

# CONTENTS

## CHAPTER 1

<b><i>Sets and Functions</i></b>	1
1.1 Sets	1
1.2 The Indexing of Sets	2
1.3 Sets Derived from Other Sets	2
1.4 The Order of a Set	4
1.5 Functions	4
1.6 Exercises	6
1.7 More Notation	8
1.8 One-to-One and Onto	8
1.9 Composition and Inversion of Functions	9
1.10 Exercises	13
1.11 Finite-State Machines	15
1.12 Construction of Machines	20
1.13 Exercises	23
1.14 Union, Intersection, and Inclusion	26
1.15 Complementation	27
1.16 Venn Diagrams	28
1.17 More Algebra of Subsets	29
1.18 The Principle of Duality	30
1.19 Boolean Algebras; Summary of Basic Laws	32
1.20 Mathematical Induction	33
1.21 The Characteristic Function of a Subset of a Set	35
1.22 Exercises	37

## CHAPTER 2

<b><i>Relations and Graphs</i></b>	41
2.1 Relations	41
2.2 A Matrix Model of Finite Relations	42
2.3 The Composition of Relations	45
2.4 Matrix Equivalent of Composition; Digraphs	46
2.5 Relations on a Set $A$	48
2.6 Functions as Relations	49
2.7 Exercises	50
2.8 Partial Orderings and Posets	53
2.9 Special Elements of Posets	57
2.10 Direct Products of Posets	60
2.11 Exercises	61
2.12 Equivalence Relations and Partitions	63
2.13 Intersection and Union of Equivalence Relations	66
2.14 Intersection and Union of Partitions	68

viii		Contents
2.15	Exercises	70
2.16	Identification of Equivalent States	71
2.17	Minimal-State Machines	75
2.18	Distinguishing Sequences for States	77
2.19	Exercises	78
2.20	Undirected Graphs	81
2.21	Trees	85
2.22	Exercises	89
2.23	Spanning Trees	91
2.24	Fundamental Circuits and Cut-Sets	94
2.25	Applications and Famous Problems	95
2.26	Exercises	99

### CHAPTER 3

	<b><i>Rings and Boolean Algebras</i></b>	102
3.1	Algebras	102
3.2	Rings	103
3.3	Congruences	106
3.4	The Ring of Integers Modulo $p$	110
3.5	Binary Arithmetic Modulo $2^n$	111
3.6	Exercises	114
3.7	Boolean Rings and Boolean Algebras	116
3.8	Independent Postulates for a Boolean Algebra	119
3.9	Exercises	121
3.10	The Algebraic Description of Logic Circuits	124
3.11	Switching Functions and Their Basic Properties	127
3.12	Exercises	132
3.13	Disjunctive and Conjunctive Normal Forms	136
3.14	The Exclusive-OR and the Ring Normal Form of $f$	140
3.15	Inequalities in Switching Algebra	143
3.16	Exercises	144
3.17	Prime Implicants and Minimal Sums of Products	149
3.18	Reusch's Method for Finding All Prime Implicants	151
3.19	The Minimal Sums of a Function	155
3.20	Reusch's Method for Finding All Minimal Sums	158
3.21	Exercises	163
3.22	Conclusion	164

### CHAPTER 4

	<b><i>Semigroups and Groups</i></b>	165
4.1	Definitions	165
4.2	Zeros and Identities	168
4.3	Cyclic Semigroups and Cyclic Groups	170

4.4	Subsemigroups and Subgroups	172
4.5	Exercises	174
4.6	Congruence Relations on Semigroups	179
4.7	Morphisms	181
4.8	The Semigroup of a Machine	183
4.9	The Machine of a Semigroup	189
4.10	Exercises	190
4.11	Equations in Semigroups	192
4.12	Lagrange's Theorem	193
4.13	Direct Products	196
4.14	Normal Subgroups	196
4.15	Exercises	199
4.16	Structure of Cyclic Groups	201
4.17	Permutation Groups	202
4.18	Dihedral Groups	205
4.19	Additive Abelian Groups	207
4.20	Exercises	208

## CHAPTER 5

<b><i>Applications of Group Theory</i></b>	211	
5.1	The Binary Symmetric Channel	211
5.2	Block Codes	213
5.3	Weight and Distance	216
5.4	Generator and Parity-Check Matrices	218
5.5	Exercises	224
5.6	Group Codes	226
5.7	Coset Decoding	227
5.8	Hamming Codes	230
5.9	Extended Hamming Codes	233
5.10	Exercises	234
5.11	Fast Adders: Winograd's Theory	235
5.12	Fast Adders: Procedures	238
5.13	Exercises	240
5.14	Pólya Enumeration Theory	242
5.15	Exercises	249
5.16	An Extension of Pólya Enumeration Theory	251
5.17	Equivalence Classes of Switching Functions	255
5.18	Exercises	263

## CHAPTER 6

<b><i>Lattices</i></b>	265	
6.1	Definition of a Lattice	265
6.2	A Basic Theorem	266

x		Contents
6.3	The Operations “Cup” and “Cap”	267
6.4	Another Description of a Lattice	268
6.5	The Modular and Distributive Laws	271
6.6	Complements in Lattices	276
6.7	Exercises	277
6.8	Free Distributive Lattices	281
6.9	Compatibility Relations and Covers	282
6.10	Atomic Lattices and Boolean Algebras	285
6.11	Exercises	288
6.12	Closed Partitions in a Finite-State Machine	290
6.13	Series and Parallel Decomposition of Machines	295
6.14	Exercises	298

## CHAPTER 7

	<b><i>Linear Algebra and Field Theory</i></b>	300
7.1	Matrices	300
7.2	Elementary Row Operations	301
7.3	The Inverse of a Matrix	303
7.4	Exercises	305
7.5	Vector Spaces	307
7.6	Linear Independence and Dimension	310
7.7	Exercises	314
7.8	Linear Transformations	316
7.9	Matrices of Linear Transformations	320
7.10	Rank	325
7.11	Exercises	327
7.12	Determinants	329
7.13	Similarity	334
7.14	Exercises	335
7.15	Ideals and Homomorphisms in Rings	337
7.16	Polynomial Rings	339
7.17	Rational Canonical Form	341
7.18	Exercises	357
7.19	Field Extensions	360
7.20	Finite Fields	366
7.21	Computation in Finite Fields	369
7.22	Exercises	373
7.23	Automorphisms of Finite Fields	375
7.24	Number of Irreducibles	377
7.25	Exercises	379

## CHAPTER 8

	<b><i>Linear Machines</i></b>	381
8.1	Definition	381

8.2	Shift Registers	382
8.3	Characterizing Matrices	387
8.4	Exercises	390
8.5	The Distinguishing Matrix	392
8.6	Minimization of Linear Machines	394
8.7	Exercises	397
8.8	Rational Transfer Functions	399
8.9	Impulse Response	408
8.10	Exercises	411
8.11	Autonomous Linear Machines	413
8.12	Cycle Structure of Feedback Shift Registers	417
8.13	Recursive Equations	422
8.14	Exercises	425
8.15	Null Sequences	426
8.16	Circulating Shift Registers	429
8.17	Section 5.17 Revisited	430
8.18	Exercises	433

## CHAPTER 9

<b><i>Algebraic Coding Theory</i></b>	435	
9.1	Codes over $GF(q)$	435
9.2	Exercises	439
9.3	Cyclic Codes	440
9.4	BCH Codes	442
9.5	Reed–Solomon Codes; Burst Error Correction	444
9.6	Encoding Cyclic Codes	445
9.7	Exercises	447
9.8	BCH Decoding as an FSR Problem	449
9.9	Shortest FSR with Given Output	453
9.10	Algorithmic BCH Decoding	458
9.11	Exercises	464
9.12	Binary BCH Decoding	465
9.13	The Cyclic Redundancy Check	469
9.14	Fire Codes	475
9.15	Some Coding Tricks	478
9.16	How Good Can a Code Be?	481
9.17	Exercises	483

<b><i>Bibliography</i></b>	486
----------------------------	-----

<b><i>Index</i></b>	491
---------------------	-----