Contents

Part I Foundations

1 Propositional Logic 3
1.1 Syntax 4
1.2 Semantics 6
1.3 Satisfiability and Validity 8
1.3.1 Truth Tables 9
1.3.2 Semantic Arguments 10
1.4 Equivalence and Implication 14
1.5 Substitution 16
1.6 Normal Forms 18
1.7 Decision Procedures for Satisfiability 21
1.7.1 Simple Decision Procedures 21
1.7.2 Reconsidering the Truth-Table Method 22
1.7.3 Conversion to an Equisatisfiable Formula in CNF 24
1.7.4 The Resolution Procedure 27
1.7.5 DPLL 28
1.8 Summary 31
Bibliographic Remarks 32
Exercises 32

2 First-Order Logic 35
2.1 Syntax 35
2.2 Semantics 39
2.3 Satisfiability and Validity 42
2.4 Substitution 45
2.4.1 Safe Substitution 47
2.4.2 Schema Substitution 48
2.5 Normal Forms 51
2.6 Decidability and Complexity 53
2.6.1 Satisfiability as a Formal Language 53

2.6.2 Decidability . . . 54
2.6.3 ★Complexity . . . 54
2.7 ★Meta-Theorems of First-Order Logic . . . 56
2.7.1 Simplifying the Language of FOL . . . 57
2.7.2 Semantic Argument Proof Rules . . . 58
2.7.3 Soundness and Completeness . . . 58
2.7.4 Additional Theorems . . . 61
2.8 Summary . . . 66
Bibliographic Remarks . . . 67
Exercises . . . 67

3 First-Order Theories . . . 69
3.1 First-Order Theories . . . 69
3.2 Equality . . . 71
3.3 Natural Numbers and Integers . . . 73
3.3.1 Peano Arithmetic . . . 73
3.3.2 Presburger Arithmetic . . . 75
3.3.3 Theory of Integers . . . 76
3.4 Rationals and Reals . . . 79
3.4.1 Theory of Reals . . . 80
3.4.2 Theory of Rationals . . . 82
3.5 Recursive Data Structures . . . 84
3.6 Arrays . . . 87
3.7 ★Survey of Decidability and Complexity . . . 90
3.8 Combination Theories . . . 91
3.9 Summary . . . 92
Bibliographic Remarks . . . 93
Exercises . . . 93

4 Induction . . . 95
4.1 Stepwise Induction . . . 95
4.2 Complete Induction . . . 99
4.3 Well-Founded Induction . . . 102
4.4 Structural Induction . . . 108
4.5 Summary . . . 110
Bibliographic Remarks . . . 111
Exercises . . . 111

5 Program Correctness: Mechanics . . . 113
5.1 pi: A Simple Imperative Language . . . 114
5.1.1 The Language . . . 115
5.1.2 Program Annotations . . . 118
5.2 Partial Correctness . . . 123
5.2.1 Basic Paths: Loops . . . 125
5.2.2 Basic Paths: Function Calls . . . 131

5.2.3 Program States . . . 135
5.2.4 Verification Conditions . . . 136
5.2.5 P-Invariant and P-Inductive . . . 142
5.3 Total Correctness . . . 143
5.4 Summary . . . 149
Bibliographic Remarks . . . 150
Exercises . . . 151

6 Program Correctness: Strategies . . . 153
6.1 Developing Inductive Annotations . . . 153
6.1.1 Basic Facts . . . 154
6.1.2 The Precondition Method . . . 156
6.1.3 A Strategy . . . 162
6.2 Extended Example: QuickSort . . . 164
6.2.1 Partial Correctness . . . 167
6.2.2 Total Correctness . . . 171
6.3 Summary . . . 172
Bibliographic Remarks . . . 173
Exercises . . . 173

Part II Algorithmic Reasoning

7 Quantified Linear Arithmetic . . . 183
7.1 Quantifier Elimination . . . 184
7.1.1 Quantifier Elimination . . . 184
7.1.2 A Simplification . . . 185
7.2 Quantifier Elimination over Integers . . . 185
7.2.1 Augmented Theory of Integers . . . 185
7.2.2 Cooper's Method . . . 187
7.2.3 A Symmetric Elimination . . . 194
7.2.4 Eliminating Blocks of Quantifiers . . . 195
7.2.5 ★Solving Divides Constraints . . . 196
7.3 Quantifier Elimination over Rationals . . . 200
7.3.1 Ferrante and Rackoff's Method . . . 200
7.4 ★Complexity . . . 204
7.5 Summary . . . 204
Bibliographic Remarks . . . 205
Exercises . . . 205

8 Quantifier-Free Linear Arithmetic . . . 207
8.1 Decision Procedures for Quantifier-Free Fragments . . . 207
8.2 Preliminary Concepts and Notation . . . 209
8.3 Linear Programs . . . 213
8.4 The Simplex Method . . . 218

8.4.1 From M to M_0 . . . 219
8.4.2 Vertex Traversal . . . 223
8.4.3 ★Complexity . . . 237
8.5 Summary . . . 237
Bibliographic Remarks . . . 238
Exercises . . . 238

9 Quantifier-Free Equality and Data Structures . . . 241
9.1 Theory of Equality . . . 242
9.2 Congruence Closure Algorithm . . . 244
9.2.1 Relations . . . 245
9.2.2 Congruence Closure Algorithm . . . 247
9.3 Congruence Closure with DAGs . . . 251
9.3.1 Directed Acyclic Graphs . . . 251
9.3.2 Basic Operations . . . 254
9.3.3 Congruence Closure Algorithm . . . 255
9.3.4 Decision Procedure for T_{E}-Satisfiability . . . 256
9.3.5 ★Complexity . . . 258
9.4 Recursive Data Structures . . . 259
9.5 Arrays . . . 263
9.6 Summary . . . 265
Bibliographic Remarks . . . 266
Exercises . . . 267

10 Combining Decision Procedures . . . 269
10.1 Combining Decision Procedures . . . 269
10.2 Nelson-Oppen Method: Nondeterministic Version . . . 271
10.2.1 Phase 1: Variable Abstraction . . . 271
10.2.2 Phase 2: Guess and Check . . . 273
10.2.3 Practical Efficiency . . . 274
10.3 Nelson-Oppen Method: Deterministic Version . . . 276
10.3.1 Convex Theories . . . 276
10.3.2 Phase 2: Equality Propagation . . . 278
10.3.3 Equality Propagation: Implementation . . . 282
10.4 ★Correctness of the Nelson-Oppen Method . . . 283
10.5 ★Complexity . . . 287
10.6 Summary . . . 288
Bibliographic Remarks . . . 288
Exercises . . . 288

11 Arrays . . . 291
11.1 Arrays with Uninterpreted Indices . . . 292
11.1.1 Array Property Fragment . . . 292
11.1.2 Decision Procedure . . . 294
11.2 Integer-Indexed Arrays . . . 299

11.2.1 Array Property Fragment 300
11.2.2 Decision Procedure 301
11.3 Hashtables 304
11.3.1 Hashtable Property Fragment 305
11.3.2 Decision Procedure 306
11.4 Larger Fragments 308
11.5 Summary 309
Bibliographic Remarks 310
Exercises 310

12 Invariant Generation 311
12.1 Invariant Generation 311
12.1.1 Weakest Precondition and Strongest Postcondition 312
12.1.2 ★General Definitions of wp and sp 315
12.1.3 Static Analysis 316
12.1.4 Abstraction 319
12.2 Interval Analysis 325
12.3 Karr's Analysis 333
12.4 ★Standard Notation and Concepts 341
12.5 Summary 344
Bibliographic Remarks 345
Exercises 345

13 Further Reading 347

References 351

Index 357