

# Contents

<b>1</b>	<b>Introduction to Model Checking</b> . . . . .	1
	Edmund M. Clarke, Thomas A. Henzinger, and Helmut Veith	
1.1	The Case for Computer-Aided Verification . . . . .	1
1.2	Temporal-Logic Model Checking in a Nutshell . . . . .	6
1.3	A Very Brief Guide Through the Chapters of the Handbook . . . . .	13
1.4	The Future of Model Checking . . . . .	19
	References . . . . .	22
<b>2</b>	<b>Temporal Logic and Fair Discrete Systems</b> . . . . .	27
	Nir Piterman and Amir Pnueli	
2.1	Introduction . . . . .	28
2.2	Fair Discrete Systems . . . . .	29
2.3	Linear Temporal Logic . . . . .	41
2.4	Computation Tree Logic . . . . .	52
2.5	Examples for LTL and CTL . . . . .	59
2.6	CTL* . . . . .	63
	References . . . . .	70
<b>3</b>	<b>Modeling for Verification</b> . . . . .	75
	Sanjit A. Seshia, Natasha Sharygina, and Stavros Tripakis	
3.1	Introduction . . . . .	75
3.2	Major Considerations in System Modeling . . . . .	77
3.3	Modeling Basics . . . . .	86
3.4	Examples . . . . .	89
3.5	Kripke Structures . . . . .	100
3.6	Summary . . . . .	103
	References . . . . .	103
<b>4</b>	<b>Automata Theory and Model Checking</b> . . . . .	107
	Orna Kupferman	
4.1	Introduction . . . . .	107
4.2	Nondeterministic Büchi Automata on Infinite Words . . . . .	108

4.3	Additional Acceptance Conditions . . . . .	122
4.4	Decision Procedures . . . . .	132
4.5	Alternating Automata on Infinite Words . . . . .	135
4.6	Automata-Based Algorithms . . . . .	141
	References . . . . .	148
<b>5</b>	<b>Explicit-State Model Checking . . . . .</b>	<b>153</b>
	Gerard J. Holzmann	
5.1	Introduction . . . . .	153
5.2	Basic Search Algorithms . . . . .	155
5.3	Linear Temporal Logic . . . . .	158
5.4	Omega Automata . . . . .	158
5.5	Nested Depth-First Search . . . . .	160
5.6	Abstraction . . . . .	162
5.7	Model-Driven Verification . . . . .	167
5.8	Incomplete Storage . . . . .	168
5.9	Extensions . . . . .	169
5.10	Synopsis . . . . .	170
	References . . . . .	170
<b>6</b>	<b>Partial-Order Reduction . . . . .</b>	<b>173</b>
	Doron Peled	
6.1	Introduction . . . . .	173
6.2	Partial Order Reduction . . . . .	174
6.3	Reducing Edges While Preserving States . . . . .	182
6.4	Conclusions . . . . .	188
	References . . . . .	188
<b>7</b>	<b>Binary Decision Diagrams . . . . .</b>	<b>191</b>
	Randal E. Bryant	
7.1	Introduction . . . . .	191
7.2	Terminology . . . . .	192
7.3	A Boolean Function API . . . . .	193
7.4	OBDD Representation . . . . .	195
7.5	Implementing OBDD Operations . . . . .	197
7.6	Implementation Techniques . . . . .	200
7.7	Variable Ordering and Reordering . . . . .	202
7.8	Variant Representations . . . . .	203
7.9	Representing Non-Boolean Functions . . . . .	206
7.10	Scaling OBDD Capacity . . . . .	210
7.11	Concluding Remarks . . . . .	213
	References . . . . .	214
<b>8</b>	<b>BDD-Based Symbolic Model Checking . . . . .</b>	<b>219</b>
	Sagar Chaki and Arie Gurfinkel	
8.1	Introduction . . . . .	219
8.2	Preliminaries . . . . .	220

8.3	Binary Decision Diagrams: The Basics . . . . .	222
8.4	Model Checking Kripke Structures . . . . .	230
8.5	Push-Down Symbolic Model Checking . . . . .	238
8.6	Conclusion . . . . .	243
	References . . . . .	244
<b>9</b>	<b>Propositional SAT Solving . . . . .</b>	<b>247</b>
	Joao Marques-Silva and Sharad Malik	
9.1	Introduction . . . . .	247
9.2	Preliminaries . . . . .	249
9.3	CDCL SAT Solvers: Organization . . . . .	252
9.4	CDCL SAT Solvers . . . . .	253
9.5	SAT-Based Problem Solving . . . . .	264
9.6	Research Directions . . . . .	269
	References . . . . .	269
<b>10</b>	<b>SAT-Based Model Checking . . . . .</b>	<b>277</b>
	Armin Biere and Daniel Kröning	
10.1	Introduction . . . . .	277
10.2	Bounded Model Checking on Kripke Structures . . . . .	278
10.3	Bounded Model Checking for Hardware Designs . . . . .	281
10.4	Bounded Model Checking for Software . . . . .	283
10.5	Encodings into Propositional SAT . . . . .	287
10.6	Complete Model Checking with SAT . . . . .	289
10.7	Abstraction Techniques Using SAT . . . . .	292
10.8	Outlook and Conclusions . . . . .	295
	References . . . . .	295
<b>11</b>	<b>Satisfiability Modulo Theories . . . . .</b>	<b>305</b>
	Clark Barrett and Cesare Tinelli	
11.1	Introduction . . . . .	305
11.2	SMT in Model Checking . . . . .	310
11.3	The Lazy Approach to SMT . . . . .	312
11.4	Theory Solvers for Specific Theories . . . . .	317
11.5	Combining Theory Solvers . . . . .	324
11.6	SMT Solving Extensions and Enhancements . . . . .	327
11.7	Eager Encodings to SAT . . . . .	330
11.8	Additional Functionalities of SMT Solvers . . . . .	332
	References . . . . .	335
<b>12</b>	<b>Compositional Reasoning . . . . .</b>	<b>345</b>
	Dimitra Giannakopoulou, Kedar S. Namjoshi, and Corina S. Păsăreanu	
12.1	Introduction . . . . .	345
12.2	Reasoning with Assertions . . . . .	348
12.3	Automata-Based Assume-Guarantee Reasoning . . . . .	362
12.4	Related Approaches . . . . .	375
12.5	Conclusion . . . . .	378
	References . . . . .	378

<b>13</b>	<b>Abstraction and Abstraction Refinement</b> . . . . .	385
	Dennis Dams and Orna Grumberg	
13.1	Introduction . . . . .	385
13.2	Preliminaries . . . . .	387
13.3	Simulation and Bisimulation Relations . . . . .	394
13.4	Abstraction Based on Simulation . . . . .	399
13.5	CounterExample-Guided Abstraction Refinement (CEGAR) . . . . .	402
13.6	Abstraction Based on Modal Simulation . . . . .	406
13.7	Completeness . . . . .	412
	References . . . . .	414
<b>14</b>	<b>Interpolation and Model Checking</b> . . . . .	421
	Kenneth L. McMillan	
14.1	Introduction . . . . .	421
14.2	Preliminaries . . . . .	423
14.3	Model of Abstraction Refinement . . . . .	424
14.4	Refinement, Local Proofs, and Interpolants . . . . .	428
14.5	Refiners as Local Proof Systems . . . . .	434
14.6	Abstractors as Proof Generalizers . . . . .	441
14.7	Summary . . . . .	443
	References . . . . .	444
<b>15</b>	<b>Predicate Abstraction for Program Verification</b> . . . . .	447
	Ranjit Jhala, Andreas Podelski, and Andrey Rybalchenko	
15.1	Introduction . . . . .	447
15.2	Definitions . . . . .	448
15.3	Characterizing Correctness via Reachability . . . . .	452
15.4	Characterizing Correctness via Inductiveness . . . . .	454
15.5	Abstraction . . . . .	459
15.6	Abstraction Refinement . . . . .	471
15.7	Solving Refinement Constraints for Predicate Abstraction . . . . .	481
15.8	Tools . . . . .	486
15.9	Conclusion . . . . .	487
	References . . . . .	487
<b>16</b>	<b>Combining Model Checking and Data-Flow Analysis</b> . . . . .	493
	Dirk Beyer, Sumit Gulwani, and David A. Schmidt	
16.1	Introduction . . . . .	494
16.2	General Considerations . . . . .	494
16.3	Unifying Formal Framework/Comparison of Algorithms . . . . .	501
16.4	Classic Examples (Component Analyses) . . . . .	511
16.5	Combination Examples (Composite Analyses) . . . . .	520
16.6	Algorithms for Constructing Program Invariants . . . . .	525
16.7	Combinations in Tool Implementations . . . . .	532
16.8	Conclusion . . . . .	532
	References . . . . .	534

<b>17</b>	<b>Model Checking Procedural Programs</b> . . . . .	541
	Rajeev Alur, Ahmed Bouajjani, and Javier Esparza	
17.1	Introduction . . . . .	541
17.2	Models of Procedural Programs . . . . .	543
17.3	Basic Verification Algorithms . . . . .	547
17.4	Specifying Requirements . . . . .	556
17.5	Bibliographical Remarks . . . . .	566
	References . . . . .	569
<b>18</b>	<b>Model Checking Concurrent Programs</b> . . . . .	573
	Aarti Gupta, Vineet Kahlon, Shaz Qadeer, and Tayssir Touili	
18.1	Introduction . . . . .	574
18.2	Concurrent System Model and Notation . . . . .	576
18.3	PDS-Based Model Checking: Synchronization Patterns . . . . .	580
18.4	PDS-Based Model-Checking: Communication Patterns . . . . .	595
18.5	Other Models: Finite State Systems and Sequential Programs . . . . .	602
	References . . . . .	607
<b>19</b>	<b>Combining Model Checking and Testing</b> . . . . .	613
	Patrice Godefroid and Koushik Sen	
19.1	Introduction . . . . .	613
19.2	Systematic Testing of Concurrent Software . . . . .	615
19.3	Systematic Testing of Sequential Software . . . . .	624
19.4	Systematic Testing of Concurrent Software with Data Inputs . . . . .	633
19.5	Other Related Work . . . . .	637
19.6	Conclusion . . . . .	640
	References . . . . .	640
<b>20</b>	<b>Combining Model Checking and Deduction</b> . . . . .	651
	Natarajan Shankar	
20.1	Introduction . . . . .	651
20.2	Logic Background . . . . .	656
20.3	Deduction and Model Checking . . . . .	670
20.4	Conclusions . . . . .	680
	References . . . . .	680
<b>21</b>	<b>Model Checking Parameterized Systems</b> . . . . .	685
	Parosh Aziz Abdulla, A. Prasad Sistla, and Muralidhar Talupur	
21.1	Introduction . . . . .	685
21.2	Petri Nets . . . . .	687
21.3	Regular Model Checking . . . . .	695
21.4	Monotonic Abstraction . . . . .	703
21.5	Compositional Reasoning for Parameterized Verification . . . . .	709
21.6	Related Work . . . . .	719
	References . . . . .	721

<b>22</b>	<b>Model Checking Security Protocols</b> . . . . .	727
	David Basin, Cas Cremers, and Catherine Meadows	
22.1	Introduction . . . . .	727
22.2	History . . . . .	731
22.3	Formal Model . . . . .	733
22.4	Issues in Developing Model-Checking Algorithms for Security Protocols . . . . .	741
22.5	Systems and Algorithms . . . . .	748
22.6	Research Problems . . . . .	753
22.7	Conclusions . . . . .	757
	References . . . . .	758
<b>23</b>	<b>Transfer of Model Checking to Industrial Practice</b> . . . . .	763
	Robert P. Kurshan	
23.1	Introduction . . . . .	763
23.2	The Technology Transfer Problem . . . . .	767
23.3	False Starts . . . . .	776
23.4	A Framework for Technology Transfer . . . . .	779
23.5	Formal Functional Verification in Commercial Use Today . . . . .	782
23.6	Algorithms . . . . .	786
23.7	Future . . . . .	788
23.8	Conclusion . . . . .	789
	References . . . . .	790
<b>24</b>	<b>Functional Specification of Hardware via Temporal Logic</b> . . . . .	795
	Cindy Eisner and Dana Fisman	
24.1	Introduction . . . . .	795
24.2	From LTL to Regular-Expression-Based Temporal Logic . . . . .	797
24.3	Clocks and Sampling . . . . .	805
24.4	Hardware Resets and Other Sources of Truncated Paths . . . . .	809
24.5	The Simple Subset . . . . .	817
24.6	Quantified and Local Variables . . . . .	818
24.7	Summary and Open Issues . . . . .	823
	References . . . . .	825
<b>25</b>	<b>Symbolic Trajectory Evaluation</b> . . . . .	831
	Tom Melham	
25.1	Introduction . . . . .	831
25.2	Notational Preliminaries . . . . .	833
25.3	Sequential Circuit Models in STE . . . . .	834
25.4	Trajectory Evaluation Logic . . . . .	838
25.5	The Fundamental Theorem of Trajectory Evaluation . . . . .	843
25.6	STE Model Checking . . . . .	844
25.7	Abstraction and Symbolic Indexing . . . . .	852
25.8	Compositional Reasoning . . . . .	857
25.9	GSTE and Other Extensions . . . . .	862

25.10	Summary and Prospects . . . . .	865
	References . . . . .	867
<b>26</b>	<b>The mu-calculus and Model Checking . . . . .</b>	<b>871</b>
	Julian Bradfield and Igor Walukiewicz	
26.1	Introduction . . . . .	871
26.2	Basics . . . . .	872
26.3	Fundamental Properties . . . . .	890
26.4	Relations with Other Logics . . . . .	904
26.5	Related Work . . . . .	912
	References . . . . .	914
<b>27</b>	<b>Graph Games and Reactive Synthesis . . . . .</b>	<b>921</b>
	Roderick Bloem, Krishnendu Chatterjee, and Barbara Jobstmann	
27.1	Introduction . . . . .	921
27.2	Theory of Graph-Based Games . . . . .	923
27.3	Reactive Synthesis . . . . .	936
27.4	Related Topics . . . . .	953
	References . . . . .	954
<b>28</b>	<b>Model Checking Probabilistic Systems . . . . .</b>	<b>963</b>
	Christel Baier, Luca de Alfaro, Vojtěch Forejt, and Marta Kwiatkowska	
28.1	Introduction . . . . .	964
28.2	Modelling Probabilistic Concurrent Systems . . . . .	966
28.3	Probabilistic Computation Tree Logic . . . . .	975
28.4	Model-Checking Algorithms for MDPs and PCTL . . . . .	980
28.5	Linear Temporal Logic . . . . .	985
28.6	Model-Checking Algorithms for MDPs and LTL . . . . .	987
28.7	Tools, Applications and Model Construction . . . . .	990
28.8	Extensions of the Model and Specification Notations . . . . .	992
28.9	Conclusion . . . . .	993
	References . . . . .	993
<b>29</b>	<b>Model Checking Real-Time Systems . . . . .</b>	<b>1001</b>
	Patricia Bouyer, Uli Fahrenberg, Kim Guldstrand Larsen, Nicolas Markey, Joël Ouaknine, and James Worrell	
29.1	Introduction . . . . .	1001
29.2	Timed Automata . . . . .	1003
29.3	Checking Reachability . . . . .	1007
29.4	(Bi)simulation Checking . . . . .	1010
29.5	Language-Theoretic Properties . . . . .	1012
29.6	Timed Temporal Logics . . . . .	1018
29.7	Symbolic Algorithms, Data Structures, Tools . . . . .	1023
29.8	Weighted Timed Automata . . . . .	1028
29.9	Timed Games . . . . .	1034
29.10	Ongoing and Future Challenges . . . . .	1037
	References . . . . .	1037

<b>30</b>	<b>Verification of Hybrid Systems</b> . . . . .	1047
	Laurent Doyen, Goran Frehse, George J. Pappas, and André Platzer	
30.1	Introduction . . . . .	1048
30.2	Basic Definitions . . . . .	1049
30.3	Decidability and Undecidability Results . . . . .	1055
30.4	Set-Based Reachability Analysis . . . . .	1058
30.5	Abstraction-Based Verification . . . . .	1075
30.6	Logic-Based Verification . . . . .	1084
30.7	Verification Tools . . . . .	1097
	References . . . . .	1102
<b>31</b>	<b>Symbolic Model Checking in Non-Boolean Domains</b> . . . . .	1111
	Rupak Majumdar and Jean-François Raskin	
31.1	Introduction . . . . .	1111
31.2	Transition Systems and Symbolic Verification . . . . .	1112
31.3	Examples of Symbolic Verification . . . . .	1119
31.4	Games and Symbolic Synthesis . . . . .	1131
31.5	Probabilistic Systems . . . . .	1137
31.6	Conclusion . . . . .	1141
	References . . . . .	1143
<b>32</b>	<b>Process Algebra and Model Checking</b> . . . . .	1149
	Rance Cleaveland, A.W. Roscoe, and Scott A. Smolka	
32.1	Introduction . . . . .	1149
32.2	Foundations . . . . .	1150
32.3	Algorithms and Methodologies . . . . .	1175
32.4	Tools . . . . .	1181
32.5	Case Studies . . . . .	1185
32.6	Conclusions . . . . .	1190
	References . . . . .	1191
	<b>Index</b> . . . . .	1197