Contents

Foreword xi
Preface xxi
Acknowledgments xxi

1 Propositional logic 1
  1.1 Declarative sentences 2
  1.2 Natural deduction 6
    1.2.1 Rules for natural deduction 7
    1.2.2 Derived rules 28
    1.2.3 Natural deduction in summary 30
    1.2.4 Provable equivalence 33
    1.2.5 An aside: proof by contradiction 34
  1.3 Propositional logic as a formal language 38
  1.4 Semantics of propositional logic 45
    1.4.1 The meaning of logical connectives 45
    1.4.2 Mathematical induction 51
    1.4.3 Soundness of propositional logic 56
    1.4.4Completeness of propositional logic 61
  1.5 Normal forms 69
    1.5.1 Semantic equivalence, satisfiability and validity 69
    1.5.2 Conjunctive normal forms and validity 76
    1.5.3 Horn clauses and satisfiability 84
  1.6 Bibliographic notes 89

2 Predicate logic 90
  2.1 The need for a richer language 90
  2.2 Predicate logic as a formal language 96
    2.2.1 Terms 96
2.2.2 Formulas 98
2.2.3 Free and bound variables 103
2.2.4 Substitution 105

2.3 Proof theory of predicate logic 109
2.3.1 Natural deduction rules 109
2.3.2 Quantifier equivalences 120

2.4 Semantics of predicate logic 128
2.4.1 Models 129
2.4.2 Semantic entailment 136
2.4.3 The semantics of equality 138

2.5 Undecidability of predicate logic 140
2.6 Bibliographic notes 147

3 Verification by model checking 148
3.1 Motivation for verification 148
3.2 The syntax of computation tree logic 152
3.3 Semantics of computation tree logic 156
3.3.1 Practical patterns of specifications 165
3.3.2 Important equivalences between CTL formulas 166

3.4 Example: mutual exclusion 169
3.4.1 The first modelling attempt 170
3.4.2 The second modelling attempt 171

3.5 A model-checking algorithm 172
3.5.1 The labelling algorithm 173
3.5.2 The pseudo-code of the model checking algorithm 177
3.5.3 The 'state explosion' problem 178

3.6 The SMV system 181
3.6.1 Modules in SMV 183
3.6.2 Synchronous and asynchronous composition 184
3.6.3 Mutual exclusion revisited 185
3.6.4 The alternating bit protocol 187

3.7 Model checking with fairness 193
3.8 Alternatives and extensions of CTL 196
3.8.1 Linear-time temporal logic 196
3.8.2 CTL* 198
3.8.3 The expressive power of CTL 201

3.9 The fixed-point characterisation of CTL 203
3.9.1 Monotone functions 205
3.9.2 The correctness of SAT_{EG} 208
3.9.3 The correctness of SAT_{EU} 210
6.2 Algorithms for reduced OBDDs
   6.2.1 The algorithm reduce 334
   6.2.2 The algorithm apply 336
   6.2.3 The algorithm restrict 342
   6.2.4 The algorithm exists 344
   6.2.5 Assessment of OBDDs 348

6.3 Symbolic model checking 351
   6.3.1 Representing subsets of the set of states 351
   6.3.2 Representing the transition relation 354
   6.3.3 Implementing the functions pre_3 and pre_y 355
   6.3.4 Synthesising OBDDs 357

6.4 A relational mu-calculus 361
   6.4.1 Syntax and semantics 362
   6.4.2 Coding CTL models and specifications 366

6.5 Bibliographic notes 374

Bibliography 375

Index 378