

Contents

1	Elementary Notions and Notations	1
1.1	A Proof Primer	2
1.1.1	Logical Statements	2
1.1.2	Something to Talk About	5
1.1.3	Proof Techniques	6
	Exercises	12
1.2	Sets	13
1.2.1	Definition of a Set	13
1.2.2	Operations on Sets	18
1.2.3	Counting Finite Sets	26
1.2.4	Bags (Multisets)	29
1.2.5	Sets Should Not Be Too Complicated	30
	Exercises	31
1.3	Ordered Structures	35
1.3.1	Tuples	35
1.3.2	Lists	39
1.3.3	Strings and Languages	41
1.3.4	Relations	46
1.3.5	Counting Tuples	49
	Exercises	52
1.4	Graphs and Trees	55
1.4.1	Definition of a Graph	55
1.4.2	Paths and Graphs	59
1.4.3	Graph Traversals	61
1.4.4	Trees	63
1.4.5	Spanning Trees	68
	Exercises	70
1.5	Chapter Summary	72

2	Facts about Functions	73
2.1	Definitions and Examples	74
2.1.1	Definition of a Function	74
2.1.2	Some Useful Functions	79
2.1.3	Partial Functions	87
	Exercises	88
2.2	Constructing Functions	91
2.2.1	Composition of Functions	91
2.2.2	The Map Function	96
	Exercises	98
2.3	Properties of Functions	100
2.3.1	Injections and Surjections	100
2.3.2	Bijections and Inverses	102
2.3.3	The Pigeonhole Principle	105
2.3.4	Simple Ciphers	106
2.3.5	Hash Functions	109
	Exercises	111
2.4	Countability	115
2.4.1	Comparing the Size of Sets	115
2.4.2	Sets that Are Countable	116
2.4.3	Diagonalization	119
2.4.4	Limits on Computability	121
	Exercises	124
2.5	Chapter Summary	125
3	Construction Techniques	127
3.1	Inductively Defined Sets	128
3.1.1	Numbers	129
3.1.2	Strings	132
3.1.3	Lists	134
3.1.4	Binary Trees	138
3.1.5	Cartesian Products of Sets	140
	Exercises	142
3.2	Recursive Functions and Procedures	145
3.2.1	Numbers	146
3.2.2	Strings	150
3.2.3	Lists	153
3.2.4	Binary Trees	159
3.2.5	Two More Problems	163
3.2.6	Infinite Sequences	165
	Exercises	168
3.3	Grammars	173
3.3.1	Recalling an English Grammar	173
3.3.2	Structure of Grammars	174
3.3.3	Derivations	177

3.3.4	Constructing Grammars	181
3.3.5	Meaning and Ambiguity	186
	Exercises	188
3.4	Chapter Summary	191
4	Equivalence, Order, and Inductive Proof	193
4.1	Properties of Binary Relations	194
4.1.1	Composition of Relations	195
4.1.2	Closures	199
4.1.3	Path Problems	204
	Exercises	209
4.2	Equivalence Relations	213
4.2.1	Definition and Examples	214
4.2.2	Equivalence Classes	218
4.2.3	Partitions	219
4.2.4	Generating Equivalence Relations	225
	Exercises	229
4.3	Order Relations	232
4.3.1	Partial Orders	233
4.3.2	Topological Sorting	239
4.3.3	Well-Founded Orders	242
4.3.4	Ordinal Numbers	250
	Exercises	251
4.4	Inductive Proof	253
4.4.1	Proof by Mathematical Induction	253
4.4.2	Proof by Well-Founded Induction	259
4.4.3	A Variety of Examples	261
	Exercises	267
4.5	Chapter Summary	272
5	Analysis Techniques	273
5.1	Analyzing Algorithms	274
5.1.1	Worst-Case Running Time	274
5.1.2	Decision Trees	277
	Exercises	281
5.2	Finding Closed Forms	281
5.2.1	Closed Forms for Sums	282
	Exercises	287
5.3	Counting and Discrete Probability	289
5.3.1	Permutations (Order Is Important)	289
5.3.2	Combinations (Order Is Not Important)	293
5.3.3	Discrete Probability	298
	Exercises	309
5.4	Solving Recurrences	312
5.4.1	Solving Simple Recurrences	313

5.4.2	Generating Functions	319
	Exercises	332
5.5	Comparing Rates of Growth	334
5.5.1	Big Theta	334
5.5.2	Little Oh	338
5.5.3	Big Oh and Big Omega	339
	Exercises	341
5.6	Chapter Summary	342
6	Elementary Logic	345
6.1	How Do We Reason?	346
6.1.1	What Is a Calculus?	347
6.1.2	How Can We Tell Whether Something Is a Proof?	348
6.2	Propositional Calculus	348
6.2.1	Well-Formed Formulas and Semantics	349
6.2.2	Equivalence	353
6.2.3	Truth Functions and Normal Forms	358
6.2.4	Complete Sets of Connectives	365
	Exercises	367
6.3	Formal Reasoning	369
6.3.1	Inference Rules	370
6.3.2	Formal Proof	372
6.3.3	Proof Notes	380
	Exercises	381
6.4	Formal Axiom Systems	384
6.4.1	An Example Axiom System	384
6.4.2	Other Axiom Systems	391
	Exercises	392
6.5	Chapter Summary	394
7	Predicate Logic	397
7.1	First-Order Predicate Calculus	397
7.1.1	Predicates and Quantifiers	398
7.1.2	Well-Formed Formulas	402
7.1.3	Semantics and Interpretations	404
7.1.4	Validity	409
7.1.5	The Validity Problem	413
	Exercises	413
7.2	Equivalent Formulas	416
7.2.1	Equivalence	416
7.2.2	Normal Forms	424
7.2.3	Formalizing English Sentences	427
7.2.4	Summary	429
	Exercises	430
7.3	Formal Proofs in Predicate Calculus	432

7.3.1	Universal Instantiation	433
7.3.2	Existential Generalization (EG)	437
7.3.3	Existential Instantiation (EI)	438
7.3.4	Universal Generalization (UG)	440
7.3.5	Examples of Formal Proofs	443
7.3.6	Summary of Quantifier Proof Rules	450
	Exercises	451
7.4	Chapter Summary	456
8	Applied Logic	457
8.1	Equality	458
8.1.1	Describing Equality	458
8.1.2	Extending Equals for Equals	464
	Exercises	465
8.2	Program Correctness	466
8.2.1	Imperative Program Correctness	467
8.2.2	Array Assignment	478
8.2.3	Termination	482
	Exercises	486
8.3	Higher-Order Logics	491
8.3.1	Classifying Higher-Order Logics	492
8.3.2	Semantics	496
8.3.3	Higher-Order Reasoning	498
	Exercises	501
8.4	Chapter Summary	503
9	Computational Logic	505
9.1	Automatic Reasoning	505
9.1.1	Clauses and Clausal Forms	506
9.1.2	Resolution for Propositions	512
9.1.3	Substitution and Unification	514
9.1.4	Resolution: The General Case	521
9.1.5	Theorem Proving with Resolution	526
9.1.6	Remarks	529
	Exercises	530
9.2	Logic Programming	533
9.2.1	Family Trees	534
9.2.2	Definition of a Logic Program	536
9.2.3	Resolution and Logic Programming	537
9.2.4	Logic Programming Techniques	549
	Exercises	553
9.3	Chapter Summary	555

10 Algebraic Structures and Techniques	557
10.1 What Is an Algebra?	558
10.1.1 Definition of an Algebra	560
10.1.2 Concrete Versus Abstract	562
10.1.3 Working in Algebras	564
Exercises	570
10.2 Boolean Algebra	572
10.2.1 Simplifying Boolean Expressions	574
10.2.2 Digital Circuits	578
Exercises	583
10.3 Abstract Data Types as Algebras	585
10.3.1 Natural Numbers	585
10.3.2 Lists and Strings	589
10.3.3 Stacks and Queues	592
10.3.4 Binary Trees and Priority Queues	596
Exercises	599
10.4 Computational Algebras	601
10.4.1 Relational Algebras	601
10.4.2 Functional Algebras	607
Exercises	611
10.5 Other Algebraic Ideas	613
10.5.1 Congruence	613
10.5.2 Cryptology: The RSA Algorithm	616
10.5.3 Subalgebras	621
10.5.4 Morphisms	623
Exercises	629
10.6 Chapter Summary	632
11 Regular Languages and Finite Automata	633
11.1 Regular Languages	634
11.1.1 Regular Expressions	635
11.1.2 The Algebra of Regular Expressions	638
Exercises	640
11.2 Finite Automata	642
11.2.1 Deterministic Finite Automata	642
11.2.2 Nondeterministic Finite Automata	646
11.2.3 Transforming Regular Expressions into Finite Automata	648
11.2.4 Transforming Finite Automata into Regular Expressions	650
11.2.5 Finite Automata as Output Devices	655
11.2.6 Representing and Executing Finite Automata	658
Exercises	664
11.3 Constructing Efficient Finite Automata	666
11.3.1 Another Regular Expression to NFA Algorithm	667
11.3.2 Transforming an NFA into a DFA	669
11.3.3 Minimum-State DFAs	675

Exercises	681
11.4 Regular Language Topics	683
11.4.1 Regular Grammars	684
11.4.2 Properties of Regular Languages	689
Exercises	693
11.5 Chapter Summary	695
12 Context-Free Languages and Pushdown Automata	697
12.1 Context-Free Languages	697
Exercises	700
12.2 Pushdown Automata	700
12.2.1 Equivalent Forms of Acceptance	703
12.2.2 Context-Free Grammars and Pushdown Automata	707
12.2.3 Representing and Executing Pushdown Automata	712
Exercises	715
12.3 Parsing Techniques	717
12.3.1 LL(k) Parsing	717
12.3.2 LR(k) Parsing	731
Exercises	744
12.4 Context-Free Language Topics	746
12.4.1 Transforming Grammars	746
12.4.2 Properties of Context-Free Languages	751
Exercises	755
12.5 Chapter Summary	756
13 Turing Machines and Equivalent Models	757
13.1 Turing Machines	757
13.1.1 Definition of a Turing Machine	758
13.1.2 Turing Machines with Output	762
13.1.3 Alternative Definitions	765
13.1.4 A Universal Turing Machine	769
Exercises	773
13.2 The Church-Turing Thesis	774
13.2.1 Equivalence of Computational Models	775
13.2.2 A Simple Programming Language	776
13.2.3 Recursive Functions	778
13.2.4 Machines That Transform Strings	781
Exercises	787
13.3 Chapter Summary	789
14 Computational Notions	791
14.1 Computability	791
14.1.1 Effective Enumerations	792
14.1.2 The Halting Problem	795
14.1.3 The Total Problem	796

14.1.4 Other Problems	798
Exercises	802
14.2 A Hierarchy of Languages	803
14.2.1 The Languages	803
14.2.2 Summary	807
Exercises	807
14.3 Complexity Classes	808
14.3.1 The Class P	809
14.3.2 The Class NP	810
14.3.3 The Class PSPACE	811
14.3.4 Intractable Problems	813
14.3.5 Completeness	815
14.3.6 Formal Complexity Theory	821
Exercises	824
14.4 Chapter Summary	825
Answers to Selected Exercises	827
Bibliography	915
Greek Alphabet	921
Symbol Glossary	923
Index	929