Contents

Foreword xiii

Preface xv

1 System Verification 1
- 1.1 Model Checking . . . 7
- 1.2 Characteristics of Model Checking . . . 11
  - 1.2.1 The Model-Checking Process . . . 11
  - 1.2.2 Strengths and Weaknesses . . . 14
- 1.3 Bibliographic Notes . . . 16

2 Modeling Concurrent Systems 19
- 2.1 Transition Systems . . . 19
  - 2.1.1 Executions . . . 24
  - 2.1.2 Modeling Hardware and Software Systems . . . 26
- 2.2 Parallelism and Communication . . . 35
  - 2.2.1 Concurrency and Interleaving . . . 35
  - 2.2.2 Communication via Shared Variables . . . 39
  - 2.2.3 Handshaking . . . 48
  - 2.2.4 Channel Systems . . . 52
  - 2.2.5 NanoPromela . . . 61
  - 2.2.6 Synchronous Parallelism . . . 73
- 2.3 The State-Space Explosion Problem . . . 75
- 2.4 Summary . . . 78
- 2.5 Bibliographic Notes . . . 78
- 2.6 Exercises . . . 80

3 Linear-Time Properties 87
- 3.1 Deadlock . . . 87
- 3.2 Linear-Time Behavior . . . 91
  - 3.2.1 Paths and State Graph . . . 92
  - 3.2.2 Traces . . . 95
  - 3.2.3 Linear-Time Properties . . . 97

3.2.4 Trace Equivalence and Linear-Time Properties . . . 101
3.3 Safety Properties and Invariants . . . 104
3.3.1 Invariants . . . 105
3.3.2 Safety Properties . . . 109
3.3.3 Trace Equivalence and Safety Properties . . . 113
3.4 Liveness Properties . . . 118
3.4.1 Liveness Properties . . . 118
3.4.2 Safety vs. Liveness Properties . . . 120
3.5 Fairness . . . 124
3.5.1 Fairness Constraints . . . 126
3.5.2 Fairness Strategies . . . 134
3.5.3 Fairness and Safety . . . 137
3.6 Summary . . . 139
3.7 Bibliographic Notes . . . 140
3.8 Exercises . . . 142

4 Regular Properties **149**
4.1 Automata on Finite Words . . . 149
4.2 Model-Checking Regular Safety Properties . . . 157
4.2.1 Regular Safety Properties . . . 157
4.2.2 Verifying Regular Safety Properties . . . 161
4.3 Automata on Infinite Words . . . 167
4.3.1 ω-Regular Languages and Properties . . . 168
4.3.2 Nondeterministic Büchi Automata . . . 171
4.3.3 Deterministic Büchi Automata . . . 185
4.3.4 Generalized Büchi Automata . . . 189
4.4 Model-Checking ω-Regular Properties . . . 195
4.4.1 Persistence Properties and Product . . . 196
4.4.2 Nested Depth-First Search . . . 202
4.5 Summary . . . 214
4.6 Bibliographic Notes . . . 215
4.7 Exercises . . . 216

5 Linear Temporal Logic **225**
5.1 Linear Temporal Logic . . . 225
5.1.1 Syntax . . . 227
5.1.2 Semantics . . . 231
5.1.3 Specifying Properties . . . 235
5.1.4 Equivalence of LTL Formulae . . . 243
5.1.5 Weak Until, Release, and Positive Normal Form . . . 247
5.1.6 Fairness in LTL . . . 253
5.2 Automata-Based LTL Model Checking . . . 265

5.2.1 Complexity of the LTL Model-Checking Problem . . . 282
5.2.2 LTL Satisfiability and Validity Checking . . . 291
5.3 Summary . . . 294
5.4 Bibliographic Notes . . . 294
5.5 Exercises . . . 296

6 Computation Tree Logic 309
6.1 Introduction . . . 309
6.2 Computation Tree Logic . . . 313
6.2.1 Syntax . . . 313
6.2.2 Semantics . . . 316
6.2.3 Equivalence of CTL Formulae . . . 325
6.2.4 Normal Forms for CTL . . . 328
6.3 Expressiveness of CTL vs. LTL . . . 330
6.4 CTL Model Checking . . . 336
6.4.1 Basic Algorithm . . . 337
6.4.2 The Until and Existential Always Operator . . . 342
6.4.3 Time and Space Complexity . . . 350
6.5 Fairness in CTL . . . 353
6.6 Counterexamples and Witnesses . . . 368
6.6.1 Counterexamples in CTL . . . 371
6.6.2 Counterexamples and Witnesses in CTL with Fairness . . . 375
6.7 Symbolic CTL Model Checking . . . 376
6.7.1 Switching Functions . . . 377
6.7.2 Encoding Transition Systems by Switching Functions . . . 381
6.7.3 Ordered Binary Decision Diagrams . . . 387
6.7.4 Implementation of ROBDD-Based Algorithms . . . 402
6.8 CTL* . . . 417
6.8.1 Logic, Expressiveness, and Equivalence . . . 417
6.8.2 CTL* Model Checking . . . 422
6.9 Summary . . . 425
6.10 Bibliographic Notes . . . 426
6.11 Exercises . . . 428

7 Equivalences and Abstraction 443
7.1 Bisimulation . . . 445
7.1.1 Bisimulation Quotient . . . 450
7.1.2 Action-Based Bisimulation . . . 457
7.2 Bisimulation and CTL* Equivalence . . . 461
7.3 Bisimulation-Quotienting Algorithms . . . 469
7.3.1 Determining the Initial Partition . . . 471
7.3.2 Refining Partitions . . . 473

7.3.3 A First Partition Refinement Algorithm . . . 479
7.3.4 An Efficiency Improvement . . . 480
7.3.5 Equivalence Checking of Transition Systems . . . 486
7.4 Simulation Relations . . . 489
7.4.1 Simulation Equivalence . . . 497
7.4.2 Bisimulation, Simulation, and Trace Equivalence . . . 503
7.5 Simulation and ∀CTL* Equivalence . . . 507
7.6 Simulation-Quotienting Algorithms . . . 513
7.7 Stutter Linear-Time Relations . . . 520
7.7.1 Stutter Trace Equivalence . . . 521
7.7.2 Stutter Trace and $\mathrm{LTL}_{\setminus\bigcirc}$ Equivalence . . . 525
7.8 Stutter Bisimulation . . . 527
7.8.1 Divergence-Sensitive Stutter Bisimulation . . . 535
7.8.2 Normed Bisimulation . . . 542
7.8.3 Stutter Bisimulation and $\mathrm{CTL}^*_{\setminus\bigcirc}$ Equivalence . . . 551
7.8.4 Stutter Bisimulation Quotienting . . . 558
7.9 Summary . . . 570
7.10 Bibliographic Notes . . . 571
7.11 Exercises . . . 573

8 Partial Order Reduction **585**
8.1 Independence of Actions . . . 588
8.2 The Linear-Time Ample Set Approach . . . 595
8.2.1 Ample Set Constraints . . . 596
8.2.2 Dynamic Partial Order Reduction . . . 609
8.2.3 Computing Ample Sets . . . 617
8.2.4 Static Partial Order Reduction . . . 625
8.3 The Branching-Time Ample Set Approach . . . 640
8.4 Summary . . . 651
8.5 Bibliographic Notes . . . 651
8.6 Exercises . . . 653

9 Timed Automata **663**
9.1 Timed Automata . . . 667
9.1.1 Semantics . . . 674
9.1.2 Time Divergence, Timelock, and Zenoness . . . 680
9.2 Timed Computation Tree Logic . . . 688
9.3 TCTL Model Checking . . . 695
9.3.1 Eliminating Timing Parameters . . . 696
9.3.2 Region Transition Systems . . . 698
9.3.3 The TCTL Model-Checking Algorithm . . . 722
9.4 Summary . . . 727

9.5 Bibliographic Notes . . . 728
9.6 Exercises . . . 730

10 Probabilistic Systems **735**
10.1 Markov Chains . . . 737
10.1.1 Reachability Probabilities . . . 749
10.1.2 Qualitative Properties . . . 760
10.2 Probabilistic Computation Tree Logic . . . 769
10.2.1 PCTL Model Checking . . . 774
10.2.2 The Qualitative Fragment of PCTL . . . 777
10.3 Linear-Time Properties . . . 785
10.4 PCTL* and Probabilistic Bisimulation . . . 794
10.4.1 PCTL* . . . 795
10.4.2 Probabilistic Bisimulation . . . 797
10.5 Markov Chains with Costs . . . 805
10.5.1 Cost-Bounded Reachability . . . 807
10.5.2 Long-Run Properties . . . 816
10.6 Markov Decision Processes . . . 821
10.6.1 Reachability Probabilities . . . 839
10.6.2 PCTL Model Checking . . . 854
10.6.3 Limiting Properties . . . 857
10.6.4 Linear-Time Properties and PCTL* . . . 868
10.6.5 Fairness . . . 871
10.7 Summary . . . 882
10.8 Bibliographic Notes . . . 884
10.9 Exercises . . . 887

A Preliminaries **897**
A.1 Frequently Used Symbols and Notations . . . 897
A.2 Formal Languages . . . 900
A.3 Propositional Logic . . . 903
A.4 Graphs . . . 908
A.5 Computational Complexity . . . 913

Bibliography **919**

Index **953**