

Contents

1	Mathematical Reasoning, Proof Principles, and Logic	1
1.1	Introduction	1
1.2	Inference Rules, Deductions, Proof Systems $\mathcal{N}_m^{\Rightarrow}$ and $\mathcal{N}\mathcal{G}_m^{\Rightarrow}$	2
1.3	Adding \wedge, \vee, \perp ; The Proof Systems $\mathcal{N}_c^{\Rightarrow, \wedge, \vee, \perp}$ and $\mathcal{N}\mathcal{G}_c^{\Rightarrow, \wedge, \vee, \perp}$	19
1.4	Clearing Up Differences Among Rules Involving \perp	28
1.5	De Morgan Laws and Other Rules of Classical Logic	32
1.6	Formal Versus Informal Proofs; Some Examples	34
1.7	Truth Values Semantics for Classical Logic	40
1.8	Kripke Models for Intuitionistic Logic	43
1.9	Adding Quantifiers; The Proof Systems $\mathcal{N}_c^{\Rightarrow, \wedge, \vee, \exists, \perp}$, $\mathcal{N}\mathcal{G}_c^{\Rightarrow, \wedge, \vee, \exists, \perp}$	45
1.10	First-Order Theories	58
1.11	Decision Procedures, Proof Normalization, Counterexamples	64
1.12	Basics Concepts of Set Theory	70
1.13	Summary	79
	Problems	82
	References	100
2	Relations, Functions, Partial Functions	101
2.1	What is a Function?	101
2.2	Ordered Pairs, Cartesian Products, Relations, etc.	104
2.3	Induction Principles on \mathbb{N}	109
2.4	Composition of Relations and Functions	117
2.5	Recursion on \mathbb{N}	118
2.6	Inverses of Functions and Relations	121
2.7	Injections, Surjections, Bijections, Permutations	124
2.8	Direct Image and Inverse Image	128
2.9	Equinumerosity; Pigeonhole Principle; Schröder–Bernstein	129
2.10	An Amazing Surjection: Hilbert’s Space-Filling Curve	141
2.11	Strings, Multisets, Indexed Families	143
2.12	Summary	147

Problems	149
References	164
3 Graphs, Part I: Basic Notions	165
3.1 Why Graphs? Some Motivations	165
3.2 Directed Graphs	167
3.3 Path in Digraphs; Strongly Connected Components	171
3.4 Undirected Graphs, Chains, Cycles, Connectivity	182
3.5 Trees and Arborescences	189
3.6 Minimum (or Maximum) Weight Spanning Trees	194
3.7 Summary	200
Problems	201
References	203
4 Some Counting Problems; Multinomial Coefficients	205
4.1 Counting Permutations and Functions	205
4.2 Counting Subsets of Size k ; Multinomial Coefficients	208
4.3 Some Properties of the Binomial Coefficients	217
4.4 The Principle of Inclusion–Exclusion	229
4.5 Summary	237
Problems	238
References	255
5 Partial Orders, GCDs, RSA, Lattices	257
5.1 Partial Orders	257
5.2 Lattices and Tarski’s Fixed-Point Theorem	263
5.3 Well-Founded Orderings and Complete Induction	269
5.4 Unique Prime Factorization in \mathbb{Z} and GCDs	278
5.5 Dirichlet’s Diophantine Approximation Theorem	288
5.6 Equivalence Relations and Partitions	291
5.7 Transitive Closure, Reflexive and Transitive Closure	295
5.8 Fibonacci and Lucas Numbers; Mersenne Primes	296
5.9 Public Key Cryptography; The RSA System	309
5.10 Correctness of The RSA System	314
5.11 Algorithms for Computing Powers and Inverses Modulo m	318
5.12 Finding Large Primes; Signatures; Safety of RSA	322
5.13 Distributive Lattices, Boolean Algebras, Heyting Algebras	327
5.14 Summary	337
Problems	340
References	362
6 Graphs, Part II: More Advanced Notions	365
6.1 Γ -Cycles, Cocycles, Cotrees, Flows, and Tensions	365
6.2 Incidence and Adjacency Matrices of a Graph	381
6.3 Eulerian and Hamiltonian Cycles	386
6.4 Network Flow Problems; The Max-Flow Min-Cut Theorem	391

6.5 Matchings, Coverings, Bipartite Graphs	409
6.6 Planar Graphs	418
6.7 Summary	435
Problems	439
References	447
Symbol Index	449
Index	453