

# Contents

<b>Foreword</b>	<b>xiii</b>
<b>Preface</b>	<b>xv</b>
<b>1 System Verification</b>	<b>1</b>
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
<b>2 Modelling Concurrent Systems</b>	<b>19</b>
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 . . . . .	36
2.2.2 Communication via Shared Variables . . . . .	39
2.2.3 Handshaking . . . . .	47
2.2.4 Channel Systems . . . . .	53
2.2.5 NanoPromela . . . . .	63
2.2.6 Synchronous Parallelism . . . . .	75
2.3 The State-Space Explosion Problem . . . . .	77
2.4 Summary . . . . .	80
2.5 Bibliographic Notes . . . . .	80
2.6 Exercises . . . . .	82
<b>3 Linear-Time Properties</b>	<b>89</b>
3.1 Deadlock . . . . .	89
3.2 Linear-Time Behavior . . . . .	94
3.2.1 Paths and State Graph . . . . .	95
3.2.2 Traces . . . . .	97
3.2.3 Linear-Time Properties . . . . .	100

3.2.4	Trace Equivalence and Linear-Time Properties . . . . .	104
3.3	Safety Properties and Invariants . . . . .	107
3.3.1	Invariants . . . . .	107
3.3.2	Safety Properties . . . . .	111
3.3.3	Trace Equivalence and Safety Properties . . . . .	116
3.4	Liveness Properties . . . . .	120
3.4.1	Liveness Properties . . . . .	121
3.4.2	Safety vs. Liveness Properties . . . . .	122
3.5	Fairness . . . . .	126
3.5.1	Fairness Constraints . . . . .	129
3.5.2	Fairness Strategies . . . . .	137
3.5.3	Fairness and Safety . . . . .	139
3.6	Summary . . . . .	141
3.7	Bibliographic Notes . . . . .	143
3.8	Exercises . . . . .	144
<b>4</b>	<b>Regular Properties</b> . . . . .	<b>151</b>
4.1	Automata on Finite Words . . . . .	151
4.2	Model-Checking Regular Safety Properties . . . . .	159
4.2.1	Regular Safety Properties . . . . .	159
4.2.2	Verifying Regular Safety Properties . . . . .	163
4.3	Automata on Infinite Words . . . . .	170
4.3.1	$\omega$ -Regular Languages and Properties . . . . .	170
4.3.2	Nondeterministic Büchi Automata . . . . .	173
4.3.3	Deterministic Büchi Automata . . . . .	188
4.3.4	Generalized Büchi Automata . . . . .	192
4.4	Model-Checking $\omega$ -Regular Properties . . . . .	198
4.4.1	Persistence Properties and Product . . . . .	199
4.4.2	Nested Depth-First Search . . . . .	203
4.5	Summary . . . . .	217
4.6	Bibliographic Notes . . . . .	218
4.7	Exercises . . . . .	219
<b>5</b>	<b>Linear Temporal Logic</b> . . . . .	<b>229</b>
5.1	Linear Temporal Logic . . . . .	229
5.1.1	Syntax . . . . .	231
5.1.2	Semantics . . . . .	235
5.1.3	Specifying Properties . . . . .	239
5.1.4	Equivalence of LTL Formulae . . . . .	247
5.1.5	Weak Until, Release, and Positive Normal Form . . . . .	252
5.1.6	Fairness in LTL . . . . .	257
5.2	Automata-Based LTL Model Checking . . . . .	270

5.2.1	Complexity of the LTL Model-Checking Problem . . . . .	287
5.2.2	LTL Satisfiability and Validity Checking . . . . .	296
5.3	Summary . . . . .	298
5.4	Bibliographic Notes . . . . .	299
5.5	Exercises . . . . .	300
<b>6</b>	<b>Computation Tree Logic</b>	<b>313</b>
6.1	Introduction . . . . .	313
6.2	Computation Tree Logic . . . . .	317
6.2.1	Syntax . . . . .	317
6.2.2	Semantics . . . . .	320
6.2.3	Equivalence of CTL Formulae . . . . .	329
6.2.4	Normal Forms for CTL . . . . .	332
6.3	Expressiveness of CTL vs. LTL . . . . .	334
6.4	CTL Model Checking . . . . .	341
6.4.1	Basic Algorithm . . . . .	341
6.4.2	The Until and Existential Always Operator . . . . .	347
6.4.3	Time and Space Complexity . . . . .	355
6.5	Fairness in CTL . . . . .	358
6.6	Counterexamples and Witnesses . . . . .	373
6.6.1	Counterexamples in CTL . . . . .	376
6.6.2	Counterexamples and Witnesses in CTL with Fairness . . . . .	380
6.7	Symbolic CTL Model Checking . . . . .	381
6.7.1	Switching Functions . . . . .	382
6.7.2	Encoding Transition Systems by Switching Functions . . . . .	386
6.7.3	Ordered Binary Decision Diagrams . . . . .	392
6.7.4	Implementation of ROBDD-Based Algorithms . . . . .	407
6.8	CTL* . . . . .	422
6.8.1	Logic, Expressiveness, and Equivalence . . . . .	422
6.8.2	CTL* Model Checking . . . . .	427
6.9	Summary . . . . .	430
6.10	Bibliographic Notes . . . . .	431
6.11	Exercises . . . . .	433
<b>7</b>	<b>Equivalences and Abstraction</b>	<b>449</b>
7.1	Bisimulation . . . . .	451
7.1.1	Bisimulation Quotient . . . . .	456
7.1.2	Action-Based Bisimulation . . . . .	465
7.2	Bisimulation and CTL* Equivalence . . . . .	468
7.3	Bisimulation-Quotienting Algorithms . . . . .	476
7.3.1	Determining the Initial Partition . . . . .	478
7.3.2	Refining Partitions . . . . .	480

7.3.3	A First Partition Refinement Algorithm . . . . .	486
7.3.4	An Efficiency Improvement . . . . .	487
7.3.5	Equivalence Checking of Transition Systems . . . . .	493
7.4	Simulation Relations . . . . .	496
7.4.1	Simulation Equivalence . . . . .	505
7.4.2	Bisimulation, Simulation, and Trace Equivalence . . . . .	510
7.5	Simulation and $\forall\text{CTL}^*$ Equivalence . . . . .	515
7.6	Simulation-Quotienting Algorithms . . . . .	521
7.7	Stutter Linear-Time Relations . . . . .	529
7.7.1	Stutter Trace Equivalence . . . . .	530
7.7.2	Stutter Trace and $\text{LTL}_{\setminus\circ}$ Equivalence . . . . .	534
7.8	Stutter Bisimulation . . . . .	536
7.8.1	Divergence-Sensitive Stutter Bisimulation . . . . .	543
7.8.2	Normed Bisimulation . . . . .	552
7.8.3	Stutter Bisimulation and $\text{CTL}_{\setminus\circ}^*$ Equivalence . . . . .	560
7.8.4	Stutter Bisimulation Quotienting . . . . .	567
7.9	Summary . . . . .	579
7.10	Bibliographic Notes . . . . .	580
7.11	Exercises . . . . .	582
<b>8</b>	<b>Partial Order Reduction</b> . . . . .	<b>595</b>
8.1	Independence of Actions . . . . .	598
8.2	The Linear-Time Ample Set Approach . . . . .	605
8.2.1	Ample Set Constraints . . . . .	606
8.2.2	Dynamic Partial Order Reduction . . . . .	619
8.2.3	Computing Ample Sets . . . . .	627
8.2.4	Static Partial Order Reduction . . . . .	635
8.3	The Branching-Time Ample Set Approach . . . . .	650
8.4	Summary . . . . .	661
8.5	Bibliographic Notes . . . . .	661
8.6	Exercises . . . . .	663
<b>9</b>	<b>Timed Automata</b> . . . . .	<b>673</b>
9.1	Timed Automata . . . . .	677
9.1.1	Semantics . . . . .	684
9.1.2	Time Divergence, Timelock, and Zenoness . . . . .	690
9.2	Timed Computation Tree Logic . . . . .	698
9.3	TCTL Model Checking . . . . .	705
9.3.1	Eliminating Timing Parameters . . . . .	706
9.3.2	Region Transition Systems . . . . .	709
9.3.3	The TCTL Model-Checking Algorithm . . . . .	732
9.4	Summary . . . . .	738

9.5	Bibliographic Notes . . . . .	739
9.6	Exercises . . . . .	740
<b>10</b>	<b>Probabilistic Systems</b>	<b>745</b>
10.1	Markov Chains . . . . .	747
10.1.1	Reachability Probabilities . . . . .	759
10.1.2	Qualitative Properties . . . . .	770
10.2	Probabilistic Computation Tree Logic . . . . .	780
10.2.1	PCTL Model Checking . . . . .	785
10.2.2	The Qualitative Fragment of PCTL . . . . .	787
10.3	Linear-Time Properties . . . . .	796
10.4	PCTL* and Probabilistic Bisimulation . . . . .	806
10.4.1	PCTL* . . . . .	806
10.4.2	Probabilistic Bisimulation . . . . .	808
10.5	Markov Chains with Costs . . . . .	816
10.5.1	Cost-Bounded Reachability . . . . .	818
10.5.2	Long-Run Properties . . . . .	827
10.6	Markov Decision Processes . . . . .	832
10.6.1	Reachability Probabilities . . . . .	851
10.6.2	PCTL Model Checking . . . . .	866
10.6.3	Limiting Properties . . . . .	869
10.6.4	Linear-Time Properties and PCTL* . . . . .	880
10.6.5	Fairness . . . . .	883
10.7	Summary . . . . .	894
10.8	Bibliographic Notes . . . . .	896
10.9	Exercises . . . . .	899
<b>A</b>	<b>Appendix: Preliminaries</b>	<b>909</b>
A.1	Frequently Used Symbols and Notations . . . . .	909
A.2	Formal Languages . . . . .	912
A.3	Propositional Logic . . . . .	915
A.4	Graphs . . . . .	920
A.5	Computational Complexity . . . . .	925
	<b>Bibliography</b>	<b>931</b>
	<b>Index</b>	<b>965</b>