

# Algorithms and Complexity

Second Edition

Herbert S. Wilf



A K Peters  
Natick, Massachusetts

Editorial, Sales, and Customer Service Office

A K Peters, Ltd.  
63 South Avenue  
Natick, MA 01760  
[www.akpeters.com](http://www.akpeters.com)

Copyright © 2002 by A K Peters, Ltd.

All rights reserved. No part of the material protected by this copyright notice may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

#### Library of Congress Cataloging-in-Publication Data

Wilf, Herbert S., 1931-

Algorithms and complexity / Herbert S. Wilf.—2nd ed.

p. cm.

ISBN 1-56881-178-0

1. Problem solving—Data processing. 2. Computer algorithms. 3. Computational complexity. I. Title.

QA63 .W55 2002

511'.8—dc21

2002072765

Printed in the United States of America

06 05 04 03 02

10 9 8 7 6 5 4 3 2 1



# Contents

<b>Preface</b>	<b>vii</b>
<b>Preface to the Second Edition</b>	<b>ix</b>
<b>0 What this Book Is About</b>	<b>1</b>
0.1 Background . . . . .	1
0.2 Hard versus Easy Problems . . . . .	3
0.3 A Preview . . . . .	6
<b>1 Mathematical Preliminaries</b>	<b>9</b>
1.1 Orders of Magnitude . . . . .	9
1.2 Positional Number Systems . . . . .	19
1.3 Manipulations with Series . . . . .	23
1.4 Recurrence Relations . . . . .	27
1.5 Counting . . . . .	34
1.6 Graphs . . . . .	39
<b>2 Recursive Algorithms</b>	<b>49</b>
2.1 Introduction . . . . .	49
2.2 Quicksort . . . . .	51
2.3 Recursive Graph Algorithms . . . . .	61
2.4 Fast Matrix Multiplication . . . . .	76
2.5 The Discrete Fourier Transform . . . . .	80
2.6 Applications of the FFT . . . . .	91
2.7 A Review . . . . .	94
2.8 Bibliography . . . . .	98

<b>3</b>	<b>The Network Flow Problem</b>	<b>99</b>
3.1	Introduction . . . . .	99
3.2	Algorithms for the Network Flow Problem . . . . .	101
3.3	The Algorithm of Ford and Fulkerson . . . . .	102
3.4	The Max-Flow Min-Cut Theorem . . . . .	108
3.5	The Complexity of the Ford-Fulkerson Algorithm . . . . .	110
3.6	Layered Networks . . . . .	113
3.7	The MPM Algorithm . . . . .	119
3.8	Applications of Network Flow . . . . .	121
<b>4</b>	<b>Algorithms in the Theory of Numbers</b>	<b>127</b>
4.1	Preliminaries . . . . .	127
4.2	The Greatest Common Divisor . . . . .	130
4.3	The Extended Euclidean Algorithm . . . . .	134
4.4	Primality Testing . . . . .	138
4.5	Interlude: The Ring of Integers Modulo $n$ . . . . .	141
4.6	Pseudoprimality Tests . . . . .	146
4.7	Proof of Goodness of the Strong Pseudoprimality Test . . . . .	150
4.8	Factoring and Cryptography . . . . .	154
4.9	Factoring Large Integers . . . . .	157
4.10	Proving Primality . . . . .	159
<b>5</b>	<b>NP-Completeness</b>	<b>165</b>
5.1	Introduction . . . . .	165
5.2	Turing Machines . . . . .	174
5.3	Cook's Theorem . . . . .	179
5.4	Some Other NP-Complete Problems . . . . .	186
5.5	Half a Loaf ... . . . .	191
5.6	Backtracking (I): Independent Sets . . . . .	195
5.7	Backtracking (II): Graph Coloring . . . . .	199
5.8	Approximate Algorithms for Hard Problems . . . . .	203
	<b>Hints and Solutions for Selected Problems</b>	<b>209</b>
	<b>Index</b>	<b>217</b>