author. | Rivest, Ronald L., author. | Stein, Clifford, author.  
Title: Introduction to algorithms / Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein.  
Description: Fourth edition. | Cambridge, Massachusetts : The MIT Press, [2022] | Includes bibliographical references and index.  
Identifiers: LCCN 2021037260 | ISBN 9780262046305  
Subjects: LCSH: Computer programming. | Computer algorithms.  
Classification: LCC QA76.6 .C662 2022 | DDC 005.13--dc23  
LC record available at <http://lccn.loc.gov/2021037260>

10 9 8 7 6 5 4 3 2 1

# Contents

Preface    *xiii*

---

## *I Foundations*

---

	<b>Introduction</b>	<b>3</b>
<b>1</b>	<b>The Role of Algorithms in Computing</b>	<b>5</b>
1.1	Algorithms	5
1.2	Algorithms as a technology	12
<b>2</b>	<b>Getting Started</b>	<b>17</b>
2.1	Insertion sort	17
2.2	Analyzing algorithms	25
2.3	Designing algorithms	34
<b>3</b>	<b>Characterizing Running Times</b>	<b>49</b>
3.1	$O$ -notation, $\Omega$ -notation, and $\Theta$ -notation	50
3.2	Asymptotic notation: formal definitions	53
3.3	Standard notations and common functions	63
<b>4</b>	<b>Divide-and-Conquer</b>	<b>76</b>
4.1	Multiplying square matrices	80
4.2	Strassen's algorithm for matrix multiplication	85
4.3	The substitution method for solving recurrences	90
4.4	The recursion-tree method for solving recurrences	95
4.5	The master method for solving recurrences	101
★ 4.6	Proof of the continuous master theorem	107
★ 4.7	Akra-Bazzi recurrences	115

<b>5</b>	<b>Probabilistic Analysis and Randomized Algorithms</b>	<b>126</b>
5.1	The hiring problem	126
5.2	Indicator random variables	130
5.3	Randomized algorithms	134
★ 5.4	Probabilistic analysis and further uses of indicator random variables	140

---

## **II   *Sorting and Order Statistics***

---

	<b>Introduction</b>	<b>157</b>
<b>6</b>	<b>Heapsort</b>	<b>161</b>
6.1	Heaps	161
6.2	Maintaining the heap property	164
6.3	Building a heap	167
6.4	The heapsort algorithm	170
6.5	Priority queues	172
<b>7</b>	<b>Quicksort</b>	<b>182</b>
7.1	Description of quicksort	183
7.2	Performance of quicksort	187
7.3	A randomized version of quicksort	191
7.4	Analysis of quicksort	193
<b>8</b>	<b>Sorting in Linear Time</b>	<b>205</b>
8.1	Lower bounds for sorting	205
8.2	Counting sort	208
8.3	Radix sort	211
8.4	Bucket sort	215
<b>9</b>	<b>Medians and Order Statistics</b>	<b>227</b>
9.1	Minimum and maximum	228
9.2	Selection in expected linear time	230
9.3	Selection in worst-case linear time	236

---

## **III   *Data Structures***

---

	<b>Introduction</b>	<b>249</b>
<b>10</b>	<b>Elementary Data Structures</b>	<b>252</b>
10.1	Simple array-based data structures: arrays, matrices, stacks, queues	252
10.2	Linked lists	258
10.3	Representing rooted trees	265



<b>11</b>	<b>Hash Tables</b>	<b>272</b>
11.1	Direct-address tables	273
11.2	Hash tables	275
11.3	Hash functions	282
11.4	Open addressing	293
11.5	Practical considerations	301
<b>12</b>	<b>Binary Search Trees</b>	<b>312</b>
12.1	What is a binary search tree?	312
12.2	Querying a binary search tree	316
12.3	Insertion and deletion	321
<b>13</b>	<b>Red-Black Trees</b>	<b>331</b>
13.1	Properties of red-black trees	331
13.2	Rotations	335
13.3	Insertion	338
13.4	Deletion	346

---

## ***IV Advanced Design and Analysis Techniques***

---

	<b>Introduction</b>	<b>361</b>
<b>14</b>	<b>Dynamic Programming</b>	<b>362</b>
14.1	Rod cutting	363
14.2	Matrix-chain multiplication	373
14.3	Elements of dynamic programming	382
14.4	Longest common subsequence	393
14.5	Optimal binary search trees	400
<b>15</b>	<b>Greedy Algorithms</b>	<b>417</b>
15.1	An activity-selection problem	418
15.2	Elements of the greedy strategy	426
15.3	Huffman codes	431
15.4	Offline caching	440
<b>16</b>	<b>Amortized Analysis</b>	<b>448</b>
16.1	Aggregate analysis	449
16.2	The accounting method	453
16.3	The potential method	456
16.4	Dynamic tables	460

---

**V Advanced Data Structures**

---

	<b>Introduction</b>	<b>477</b>
<b>17</b>	<b>Augmenting Data Structures</b>	<b>480</b>
	17.1 Dynamic order statistics	480
	17.2 How to augment a data structure	486
	17.3 Interval trees	489
<b>18</b>	<b>B-Trees</b>	<b>497</b>
	18.1 Definition of B-trees	501
	18.2 Basic operations on B-trees	504
	18.3 Deleting a key from a B-tree	513
<b>19</b>	<b>Data Structures for Disjoint Sets</b>	<b>520</b>
	19.1 Disjoint-set operations	520
	19.2 Linked-list representation of disjoint sets	523
	19.3 Disjoint-set forests	527
★	19.4 Analysis of union by rank with path compression	531

---

**VI Graph Algorithms**

---

	<b>Introduction</b>	<b>547</b>
<b>20</b>	<b>Elementary Graph Algorithms</b>	<b>549</b>
	20.1 Representations of graphs	549
	20.2 Breadth-first search	554
	20.3 Depth-first search	563
	20.4 Topological sort	573
	20.5 Strongly connected components	576
<b>21</b>	<b>Minimum Spanning Trees</b>	<b>585</b>
	21.1 Growing a minimum spanning tree	586
	21.2 The algorithms of Kruskal and Prim	591
<b>22</b>	<b>Single-Source Shortest Paths</b>	<b>604</b>
	22.1 The Bellman-Ford algorithm	612
	22.2 Single-source shortest paths in directed acyclic graphs	616
	22.3 Dijkstra's algorithm	620
	22.4 Difference constraints and shortest paths	626
	22.5 Proofs of shortest-paths properties	633

<b>23</b>	<b>All-Pairs Shortest Paths</b>	<b>646</b>
23.1	Shortest paths and matrix multiplication	648
23.2	The Floyd-Warshall algorithm	655
23.3	Johnson's algorithm for sparse graphs	662
<b>24</b>	<b>Maximum Flow</b>	<b>670</b>
24.1	Flow networks	671
24.2	The Ford-Fulkerson method	676
24.3	Maximum bipartite matching	693
<b>25</b>	<b>Matchings in Bipartite Graphs</b>	<b>704</b>
25.1	Maximum bipartite matching (revisited)	705
25.2	The stable-marriage problem	716
25.3	The Hungarian algorithm for the assignment problem	723

---

## VII Selected Topics

---

	<b>Introduction</b>	<b>745</b>
<b>26</b>	<b>Parallel Algorithms</b>	<b>748</b>
26.1	The basics of fork-join parallelism	750
26.2	Parallel matrix multiplication	770
26.3	Parallel merge sort	775
<b>27</b>	<b>Online Algorithms</b>	<b>791</b>
27.1	Waiting for an elevator	792
27.2	Maintaining a search list	795
27.3	Online caching	802
<b>28</b>	<b>Matrix Operations</b>	<b>819</b>
28.1	Solving systems of linear equations	819
28.2	Inverting matrices	833
28.3	Symmetric positive-definite matrices and least-squares approximation	838
<b>29</b>	<b>Linear Programming</b>	<b>850</b>
29.1	Linear programming formulations and algorithms	853
29.2	Formulating problems as linear programs	860
29.3	Duality	866
<b>30</b>	<b>Polynomials and the FFT</b>	<b>877</b>
30.1	Representing polynomials	879
30.2	The DFT and FFT	885
30.3	FFT circuits	894

<b>31</b>	<b>Number-Theoretic Algorithms</b>	<b>903</b>
31.1	Elementary number-theoretic notions	904
31.2	Greatest common divisor	911
31.3	Modular arithmetic	916
31.4	Solving modular linear equations	924
31.5	The Chinese remainder theorem	928
31.6	Powers of an element	932
31.7	The RSA public-key cryptosystem	936
★ 31.8	Primality testing	942
<b>32</b>	<b>String Matching</b>	<b>957</b>
32.1	The naive string-matching algorithm	960
32.2	The Rabin-Karp algorithm	962
32.3	String matching with finite automata	967
★ 32.4	The Knuth-Morris-Pratt algorithm	975
32.5	Suffix arrays	985
<b>33</b>	<b>Machine-Learning Algorithms</b>	<b>1003</b>
33.1	Clustering	1005
33.2	Multiplicative-weights algorithms	1015
33.3	Gradient descent	1022
<b>34</b>	<b>NP-Completeness</b>	<b>1042</b>
34.1	Polynomial time	1048
34.2	Polynomial-time verification	1056
34.3	NP-completeness and reducibility	1061
34.4	NP-completeness proofs	1072
34.5	NP-complete problems	1080
<b>35</b>	<b>Approximation Algorithms</b>	<b>1104</b>
35.1	The vertex-cover problem	1106
35.2	The traveling-salesperson problem	1109
35.3	The set-covering problem	1115
35.4	Randomization and linear programming	1119
35.5	The subset-sum problem	1124

---

## VIII Appendix: Mathematical Background

---

	<b>Introduction</b>	<b>1139</b>
<b>A</b>	<b>Summations</b>	<b>1140</b>
A.1	Summation formulas and properties	1140
A.2	Bounding summations	1145

<b>B</b>	<b>Sets, Etc.</b>	<b>1153</b>
	B.1 Sets	1153
	B.2 Relations	1158
	B.3 Functions	1161
	B.4 Graphs	1164
	B.5 Trees	1169
<b>C</b>	<b>Counting and Probability</b>	<b>1178</b>
	C.1 Counting	1178
	C.2 Probability	1184
	C.3 Discrete random variables	1191
	C.4 The geometric and binomial distributions	1196
★	C.5 The tails of the binomial distribution	1203
<b>D</b>	<b>Matrices</b>	<b>1214</b>
	D.1 Matrices and matrix operations	1214
	D.2 Basic matrix properties	1219

---

**Bibliography** 1227

**Index** 1251

---

## 3 Characterizing Running Times

The order of growth of the running time of an algorithm, defined in Chapter 2, gives a simple way to characterize the algorithm's efficiency and also allows us to compare it with alternative algorithms. Once the input size  $n$  becomes large enough, merge sort, with its  $\Theta(n \lg n)$  worst-case running time, beats insertion sort, whose worst-case running time is  $\Theta(n^2)$ . Although we can sometimes determine the exact running time of an algorithm, as we did for insertion sort in Chapter 2, the extra precision is rarely worth the effort of computing it. For large enough inputs, the multiplicative constants and lower-order terms of an exact running time are dominated by the effects of the input size itself.

When we look at input sizes large enough to make relevant only the order of growth of the running time, we are studying the *asymptotic* efficiency of algorithms. That is, we are concerned with how the running time of an algorithm increases with the size of the input *in the limit*, as the size of the input increases without bound. Usually, an algorithm that is asymptotically more efficient is the best choice for all but very small inputs.

This chapter gives several standard methods for simplifying the asymptotic analysis of algorithms. The next section presents informally the three most commonly used types of “asymptotic notation,” of which we have already seen an example in  $\Theta$ -notation. It also shows one way to use these asymptotic notations to reason about the worst-case running time of insertion sort. Then we look at asymptotic notations more formally and present several notational conventions used throughout this book. The last section reviews the behavior of functions that commonly arise when analyzing algorithms.

### 3.1 $O$ -notation, $\Omega$ -notation, and $\Theta$ -notation

When we analyzed the worst-case running time of insertion sort in Chapter 2, we started with the complicated expression

$$\left(\frac{c_5}{2} + \frac{c_6}{2} + \frac{c_7}{2}\right)n^2 + \left(c_1 + c_2 + c_4 + \frac{c_5}{2} - \frac{c_6}{2} - \frac{c_7}{2} + c_8\right)n - (c_2 + c_4 + c_5 + c_8).$$

We then discarded the lower-order terms  $(c_1 + c_2 + c_4 + c_5/2 - c_6/2 - c_7/2 + c_8)n$  and  $c_2 + c_4 + c_5 + c_8$ , and we also ignored the coefficient  $c_5/2 + c_6/2 + c_7/2$  of  $n^2$ . That left just the factor  $n^2$ , which we put into  $\Theta$ -notation as  $\Theta(n^2)$ . We use this style to characterize running times of algorithms: discard the lower-order terms and the coefficient of the leading term, and use a notation that focuses on the rate of growth of the running time.

$\Theta$ -notation is not the only such “asymptotic notation.” In this section, we’ll see other forms of asymptotic notation as well. We start with intuitive looks at these notations, revisiting insertion sort to see how we can apply them. In the next section, we’ll see the formal definitions of our asymptotic notations, along with conventions for using them.

Before we get into specifics, bear in mind that the asymptotic notations we’ll see are designed so that they characterize functions in general. It so happens that the functions we are most interested in denote the running times of algorithms. But asymptotic notation can apply to functions that characterize some other aspect of algorithms (the amount of space they use, for example), or even to functions that have nothing whatsoever to do with algorithms.

#### $O$ -notation

$O$ -notation characterizes an *upper bound* on the asymptotic behavior of a function. In other words, it says that a function grows *no faster* than a certain rate, based on the highest-order term. Consider, for example, the function  $7n^3 + 100n^2 - 20n + 6$ . Its highest-order term is  $7n^3$ , and so we say that this function’s rate of growth is  $n^3$ . Because this function grows no faster than  $n^3$ , we can write that it is  $O(n^3)$ . You might be surprised that we can also write that the function  $7n^3 + 100n^2 - 20n + 6$  is  $O(n^4)$ . Why? Because the function grows more slowly than  $n^4$ , we are correct in saying that it grows no faster. As you might have guessed, this function is also  $O(n^5)$ ,  $O(n^6)$ , and so on. More generally, it is  $O(n^c)$  for any constant  $c \geq 3$ .

**$\Omega$ -notation**

$\Omega$ -notation characterizes a *lower bound* on the asymptotic behavior of a function. In other words, it says that a function grows *at least as fast* as a certain rate, based—as in  $O$ -notation—on the highest-order term. Because the highest-order term in the function  $7n^3 + 100n^2 - 20n + 6$  grows at least as fast as  $n^3$ , this function is  $\Omega(n^3)$ . This function is also  $\Omega(n^2)$  and  $\Omega(n)$ . More generally, it is  $\Omega(n^c)$  for any constant  $c \leq 3$ .

 **$\Theta$ -notation**

$\Theta$ -notation characterizes a *tight bound* on the asymptotic behavior of a function. It says that a function grows *precisely* at a certain rate, based—once again—on the highest-order term. Put another way,  $\Theta$ -notation characterizes the rate of growth of the function to within a constant factor from above and to within a constant factor from below. These two constant factors need not be equal.

If you can show that a function is both  $O(f(n))$  and  $\Omega(f(n))$  for some function  $f(n)$ , then you have shown that the function is  $\Theta(f(n))$ . (The next section states this fact as a theorem.) For example, since the function  $7n^3 + 100n^2 - 20n + 6$  is both  $O(n^3)$  and  $\Omega(n^3)$ , it is also  $\Theta(n^3)$ .

**Example: Insertion sort**

Let's revisit insertion sort and see how to work with asymptotic notation to characterize its  $\Theta(n^2)$  worst-case running time without evaluating summations as we did in Chapter 2. Here is the INSERTION-SORT procedure once again:

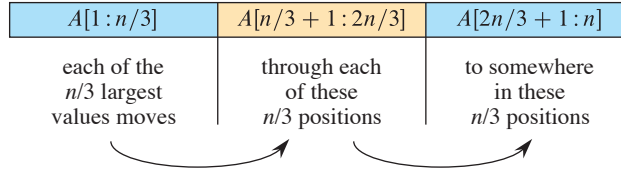
```

INSERTION-SORT( $A, n$ )
1  for  $i = 2$  to  $n$ 
2       $key = A[i]$ 
3      // Insert  $A[i]$  into the sorted subarray  $A[1 : i - 1]$ .
4       $j = i - 1$ 
5      while  $j > 0$  and  $A[j] > key$ 
6           $A[j + 1] = A[j]$ 
7           $j = j - 1$ 
8       $A[j + 1] = key$ 

```

What can we observe about how the pseudocode operates? The procedure has nested loops. The outer loop is a **for** loop that runs  $n - 1$  times, regardless of the values being sorted. The inner loop is a **while** loop, but the number of iterations it makes depends on the values being sorted. The loop variable  $j$  starts at  $i - 1$





**Figure 3.1** The  $\Omega(n^2)$  lower bound for insertion sort. If the first  $n/3$  positions contain the  $n/3$  largest values, each of these values must move through each of the middle  $n/3$  positions, one position at a time, to end up somewhere in the last  $n/3$  positions. Since each of  $n/3$  values moves through at least each of  $n/3$  positions, the time taken in this case is at least proportional to  $(n/3)(n/3) = n^2/9$ , or  $\Omega(n^2)$ .

and decreases by 1 in each iteration until either it reaches 0 or  $A[j] \leq \text{key}$ . For a given value of  $i$ , the **while** loop might iterate 0 times,  $i - 1$  times, or anywhere in between. The body of the **while** loop (lines 6–7) takes constant time per iteration of the **while** loop.

These observations suffice to deduce an  $O(n^2)$  running time for any case of INSERTION-SORT, giving us a blanket statement that covers all inputs. The running time is dominated by the inner loop. Because each of the  $n - 1$  iterations of the outer loop causes the inner loop to iterate at most  $i - 1$  times, and because  $i$  is at most  $n$ , the total number of iterations of the inner loop is at most  $(n - 1)(n - 1)$ , which is less than  $n^2$ . Since each iteration of the inner loop takes constant time, the total time spent in the inner loop is at most a constant times  $n^2$ , or  $O(n^2)$ .

With a little creativity, we can also see that the worst-case running time of INSERTION-SORT is  $\Omega(n^2)$ . By saying that the worst-case running time of an algorithm is  $\Omega(n^2)$ , we mean that for every input size  $n$  above a certain threshold, there is at least one input of size  $n$  for which the algorithm takes at least  $cn^2$  time, for some positive constant  $c$ . It does not necessarily mean that the algorithm takes at least  $cn^2$  time for all inputs.

Let's now see why the worst-case running time of INSERTION-SORT is  $\Omega(n^2)$ . For a value to end up to the right of where it started, it must have been moved in line 6. In fact, for a value to end up  $k$  positions to the right of where it started, line 6 must have executed  $k$  times. As Figure 3.1 shows, let's assume that  $n$  is a multiple of 3 so that we can divide the array  $A$  into groups of  $n/3$  positions. Suppose that in the input to INSERTION-SORT, the  $n/3$  largest values occupy the first  $n/3$  array positions  $A[1 : n/3]$ . (It does not matter what relative order they have within the first  $n/3$  positions.) Once the array has been sorted, each of these  $n/3$  values ends up somewhere in the last  $n/3$  positions  $A[2n/3 + 1 : n]$ . For that to happen, each of these  $n/3$  values must pass through each of the middle  $n/3$  positions  $A[n/3 + 1 : 2n/3]$ . Each of these  $n/3$  values passes through these middle

$n/3$  positions one position at a time, by at least  $n/3$  executions of line 6. Because at least  $n/3$  values have to pass through at least  $n/3$  positions, the time taken by INSERTION-SORT in the worst case is at least proportional to  $(n/3)(n/3) = n^2/9$ , which is  $\Omega(n^2)$ .

Because we have shown that INSERTION-SORT runs in  $O(n^2)$  time in all cases and that there is an input that makes it take  $\Omega(n^2)$  time, we can conclude that the worst-case running time of INSERTION-SORT is  $\Theta(n^2)$ . It does not matter that the constant factors for upper and lower bounds might differ. What matters is that we have characterized the worst-case running time to within constant factors (discounting lower-order terms). This argument does not show that INSERTION-SORT runs in  $\Theta(n^2)$  time in *all* cases. Indeed, we saw in Chapter 2 that the best-case running time is  $\Theta(n)$ .

### Exercises

#### 3.1-1

Modify the lower-bound argument for insertion sort to handle input sizes that are not necessarily a multiple of 3.

#### 3.1-2

Using reasoning similar to what we used for insertion sort, analyze the running time of the selection sort algorithm from Exercise 2.2-2.

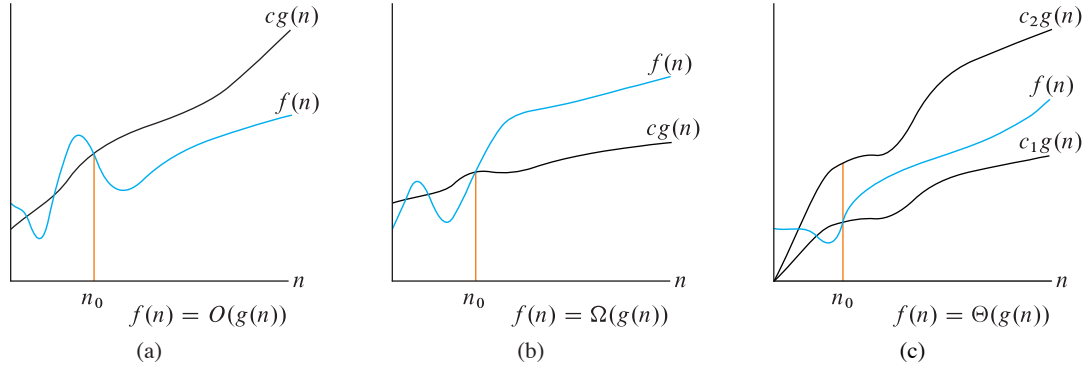
#### 3.1-3

Suppose that  $\alpha$  is a fraction in the range  $0 < \alpha < 1$ . Show how to generalize the lower-bound argument for insertion sort to consider an input in which the  $\alpha n$  largest values start in the first  $\alpha n$  positions. What additional restriction do you need to put on  $\alpha$ ? What value of  $\alpha$  maximizes the number of times that the  $\alpha n$  largest values must pass through each of the middle  $(1 - 2\alpha)n$  array positions?

---

## 3.2 Asymptotic notation: formal definitions

Having seen asymptotic notation informally, let's get more formal. The notations we use to describe the asymptotic running time of an algorithm are defined in terms of functions whose domains are typically the set  $\mathbb{N}$  of natural numbers or the set  $\mathbb{R}$  of real numbers. Such notations are convenient for describing a running-time function  $T(n)$ . This section defines the basic asymptotic notations and also introduces some common "proper" notational abuses.



**Figure 3.2** Graphic examples of the  $O$ ,  $\Omega$ , and  $\Theta$  notations. In each part, the value of  $n_0$  shown is the minimum possible value, but any greater value also works. **(a)**  $O$ -notation gives an upper bound for a function to within a constant factor. We write  $f(n) = O(g(n))$  if there are positive constants  $n_0$  and  $c$  such that at and to the right of  $n_0$ , the value of  $f(n)$  always lies on or below  $cg(n)$ . **(b)**  $\Omega$ -notation gives a lower bound for a function to within a constant factor. We write  $f(n) = \Omega(g(n))$  if there are positive constants  $n_0$  and  $c$  such that at and to the right of  $n_0$ , the value of  $f(n)$  always lies on or above  $cg(n)$ . **(c)**  $\Theta$ -notation bounds a function to within constant factors. We write  $f(n) = \Theta(g(n))$  if there exist positive constants  $n_0$ ,  $c_1$ , and  $c_2$  such that at and to the right of  $n_0$ , the value of  $f(n)$  always lies between  $c_1g(n)$  and  $c_2g(n)$  inclusive.

### **$O$ -notation**

As we saw in Section 3.1,  $O$ -notation describes an *asymptotic upper bound*. We use  $O$ -notation to give an upper bound on a function, to within a constant factor.

Here is the formal definition of  $O$ -notation. For a given function  $g(n)$ , we denote by  $O(g(n))$  (pronounced “big-oh of  $g$  of  $n$ ” or sometimes just “oh of  $g$  of  $n$ ”) the *set of functions*

$$O(g(n)) = \{f(n) : \text{there exist positive constants } c \text{ and } n_0 \text{ such that } 0 \leq f(n) \leq cg(n) \text{ for all } n \geq n_0\}^1$$

A function  $f(n)$  belongs to the set  $O(g(n))$  if there exists a positive constant  $c$  such that  $f(n) \leq cg(n)$  for sufficiently large  $n$ . Figure 3.2(a) shows the intuition behind  $O$ -notation. For all values  $n$  at and to the right of  $n_0$ , the value of the function  $f(n)$  is on or below  $cg(n)$ .

The definition of  $O(g(n))$  requires that every function  $f(n)$  in the set  $O(g(n))$  be *asymptotically nonnegative*:  $f(n)$  must be nonnegative whenever  $n$  is sufficiently large. (An *asymptotically positive* function is one that is positive for all

<sup>1</sup> Within set notation, a colon means “such that.”

sufficiently large  $n$ .) Consequently, the function  $g(n)$  itself must be asymptotically nonnegative, or else the set  $O(g(n))$  is empty. We therefore assume that every function used within  $O$ -notation is asymptotically nonnegative. This assumption holds for the other asymptotic notations defined in this chapter as well.

You might be surprised that we define  $O$ -notation in terms of sets. Indeed, you might expect that we would write “ $f(n) \in O(g(n))$ ” to indicate that  $f(n)$  belongs to the set  $O(g(n))$ . Instead, we usually write “ $f(n) = O(g(n))$ ” and say “ $f(n)$  is big-oh of  $g(n)$ ” to express the same notion. Although it may seem confusing at first to abuse equality in this way, we’ll see later in this section that doing so has its advantages.

Let’s explore an example of how to use the formal definition of  $O$ -notation to justify our practice of discarding lower-order terms and ignoring the constant coefficient of the highest-order term. We’ll show that  $4n^2 + 100n + 500 = O(n^2)$ , even though the lower-order terms have much larger coefficients than the leading term. We need to find positive constants  $c$  and  $n_0$  such that  $4n^2 + 100n + 500 \leq cn^2$  for all  $n \geq n_0$ . Dividing both sides by  $n^2$  gives  $4 + 100/n + 500/n^2 \leq c$ . This inequality is satisfied for many choices of  $c$  and  $n_0$ . For example, if we choose  $n_0 = 1$ , then this inequality holds for  $c = 604$ . If we choose  $n_0 = 10$ , then  $c = 19$  works, and choosing  $n_0 = 100$  allows us to use  $c = 5.05$ .

We can also use the formal definition of  $O$ -notation to show that the function  $n^3 - 100n^2$  does not belong to the set  $O(n^2)$ , even though the coefficient of  $n^2$  is a large negative number. If we had  $n^3 - 100n^2 = O(n^2)$ , then there would be positive constants  $c$  and  $n_0$  such that  $n^3 - 100n^2 \leq cn^2$  for all  $n \geq n_0$ . Again, we divide both sides by  $n^2$ , giving  $n - 100 \leq c$ . Regardless of what value we choose for the constant  $c$ , this inequality does not hold for any value of  $n > c + 100$ .

### $\Omega$ -notation

Just as  $O$ -notation provides an asymptotic *upper* bound on a function,  $\Omega$ -notation provides an *asymptotic lower bound*. For a given function  $g(n)$ , we denote by  $\Omega(g(n))$  (pronounced “big-omega of  $g$  of  $n$ ” or sometimes just “omega of  $g$  of  $n$ ”) the set of functions

$$\Omega(g(n)) = \{f(n) : \text{there exist positive constants } c \text{ and } n_0 \text{ such that } 0 \leq cg(n) \leq f(n) \text{ for all } n \geq n_0\}.$$

Figure 3.2(b) shows the intuition behind  $\Omega$ -notation. For all values  $n$  at or to the right of  $n_0$ , the value of  $f(n)$  is on or above  $cg(n)$ .

We’ve already shown that  $4n^2 + 100n + 500 = O(n^2)$ . Now let’s show that  $4n^2 + 100n + 500 = \Omega(n^2)$ . We need to find positive constants  $c$  and  $n_0$  such that  $4n^2 + 100n + 500 \geq cn^2$  for all  $n \geq n_0$ . As before, we divide both sides by  $n^2$ ,

giving  $4 + 100/n + 500/n^2 \geq c$ . This inequality holds when  $n_0$  is any positive integer and  $c = 4$ .

What if we had subtracted the lower-order terms from the  $4n^2$  term instead of adding them? What if we had a small coefficient for the  $n^2$  term? The function would still be  $\Omega(n^2)$ . For example, let's show that  $n^2/100 - 100n - 500 = \Omega(n^2)$ . Dividing by  $n^2$  gives  $1/100 - 100/n - 500/n^2 \geq c$ . We can choose any value for  $n_0$  that is at least 10,005 and find a positive value for  $c$ . For example, when  $n_0 = 10,005$ , we can choose  $c = 2.49 \times 10^{-9}$ . Yes, that's a tiny value for  $c$ , but it is positive. If we select a larger value for  $n_0$ , we can also increase  $c$ . For example, if  $n_0 = 100,000$ , then we can choose  $c = 0.0089$ . The higher the value of  $n_0$ , the closer to the coefficient  $1/100$  we can choose  $c$ .

### **$\Theta$ -notation**

We use  $\Theta$ -notation for *asymptotically tight bounds*. For a given function  $g(n)$ , we denote by  $\Theta(g(n))$  (“theta of  $g$  of  $n$ ”) the set of functions

$$\Theta(g(n)) = \{f(n) : \text{there exist positive constants } c_1, c_2, \text{ and } n_0 \text{ such that} \\ 0 \leq c_1 g(n) \leq f(n) \leq c_2 g(n) \text{ for all } n \geq n_0\}.$$

Figure 3.2(c) shows the intuition behind  $\Theta$ -notation. For all values of  $n$  at and to the right of  $n_0$ , the value of  $f(n)$  lies at or above  $c_1 g(n)$  and at or below  $c_2 g(n)$ . In other words, for all  $n \geq n_0$ , the function  $f(n)$  is equal to  $g(n)$  to within constant factors.

The definitions of  $O$ -,  $\Omega$ -, and  $\Theta$ -notations lead to the following theorem, whose proof we leave as Exercise 3.2-4.

#### **Theorem 3.1**

For any two functions  $f(n)$  and  $g(n)$ , we have  $f(n) = \Theta(g(n))$  if and only if  $f(n) = O(g(n))$  and  $f(n) = \Omega(g(n))$ . ■

We typically apply Theorem 3.1 to prove asymptotically tight bounds from asymptotic upper and lower bounds.

### **Asymptotic notation and running times**

When you use asymptotic notation to characterize an algorithm's running time, make sure that the asymptotic notation you use is as precise as possible without overstating which running time it applies to. Here are some examples of using asymptotic notation properly and improperly to characterize running times.

Let's start with insertion sort. We can correctly say that insertion sort's worst-case running time is  $O(n^2)$ ,  $\Omega(n^2)$ , and—due to Theorem 3.1— $\Theta(n^2)$ . Although

all three ways to characterize the worst-case running times are correct, the  $\Theta(n^2)$  bound is the most precise and hence the most preferred. We can also correctly say that insertion sort's best-case running time is  $O(n)$ ,  $\Omega(n)$ , and  $\Theta(n)$ , again with  $\Theta(n)$  the most precise and therefore the most preferred.

Here is what we *cannot* correctly say: insertion sort's running time is  $\Theta(n^2)$ . That is an overstatement because by omitting "worst-case" from the statement, we're left with a blanket statement covering all cases. The error here is that insertion sort does not run in  $\Theta(n^2)$  time in all cases since, as we've seen, it runs in  $\Theta(n)$  time in the best case. We can correctly say that insertion sort's running time is  $O(n^2)$ , however, because in all cases, its running time grows no faster than  $n^2$ . When we say  $O(n^2)$  instead of  $\Theta(n^2)$ , there is no problem in having cases whose running time grows more slowly than  $n^2$ . Likewise, we cannot correctly say that insertion sort's running time is  $\Theta(n)$ , but we can say that its running time is  $\Omega(n)$ .

How about merge sort? Since merge sort runs in  $\Theta(n \lg n)$  time in all cases, we can just say that its running time is  $\Theta(n \lg n)$  without specifying worst-case, best-case, or any other case.

People occasionally conflate  $O$ -notation with  $\Theta$ -notation by mistakenly using  $O$ -notation to indicate an asymptotically tight bound. They say things like "an  $O(n \lg n)$ -time algorithm runs faster than an  $O(n^2)$ -time algorithm." Maybe it does, maybe it doesn't. Since  $O$ -notation denotes only an asymptotic upper bound, that so-called  $O(n^2)$ -time algorithm might actually run in  $\Theta(n)$  time. You should be careful to choose the appropriate asymptotic notation. If you want to indicate an asymptotically tight bound, use  $\Theta$ -notation.

We typically use asymptotic notation to provide the simplest and most precise bounds possible. For example, if an algorithm has a running time of  $3n^2 + 20n$  in all cases, we use asymptotic notation to write that its running time is  $\Theta(n^2)$ . Strictly speaking, we are also correct in writing that the running time is  $O(n^3)$  or  $\Theta(3n^2 + 20n)$ . Neither of these expressions is as useful as writing  $\Theta(n^2)$  in this case, however:  $O(n^3)$  is less precise than  $\Theta(n^2)$  if the running time is  $3n^2 + 20n$ , and  $\Theta(3n^2 + 20n)$  introduces complexity that obscures the order of growth. By writing the simplest and most precise bound, such as  $\Theta(n^2)$ , we can categorize and compare different algorithms. Throughout the book, you will see asymptotic running times that are almost always based on polynomials and logarithms: functions such as  $n$ ,  $n \lg^2 n$ ,  $n^2 \lg n$ , or  $n^{1/2}$ . You will also see some other functions, such as exponentials,  $\lg \lg n$ , and  $\lg^* n$  (see Section 3.3). It is usually fairly easy to compare the rates of growth of these functions. Problem 3-3 gives you good practice.

### Asymptotic notation in equations and inequalities

Although we formally define asymptotic notation in terms of sets, we use the equal sign ( $=$ ) instead of the set membership sign ( $\in$ ) within formulas. For example, we wrote that  $4n^2 + 100n + 500 = O(n^2)$ . We might also write  $2n^2 + 3n + 1 = 2n^2 + \Theta(n)$ . How do we interpret such formulas?

When the asymptotic notation stands alone (that is, not within a larger formula) on the right-hand side of an equation (or inequality), as in  $4n^2 + 100n + 500 = O(n^2)$ , the equal sign means set membership:  $4n^2 + 100n + 500 \in O(n^2)$ . In general, however, when asymptotic notation appears in a formula, we interpret it as standing for some anonymous function that we do not care to name. For example, the formula  $2n^2 + 3n + 1 = 2n^2 + \Theta(n)$  means that  $2n^2 + 3n + 1 = 2n^2 + f(n)$ , where  $f(n) \in \Theta(n)$ . In this case, we let  $f(n) = 3n + 1$ , which indeed belongs to  $\Theta(n)$ .

Using asymptotic notation in this manner can help eliminate inessential detail and clutter in an equation. For example, in Chapter 2 we expressed the worst-case running time of merge sort as the recurrence

$$T(n) = 2T(n/2) + \Theta(n) .$$

If we are interested only in the asymptotic behavior of  $T(n)$ , there is no point in specifying all the lower-order terms exactly, because they are all understood to be included in the anonymous function denoted by the term  $\Theta(n)$ .

The number of anonymous functions in an expression is understood to be equal to the number of times the asymptotic notation appears. For example, in the expression

$$\sum_{i=1}^n O(i) ,$$

there is only a single anonymous function (a function of  $i$ ). This expression is thus *not* the same as  $O(1) + O(2) + \cdots + O(n)$ , which doesn't really have a clean interpretation.

In some cases, asymptotic notation appears on the left-hand side of an equation, as in

$$2n^2 + \Theta(n) = \Theta(n^2) .$$

Interpret such equations using the following rule: *No matter how the anonymous functions are chosen on the left of the equal sign, there is a way to choose the anonymous functions on the right of the equal sign to make the equation valid.* Thus, our example means that for *any* function  $f(n) \in \Theta(n)$ , there is *some* function  $g(n) \in \Theta(n^2)$  such that  $2n^2 + f(n) = g(n)$  for all  $n$ . In other words, the right-hand side of an equation provides a coarser level of detail than the left-hand side.

We can chain together a number of such relationships, as in

$$\begin{aligned} 2n^2 + 3n + 1 &= 2n^2 + \Theta(n) \\ &= \Theta(n^2) . \end{aligned}$$

By the rules above, interpret each equation separately. The first equation says that there is *some* function  $f(n) \in \Theta(n)$  such that  $2n^2 + 3n + 1 = 2n^2 + f(n)$  for all  $n$ . The second equation says that for *any* function  $g(n) \in \Theta(n)$  (such as the  $f(n)$  just mentioned), there is *some* function  $h(n) \in \Theta(n^2)$  such that  $2n^2 + g(n) = h(n)$  for all  $n$ . This interpretation implies that  $2n^2 + 3n + 1 = \Theta(n^2)$ , which is what the chaining of equations intuitively says.

### Proper abuses of asymptotic notation

Besides the abuse of equality to mean set membership, which we now see has a precise mathematical interpretation, another abuse of asymptotic notation occurs when the variable tending toward  $\infty$  must be inferred from context. For example, when we say  $O(g(n))$ , we can assume that we're interested in the growth of  $g(n)$  as  $n$  grows, and if we say  $O(g(m))$  we're talking about the growth of  $g(m)$  as  $m$  grows. The free variable in the expression indicates what variable is going to  $\infty$ .

The most common situation requiring contextual knowledge of which variable tends to  $\infty$  occurs when the function inside the asymptotic notation is a constant, as in the expression  $O(1)$ . We cannot infer from the expression which variable is going to  $\infty$ , because no variable appears there. The context must disambiguate. For example, if the equation using asymptotic notation is  $f(n) = O(1)$ , it's apparent that the variable we're interested in is  $n$ . Knowing from context that the variable of interest is  $n$ , however, allows us to make perfect sense of the expression by using the formal definition of  $O$ -notation: the expression  $f(n) = O(1)$  means that the function  $f(n)$  is bounded from above by a constant as  $n$  goes to  $\infty$ . Technically, it might be less ambiguous if we explicitly indicated the variable tending to  $\infty$  in the asymptotic notation itself, but that would clutter the notation. Instead, we simply ensure that the context makes it clear which variable (or variables) tend to  $\infty$ .

When the function inside the asymptotic notation is bounded by a positive constant, as in  $T(n) = O(1)$ , we often abuse asymptotic notation in yet another way, especially when stating recurrences. We may write something like  $T(n) = O(1)$  for  $n < 3$ . According to the formal definition of  $O$ -notation, this statement is meaningless, because the definition only says that  $T(n)$  is bounded above by a positive constant  $c$  for  $n \geq n_0$  for some  $n_0 > 0$ . The value of  $T(n)$  for  $n < n_0$  need not be so bounded. Thus, in the example  $T(n) = O(1)$  for  $n < 3$ , we cannot infer any constraint on  $T(n)$  when  $n < 3$ , because it might be that  $n_0 > 3$ .

What is conventionally meant when we say  $T(n) = O(1)$  for  $n < 3$  is that there exists a positive constant  $c$  such that  $T(n) \leq c$  for  $n < 3$ . This convention saves



us the trouble of naming the bounding constant, allowing it to remain anonymous while we focus on more important variables in an analysis. Similar abuses occur with the other asymptotic notations. For example,  $T(n) = \Theta(1)$  for  $n < 3$  means that  $T(n)$  is bounded above and below by positive constants when  $n < 3$ .

Occasionally, the function describing an algorithm's running time may not be defined for certain input sizes, for example, when an algorithm assumes that the input size is an exact power of 2. We still use asymptotic notation to describe the growth of the running time, understanding that any constraints apply only when the function is defined. For example, suppose that  $f(n)$  is defined only on a subset of the natural or nonnegative real numbers. Then  $f(n) = O(g(n))$  means that the bound  $0 \leq T(n) \leq cg(n)$  in the definition of  $O$ -notation holds for all  $n \geq n_0$  over the domain of  $f(n)$ , that is, where  $f(n)$  is defined. This abuse is rarely pointed out, since what is meant is generally clear from context.

In mathematics, it's okay—and often desirable—to abuse a notation, as long as we don't misuse it. If we understand precisely what is meant by the abuse and don't draw incorrect conclusions, it can simplify our mathematical language, contribute to our higher-level understanding, and help us focus on what really matters.

### ***o*-notation**

The asymptotic upper bound provided by  $O$ -notation may or may not be asymptotically tight. The bound  $2n^2 = O(n^2)$  is asymptotically tight, but the bound  $2n = O(n^2)$  is not. We use  $o$ -notation to denote an upper bound that is not asymptotically tight. We formally define  $o(g(n))$  ("little-oh of  $g$  of  $n$ ") as the set

$$o(g(n)) = \{f(n) : \text{for any positive constant } c > 0, \text{ there exists a constant } n_0 > 0 \text{ such that } 0 \leq f(n) < cg(n) \text{ for all } n \geq n_0\}.$$

For example,  $2n = o(n^2)$ , but  $2n^2 \neq o(n^2)$ .

The definitions of  $O$ -notation and  $o$ -notation are similar. The main difference is that in  $f(n) = O(g(n))$ , the bound  $0 \leq f(n) \leq cg(n)$  holds for *some* constant  $c > 0$ , but in  $f(n) = o(g(n))$ , the bound  $0 \leq f(n) < cg(n)$  holds for *all* constants  $c > 0$ . Intuitively, in  $o$ -notation, the function  $f(n)$  becomes insignificant relative to  $g(n)$  as  $n$  gets large:

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0.$$

Some authors use this limit as a definition of the  $o$ -notation, but the definition in this book also restricts the anonymous functions to be asymptotically nonnegative.

**$\omega$ -notation**

By analogy,  $\omega$ -notation is to  $\Omega$ -notation as  $o$ -notation is to  $O$ -notation. We use  $\omega$ -notation to denote a lower bound that is not asymptotically tight. One way to define it is by

$f(n) \in \omega(g(n))$  if and only if  $g(n) \in o(f(n))$ .

Formally, however, we define  $\omega(g(n))$  (“little-omega of  $g$  of  $n$ ”) as the set

$$\omega(g(n)) = \{f(n) : \text{for any positive constant } c > 0, \text{ there exists a constant } n_0 > 0 \text{ such that } 0 \leq cg(n) < f(n) \text{ for all } n \geq n_0\}.$$

Where the definition of  $o$ -notation says that  $f(n) < cg(n)$ , the definition of  $\omega$ -notation says the opposite: that  $cg(n) < f(n)$ . For examples of  $\omega$ -notation, we have  $n^2/2 = \omega(n)$ , but  $n^2/2 \neq \omega(n^2)$ . The relation  $f(n) = \omega(g(n))$  implies that

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = \infty,$$

if the limit exists. That is,  $f(n)$  becomes arbitrarily large relative to  $g(n)$  as  $n$  gets large.

**Comparing functions**

Many of the relational properties of real numbers apply to asymptotic comparisons as well. For the following, assume that  $f(n)$  and  $g(n)$  are asymptotically positive.

**Transitivity:**

$$\begin{aligned} f(n) = \Theta(g(n)) \text{ and } g(n) = \Theta(h(n)) & \text{ imply } f(n) = \Theta(h(n)), \\ f(n) = O(g(n)) \text{ and } g(n) = O(h(n)) & \text{ imply } f(n) = O(h(n)), \\ f(n) = \Omega(g(n)) \text{ and } g(n) = \Omega(h(n)) & \text{ imply } f(n) = \Omega(h(n)), \\ f(n) = o(g(n)) \text{ and } g(n) = o(h(n)) & \text{ imply } f(n) = o(h(n)), \\ f(n) = \omega(g(n)) \text{ and } g(n) = \omega(h(n)) & \text{ imply } f(n) = \omega(h(n)). \end{aligned}$$

**Reflexivity:**

$$\begin{aligned} f(n) &= \Theta(f(n)), \\ f(n) &= O(f(n)), \\ f(n) &= \Omega(f(n)). \end{aligned}$$

**Symmetry:**

$$f(n) = \Theta(g(n)) \text{ if and only if } g(n) = \Theta(f(n)).$$

**Transpose symmetry:**

$f(n) = O(g(n))$  if and only if  $g(n) = \Omega(f(n))$ ,

$f(n) = o(g(n))$  if and only if  $g(n) = \omega(f(n))$ .

Because these properties hold for asymptotic notations, we can draw an analogy between the asymptotic comparison of two functions  $f$  and  $g$  and the comparison of two real numbers  $a$  and  $b$ :

$f(n) = O(g(n))$  is like  $a \leq b$ ,

$f(n) = \Omega(g(n))$  is like  $a \geq b$ ,

$f(n) = \Theta(g(n))$  is like  $a = b$ ,

$f(n) = o(g(n))$  is like  $a < b$ ,

$f(n) = \omega(g(n))$  is like  $a > b$ .

We say that  $f(n)$  is *asymptotically smaller* than  $g(n)$  if  $f(n) = o(g(n))$ , and  $f(n)$  is *asymptotically larger* than  $g(n)$  if  $f(n) = \omega(g(n))$ .

One property of real numbers, however, does not carry over to asymptotic notation:

**Trichotomy:** For any two real numbers  $a$  and  $b$ , exactly one of the following must hold:  $a < b$ ,  $a = b$ , or  $a > b$ .

Although any two real numbers can be compared, not all functions are asymptotically comparable. That is, for two functions  $f(n)$  and  $g(n)$ , it may be the case that neither  $f(n) = O(g(n))$  nor  $f(n) = \Omega(g(n))$  holds. For example, we cannot compare the functions  $n$  and  $n^{1+\sin n}$  using asymptotic notation, since the value of the exponent in  $n^{1+\sin n}$  oscillates between 0 and 2, taking on all values in between.

**Exercises****3.2-1**

Let  $f(n)$  and  $g(n)$  be asymptotically nonnegative functions. Using the basic definition of  $\Theta$ -notation, prove that  $\max\{f(n), g(n)\} = \Theta(f(n) + g(n))$ .

**3.2-2**

Explain why the statement, “The running time of algorithm  $A$  is at least  $O(n^2)$ ,” is meaningless.

**3.2-3**

Is  $2^{n+1} = O(2^n)$ ? Is  $2^{2n} = O(2^n)$ ?

**3.2-4**

Prove Theorem 3.1.

**3.2-5**

Prove that the running time of an algorithm is  $\Theta(g(n))$  if and only if its worst-case running time is  $O(g(n))$  and its best-case running time is  $\Omega(g(n))$ .

**3.2-6**

Prove that  $o(g(n)) \cap \omega(g(n))$  is the empty set.

**3.2-7**

We can extend our notation to the case of two parameters  $n$  and  $m$  that can go to  $\infty$  independently at different rates. For a given function  $g(n, m)$ , we denote by  $O(g(n, m))$  the set of functions

$$O(g(n, m)) = \{f(n, m) : \text{there exist positive constants } c, n_0, \text{ and } m_0 \\ \text{such that } 0 \leq f(n, m) \leq cg(n, m) \\ \text{for all } n \geq n_0 \text{ or } m \geq m_0\}.$$

Give corresponding definitions for  $\Omega(g(n, m))$  and  $\Theta(g(n, m))$ .

### 3.3 Standard notations and common functions

This section reviews some standard mathematical functions and notations and explores the relationships among them. It also illustrates the use of the asymptotic notations.

#### Monotonicity

A function  $f(n)$  is *monotonically increasing* if  $m \leq n$  implies  $f(m) \leq f(n)$ . Similarly, it is *monotonically decreasing* if  $m \leq n$  implies  $f(m) \geq f(n)$ . A function  $f(n)$  is *strictly increasing* if  $m < n$  implies  $f(m) < f(n)$  and *strictly decreasing* if  $m < n$  implies  $f(m) > f(n)$ .

#### Floors and ceilings

For any real number  $x$ , we denote the greatest integer less than or equal to  $x$  by  $\lfloor x \rfloor$  (read “the floor of  $x$ ”) and the least integer greater than or equal to  $x$  by  $\lceil x \rceil$  (read “the ceiling of  $x$ ”). The floor function is monotonically increasing, as is the ceiling function.

Floors and ceilings obey the following properties. For any integer  $n$ , we have

$$\lfloor n \rfloor = n = \lceil n \rceil. \quad (3.1)$$

For all real  $x$ , we have

$$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1 . \quad (3.2)$$

We also have

$$-\lfloor x \rfloor = \lceil -x \rceil , \quad (3.3)$$

or equivalently,

$$-\lceil x \rceil = \lfloor -x \rfloor . \quad (3.4)$$

For any real number  $x \geq 0$  and integers  $a, b > 0$ , we have

$$\left\lceil \frac{\lfloor x/a \rfloor}{b} \right\rceil = \left\lceil \frac{x}{ab} \right\rceil , \quad (3.5)$$

$$\left\lfloor \frac{\lceil x/a \rceil}{b} \right\rfloor = \left\lfloor \frac{x}{ab} \right\rfloor , \quad (3.6)$$

$$\left\lceil \frac{a}{b} \right\rceil \leq \frac{a + (b - 1)}{b} , \quad (3.7)$$

$$\left\lfloor \frac{a}{b} \right\rfloor \geq \frac{a - (b - 1)}{b} . \quad (3.8)$$

For any integer  $n$  and real number  $x$ , we have

$$\lfloor n + x \rfloor = n + \lfloor x \rfloor , \quad (3.9)$$

$$\lceil n + x \rceil = n + \lceil x \rceil . \quad (3.10)$$

### Modular arithmetic

For any integer  $a$  and any positive integer  $n$ , the value  $a \bmod n$  is the *remainder* (or *residue*) of the quotient  $a/n$ :

$$a \bmod n = a - n \lfloor a/n \rfloor . \quad (3.11)$$

It follows that

$$0 \leq a \bmod n < n , \quad (3.12)$$

even when  $a$  is negative.

Given a well-defined notion of the remainder of one integer when divided by another, it is convenient to provide special notation to indicate equality of remainders. If  $(a \bmod n) = (b \bmod n)$ , we write  $a = b \pmod{n}$  and say that  $a$  is *equivalent* to  $b$ , modulo  $n$ . In other words,  $a = b \pmod{n}$  if  $a$  and  $b$  have the same remainder when divided by  $n$ . Equivalently,  $a = b \pmod{n}$  if and only if  $n$  is a divisor of  $b - a$ . We write  $a \neq b \pmod{n}$  if  $a$  is not equivalent to  $b$ , modulo  $n$ .

### Polynomials

Given a nonnegative integer  $d$ , a **polynomial in  $n$  of degree  $d$**  is a function  $p(n)$  of the form

$$p(n) = \sum_{i=0}^d a_i n^i ,$$

where the constants  $a_0, a_1, \dots, a_d$  are the **coefficients** of the polynomial and  $a_d \neq 0$ . A polynomial is asymptotically positive if and only if  $a_d > 0$ . For an asymptotically positive polynomial  $p(n)$  of degree  $d$ , we have  $p(n) = \Theta(n^d)$ . For any real constant  $a \geq 0$ , the function  $n^a$  is monotonically increasing, and for any real constant  $a \leq 0$ , the function  $n^a$  is monotonically decreasing. We say that a function  $f(n)$  is **polynomially bounded** if  $f(n) = O(n^k)$  for some constant  $k$ .

### Exponentials

For all real  $a > 0$ ,  $m$ , and  $n$ , we have the following identities:

$$\begin{aligned} a^0 &= 1 , \\ a^1 &= a , \\ a^{-1} &= 1/a , \\ (a^m)^n &= a^{mn} , \\ (a^m)^n &= (a^n)^m , \\ a^m a^n &= a^{m+n} . \end{aligned}$$

For all  $n$  and  $a \geq 1$ , the function  $a^n$  is monotonically increasing in  $n$ . When convenient, we assume that  $0^0 = 1$ .

We can relate the rates of growth of polynomials and exponentials by the following fact. For all real constants  $a > 1$  and  $b$ , we have

$$\lim_{n \rightarrow \infty} \frac{n^b}{a^n} = 0 ,$$

from which we can conclude that

$$n^b = o(a^n) . \tag{3.13}$$

Thus, any exponential function with a base strictly greater than 1 grows faster than any polynomial function.

Using  $e$  to denote  $2.71828\dots$ , the base of the natural-logarithm function, we have for all real  $x$ ,

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots = \sum_{i=0}^{\infty} \frac{x^i}{i!} ,$$

where “!” denotes the factorial function defined later in this section. For all real  $x$ , we have the inequality

$$1 + x \leq e^x, \quad (3.14)$$

where equality holds only when  $x = 0$ . When  $|x| \leq 1$ , we have the approximation

$$1 + x \leq e^x \leq 1 + x + x^2. \quad (3.15)$$

When  $x \rightarrow 0$ , the approximation of  $e^x$  by  $1 + x$  is quite good:

$$e^x = 1 + x + \Theta(x^2).$$

(In this equation, the asymptotic notation is used to describe the limiting behavior as  $x \rightarrow 0$  rather than as  $x \rightarrow \infty$ .) We have for all  $x$ ,

$$\lim_{n \rightarrow \infty} \left(1 + \frac{x}{n}\right)^n = e^x. \quad (3.16)$$

### Logarithms

We use the following notations:

$$\lg n = \log_2 n \quad (\text{binary logarithm}),$$

$$\ln n = \log_e n \quad (\text{natural logarithm}),$$

$$\lg^k n = (\lg n)^k \quad (\text{exponentiation}),$$

$$\lg \lg n = \lg(\lg n) \quad (\text{composition}).$$

We adopt the following notational convention: in the absence of parentheses, *a logarithm function applies only to the next term in the formula*, so that  $\lg n + 1$  means  $(\lg n) + 1$  and not  $\lg(n + 1)$ .

For any constant  $b > 1$ , the function  $\log_b n$  is undefined if  $n \leq 0$ , strictly increasing if  $n > 0$ , negative if  $0 < n < 1$ , positive if  $n > 1$ , and 0 if  $n = 1$ . For all real  $a > 0$ ,  $b > 0$ ,  $c > 0$ , and  $n$ , we have

$$a = b^{\log_b a}, \quad (3.17)$$

$$\log_c(ab) = \log_c a + \log_c b, \quad (3.18)$$

$$\log_b a^n = n \log_b a,$$

$$\log_b a = \frac{\log_c a}{\log_c b}, \quad (3.19)$$

$$\log_b(1/a) = -\log_b a, \quad (3.20)$$

$$\log_b a = \frac{1}{\log_a b},$$

$$a^{\log_b c} = c^{\log_b a}, \quad (3.21)$$

where, in each equation above, logarithm bases are not 1.

By equation (3.19), changing the base of a logarithm from one constant to another changes the value of the logarithm by only a constant factor. Consequently, we often use the notation “ $\lg n$ ” when we don’t care about constant factors, such as in  $O$ -notation. Computer scientists find 2 to be the most natural base for logarithms because so many algorithms and data structures involve splitting a problem into two parts.

There is a simple series expansion for  $\ln(1 + x)$  when  $|x| < 1$ :

$$\ln(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \cdots . \quad (3.22)$$

We also have the following inequalities for  $x > -1$ :

$$\frac{x}{1+x} \leq \ln(1+x) \leq x , \quad (3.23)$$

where equality holds only for  $x = 0$ .

We say that a function  $f(n)$  is *polylogarithmically bounded* if  $f(n) = O(\lg^k n)$  for some constant  $k$ . We can relate the growth of polynomials and polylogarithms by substituting  $\lg n$  for  $n$  and  $2^a$  for  $a$  in equation (3.13). For all real constants  $a > 0$  and  $b$ , we have

$$\lg^b n = o(n^a) . \quad (3.24)$$

Thus, any positive polynomial function grows faster than any polylogarithmic function.

### Factorials

The notation  $n!$  (read “ $n$  factorial”) is defined for integers  $n \geq 0$  as

$$n! = \begin{cases} 1 & \text{if } n = 0 , \\ n \cdot (n-1)! & \text{if } n > 0 . \end{cases}$$

Thus,  $n! = 1 \cdot 2 \cdot 3 \cdots n$ .

A weak upper bound on the factorial function is  $n! \leq n^n$ , since each of the  $n$  terms in the factorial product is at most  $n$ . *Stirling’s approximation*,

$$n! = \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \left(1 + \Theta\left(\frac{1}{n}\right)\right) , \quad (3.25)$$

where  $e$  is the base of the natural logarithm, gives us a tighter upper bound, and a lower bound as well. Exercise 3.3-4 asks you to prove the three facts

$$n! = o(n^n) , \quad (3.26)$$

$$n! = \omega(2^n) , \quad (3.27)$$

$$\lg(n!) = \Theta(n \lg n) , \quad (3.28)$$



where Stirling's approximation is helpful in proving equation (3.28). The following equation also holds for all  $n \geq 1$ :

$$n! = \sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\alpha_n} \quad (3.29)$$

where

$$\frac{1}{12n+1} < \alpha_n < \frac{1}{12n} .$$

### Functional iteration

We use the notation  $f^{(i)}(n)$  to denote the function  $f(n)$  iteratively applied  $i$  times to an initial value of  $n$ . Formally, let  $f(n)$  be a function over the reals. For non-negative integers  $i$ , we recursively define

$$f^{(i)}(n) = \begin{cases} n & \text{if } i = 0 , \\ f(f^{(i-1)}(n)) & \text{if } i > 0 . \end{cases} \quad (3.30)$$

For example, if  $f(n) = 2n$ , then  $f^{(i)}(n) = 2^i n$ .

### The iterated logarithm function

We use the notation  $\lg^* n$  (read “log star of  $n$ ”) to denote the iterated logarithm, defined as follows. Let  $\lg^{(i)} n$  be as defined above, with  $f(n) = \lg n$ . Because the logarithm of a nonpositive number is undefined,  $\lg^{(i)} n$  is defined only if  $\lg^{(i-1)} n > 0$ . Be sure to distinguish  $\lg^{(i)} n$  (the logarithm function applied  $i$  times in succession, starting with argument  $n$ ) from  $\lg^i n$  (the logarithm of  $n$  raised to the  $i$ th power). Then we define the iterated logarithm function as

$$\lg^* n = \min \{i \geq 0 : \lg^{(i)} n \leq 1\} .$$

The iterated logarithm is a *very* slowly growing function:

$$\begin{aligned} \lg^* 2 &= 1 , \\ \lg^* 4 &= 2 , \\ \lg^* 16 &= 3 , \\ \lg^* 65536 &= 4 , \\ \lg^*(2^{65536}) &= 5 . \end{aligned}$$

Since the number of atoms in the observable universe is estimated to be about  $10^{80}$ , which is much less than  $2^{65536} = 10^{65536/\lg 10} \approx 10^{19,728}$ , we rarely encounter an input size  $n$  for which  $\lg^* n > 5$ .

### Fibonacci numbers

We define the *Fibonacci numbers*  $F_i$ , for  $i \geq 0$ , as follows:

$$F_i = \begin{cases} 0 & \text{if } i = 0, \\ 1 & \text{if } i = 1, \\ F_{i-1} + F_{i-2} & \text{if } i \geq 2. \end{cases} \quad (3.31)$$

Thus, after the first two, each Fibonacci number is the sum of the two previous ones, yielding the sequence

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

Fibonacci numbers are related to the *golden ratio*  $\phi$  and its conjugate  $\hat{\phi}$ , which are the two roots of the equation

$$x^2 = x + 1.$$

As Exercise 3.3-7 asks you to prove, the golden ratio is given by

$$\begin{aligned} \phi &= \frac{1 + \sqrt{5}}{2} \\ &= 1.61803\dots, \end{aligned} \quad (3.32)$$

and its conjugate, by

$$\begin{aligned} \hat{\phi} &= \frac{1 - \sqrt{5}}{2} \\ &= -.61803\dots \end{aligned} \quad (3.33)$$

Specifically, we have

$$F_i = \frac{\phi^i - \hat{\phi}^i}{\sqrt{5}},$$

which can be proved by induction (Exercise 3.3-8). Since  $|\hat{\phi}| < 1$ , we have

$$\begin{aligned} \frac{|\hat{\phi}^i|}{\sqrt{5}} &< \frac{1}{\sqrt{5}} \\ &< \frac{1}{2}, \end{aligned}$$

which implies that

$$F_i = \left\lfloor \frac{\phi^i}{\sqrt{5}} + \frac{1}{2} \right\rfloor, \quad (3.34)$$

which is to say that the  $i$ th Fibonacci number  $F_i$  is equal to  $\phi^i / \sqrt{5}$  rounded to the nearest integer. Thus, Fibonacci numbers grow exponentially.

**Exercises****3.3-1**

Show that if  $f(n)$  and  $g(n)$  are monotonically increasing functions, then so are the functions  $f(n) + g(n)$  and  $f(g(n))$ , and if  $f(n)$  and  $g(n)$  are in addition nonnegative, then  $f(n) \cdot g(n)$  is monotonically increasing.

**3.3-2**

Prove that  $\lfloor \alpha n \rfloor + \lceil (1 - \alpha)n \rceil = n$  for any integer  $n$  and real number  $\alpha$  in the range  $0 \leq \alpha \leq 1$ .

**3.3-3**

Use equation (3.14) or other means to show that  $(n + o(n))^k = \Theta(n^k)$  for any real constant  $k$ . Conclude that  $\lceil n \rceil^k = \Theta(n^k)$  and  $\lfloor n \rfloor^k = \Theta(n^k)$ .

**3.3-4**

Prove the following:

- a. Equation (3.21).
- b. Equations (3.26)–(3.28).
- c.  $\lg(\Theta(n)) = \Theta(\lg n)$ .

**★ 3.3-5**

Is the function  $\lceil \lg n \rceil!$  polynomially bounded? Is the function  $\lceil \lg \lg n \rceil!$  polynomially bounded?

**★ 3.3-6**

Which is asymptotically larger:  $\lg(\lg^* n)$  or  $\lg^*(\lg n)$ ?

**3.3-7**

Show that the golden ratio  $\phi$  and its conjugate  $\hat{\phi}$  both satisfy the equation  $x^2 = x + 1$ .

**3.3-8**

Prove by induction that the  $i$ th Fibonacci number satisfies the equation

$$F_i = (\phi^i - \hat{\phi}^i) / \sqrt{5},$$

where  $\phi$  is the golden ratio and  $\hat{\phi}$  is its conjugate.

**3.3-9**

Show that  $k \lg k = \Theta(n)$  implies  $k = \Theta(n / \lg n)$ .

---

**Problems**
**3-1 Asymptotic behavior of polynomials**

Let

$$p(n) = \sum_{i=0}^d a_i n^i,$$

where  $a_d > 0$ , be a degree- $d$  polynomial in  $n$ , and let  $k$  be a constant. Use the definitions of the asymptotic notations to prove the following properties.

- a. If  $k \geq d$ , then  $p(n) = O(n^k)$ .
- b. If  $k \leq d$ , then  $p(n) = \Omega(n^k)$ .
- c. If  $k = d$ , then  $p(n) = \Theta(n^k)$ .
- d. If  $k > d$ , then  $p(n) = o(n^k)$ .
- e. If  $k < d$ , then  $p(n) = \omega(n^k)$ .

**3-2 Relative asymptotic growths**

Indicate, for each pair of expressions  $(A, B)$  in the table below whether  $A$  is  $O$ ,  $o$ ,  $\Omega$ ,  $\omega$ , or  $\Theta$  of  $B$ . Assume that  $k \geq 1$ ,  $\epsilon > 0$ , and  $c > 1$  are constants. Write your answer in the form of the table with “yes” or “no” written in each box.

	$A$	$B$	$O$	$o$	$\Omega$	$\omega$	$\Theta$
a.	$\lg^k n$	$n^\epsilon$					
b.	$n^k$	$c^n$					
c.	$\sqrt{n}$	$n^{\sin n}$					
d.	$2^n$	$2^{n/2}$					
e.	$n^{\lg c}$	$c^{\lg n}$					
f.	$\lg(n!)$	$\lg(n^n)$					

**3-3 Ordering by asymptotic growth rates**

- a. Rank the following functions by order of growth. That is, find an arrangement  $g_1, g_2, \dots, g_{30}$  of the functions satisfying  $g_1 = \Omega(g_2)$ ,  $g_2 = \Omega(g_3)$ ,  $\dots$ ,  $g_{29} = \Omega(g_{30})$ . Partition your list into equivalence classes such that functions  $f(n)$  and  $g(n)$  belong to the same class if and only if  $f(n) = \Theta(g(n))$ .

$$\begin{array}{cccccc}
\lg(\lg^* n) & 2^{\lg^* n} & (\sqrt{2})^{\lg n} & n^2 & n! & (\lg n)! \\
(3/2)^n & n^3 & \lg^2 n & \lg(n!) & 2^{2^n} & n^{1/\lg n} \\
\ln \ln n & \lg^* n & n \cdot 2^n & n^{\lg \lg n} & \ln n & 1 \\
2^{\lg n} & (\lg n)^{\lg n} & e^n & 4^{\lg n} & (n+1)! & \sqrt{\lg n} \\
\lg^*(\lg n) & 2^{\sqrt{2 \lg n}} & n & 2^n & n \lg n & 2^{2^{n+1}}
\end{array}$$

- b.** Give an example of a single nonnegative function  $f(n)$  such that for all functions  $g_i(n)$  in part (a),  $f(n)$  is neither  $O(g_i(n))$  nor  $\Omega(g_i(n))$ .

### 3-4 Asymptotic notation properties

Let  $f(n)$  and  $g(n)$  be asymptotically positive functions. Prove or disprove each of the following conjectures.

- a.**  $f(n) = O(g(n))$  implies  $g(n) = O(f(n))$ .
- b.**  $f(n) + g(n) = \Theta(\min\{f(n), g(n)\})$ .
- c.**  $f(n) = O(g(n))$  implies  $\lg f(n) = O(\lg g(n))$ , where  $\lg g(n) \geq 1$  and  $f(n) \geq 1$  for all sufficiently large  $n$ .
- d.**  $f(n) = O(g(n))$  implies  $2^{f(n)} = O(2^{g(n)})$ .
- e.**  $f(n) = O((f(n))^2)$ .
- f.**  $f(n) = O(g(n))$  implies  $g(n) = \Omega(f(n))$ .
- g.**  $f(n) = \Theta(f(n/2))$ .
- h.**  $f(n) + o(f(n)) = \Theta(f(n))$ .

### 3-5 Manipulating asymptotic notation

Let  $f(n)$  and  $g(n)$  be asymptotically positive functions. Prove the following identities:

- a.**  $\Theta(\Theta(f(n))) = \Theta(f(n))$ .
- b.**  $\Theta(f(n)) + O(f(n)) = \Theta(f(n))$ .
- c.**  $\Theta(f(n)) + \Theta(g(n)) = \Theta(f(n) + g(n))$ .
- d.**  $\Theta(f(n)) \cdot \Theta(g(n)) = \Theta(f(n) \cdot g(n))$ .

- e. Argue that for any real constants  $a_1, b_1 > 0$  and integer constants  $k_1, k_2$ , the following asymptotic bound holds:

$$(a_1 n)^{k_1} \lg^{k_2}(a_2 n) = \Theta(n^{k_1} \lg^{k_2} n) .$$

- ★ f. Prove that for  $S \subseteq \mathbb{Z}$ , we have

$$\sum_{k \in S} \Theta(f(k)) = \Theta \left( \sum_{k \in S} f(k) \right) ,$$

assuming that both sums converge.

- ★ g. Show that for  $S \subseteq \mathbb{Z}$ , the following asymptotic bound does not necessarily hold, even assuming that both products converge, by giving a counterexample:

$$\prod_{k \in S} \Theta(f(k)) = \Theta \left( \prod_{k \in S} f(k) \right) .$$

### 3-6 Variations on $O$ and $\Omega$

Some authors define  $\Omega$ -notation in a slightly different way than this textbook does. We'll use the nomenclature  $\overset{\infty}{\Omega}$  (read “omega infinity”) for this alternative definition. We say that  $f(n) = \overset{\infty}{\Omega}(g(n))$  if there exists a positive constant  $c$  such that  $f(n) \geq cg(n) \geq 0$  for infinitely many integers  $n$ .

- Show that for any two asymptotically nonnegative functions  $f(n)$  and  $g(n)$ , we have  $f(n) = O(g(n))$  or  $f(n) = \overset{\infty}{\Omega}(g(n))$  (or both).
- Show that there exist two asymptotically nonnegative functions  $f(n)$  and  $g(n)$  for which neither  $f(n) = O(g(n))$  nor  $f(n) = \Omega(g(n))$  holds.
- Describe the potential advantages and disadvantages of using  $\overset{\infty}{\Omega}$ -notation instead of  $\Omega$ -notation to characterize the running times of programs.

Some authors also define  $O$  in a slightly different manner. We'll use  $O'$  for the alternative definition:  $f(n) = O'(g(n))$  if and only if  $|f(n)| = O(g(n))$ .

- What happens to each direction of the “if and only if” in Theorem 3.1 on page 56 if we substitute  $O'$  for  $O$  but still use  $\Omega$ ?

Some authors define  $\tilde{O}$  (read “soft-oh”) to mean  $O$  with logarithmic factors ignored:

$$\widetilde{O}(g(n)) = \{f(n) : \text{there exist positive constants } c, k, \text{ and } n_0 \text{ such that} \\ 0 \leq f(n) \leq cg(n) \lg^k(n) \text{ for all } n \geq n_0\}.$$

- e. Define  $\widetilde{\Omega}$  and  $\widetilde{\Theta}$  in a similar manner. Prove the corresponding analog to Theorem 3.1.

### 3-7 Iterated functions

We can apply the iteration operator  $*$  used in the  $\lg^*$  function to any monotonically increasing function  $f(n)$  over the reals. For a given constant  $c \in \mathbb{R}$ , we define the iterated function  $f_c^*$  by

$$f_c^*(n) = \min \{i \geq 0 : f^{(i)}(n) \leq c\},$$

which need not be well defined in all cases. In other words, the quantity  $f_c^*(n)$  is the minimum number of iterated applications of the function  $f$  required to reduce its argument down to  $c$  or less.

For each of the functions  $f(n)$  and constants  $c$  in the table below, give as tight a bound as possible on  $f_c^*(n)$ . If there is no  $i$  such that  $f^{(i)}(n) \leq c$ , write “undefined” as your answer.

	$f(n)$	$c$	$f_c^*(n)$
a.	$n - 1$	0	
b.	$\lg n$	1	
c.	$n/2$	1	
d.	$n/2$	2	
e.	$\sqrt{n}$	2	
f.	$\sqrt{n}$	1	
g.	$n^{1/3}$	2	

---

### Chapter notes

Knuth [259] traces the origin of the  $O$ -notation to a number-theory text by P. Bachmann in 1892. The  $o$ -notation was invented by E. Landau in 1909 for his discussion of the distribution of prime numbers. The  $\Omega$  and  $\Theta$  notations were advocated by Knuth [265] to correct the popular, but technically sloppy, practice in the literature of using  $O$ -notation for both upper and lower bounds. As noted earlier in this chapter, many people continue to use the  $O$ -notation where the  $\Theta$ -notation is more technically precise. The soft-oh notation  $\widetilde{O}$  in Problem 3-6 was introduced

by Babai, Luks, and Seress [31], although it was originally written as  $O\sim$ . Some authors now define  $\widetilde{O}(g(n))$  as ignoring factors that are logarithmic in  $g(n)$ , rather than in  $n$ . With this definition, we can say that  $n2^n = \widetilde{O}(2^n)$ , but with the definition in Problem 3-6, this statement is not true. Further discussion of the history and development of asymptotic notations appears in works by Knuth [259, 265] and Brassard and Bratley [70].

Not all authors define the asymptotic notations in the same way, although the various definitions agree in most common situations. Some of the alternative definitions encompass functions that are not asymptotically nonnegative, as long as their absolute values are appropriately bounded.

Equation (3.29) is due to Robbins [381]. Other properties of elementary mathematical functions can be found in any good mathematical reference, such as Abramowitz and Stegun [1] or Zwillinger [468], or in a calculus book, such as Apostol [19] or Thomas et al. [433]. Knuth [259] and Graham, Knuth, and Patashnik [199] contain a wealth of material on discrete mathematics as used in computer science.