

Contents

List of Figures	xiii
Foreword	xix
1 Introduction to the Second Edition	1
2 Introduction to the First Edition	3
2.1 The Need for Formal Methods	3
2.2 Hardware and Software Verification	4
2.3 The Process of Model Checking	6
2.4 Temporal Logic and Model Checking	6
2.5 Symbolic Algorithms	8
2.6 Partial Order Reduction	10
2.7 Other Approaches to the State Explosion Problem	11
3 Modeling Systems	15
3.1 Transition Systems and Kripke Structures	16
3.2 Nondeterminism and Inputs	17
3.3 First-Order Logic and Symbolic Representations	18
3.4 Boolean Encoding	22
3.5 Modeling Digital Circuits	23
3.6 Modeling Programs	26
3.7 Fairness	33
4 Temporal Logic	37
4.1 The Computation Tree Logic CTL*	37
4.2 Syntax and Semantics of CTL*	39
4.3 Temporal Logics Based on CTL*	43
4.4 Temporal Logic with Set Atomic Propositions and Set Semantics	47

4.5	Fairness	47
4.6	Counterexamples	48
4.7	Safety and Liveness Properties	50
5	CTL Model Checking	53
5.1	Explicit-State CTL Model Checking	53
5.2	Model-Checking CTL with Fairness Constraints	58
5.3	CTL Model Checking via Fixpoint Computation	60
6	LTL and CTL* Model Checking	71
6.1	The Tableau Construction	72
6.2	LTL Model Checking with Tableau	74
6.3	Correctness Proof of the Tableau Construction	76
6.4	CTL* Model Checking	80
7	Automata on Infinite Words and LTL Model Checking	85
7.1	Finite Automata on Finite Words	85
7.2	Automata on Infinite Words	87
7.3	Deterministic versus Nondeterministic Büchi Automata	88
7.4	Intersection of Büchi Automata	89
7.5	Checking Emptiness	91
7.6	Generalized Büchi Automata	95
7.7	Automata and Kripke Structures	96
7.8	Model Checking using Automata	97
7.9	From LTL to Büchi Automata	98
7.10	Efficient Translation of LTL into Automata	100
7.11	On-the-Fly Model Checking	108
8	Binary Decision Diagrams and Symbolic Model Checking	113
8.1	Representing Boolean Formulas	113
8.2	Representing Kripke Structures with OBDDs	119
8.3	Symbolic Model Checking for CTL	121
8.4	Fairness in Symbolic Model Checking	124
8.5	Counterexamples and Witnesses	125
8.6	Relational Product Computations	128
9	Propositional Satisfiability	137
9.1	Conjunctive Normal Form	137
9.2	Encoding Propositional Logic into CNF	139
9.3	Propositional Satisfiability using Binary Search	140

9.4	Boolean Constraint Propagation (BCP)	144
9.5	Conflict-Driven Clause Learning	145
9.6	Decision Heuristics	148
10	SAT-Based Model Checking	153
10.1	Bounded Model Checking	153
10.2	Verifying Reachability Properties with k -Induction	161
10.3	Model Checking with Inductive Invariants	164
10.4	Model Checking with Craig Interpolants	165
10.5	Property-Directed Reachability	170
11	Equivalences and Preorders between Structures	177
11.1	Bisimulation Equivalence	177
11.2	Fair Bisimulation	182
11.3	Preorders between Structures	182
11.4	Games for Bisimulation and Simulation	185
11.5	Equivalence and Preorder Algorithms	186
12	Partial Order Reduction	189
12.1	Concurrency in Asynchronous Systems	190
12.2	Independence and Invisibility	192
12.3	Partial Order Reduction for LTL_{-X}	195
12.4	An Example	199
12.5	Calculating Ample Sets	202
12.6	Correctness of the Algorithm	207
12.7	Partial Order Reduction in SPIN	211
13	Abstraction	219
13.1	Existential Abstraction	220
13.2	Computation of Abstract Models	226
13.3	Counterexample-Guided Abstraction Refinement (CEGAR)	231
14	Software Model Checking	241
14.1	Representing Programs as Control-Flow Graphs	241
14.2	Checking Assertions using Symbolic Execution	242
14.3	Program Verification with Predicate Abstraction	244
14.4	A Full Example	248
15	Verification with Automata Learning	257
15.1	Angluin's L^* Learning Algorithm	257

15.2	Compositional Reasoning	260
15.3	Assume-Guarantee Reasoning for Communicating Components	262
15.4	Black Box Checking	270
16	Model Checking for the μ-Calculus	277
16.1	Introduction	277
16.2	The Propositional μ -Calculus	277
16.3	Evaluating Fixpoint Formulas	281
16.4	Representing μ -Calculus Formulas using OBDDs	284
16.5	Translating CTL into the μ -Calculus	287
17	Symmetry	291
17.1	Groups and Symmetry	291
17.2	Quotient Models	294
17.3	Model Checking with Symmetry	297
17.4	Complexity Issues	299
17.5	Empirical Results	303
18	Infinite Families of Finite-State Systems	307
18.1	Temporal Logic for Infinite Families	307
18.2	Invariants	308
18.3	Futurebus+ Example Reconsidered	310
18.4	Graph and Network Grammars	313
18.5	Undecidability Result for a Family of Token Rings	323
19	Discrete Real-Time and Quantitative Temporal Analysis	329
19.1	Real-Time Systems and Rate-Monotonic Scheduling	329
19.2	Model-Checking Real-Time Systems	330
19.3	RTCTL Model Checking	331
19.4	Quantitative Temporal Analysis: Minimum/Maximum Delay	332
19.5	Example: An Aircraft Controller	335
20	Continuous Real Time	341
20.1	Timed Automata	342
20.2	Parallel Composition	344
20.3	Modeling with Timed Automata	345
20.4	Clock Regions	346
20.5	Clock Zones	354
20.6	Difference-Bound Matrices	360
20.7	Complexity Considerations	364

Bibliography	367
Index	399