DISCRETE MATHEMATICS FOR COMPUTER SCIENTISTS

Clifford Stein
Columbia University

Robert L. Drysdale
Dartmouth College

Kenneth Bogart

TECHNISCHE
INFORMATIONSBIBLIOTHEK
UNIVERSITÄTSBIBLIOTHEK
HANNOVER

PEARSON

Boston Columbus Indianapolis New York San Francisco Upper Saddle River
Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montreal Toronto
Delhi Mexico City Sao Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

Contents

List of Theorems, Lemmas, and Corollaries 19

Preface 21

CHAPTER 1 Counting 31

1.1 Basic Counting 31

The Sum Principle 31

Abstraction 33

Summing Consecutive Integers 33

The Product Principle 34

Two-Element Subsets 36

Important Concepts, Formulas, and Theorems 37

Problems 38

1.2 Counting Lists, Permutations, and Subsets 40

Using the Sum and Product Principles 40

Lists and Functions 42

The Bijection Principle 44

k-Element Permutations of a Set 45

Counting Subsets of a Set 46

Important Concepts, Formulas, and Theorems 48

Problems 50

1.3 Binomial Coefficients 52

Pascal's Triangle 52

A Proof Using the Sum Principle 54

The Binomial Theorem 56

Labeling and Trinomial Coefficients 58

Important Concepts, Formulas, and Theorems 59

Problems 60

1.4 **Relations** **62**

What Is a Relation? 62

Functions as Relations 63

Properties of Relations 63

Equivalence Relations 66

Partial and Total Orders 69

Important Concepts, Formulas, and Theorems 71

Problems 72

1.5 **Using Equivalence Relations in Counting** **73**

The Symmetry Principle 73

Equivalence Relations 75

The Quotient Principle 76

Equivalence Class Counting 76

Multisets 78

The Bookcase Arrangement Problem 80

The Number of k-Element Multisets of an n-Element Set 81

Using the Quotient Principle to Explain a Quotient 82

Important Concepts, Formulas, and Theorems 83

Problems 84

CHAPTER 2 Cryptography and Number Theory **89**

2.1 **Cryptography and Modular Arithmetic** **89**

Introduction to Cryptography 89

Private-Key Cryptography 90

Public-Key Cryptosystems 93

Arithmetic Modulo n 95

Cryptography Using Addition mod n 98

Cryptography Using Multiplication mod n 99

Important Concepts, Formulas, and Theorems 101

Problems 102

2.2 **Inverses and Greatest Common Divisors** **105**

Solutions to Equations and Inverses mod *n* 105

Inverses mod *n* 106

Converting Modular Equations to Normal Equations 109

Greatest Common Divisors 110

Euclid's Division Theorem 111

Euclid's GCD Algorithm 114

Extended GCD Algorithm 115

Computing Inverses 118

Important Concepts, Formulas, and Theorems 119

Problems 120

2.3 **The RSA Cryptosystem** **123**

Exponentiation mod *n* 123

The Rules of Exponents 123

Fermat's Little Theorem 126

The RSA Cryptosystem 127

The Chinese Remainder Theorem 131

Important Concepts, Formulas, and Theorems 132

Problems 134

2.4 **Details of the RSA Cryptosystem** **136**

Practical Aspects of Exponentiation mod *n* 136

How Long Does It Take to Use the RSA Algorithm? 139

How Hard Is Factoring? 140

Finding Large Primes 140

Important Concepts, Formulas, and Theorems 143

Problems 144

CHAPTER 3 Reflections on Logic and Proof **147**

3.1 **Equivalence and Implication** **147**

Equivalence of Statements 147

Truth Tables 150

DeMorgan's Laws 153

Implication 155

If and Only If 156

Important Concepts, Formulas, and Theorems 159

Problems 161

3.2 Variables and Quantifiers 163

Variables and Universes 163

Quantifiers 164

Standard Notation for Quantification 166

Statements about Variables 168

Rewriting Statements to Encompass Larger Universes 168

Proving Quantified Statements True or False 169

Negation of Quantified Statements 170

Implicit Quantification 173

Proof of Quantified Statements 174

Important Concepts, Formulas, and Theorems 175

Problems 177

3.3 Inference 179

Direct Inference (Modus Ponens) and Proofs 179

Rules of Inference for Direct Proofs 181

Contrapositive Rule of Inference 183

Proof by Contradiction 185

Important Concepts, Formulas, and Theorems 188

Problems 189

CHAPTER 4 Induction, Recursion, and Recurrences 191

4.1 Mathematical Induction 191

Smallest Counterexamples 191

The Principle of Mathematical Induction 195

Strong Induction 199

Induction in General 201

A Recursive View of Induction 203

Structural Induction 206

Important Concepts, Formulas, and Theorems 208

Problems 210

4.2 Recursion, Recurrences, and Induction 213

Recursion 213

Examples of First-Order Linear Recurrences 215

Iterating a Recurrence 217

Geometric Series 218

First-Order Linear Recurrences 221

Important Concepts, Formulas, and Theorems 225

Problems 227

4.3 Growth Rates of Solutions to Recurrences 228

Divide and Conquer Algorithms 228

Recursion Trees 231

Three Different Behaviors 239

Important Concepts, Formulas, and Theorems 240

Problems 242

4.4 The Master Theorem 244

Master Theorem 244

Solving More General Kinds of Recurrences 247

Extending the Master Theorem 248

Important Concepts, Formulas, and Theorems 250

Problems 251

4.5 More General Kinds of Recurrences 252

Recurrence Inequalities 252

The Master Theorem for Inequalities 253

A Wrinkle with Induction 255

Further Wrinkles in Induction Proofs 257

Dealing with Functions Other Than n^c 260

Important Concepts, Formulas, and Theorems 262

Problems 263

4.6 Recurrences and Selection 265

The Idea of Selection 265

A Recursive Selection Algorithm 266

Selection without Knowing the Median in Advance 267

An Algorithm to Find an Element in the Middle Half 269

An Analysis of the Revised Selection Algorithm 272

Uneven Divisions 274

Important Concepts, Formulas, and Theorems 276

Problems 277

CHAPTER 5 Probability 279

5.1 Introduction to Probability 279

Why Study Probability? 279

Some Examples of Probability Computations 282

Complementary Probabilities 283

Probability and Hashing 284

The Uniform Probability Distribution 286

Important Concepts, Formulas, and Theorems 289

Problems 290

5.2 Unions and Intersections 292

The Probability of a Union of Events 292

Principle of Inclusion and Exclusion for Probability 295

The Principle of Inclusion and Exclusion for Counting 301

Important Concepts, Formulas, and Theorems 303

Problems 304

5.3 Conditional Probability and Independence 306

Conditional Probability 306

Bayes' Theorem 310

Independence 310

Independent Trials Processes 312

Tree Diagrams 314

Primality Testing 318

Important Concepts, Formulas, and Theorems 319

Problems 320

5.4 Random Variables 322

What Are Random Variables? 322

Binomial Probabilities 323

A Taste of Generating Functions 325

Expected Value 326

Expected Values of Sums and Numerical Multiples 329

Indicator Random Variables 332

The Number of Trials until the First Success 334

Important Concepts, Formulas, and Theorems 336

Problems 337

5.5 Probability Calculations in Hashing 340

Expected Number of Items per Location 340

Expected Number of Empty Locations 341

Expected Number of Collisions 342

Expected Maximum Number of Elements in a Location of a Hash Table 345

Important Concepts, Formulas, and Theorems 350

Problems 351

5.6 Conditional Expectations, Recurrences, and Algorithms 355

When Running Times Depend on More than Size of Inputs 355

Conditional Expected Values 357

Randomized Algorithms 359

Selection Revisited 361

QuickSort 363

A More Careful Analysis of RandomSelect 366

Important Concepts, Formulas, and Theorems 369

Problems 370

5.7 **Probability Distributions and Variance** **373**
Distributions of Random Variables 373
Variance 376
Important Concepts, Formulas, and Theorems 384
Problems 385

CHAPTER 6 Graphs 389

6.1 **Graphs** **389**
The Degree of a Vertex 393
Connectivity 395
Cycles 397
Trees 398
Other Properties of Trees 398
Important Concepts, Formulas, and Theorems 401
Problems 403

6.2 **Spanning Trees and Rooted Trees** **405**
Spanning Trees 405
Breadth-First Search 407
Rooted Trees 412
Important Concepts, Formulas, and Theorems 416
Problems 417

6.3 **Eulerian and Hamiltonian Graphs** **419**
Eulerian Tours and Trails 419
Finding Eulerian Tours 424
Hamiltonian Paths and Cycles 425
NP-Complete Problems 431
Proving That Problems Are NP-Complete 433
Important Concepts, Formulas, and Theorems 436
Problems 437

6.4 **Matching Theory** **440**
The Idea of a Matching 440
Making Matchings Bigger 444

Matching in Bipartite Graphs 447
Searching for Augmenting Paths in Bipartite Graphs 447
The Augmentation-Cover Algorithm 450
Efficient Algorithms 456
Important Concepts, Formulas, and Theorems 457
Problems 458

6.5 Coloring and Planarity 460
The Idea of Coloring 460
Interval Graphs 463
Planarity 465
The Faces of a Planar Drawing 467
The Five-Color Theorem 471
Important Concepts, Formulas, and Theorems 474
Problems 475

APPENDIX A Derivation of the More General Master Theorem 479
More General Recurrences 479
Recurrences for General *n* 481
Removing Floors and Ceilings 482
Floors and Ceilings in the Stronger Version of the Master Theorem 483
Proofs of Theorems 483
Important Concepts, Formulas, and Theorems 487
Problems 488

APPENDIX B Answers and Hints to Selected Problems 491

Bibliography 507

Index 509