

---

# Contents

<b>Preface</b>	<b>vii</b>
<b>I Discrete Mathematics</b>	<b>1</b>
<b>0 Background and Pep Talk</b>	<b>3</b>
<b>1 A Taste of Discrete Mathematics</b>	<b>7</b>
1.1 Modeling Epidemics . . . . .	7
1.2 Speed Dating . . . . .	8
1.3 Friendship Networks and Ads . . . . .	8
1.4 Computing . . . . .	9
1.5 Proof . . . . .	9
1.6 Problems . . . . .	11
<b>2 Discrete Objects</b>	<b>15</b>
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
<b>3 Making Precise Statements</b>	<b>25</b>
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 Prelude to Proof: Deduction Versus Induction . . . . .	34
3.5 Problems . . . . .	35
<b>4 Proofs</b>	<b>41</b>
4.1 Direct Proof . . . . .	41
4.1.1 Proving For All . . . . .	43
4.1.2 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
<b>5</b>	<b>Induction: Proving “FOR ALL ...”</b>	<b>55</b>
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
<b>6</b>	<b>Strong Induction</b>	<b>71</b>
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
<b>7</b>	<b>Recursion</b>	<b>85</b>
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
<b>8</b>	<b>Proofs About Recursive Objects</b>	<b>101</b>
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
<b>9</b>	<b>Sums and Asymptotics</b>	<b>113</b>
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
<b>10</b>	<b>Number Theory</b>	<b>129</b>
10.1	Greatest Common Divisor . . . . .	130
10.2	Fundamental Theorem of Arithmetic . . . . .	133
10.3	Modular Arithmetic and Cryptography . . . . .	133
10.3.1	Modular Multiplicative Inverse . . . . .	135
10.3.2	RSA Public Key Cryptography . . . . .	136
10.4	Problems . . . . .	139
<b>11</b>	<b>Graphs</b>	<b>145</b>
11.1	Degree Sequence . . . . .	146
11.2	Handshaking Theorem . . . . .	148
11.3	Trees . . . . .	149
11.4	Planar Graphs . . . . .	149
11.5	Other Types of Graphs . . . . .	150
11.5.1	Directed Graphs (Digraphs) . . . . .	152

11.6 Problem Solving with Graphs . . . . .	153
11.7 Problems . . . . .	154
<b>12 Matching and Coloring</b>	<b>161</b>
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
<b>13 Counting</b>	<b>179</b>
13.1 Counting Sequences: Sum and Product Rules . . . . .	179
13.2 Build-up Counting . . . . .	182
13.3 Counting One Set By Counting Another . . . . .	184
13.3.1 Bijection . . . . .	184
13.3.2 Bijection and Counting . . . . .	185
13.4 Permutations and Combinations: a Formula for $\binom{n}{k}$ . . . . .	186
13.5 Problems . . . . .	188
<b>14 Anagrams, Overlapping Sets, Pigeonhole</b>	<b>197</b>
14.1 Generalized Sum Rule: Inclusion-Exclusion . . . . .	199
14.1.1 Union of More than Two Sets . . . . .	200
14.2 Pigeonhole Principle . . . . .	202
14.3 Problems . . . . .	206
<b>15 Probability</b>	<b>211</b>
15.1 Computing Probabilities . . . . .	211
15.1.1 Ask A Question: 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
<b>16 Conditional Probability</b>	<b>225</b>
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
<b>17 Independent Events</b>	<b>243</b>
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
<b>18 Random Variables</b>	<b>259</b>
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 . . . . .	265

18.4 Binomial . . . . .	266
18.5 Waiting Time to Success . . . . .	268
18.6 Problems . . . . .	269
<b>19 Expected Value</b>	<b>277</b>
19.1 Expected Value of Common Random Variables . . . . .	279
19.1.1 Binomial Distribution . . . . .	279
19.1.2 Waiting Time to Success . . . . .	280
19.2 Conditional Expectation . . . . .	281
19.2.1 Law of Total Expectation . . . . .	283
19.3 Problems . . . . .	287
<b>20 Expected Value of a Sum</b>	<b>293</b>
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
<b>21 Deviations from the Mean</b>	<b>309</b>
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
<b>II Theory of Computing</b>	<b>325</b>
<b>22 Infinity</b>	<b>327</b>
22.1 Countable . . . . .	328
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
<b>23 Languages: What is Computing?</b>	<b>339</b>
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
<b>24 Deterministic Finite Automaton, DFA</b>	<b>349</b>
24.1 Regular Languages . . . . .	351
24.2 Provably Non-Regular . . . . .	355
24.3 Adding External Memory . . . . .	356
24.4 Problems . . . . .	358

<b>25 Context Free Grammars</b>	<b>365</b>
25.1 Parse Trees . . . . .	369
25.2 Pushdown Automata (PDA) . . . . .	371
25.3 Provably Not Context Free . . . . .	373
25.4 Problems . . . . .	374
<b>26 Turing Machines</b>	<b>377</b>
26.1 Transducer Turing Machines . . . . .	381
26.2 Infinite Loops . . . . .	383
26.3 Encodings of Turing Machines . . . . .	384
26.4 Problems . . . . .	386
<b>27 Unsolvable Problems</b>	<b>387</b>
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 Auto-Grading “Hello World!” . . . . .	394
27.4.3 Non-Recognizable Languages . . . . .	395
27.5 Problems . . . . .	396
<b>28 Efficiency: The Class P</b>	<b>403</b>
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 . . . . .	410
28.5 Problems . . . . .	412
<b>29 Hard Problems: NP</b>	<b>413</b>
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 Boolean 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
<b>Epilogue</b>	<b>431</b>
<b>THE END</b>	<b>432</b>
<b>30 Solutions to Quizzes &amp; Exercises</b>	<b>SOL – 1</b>
End Quiz and Exercise Solutions . . . . .	SOL – 95
<b>Further Reading</b>	<b>433</b>
<b>Glossary of Notation</b>	<b>437</b>
<b>Index</b>	<b>441</b>