Contents

Prefaces ix

Part 1. Counting

Chapter 1. Fundamentals 7
§1.1. Elementary Counting Principles 7
§1.2. The Fundamental Counting Coefficients 10
§1.3. Permutations 14
§1.4. Recurrence Equations 17
§1.5. Discrete Probability 23
§1.6. Existence Theorems 29
Exercises for Chapter 1 33

Chapter 2. Summation 41
§2.1. Direct Methods 41
§2.2. The Calculus of Finite Differences 46
§2.3. Inversion 52
§2.4. Inclusion–Exclusion 55
Exercises for Chapter 2 60

Chapter 3. Generating Functions 65
§3.1. Definitions and Examples 65
§3.2. Solving Recurrences 67
§3.3. Generating Functions of Exponential Type 74
Exercises for Chapter 3 76
## Contents

Chapter 4. Counting Patterns 81
   §4.1. Symmetries 81
   §4.2. Statement of the Problem 84
   §4.3. Patterns and the Cycle Indicator 86
   §4.4. Pólya's Theorem 88
   Exercises for Chapter 4 94

Chapter 5. Asymptotic Analysis 99
   §5.1. The Growth of Functions 99
   §5.2. Order of Magnitude of Recurrence Relations 103
   §5.3. Running Times of Algorithms 106
   Exercises for Chapter 5 109

Bibliography for Part 1 113

**Part 2. Graphs and Algorithms**

Chapter 6. Graphs 119
   §6.1. Definitions and Examples 119
   §6.2. Representation of Graphs 124
   §6.3. Paths and Circuits 126
   §6.4. Directed Graphs 129
   Exercises for Chapter 6 132

Chapter 7. Trees 137
   §7.1. What Is a Tree? 137
   §7.2. Breadth-First and Depth-First Search 141
   §7.3. Minimal Spanning Trees 143
   §7.4. The Shortest Path in a Graph 146
   Exercises for Chapter 7 148

Chapter 8. Matchings and Networks 153
   §8.1. Matchings in Bipartite Graphs 153
   §8.2. Construction of Optimal Matchings 157
   §8.3. Flows in Networks 164
   §8.4. Eulerian Graphs and the Traveling Salesman Problem 170
   §8.5. The Complexity Classes P and NP 178
   Exercises for Chapter 8 181
## Contents

Chapter 9. Searching and Sorting 187
   §9.1. Search Problems and Decision Trees 187
   §9.2. The Fundamental Theorem of Search Theory 191
   §9.3. Sorting Lists 197
   §9.4. Binary Search Trees 203
   Exercises for Chapter 9 208

Chapter 10. General Optimization Methods 215
   §10.1. Backtracking 215
   §10.2. Dynamic Programming 219
   §10.3. The Greedy Algorithm 226
   Exercises for Chapter 10 229

Bibliography for Part 2 233

### Part 3. Algebraic Systems

Chapter 11. Boolean Algebras 239
   §11.1. Definition and Properties 239
   §11.2. Propositional Logic and Boolean Functions 241
   §11.3. Logical Nets 246
   §11.4. Boolean Lattices, Orders, and Hypergraphs 249
   Exercises for Chapter 11 255

Chapter 12. Modular Arithmetic 259
   §12.1. Calculating with Congruences 259
   §12.2. Finite Fields 262
   §12.3. Latin Squares 265
   §12.4. Combinatorial Designs 268
   Exercises for Chapter 12 276

Chapter 13. Coding 281
   §13.1. Statement of the Problem 281
   §13.2. Source Encoding 282
   §13.3. Error Detection and Correction 284
   §13.4. Linear Codes 289
   §13.5. Cyclic Codes 294
   Exercises for Chapter 13 297
<table>
<thead>
<tr>
<th>Chapter 14. Cryptography</th>
<th>303</th>
</tr>
</thead>
<tbody>
<tr>
<td>§14.1. Cryptosystems</td>
<td>303</td>
</tr>
<tr>
<td>§14.2. Linear Shift Registers</td>
<td>306</td>
</tr>
<tr>
<td>§14.3. Public-Key Cryptosystems</td>
<td>312</td>
</tr>
<tr>
<td>§14.4. Zero-Knowledge Protocols</td>
<td>316</td>
</tr>
<tr>
<td>Exercises for Chapter 14</td>
<td>319</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 15. Linear Optimization</th>
<th>323</th>
</tr>
</thead>
<tbody>
<tr>
<td>§15.1. Examples and Definitions</td>
<td>323</td>
</tr>
<tr>
<td>§15.2. Duality</td>
<td>325</td>
</tr>
<tr>
<td>§15.3. The Fundamental Theorem of Linear Optimization</td>
<td>331</td>
</tr>
<tr>
<td>§15.4. Admissible Solutions and Optimal Solutions</td>
<td>336</td>
</tr>
<tr>
<td>§15.5. The Simplex Algorithm</td>
<td>340</td>
</tr>
<tr>
<td>§15.6. Integer Linear Optimization</td>
<td>347</td>
</tr>
<tr>
<td>Exercises for Chapter 15</td>
<td>349</td>
</tr>
</tbody>
</table>

Bibliography for Part 3 353

Solutions to Selected Exercises 355

Index 383