

---

# Contents

<b>Preface</b>	<b>iii</b>
<b>I Discrete Mathematics</b>	<b>1</b>
<b>0 Background and Pep Talk</b>	<b>5</b>
<b>1 A Taste of Discrete Mathematics</b>	<b>9</b>
1.1 Modeling Epidemics . . . . .	9
1.2 Speed Dating . . . . .	10
1.3 Friendship Networks and Ads . . . . .	10
1.4 Modeling Computers . . . . .	11
1.5 Proof . . . . .	11
1.6 Problems . . . . .	13
<b>2 Discrete Objects</b>	<b>17</b>
2.1 Sets . . . . .	17
2.2 Sequences . . . . .	19
2.3 Graphs . . . . .	19
2.4 Easing into Proofs . . . . .	21
2.4.1 An Axiom: The Well Ordering Principle . . . . .	22
2.5 Problems . . . . .	25
<b>3 Making Precise Statements</b>	<b>27</b>
3.1 Compound Propositions . . . . .	28
3.2 Truth-Tables . . . . .	30
3.2.1 Proving an Implication . . . . .	32
3.3 Quantifiers: Statements About Many Things . . . . .	32
3.3.1 Predicates . . . . .	33
3.3.2 Negation . . . . .	35
3.3.3 Mixing Quantifiers . . . . .	35
3.3.4 Proofs with Quantifiers . . . . .	36
3.4 Deduction Versus Induction . . . . .	36
3.5 Problems . . . . .	37
<b>4 Proofs</b>	<b>43</b>
4.1 Direct Proof . . . . .	43
4.1.1 Proof by Contraposition . . . . .	47
4.2 Proving Equivalence: If and Only If . . . . .	47
4.3 Proof by Contradiction (Reductio ad Absurdum) . . . . .	49
4.4 Proofs about Sets . . . . .	50

4.5	Problems . . . . .	52
<b>5</b>	<b>Induction: Proving “for all . . .”</b>	<b>57</b>
5.1	The Principle of Induction . . . . .	58
5.1.1	Ordinary Induction . . . . .	59
5.1.2	Sum of Powers of Integers . . . . .	60
5.1.3	Induction Gone Wrong . . . . .	63
5.2	Induction and Well-ordering . . . . .	65
5.3	Problems . . . . .	66
<b>6</b>	<b>Strong Induction</b>	<b>73</b>
6.1	Strengthening the Induction Hypothesis . . . . .	73
6.2	Leaping Induction . . . . .	76
6.3	Strong Induction . . . . .	77
6.4	Many Flavors of Induction . . . . .	80
6.5	Problems . . . . .	82
<b>7</b>	<b>Recursion</b>	<b>87</b>
7.1	Recursive Functions . . . . .	88
7.1.1	Recurrences . . . . .	91
7.1.2	Recursive Programs . . . . .	92
7.2	Recursive Sets . . . . .	93
7.3	Recursive Structures – Trees . . . . .	94
7.4	Problems . . . . .	96
<b>8</b>	<b>Proofs with Recursive Objects</b>	<b>103</b>
8.1	Structural Induction . . . . .	103
8.2	Structural Induction on $\mathbb{N}$ . . . . .	105
8.3	Palindromes . . . . .	106
8.4	Well-Formed Arithmetic Expressions . . . . .	106
8.5	Properties of Rooted Binary Trees . . . . .	107
8.6	Problems . . . . .	109
<b>9</b>	<b>Sums and Asymptotics</b>	<b>115</b>
9.1	Computing Sums . . . . .	116
9.2	Asymptotics: Big-Theta, Big-Oh and Big-Omega . . . . .	119
9.3	Approximation via Integration . . . . .	121
9.4	Problems . . . . .	124
<b>10</b>	<b>Number Theory</b>	<b>131</b>
10.1	Greatest Common Divisor . . . . .	132
10.2	Fundamental Theorem of Arithmetic . . . . .	135
10.3	Modular Arithmetic and Cryptography . . . . .	135
10.3.1	Modular Multiplicative Inverse . . . . .	137
10.3.2	RSA Public Key Cryptography . . . . .	138
10.4	Problems . . . . .	141
<b>11</b>	<b>Graphs</b>	<b>147</b>
11.1	Degree Sequence . . . . .	148
11.1.1	Handshaking Theorem . . . . .	150
11.2	Trees . . . . .	151
11.3	Planar Graphs . . . . .	151
11.4	Other Types of Graphs . . . . .	152

11.4.1 Directed Graphs (Digraphs) . . . . .	154
11.5 Problem Solving with Graphs . . . . .	155
11.6 Problems . . . . .	156
<b>12 Matching and Coloring</b> . . . . .	<b>163</b>
12.1 Bipartite Graph Matchings . . . . .	164
12.1.1 Stable Marriage: Mathematics of Dating . . . . .	166
12.2 Coloring . . . . .	168
12.3 Whirlwind Tour of Graph Problems . . . . .	170
12.4 Problems . . . . .	172
<b>13 Counting</b> . . . . .	<b>181</b>
13.1 Counting Sequences . . . . .	181
13.2 Build-up Counting . . . . .	184
13.3 Counting One Set By Counting Another: Bijection . . . . .	186
13.3.1 Bijection . . . . .	186
13.3.2 Bijection and Counting . . . . .	187
13.4 Permutations and Combinations . . . . .	188
13.5 Problems . . . . .	190
<b>14 Advanced Counting</b> . . . . .	<b>199</b>
14.1 Inclusion-Exclusion . . . . .	201
14.1.1 Union of More than Two Sets . . . . .	202
14.2 Pigeonhole Principle . . . . .	204
14.3 Problems . . . . .	208
<b>15 Probability</b> . . . . .	<b>213</b>
15.1 Computing Probabilities . . . . .	213
15.1.1 The “Event” of Interest . . . . .	215
15.2 Probability and Sets . . . . .	218
15.3 Uniform Probability Spaces . . . . .	220
15.4 Infinite Probability Spaces . . . . .	221
15.5 Problems . . . . .	223
<b>16 Conditional Probability</b> . . . . .	<b>227</b>
16.1 Definition . . . . .	227
16.2 Examples . . . . .	228
16.3 Conditional Probability Traps . . . . .	231
16.3.1 Sampling Bias . . . . .	232
16.3.2 Transposed Conditional . . . . .	232
16.4 Law of Total Probability . . . . .	233
16.5 Problems . . . . .	236
<b>17 Independent Events</b> . . . . .	<b>245</b>
17.1 Coincidence: The Birthday Paradox . . . . .	248
17.1.1 Hashing . . . . .	250
17.2 Random Walk and Gambler’s Ruin . . . . .	252
17.3 Problems . . . . .	255

<b>18 Random Variables</b>	<b>261</b>
18.1 Probability Distribution Function (PDF)	262
18.1.1 Joint Probability Distribution	264
18.1.2 Cumulative Distribution Function (CDF)	266
18.2 Bernoulli/Binary	267
18.3 Uniform	268
18.4 Binomial	269
18.5 Waiting Time to Success	270
18.6 Problems	271
<b>19 Expected Value</b>	<b>279</b>
19.1 Expected Value of Common Random Variables	281
19.1.1 Binomial Distribution	282
19.1.2 Waiting Time to Success	282
19.2 Conditional Expectation	283
19.2.1 Law of Total Expectation	286
19.3 Problems	289
<b>20 Expected Value: Sums and Other Tools</b>	<b>295</b>
20.1 Linearity	295
20.2 Iterated Expectation	297
20.3 Build-up Expectation	299
20.4 Expected Value of a Product	299
20.5 Sums of Indicators	301
20.6 Problems	304
<b>21 Deviations from the Mean</b>	<b>311</b>
21.1 Variance	312
21.1.1 Computing Variance	313
21.1.2 Variance is Non-Negative	314
21.2 Variance of a Sum	315
21.3 Law of Large Numbers	317
21.3.1 Weak Law of Large Numbers	319
21.3.2 Strong Law of Large Numbers	319
21.4 Problems	321
<b>II Theory of Computing</b>	<b>327</b>
<b>22 Infinity</b>	<b>329</b>
22.1 Countable	329
22.1.1 Every Countable Set Can Be “Listed”	331
22.1.2 Rationals are Countable	333
22.2 Reals are Uncountable	334
22.3 Infinity and Computing	336
22.4 Problems	337
<b>23 Languages: What is Computation?</b>	<b>341</b>
23.1 Decision Problems	341
23.2 Languages	343
23.2.1 Describing a Language	344
23.3 Complexity of a Computing Problem	346
23.4 Problems	348

<b>24 Deterministic Finite Automata</b>	<b>351</b>
24.1 Regular Languages . . . . .	353
24.2 Provably Non-Regular . . . . .	357
24.3 Adding External Memory . . . . .	358
24.4 Problems . . . . .	360
<b>25 Context Free Grammars</b>	<b>367</b>
25.1 Parse Trees . . . . .	371
25.2 Pushdown Automata (PDA) . . . . .	373
25.3 Provably Not Context Free . . . . .	374
25.4 Problems . . . . .	376
<b>26 Turing Machines</b>	<b>379</b>
26.1 Transducer Turing Machines . . . . .	383
26.2 Infinite Loops . . . . .	385
26.3 Encodings of Turing Machines . . . . .	386
26.4 Problems . . . . .	388
<b>27 Unsolvable Problems</b>	<b>389</b>
27.1 Sketching Turing Machines . . . . .	389
27.2 Programmable Turing Machines . . . . .	390
27.3 $\mathcal{L}_{\text{TM}}$ is Undecidable: There's No Mega-Compiler . . . . .	392
27.4 Other Unsolvable Problems: Reduction . . . . .	393
27.4.1 Post's Correspondence Problem (PCP) . . . . .	395
27.4.2 Program Verification: "Hello World!" . . . . .	396
27.4.3 Non-Recognizable Languages . . . . .	397
27.5 Problems . . . . .	398
<b>28 Efficiency: The Class P</b>	<b>405</b>
28.1 Time Complexity . . . . .	406
28.2 Efficiently Solvable Problems: The Class P . . . . .	407
28.3 A Decidable Non-Polynomial Problem . . . . .	411
28.4 Boundary Between Efficient and Inefficient . . . . .	413
28.5 Problems . . . . .	414
<b>29 Hard Problems: NP</b>	<b>415</b>
29.1 Verifiable versus Solvable . . . . .	415
29.1.1 NP: Polynomially Verifiable . . . . .	416
29.1.2 NP and Nondeterminism . . . . .	418
29.2 A Hardest Problem in NP . . . . .	420
29.2.1 Circuits and Satisfiability . . . . .	420
29.2.2 CIRCUIT-SAT is Harder than Every Problem in NP . . . . .	420
29.3 Other Hardest Problems: NP-completeness . . . . .	423
29.4 Problems . . . . .	427
<b>30 Solutions to Quizzes &amp; Exercises</b>	<b>433</b>
<b>Index</b>	<b>537</b>