
Contents

Preface	vii
I Discrete Mathematics	1
0 Background and Pep Talk	3
1 A Taste of Discrete Mathematics	7
1.1 Modeling Epidemics	7
1.2 Speed Dating	8
1.3 Friendship Networks and Ads	8
1.4 Modeling Computers	9
1.5 Proof	9
1.6 Problems	11
2 Discrete Objects	15
2.1 Sets	15
2.2 Sequences	17
2.3 Graphs	17
2.4 Easing into Proofs	19
2.4.1 An Axiom: The Well-Ordering Principle	20
2.5 Problems	23
3 Making Precise Statements	25
3.1 Compound Propositions	26
3.2 Truth-Tables	28
3.2.1 Proving an Implication	30
3.3 Quantifiers: Statements About Many Things	30
3.3.1 Predicates	31
3.3.2 Negation	33
3.3.3 Mixing Quantifiers	33
3.3.4 Proofs with Quantifiers	34
3.4 Deduction Versus Induction	34
3.5 Problems	35
4 Proofs	41
4.1 Direct Proof	41
4.1.1 Disproving Implication	44
4.2 Proof by Contraposition	45
4.3 Equivalence: If and Only If	45
4.4 Proof by Contradiction (Reductio ad Absurdum)	47
4.5 Proofs about Sets	48

4.6	Problems	50
5	Induction: Proving “FOR ALL ...”	55
5.1	Ordinary Induction	57
5.1.1	Sum of Powers of Integers	58
5.1.2	Induction Gone Wrong	61
5.2	Induction and Well-ordering	63
5.3	Problems	64
6	Strong Induction	71
6.1	Strengthening the Induction Hypothesis	71
6.2	Leaping Induction	74
6.3	Strong Induction	75
6.4	Many Flavors of Induction	78
6.5	Problems	80
7	Recursion	85
7.1	Recursive Functions	86
7.1.1	Recurrences	89
7.1.2	Recursive Programs	90
7.2	Recursive Sets	91
7.3	Recursive Structures – Trees	92
7.4	Problems	94
8	Proofs with Recursive Objects	101
8.1	Structural Induction	101
8.2	Structural Induction on \mathbb{N}	103
8.3	Palindromes	104
8.4	Well-Formed Arithmetic Expressions	104
8.5	Properties of Rooted Binary Trees	105
8.6	Problems	107
9	Sums and Asymptotics	113
9.1	Computing Sums	114
9.2	Asymptotics: Big-Theta, Big-Oh and Big-Omega	117
9.3	Approximation via Integration	119
9.4	Problems	122
10	Number Theory	129
10.1	Greatest Common Divisor	130
10.2	Fundamental Theorem of Arithmetic	132
10.3	Modular Arithmetic and Cryptography	133
10.3.1	Modular Multiplicative Inverse	135
10.3.2	RSA Public Key Cryptography	137
10.4	Problems	139
11	Graphs	145
11.1	Degree Sequence	146
11.1.1	Handshaking Theorem	148
11.2	Trees	149
11.3	Planar Graphs	149
11.4	Other Types of Graphs	150
11.4.1	Directed Graphs (Digraphs)	152
11.5	Problem Solving with Graphs	153

11.6 Problems	154
12 Matching and Coloring	161
12.1 Bipartite Graph Matchings	162
12.1.1 Stable Marriage: Mathematics of Dating	164
12.2 Coloring	166
12.3 Whirlwind Tour of Graph Problems	168
12.4 Problems	170
13 Counting	179
13.1 Counting Sequences	179
13.2 Build-up Counting	182
13.3 Counting One Set By Counting Another: Bijection	184
13.3.1 Bijection	184
13.3.2 Bijection and Counting	185
13.4 Permutations and Combinations	186
13.5 Problems	188
14 Advanced Counting	197
14.1 Inclusion-Exclusion	199
14.1.1 Union of More than Two Sets	200
14.2 Pigeonhole Principle	202
14.3 Problems	206
15 Probability	211
15.1 Computing Probabilities	211
15.1.1 The Event of Interest	213
15.2 Probability and Sets	216
15.3 Uniform Probability Spaces	218
15.4 Infinite Probability Spaces	219
15.5 Problems	221
16 Conditional Probability	225
16.1 Definition	225
16.2 Examples	226
16.3 Conditional Probability Traps	229
16.3.1 Sampling Bias	229
16.3.2 Transposed Conditional	230
16.4 Law of Total Probability	231
16.5 Problems	234
17 Independent Events	243
17.1 Coincidence: The Birthday Paradox	246
17.1.1 Hashing	248
17.2 Random Walk and Gambler's Ruin	250
17.3 Problems	253
18 Random Variables	259
18.1 Probability Distribution Function (PDF)	260
18.1.1 Joint Probability Distribution	262
18.1.2 Cumulative Distribution Function (CDF)	264
18.2 Bernoulli/Binary	265
18.3 Uniform	266
18.4 Binomial	267

18.5	Waiting Time to Success	268
18.6	Problems	269
19	Expected Value	277
19.1	Expected Value of Common Random Variables	279
19.1.1	Binomial Distribution	280
19.1.2	Waiting Time to Success	280
19.2	Conditional Expectation	281
19.2.1	Law of Total Expectation	284
19.3	Problems	287
20	Expected Value: Sums and Other Tools	293
20.1	Linearity	293
20.2	Iterated Expectation	295
20.3	Build-up Expectation	297
20.4	Expected Value of a Product	297
20.5	Sums of Indicators	299
20.6	Problems	302
21	Deviations from the Mean	309
21.1	Variance	310
21.1.1	Computing Variance	311
21.1.2	Variance is Non-Negative	312
21.2	Variance of a Sum	313
21.3	Law of Large Numbers	315
21.3.1	Weak Law of Large Numbers	317
21.3.2	Strong Law of Large Numbers	317
21.4	Problems	319
II	Theory of Computing	325
22	Infinity	327
22.1	Countable	327
22.1.1	Every Countable Set Can Be Listed	329
22.1.2	Rationals are Countable	331
22.2	Reals are Uncountable	332
22.3	Infinity and Computing	334
22.4	Problems	335
23	Languages: What is Computing?	339
23.1	Decision Problems	339
23.2	Languages	341
23.2.1	Describing a Language	342
23.3	Complexity of a Computing Problem	343
23.4	Problems	346
24	Deterministic Finite Automata	349
24.1	Regular Languages	351
24.2	Provably Non-Regular	355
24.3	Adding External Memory	356
24.4	Problems	358

25 Context Free Grammars	365
25.1 Parse Trees	369
25.2 Pushdown Automata (PDA)	371
25.3 Provably Not Context Free	372
25.4 Problems	374
26 Turing Machines	377
26.1 Transducer Turing Machines	381
26.2 Infinite Loops	383
26.3 Encodings of Turing Machines	384
26.4 Problems	386
27 Unsolvable Problems	387
27.1 Sketching Turing Machines	387
27.2 Programmable Turing Machines	388
27.3 \mathcal{L}_{TM} is Undecidable: There’s No Mega-Compiler	390
27.4 Other Unsolvable Problems: Reduction	391
27.4.1 Post’s Correspondence Problem (PCP)	393
27.4.2 Program Verification: “Hello World!”	394
27.4.3 Non-Recognizable Languages	395
27.5 Problems	396
28 Efficiency: The Class P	403
28.1 Time Complexity	404
28.2 Efficiently Solvable Problems: The Class P	405
28.3 A Decidable Non-Polynomial Problem	409
28.4 Boundary Between Efficient and Inefficient	411
28.5 Problems	412
29 Hard Problems: NP	413
29.1 Verifiable versus Solvable	413
29.1.1 NP: Polynomially Verifiable	414
29.1.2 NP and Nondeterminism	416
29.2 A Hardest Problem in NP	418
29.2.1 Circuits and Satisfiability	418
29.2.2 CIRCUIT-SAT is Harder than Every Problem in NP	418
29.3 Other Hardest Problems: NP-completeness	421
29.4 Problems	425
Epilogue	431
THE END	432
30 Solutions to Quizzes & Exercises	SOL – 1
End Quiz and Exercise Solutions	SOL – 96
Further Reading	433
Glossary of Notation	437
Index	441