Contents

Preface xiii

Outline xv

A Theory 1

0 Boolean Algebraic Logic 3

0.0 INTRODUCTION . . . 3
0.1 LOGICAL FORMULAE . . . 5
0.1.1 The Empty Set . . . 5
0.1.2 An Alphabet for Logic . . . 6
0.1.3 Well-Formed Formulae . . . 7
0.1.4 Exercises . . . 9
0.2 LOGICAL TRUTH AND CONNECTIVES . . . 14
0.2.1 Logical Truth . . . 14
0.2.2 Logical Connectives . . . 15
0.2.3 Truth Tables . . . 18
0.2.4 Exercises . . . 20
0.3 TAUTOLOGIES AND CONTRADICTIONS . . . 21
0.3.1 Examples of Tautologies . . . 21
0.3.2 Contradictions . . . 26
0.3.3 Exercises . . . 27
0.4 OTHER METHODS OF PROOF . . . 32
0.4.1 Proofs by Tautologies . . . 32
0.4.2 Proofs by Contradictions . . . 34
0.4.3 Exercises . . . 36
0.5 SYNTHESIS OF LOGICAL FORMULAE . . . 36
0.5.1 Design of Logical Formulae with Specified Truth Values . . . 36
0.5.2 Simplification by Distributivity and Excluded Middle . . . 38
0.5.3 Exercises . . . 40
0.6 OTHER CONNECTIVES AND APPLICATIONS . . . 41
0.6.1 Other Logical Connectives . . . 41
0.6.2 Logical Connectives in Binary Arithmetic . . . 44
0.6.3 Exercises . . . 45
0.7 SYNTHESIS BY KARNAUGH TABLES . . . 46
0.7.1 Karnaugh Tables . . . 46
0.7.2 Exercises . . . 50
0.8 AN APPLICATION TO CIRCUITS . . . 52

0.9 PROJECTS 53

1 Logic and Deductive Reasoning 55

1.0 INTRODUCTION 55
1.1 PROPOSITIONAL CALCULUS 56
1.1.1 Formulae, Axioms, Rules, and Proofs 56
1.1.2 Examples of Proofs with Axioms P1 and P2 59
1.1.3 Exercises 60
1.2 CLASSICAL IMPLICATIONAL CALCULUS 62
1.2.1 Derived Rules: Implications Subject to Hypotheses 62
1.2.2 Examples of Proofs of Implicational Theorems 65
1.2.3 Exercises 67
1.3 PROOFS BY CONTRAPOSITION 67
1.3.1 Examples of Proofs with Axiom P3 67
1.3.2 Proofs by Reductio ad Absurdum 69
1.3.3 Exercises 70
1.4 OTHER CONNECTIVES 71
1.4.1 Definitions of Other Connectives 71
1.4.2 Examples of Proofs of Theorems with Conjunctions 72
1.4.3 Examples of Proofs of Theorems with Equivalences 74
1.4.4 Examples of Proofs of Theorems with Disjunctions 75
1.4.5 Examples of Proofs with Conjunctions and Disjunctions 76
1.4.6 Exercises 77
1.5 OTHER FORMS OF DEDUCTIVE REASONING 78
1.5.1 Conjunctions of Implications 78
1.5.2 Proofs by Cases or by Contradiction 80
1.5.3 Exercises 81
1.6 PREDICATE CALCULUS 82
1.6.1 Predicates, Quantifiers, Free or Bound Variables 82
1.6.2 Axioms and Rules for the Predicate Calculus 85
1.6.3 Examples of Proofs with the Predicate Calculus 86
1.6.4 Exercises 88
1.7 INFERENCE WITH QUANTIFIERS 88
1.7.1 Proofs with Quantifiers 88
1.7.2 Proofs With Universal Quantifiers and Other Connectives 90
1.7.3 Proofs with Quantifiers and Other Connectives 92
1.7.4 Proofs with Restrictions On a Quantified Variable 92
1.7.5 Proofs with More than One Quantified Variable 94
1.7.6 Exercises 95
1.8 FURTHER ISSUES IN LOGIC 96
1.9 PROJECTS 96

2 Set Theory 97

2.0 INTRODUCTION 97
2.1 SETS AND SUBSETS 98
2.1.1 Equality and Extensionality 98
2.1.2 The Empty Set 101
2.1.3 Subsets and Supersets 101
2.1.4 Exercises 103
2.2 PAIRING, POWER, AND SEPARATION 104
2.2.1 Pairing 104

2.2.2 Power Sets . . . 106
2.2.3 Separation of Sets . . . 108
2.2.4 Exercises . . . 109
2.3 UNIONS AND INTERSECTIONS OF SETS . . . 110
2.3.1 Unions of Sets . . . 110
2.3.2 Intersections of Sets . . . 114
2.3.3 Unions and Intersections of Sets . . . 117
2.3.4 Exercises . . . 121
2.4 CARTESIAN PRODUCTS AND RELATIONS . . . 124
2.4.1 Cartesian Products of Sets . . . 124
2.4.2 Cartesian Products of Unions and Intersections . . . 128
2.4.3 Mathematical Relations . . . 130
2.4.4 Exercises . . . 133
2.5 MATHEMATICAL FUNCTIONS . . . 134
2.5.1 Mathematical Functions . . . 134
2.5.2 Images and Inverse Images of Sets by Functions . . . 137
2.5.3 Exercises . . . 140
2.6 COMPOSITE AND INVERSE FUNCTIONS . . . 142
2.6.1 Compositions of Functions . . . 142
2.6.2 Injective, Surjective, Bijective, and Inverse Functions . . . 143
2.6.3 Exercises . . . 147
2.7 EQUIVALENCE RELATIONS . . . 147
2.7.1 Reflexive, Symmetric, Transitive, or Anti-Symmetric Relations . . . 147
2.7.2 Partitions and Equivalence Relations . . . 148
2.7.3 Exercises . . . 151
2.8 ORDERING RELATIONS . . . 152
2.8.1 Preorders and Partial Orders . . . 152
2.8.2 Total Orders and Well-Orderings . . . 154
2.8.3 Exercises . . . 156
2.9 PROJECTS . . . 158

3 Induction, Recursion, Arithmetic, Cardinality 159
3.0 INTRODUCTION . . . 159
3.1 MATHEMATICAL INDUCTION . . . 159
3.1.1 The Axiom of Infinity . . . 159
3.1.2 The Principle of Mathematical Induction . . . 162
3.1.3 Definitions by Mathematical Induction or Recursion . . . 163
3.1.4 Exercises . . . 165
3.2 ARITHMETIC WITH NATURAL NUMBERS . . . 166
3.2.1 Addition with Natural Numbers . . . 166
3.2.2 Multiplication with Natural Numbers . . . 167
3.2.3 Exercises . . . 170
3.3 ORDERS AND CANCELLATIONS . . . 171
3.3.1 Orders on the Natural Numbers . . . 171
3.3.2 Laws of Arithmetic Cancellations . . . 175
3.3.3 Exercises . . . 177
3.4 INTEGERS . . . 178
3.4.1 Negative Integers . . . 178
3.4.2 Arithmetic with Integers . . . 181
3.4.3 Order on the Integers . . . 183
3.4.4 Non-Negative Integral Powers of Integers . . . 187

3.4.5 Exercises 188
3.5 RATIONAL NUMBERS 189
3.5.1 Definition of Rational Numbers 189
3.5.2 Arithmetic with Rational Numbers 191
3.5.3 Notation for Sums and Products 195
3.5.4 Order on the Rational Numbers 199
3.5.5 Exercises 201
3.6 FINITE CARDINALITY 201
3.6.1 Equal Cardinalities 201
3.6.2 Finite Sets 204
3.6.3 Exercises 208
3.7 INFINITE CARDINALITY 208
3.7.1 Infinite Sets 208
3.7.2 Denumerable Sets 209
3.7.3 The Bernstein–Cantor–Schröder Theorem 212
3.7.4 Other Infinite Sets 214
3.7.5 Further Issues in Cardinality 215
3.7.6 Exercises 216
3.8 ARITHMETIC IN FINANCE 217
3.8.1 Introduction 217
3.8.2 Percentages and Rates 217
3.8.3 Sales and Income Taxes 217
3.8.4 Compounded Interest 218
3.8.5 Loans, Mortgages, and Savings Plans 219
3.8.6 Perpetuities 220
3.8.7 Exercises 220
3.9 PROJECTS 221

4 Decidability and Completeness **223**
4.0 INTRODUCTION 223
4.1 LOGICS FOR SCIENTIFIC REASONING 224
4.1.1 Scientific Reasoning 224
4.1.2 Hypothesis Testing 225
4.1.3 Brouwer & Heyting's Intuitionistic Logic 226
4.1.4 Kolmogorov & Johansson's Minimal Propositional Calculus 228
4.1.5 Exercises 230
4.2 INCOMPLETENESS 231
4.2.1 Tautologies and Theorems 231
4.2.2 Incompleteness of the Implicational Calculus 232
4.2.3 Exercises 234
4.3 LOGICS NOT AMENABLE TO TRUTH TABLES 236
4.3.1 Logics with Any Number of Values 236
4.3.2 Practical Logics Not Amenable to Truth Tables 237
4.3.3 Exercises 239
4.4 AUTOMATED THEOREM PROVING 240
4.4.1 The Deduction Theorem 240
4.4.2 Example: Law of Assertion from the Deduction Theorem 242
4.4.3 The Provability Theorem 244
4.4.4 The Completeness Theorem 246
4.4.5 Example: Peirce's Law from the Completeness Theorem 246
4.4.6 Exercises 248

4.5 TRANSFINITE METHODS . . . 250
4.5.1 Transfinite Induction . . . 250
4.5.2 Transfinite Construction . . . 251
4.5.3 Exercises . . . 252
4.6 TRANSITIVE SETS AND ORDINALS . . . 253
4.6.1 Transitive Sets . . . 253
4.6.2 Ordinals . . . 254
4.6.3 Well-Ordered Sets of Ordinals . . . 255
4.6.4 Unions and Intersections of Sets of Ordinals . . . 256
4.6.5 Exercises . . . 257
4.7 REGULARITY OF WELL-FORMED SETS . . . 258
4.7.1 Well-Formed Sets . . . 258
4.7.2 Regularity . . . 259
4.7.3 Exercises . . . 260
4.8 FURTHER ISSUES IN DECIDABILITY . . . 261
4.9 PROJECTS . . . 262

B Applications 263

5 Number Theory and Codes 265
5.0 INTRODUCTION . . . 265
5.1 THE EUCLIDEAN ALGORITHM . . . 265
5.1.1 Division With Integers . . . 265
5.1.2 Greatest Common Divisors . . . 267
5.1.3 Exercises . . . 270
5.2 DIGITAL EXPANSION AND ARITHMETIC . . . 271
5.2.1 Expansion of Integers in Powers of an Integral Base . . . 271
5.2.2 Digital Integer Arithmetic . . . 273
5.2.3 Exercises . . . 275
5.3 PRIME NUMBERS . . . 276
5.3.1 Prime Numbers . . . 276
5.3.2 Prime-Number Factorization . . . 277
5.3.3 Primality Testing . . . 279
5.3.4 Exercises . . . 279
5.4 MODULAR ARITHMETIC . . . 280
5.4.1 Modular Integers . . . 280
5.4.2 Modular Addition . . . 282
5.4.3 Modular Multiplication . . . 284
5.4.4 Modular Division . . . 285
5.4.5 Divisibility Tests . . . 287
5.4.6 Exercises . . . 289
5.5 MODULAR CODES . . . 290
5.5.1 The International Standard Book Number (ISBN) Code . . . 290
5.5.2 The Universal Product Code (UPC) . . . 291
5.5.3 The Bank Identification Code . . . 291
5.5.4 The U.S. postal nine-digit ZIP Code . . . 292
5.5.5 Exercises . . . 292
5.6 EUCLID, EULER, & FERMAT'S THEOREMS . . . 294
5.6.1 Fermat's Little Theorem . . . 294
5.6.2 The Euler–Fermat Theorem . . . 295

5.6.3 Exercises 296
5.7 RIVEST–SHAMIR–ADLEMAN (RSA) CODES 297
5.7.1 The Rivest–Shamir–Adleman (RSA) Public-Key 297
5.7.2 Proof of the Correctness of the RSA Algorithm 298
5.7.3 Exercises 300
5.8 FURTHER ISSUES IN NUMBER THEORY 301
5.9 PROJECTS 302

6 Ciphers, Combinatorics, and Probabilities 303
6.0 INTRODUCTION 303
6.1 ALGEBRA 304
6.1.1 Definitions and Examples of Mathematical Groups 304
6.1.2 Existence and Uniqueness of Identities and Inverses 305
6.1.3 Bijections of Groups 308
6.1.4 Exercises 311
6.2 PERMUTATIONS 313
6.2.1 Permutations and Orbits 313
6.2.2 Transpositions 316
6.2.3 Exercises 319
6.3 CYCLIC PERMUTATIONS 320
6.3.1 Cycles 320
6.3.2 Factorization of Permutations by Cycles 322
6.3.3 Exercises 323
6.4 SIGNATURES OF PERMUTATIONS 324
6.4.1 Even and Odd Permutations 324
6.4.2 Signatures of Composite Permutations 326
6.4.3 Exercises 328
6.5 ARRANGEMENTS 328
6.5.1 Arrangements Without Repetition 328
6.5.2 Arrangements With Repetitions 329
6.5.3 Exercises 330
6.6 COMBINATIONS 331
6.6.1 Combinations Without Repetition 331
6.6.2 Combinations With Repetition 335
6.6.3 Permutations With Repetition 336
6.6.4 Exercises 339
6.7 PROBABILITY 339
6.7.1 Probability Spaces 339
6.7.2 The Exclusion-Inclusion Principle 343
6.7.3 Conditional Probabilities 344
6.7.4 Applications of Binomial Probabilities 347
6.7.5 Exercises 350
6.8 THE ENIGMA MACHINES 351
6.8.1 Design and Operation of the ENIGMA Machines 351
6.8.2 Breaking the ENIGMA Ciphers 354
6.8.3 Reconstructing the ENIGMA Wiring 355
6.8.4 Exercises 357
6.9 PROJECTS 359

7 Graph Theory **361**
7.0 INTRODUCTION . . . 361
7.1 MATHEMATICAL GRAPHS . . . 362
7.1.1 Directed Graphs . . . 362
7.1.2 Undirected Graphs . . . 363
7.1.3 Degrees of Vertices . . . 366
7.1.4 Exercises . . . 368
7.2 PATH-CONNECTED GRAPHS . . . 369
7.2.1 Walks in Graphs . . . 369
7.2.2 Path-Connected Components of Graphs . . . 371
7.2.3 Longer Walks . . . 373
7.2.4 Longest Paths . . . 374
7.2.5 Exercises . . . 375
7.3 EULER AND HAMILTONIAN CIRCUITS . . . 375
7.3.1 Circuits . . . 375
7.3.2 Hamiltonian Paths and Circuits . . . 376
7.3.3 Eulerian Paths and Circuits . . . 378
7.3.4 Exercises . . . 379
7.4 MATHEMATICAL TREES . . . 380
7.4.1 Trees . . . 380
7.4.2 Spanning Trees . . . 380
7.4.3 Directed Trees and Star-Shaped Graphs . . . 381
7.4.4 Exercises . . . 382
7.5 WEIGHTED GRAPHS AND MULTIGRAPHS . . . 382
7.5.1 Weighted Graphs . . . 382
7.5.2 Shortest Path and Minimum-Weight Paths or Trees . . . 383
7.5.3 Maximal Flows in Transportation Graphs . . . 385
7.5.4 Exercises . . . 387
7.6 BIPARTITE GRAPHS AND MATCHINGS . . . 388
7.6.1 Bipartite Graphs . . . 388
7.6.2 Maximum Matching . . . 390
7.6.3 Exercises . . . 392
7.7 GRAPH THEORY IN SCIENCE . . . 392
7.7.1 The Shape of Molecules . . . 392
7.7.2 The Shape of Hydrocarbons . . . 393
7.7.3 Sequences of Radioactive Decays . . . 395
7.7.4 Exercises . . . 396
7.8 FURTHER ISSUES: PLANAR GRAPHS . . . 397
7.9 PROJECTS . . . 398

Bibliography **399**

Index **405**