Contents

	Foreword by Amir Pnueli	xi
	Preface	xiii
1	**Introduction**	1
1.1	The Need for Formal Methods	1
1.2	Hardware and Software Verification	2
1.3	The Process of Model Checking	4
1.4	Temporal Logic and Model Checking	4
1.5	Symbolic Algorithms	6
1.6	Partial Order Reduction	8
1.7	Other Approaches to the State Explosion Problem	10
2	**Modeling Systems**	13
2.1	Modeling Concurrent Systems	14
2.2	Concurrent Systems	17
2.3	Example of Program Translation	24
3	**Temporal Logics**	27
3.1	The Computation Tree Logic CTL*	27
3.2	CTL and LTL	30
3.3	Fairness	32
4	**Model Checking**	35
4.1	CTL Model Checking	35
4.2	LTL Model Checking by Tableau	41
4.3	CTL* Model Checking	46
5	**Binary Decision Diagram**	51
5.1	Representing Boolean Formulas	51
5.2	Representing Kripke Structures	57
6	**Symbolic Model Checking**	61
6.1	Fixpoint Representations	61
6.2	Symbolic Model Checking for CTL	66
6.3	Fairness in Symbolic Model Checking	68
6.4	Counterexamples and Witnesses	71
6.5	An ALU Example	75
6.6	Relational Product Computations	77
6.7	Symbolic LTL Model Checking	87

7	**Model Checking for the μ-Calculus**	97
	7.1 Introduction	97
	7.2 The Propositional μ-Calculus	98
	7.3 Evaluating Fixpoint Formulas	101
	7.4 Representing μ-Calculus Formulas Using OBDDs	104
	7.5 Translating CTL into the μ-Calculus	107
	7.6 Complexity Considerations	108
8	**Model Checking in Practice**	109
	8.1 The SMV Model Checker	109
	8.2 A Realistic Example	112
9	**Model Checking and Automata Theory**	121
	9.1 Automata on Finite and Infinite Words	121
	9.2 Model Checking Using Automata	123
	9.3 Checking Emptiness	129
	9.4 Translating LTL into Automata	132
	9.5 On-the-Fly Model Checking	138
	9.6 Checking Language Containment Symbolically	139
10	**Partial Order Reduction**	141
	10.1 Concurrency in Asynchronous Systems	142
	10.2 Independence and Invisibility	144
	10.3 Partial Order Reduction for LTL_{-X}	147
	10.4 An Example	151
	10.5 Calculating Ample Sets	154
	10.6 Correctness of the Algorithm	160
	10.7 Partial Order Reduction in SPIN	164
11	**Equivalences and Preorders between Structures**	171
	11.1 Equivalence and Preorder Algorithms	178
	11.2 Tableau Construction	180
12	**Compositional Reasoning**	185
	12.1 Composition of Structures	187
	12.2 Justifying Assume-Guarantee Proofs	189
	12.3 Verifying a CPU Controller	190

13 Abstraction 193
13.1 Cone of Influence Reduction 193
13.2 Data Abstraction 195

14 Symmetry 215
14.1 Groups and Symmetry 215
14.2 Quotient Models 218
14.3 Model Checking with Symmetry 221
14.4 Complexity Issues 224
14.5 Empirical Results 228

15 Infinite Families of Finite-State Systems 231
15.1 Temporal Logic for Infinite Families 231
15.2 Invariants 232
15.3 Futurebus+ Example Reconsidered 235
15.4 Graph and Network Grammars 238
15.5 Undecidability Result for a Family of Token Rings 248

16 Discrete Real-Time and Quantitative Temporal Analysis 253
16.1 Real-Time Systems and Rate-Monotonic Scheduling 253
16.2 Model Checking Real-Time Systems 254
16.3 RTCTL Model Checking 255
16.4 Quantitative Temporal Analysis: Minimum/Maximum Delay 256
16.5 Example: An Aircraft Controller 259

17 Continuous Real Time 265
17.1 Timed Automata 265
17.2 Parallel Composition 268
17.3 Modeling with Timed Automata 269
17.4 Clock Regions 274
17.5 Clock Zones 280
17.6 Difference Bound Matrices 287
17.7 Complexity Considerations 291

18 Conclusion 293

References 297
Index 309