Handbook of Model Checking

Edmund M. Clarke • Thomas A. Henzinger •
Helmut Veith • Roderick Bloem
Editors

Handbook of Model Checking

Springer

Editors
Edmund M. Clarke
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA

Helmut Veith
Arbeitsbereich Formal Methods in Systems Engineering
Technische Universität Wien
Wien, Austria

Thomas A. Henzinger
Institute of Science and Technology Austria (IST Austria)
Klosterneuburg, Austria

Roderick Bloem
Institut für angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK)
Technische Universität Graz
Graz, Austria

ISBN 978-3-319-10574-1
ISBN 978-3-319-10575-8 (eBook)
DOI 10.1007/978-3-319-10575-8

Library of Congress Control Number: 2018943403

© Springer International Publishing AG, part of Springer Nature 2018
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

The image on the book cover was designed by Anna Petukhova

Printed on acid-free paper

This Springer imprint is published by the registered company
Springer International Publishing AG part of Springer Nature.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To Helmut

Foreword

With 32 technical articles and 76 authors, this handbook represents a full post-graduate course in Model Checking. If a reader can verify that he or she has read and studied every article, then Springer should certainly award that reader a Master's Degree in Model Checking! Departments in Computer Science everywhere will certainly welcome access to this major resource.

Model Checking has become a major area of research and development both for hardware and software verification owing to many factors. First, the improved speed and capacity of computers in recent times have made all kinds of problem solving both practical and efficient. Moreover, in the area of Model Checking the methods of design of models have contributed to the best formulation of problems. Then we have seen SAT solvers gain unexpected and truly remarkable efficiency improvements—despite theoretical limitations. Additionally, the methodology of Satisfiability Modulo Theories (SMT) has contributed to finding excellent ways to pose and solve problems. Uses of temporal logic and data-flow-analysis techniques have also made model checking more naturally efficient. All these contributions have helped solve the ever-present "state explosion problem." The urgency to make greater strides has increased because new applications in such diverse areas as health care, transportation, security, and robotics require work in the field to achieve greater scale, expressivity, and automation.

I would definitely recommend new Ph.D. candidates look seriously into going into research in this field, because success in Model Checking can directly lead to future success in many other activities in Computer Science.

Finally, the recent tragic loss of Helmut Veith has been a dreadful blow to his family, friends, colleagues, and students. Let's take up the flag in his honor to help promote and expand the field in which he was poised to become a recognized world leader.

Carnegie Mellon University — Dana S. Scott
Department of Mathematics, University of California, Berkeley

Preface

This handbook is intended to give an in-depth description of the many research areas that make up the expanding field of model checking. In 32 chapters, 76 of the world's leading researchers in this domain present a thorough review of the origins, theory, methods, and applications of model checking. The book is meant for researchers and graduate students who are interested in the development of formalisms, algorithms, and software tools for the computer-aided verification of complex systems in general, and of hardware and software systems in particular.

The idea for this handbook originated with Helmut Veith around 2006. It was clear to Helmut that a field as strong and useful as model checking needed a handbook to make its foundations broadly accessible. Helmut was in many ways the soul of this project. His untimely death in March 2016, with the project in its final phase, was a shock to all of us and we greatly miss him. His visionary ideas, his unbelievable energy in bringing these ideas to life, and his wonderful sense of community left a lasting mark, and this book will serve as an enduring memorial to his contributions to the field and the community.

Graz, Klosterneuburg, Pittsburgh
November 2016

Roderick Bloem
Thomas A. Henzinger
Edmund M. Clarke

Acknowledgements

Very special thanks go to Katarina Singer and Sasha Rubin. As project coordinators, they assisted the editors in all managerial, organizational, and technical matters necessary for bringing such a large project to fruition: they managed the collaboration software and the interaction with the authors, reviewers, copy editors, and the publisher throughout much of the project. They kept track of all the loose ends and spent many hours making sure that every chapter got into shape. Jessica Davies and Andrey Kupriyanov performed some of these coordination tasks for shorter periods of time towards the end of the project. Thank you!

We would like to thank Alfred Hofmann of Springer for his support of the project. Ronan Nugent, our editor at Springer, was closely involved in all aspects of the book from the beginning to its completion. He deserves special credit for flexibility, patience, and for keeping an unrelenting trust in the project. We also thank Philip R. Watson, Springer's copy editor, who labored through each and every chapter and found countless mistakes. The copy editing was supported by many volunteers, who proofread individual chapters, integrated changes suggested by Springer, discussed problems with the authors, and helped create the index. The editing team was largely based at IST Austria, TU Graz and TU Vienna and consisted of Guy Avni, Sergiy Bogomolov, Przemysław Daca, Jessica Davies, Masoud Ebrahimi, Thomas Ferrère, Miriam García Soto, Mirco Giacobbe, Vedad Hadzic, Rinat Iusupov, Barbara Jobstmann, Anja Karl, Ayrat Khalimov, Bettina Könighofer, Hui Kong, Igor Konnov, Tomer Kotek, Bernhard Kragl, Jan Křetínský, Orna Kupferman, Andrey Kupriyanov, Alfons Laarman, Kurt Nistelberger, Jan Otop, Leo Prikler, Heinz Riener, Franz Röck, Sasha Rubin, Roopsha Samanta, Moritz Sinn, Ana Sokolova, Thorsten Tarrach, Ursula Urwanisch, and Georg Weissenbacher. Thank you!

A large group of people reviewed all of the chapters, often in great detail. We are grateful to Parosh Aziz Abdulla, Rajeev Alur, Domagoj Babic, Christel Baier, Clark Barrett, David Basin, Jason Baumgartner, Saddek Bensalem, Dietmar Berwanger, Dirk Beyer, Armin Biere, Bernard Boigelot, Marius Bozga, Julian Bradfield, Robert K. Brayton, Tomáš Brázdil, Randal E. Bryant, Pavol Černy, Sagar Chaki, Krishnendu Chatterjee, Swarat Chaudhuri, Wei-Ngan Chin, Hana Chockler,

Alessandro Cimatti, Rance Cleaveland, Cas Cremers, Dennis Dams, Thao Dang, Leonardo de Moura, David Dill, Laurent Doyen, Cezara Drăgoi, Rolf Drechsler, Matt Dwyer, Cindy Eisner, Javier Esparza, Kousha Etessami, Marco Faella, Azadeh Farzan, Bernd Finkbeiner, Alain Finkel, Dana Fisman, Vojtěch Forejt, Goran Frehse, Masahiro Fujita, Sicun Gao, Patrice Godefroid, Ganesh Gopalakrishnan, Erich Grädel, Alex Groce, Radu Grosu, Orna Grumberg, Sumit Gulwani, Aarti Gupta, Arie Gurfinkel, Reiner Hähnle, John Hatcliff, Keijo Heljanko, David Henriques, Holger Hermanns, Kryštof Hoder, Martin Hofmann, Andreas Holzer, Gerard Holzmann, Radu Iosif, Franjo Ivančić, Ranjit Jhala, Barbara Jobstmann, Joost-Pieter Katoen, Shmuel Katz, Stefan Katzenbeisser, Stefan Kiefer, Johannes Kinder, Felix Klaedtke, Igor Konnov, Eric Koskinen, Laura Kovács, Daniel Kroening, Antonín Kučera, Andreas Kuehlmann, Viktor Kunčak, Orna Kupferman, Robert P. Kurshan, Marta Kwiatowska, Shuvendu Lahiri, Yassine Lakhnech, Akash Lal, Salvatore La Torre, Martin Leucker, Rupak Majumdar, Oded Maler, Tiziana Margaria, Nicolas Markey, Joao Marquez-Silva, Wilfredo Marrero, João Martins, Richard Mayr, Catherine Meadows, Tom Melham, Shin-ichi Minato, Marius Minea, David Monniaux, Kedar S. Namjoshi, Dejan Ničković, Joël Ouaknine, Madhusudan Parthasarathy, Corina Păsăreanu, Doron Peled, Ruzica Piskac, André Platzer, Stefano Quer, Jan-David Quesel, Jean-François Raskin, Tom Reps, Sasha Rubin, John Rushby, Andrey Rybalchenko, Mooly Sagiv, Sriram Sankaranarayanan, Christian Schallhart, Sven Schewe, Holger Schlingloff, David A. Schmidt, Philippe Schnoebelen, Stefan Schwoon, Helmut Seidl, Martina Seidl, Koushik Sen, Sanjit A. Seshia, Natarajan Shankar, Natasha Sharygina, Nishant Sinha, Prasad Sistla, Ana Sokolova, Dawn Song, Bernhard Steffen, Wilfried Steiner, Andreas Steininger, Mariëlle Stoelinga, Ofer Strichman, Aaron Stump, Stefan Szeider, Murali Talupur, Wolfgang Thomas, Cesare Tinelli, Ashish Tiwari, Stavros Tripakis, Rachel Tzoref, Viktor Vafeiadis, Allen Van Gelder, Martin Vechev, Thomas Wahl, Igor Walukiewicz, Bow-Yaw Wang, Farn Wang, Georg Weissenbacher, Thomas Wies, Karsten Wolf, Pierre Wolper, Eran Yahav, Karen Yorav, Greta Yorsh, Vladimir Zakharov, and Paolo Zuliani.

The greatest debt of gratitude we owe to the authors, who did the most important job: writing the book. The editors were supported in the initial selection of topics and authors by an advisory board consisting of Rajeev Alur, Armin Biere, Robert K. Brayton, Randal E. Bryant, Rance Cleaveland, Cindy Eisner, Javier Esparza, Orna Grumberg, Aarti Gupta, Pei-Hsin Ho, Gerard Holzmann, Orna Kupferman, Robert P. Kurshan, Kim G. Larsen, Ken McMillan, Doron Peled, Amir Pnueli, Sriram Rajamani, Joseph Sifakis, Prasad Sistla, Scott Smolka, Wolfgang Thomas, and Pierre Wolper. Many of them contributed also to individual chapters. Finally, we thank Dana Scott for writing the Foreword, Andrei Voronkov for letting us use his EasyChair software for the initial writing and reviewing process, and Anna Petukhova for the design of the cover image, which is based on her design for the 2014 Vienna Summer of Logic.

Roderick Bloem
Thomas A. Henzinger
Edmund M. Clarke

Contents

1 Introduction to Model Checking 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

2 Temporal Logic and Fair Discrete Systems 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

3 Modeling for Verification 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

4 Automata Theory and Model Checking 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

5 Explicit-State Model Checking 153
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

6 Partial-Order Reduction 173
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

7 Binary Decision Diagrams 191
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

8 BDD-Based Symbolic Model Checking 219
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

9 Propositional SAT Solving 247
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

10 SAT-Based Model Checking 277
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

11 Satisfiability Modulo Theories 305
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

12 Compositional Reasoning 345
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

13 Abstraction and Abstraction Refinement 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

14 Interpolation and Model Checking 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

15 Predicate Abstraction for Program Verification 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

16 Combining Model Checking and Data-Flow Analysis 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

17 Model Checking Procedural Programs 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

18 Model Checking Concurrent Programs 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

19 Combining Model Checking and Testing 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

20 Combining Model Checking and Deduction 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

21 Model Checking Parameterized Systems 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

22 Model Checking Security Protocols 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

23 Transfer of Model Checking to Industrial Practice 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

24 Functional Specification of Hardware via Temporal Logic 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

25 Symbolic Trajectory Evaluation 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

26 The mu-calculus and Model Checking 871
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

27 Graph Games and Reactive Synthesis 921
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

28 Model Checking Probabilistic Systems 963
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

29 Model Checking Real-Time Systems 1001
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

30 Verification of Hybrid Systems 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

31 Symbolic Model Checking in Non-Boolean Domains 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

32 Process Algebra and Model Checking 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

Index 1197

Contributors

Parosh Aziz Abdulla Uppsala University, Uppsala, Sweden

Rajeev Alur University of Pennsylvania, Philadelphia, PA, USA

Christel Baier Technische Universität Dresden, Dresden, Germany

Clark Barrett Stanford University, Stanford, CA, USA

David Basin ETH Zürich, Zürich, Switzerland

Dirk Beyer Ludwig-Maximilians-Universität München, Munich, Germany

Armin Biere Johannes Kepler University, Linz, Austria

Roderick Bloem Graz University of Technology, Graz, Austria

Ahmed Bouajjani Institut Universitaire de France, Paris Diderot University (Paris 7), Paris, France

Patricia Bouyer LSV, CNRS & ENS Paris-Saclay, Cachan, France

Julian Bradfield University of Edinburgh, Edinburgh, UK

Randal E. Bryant Carnegie Mellon University, Pittsburgh, PA, USA

Sagar Chaki Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA

Krishnendu Chatterjee IST Austria, Klosterneuburg, Austria

Edmund M. Clarke Carnegie Mellon University, Pittsburgh, PA, USA

Rance Cleaveland University of Maryland, College Park, College Park, MD, USA

Cas Cremers University of Oxford, Oxford, UK

Dennis Dams Embedded Systems Innovation by TNO, Eindhoven, The Netherlands

Luca de Alfaro University of California, Santa Cruz, Santa Cruz, CA, USA

Laurent Doyen LSV, CNRS & ENS Paris-Saclay, Cachan, France

Cindy Eisner IBM Research – Haifa, Haifa, Israel

Javier Esparza Technical University of Munich, Munich, Germany

Uli Fahrenberg École Polytechnique, Palaiseau, France

Dana Fisman Ben-Gurion University, Be'er Sheva, Israel

Vojtěch Forejt University of Oxford, Oxford, UK

Goran Frehse Verimag, University Grenoble Alpes, Grenoble, France

Dimitra Giannakopoulou NASA Ames Research Center, Moffett Field, CA, USA

Patrice Godefroid Microsoft Research, Redmond, WA, USA

Orna Grumberg Technion, Israel Institute of Technology, Haifa, Israel

Sumit Gulwani Microsoft Research, Redmond, WA, USA

Aarti Gupta Princeton University, Princeton, NJ, USA

Arie Gurfinkel University of Waterloo, Waterloo, ON, Canada

Thomas A. Henzinger IST Austria, Klosterneuburg, Austria

Gerard J. Holzmann Nimble Research, Monrovia, CA, USA

Ranjit Jhala Jacobs School of Engineering, University of California, San Diego, San Diego, CA, USA

Barbara Jobstmann École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland

Vineet Kahlon Google Inc., New York, NY, USA

Daniel Kröning University of Oxford, Oxford, UK

Orna Kupferman Hebrew University, Jerusalem, Israel

Robert P. Kurshan New York, NY, USA

Marta Kwiatkowska University of Oxford, Oxford, UK

Kim Guldstrand Larsen Aalborg University, Aalborg, Denmark

Rupak Majumdar Max Planck Institute for Software Systems, Kaiserslautern, Germany

Sharad Malik Princeton University, Princeton, NJ, USA

Nicolas Markey LSV, CNRS & ENS Paris-Saclay, Cachan, France; IRISA, CNRS & INRIA & Univ. Rennes 1, Rennes, France

Joao Marques-Silva University of Lisbon, Lisbon, Portugal

Kenneth L. McMillan Microsoft Research, Redmond, WA, USA

Catherine Meadows Naval Research Laboratory, Washington, DC, USA

Tom Melham University of Oxford, Oxford, UK

Kedar S. Namjoshi Bell Labs, Nokia, Murray Hill, NJ, USA

Joël Ouaknine University of Oxford, Oxford, UK; Max Planck Institute for Software Systems, Saarbrücken, Germany

George J. Pappas University of Pennsylvania, Philadelphia, PA, USA

Corina S. Păsăreanu NASA Ames Research Center, Moffett Field, CA, USA

Doron Peled Bar Ilan University, Ramat Gan, Israel

Nir Piterman University of Leicester, Leicester, UK

André Platzer Carnegie Mellon University, Pittsburgh, PA, USA

Amir Pnueli New York University, New York, USA; The Weizmann Institute of Science, Rehovot, Israel

Andreas Podelski University of Freiburg, Freiburg, Germany

Shaz Qadeer Microsoft Research, Redmond, WA, USA

Jean-François Raskin Université libre de Bruxelles, Brussels, Belgium

A.W. Roscoe University of Oxford, Oxford, UK

Andrey Rybalchenko Microsoft Research, Cambridge, UK

David A. Schmidt Kansas State University, Manhattan, KS, USA

Koushik Sen University of California, Berkeley, Berkeley, CA, USA

Sanjit A. Seshia University of California, Berkeley, Berkeley, CA, USA

Natarajan Shankar SRI International, Menlo Park, CA, USA

Natasha Sharygina Università della Svizzera italiana, Lugano, Switzerland

A. Prasad Sistla University of Illinois, Chicago, IL, USA

Scott A. Smolka Stony Brook University, Stony Brook, NY, USA

Muralidhar Talupur Intel's Strategic CAD Labs, Hillsboro, OR, USA

Cesare Tinelli The University of Iowa, Iowa City, IA, USA

Tayssir Touili CNRS, Paris, France

Stavros Tripakis University of California, Berkeley, Berkeley, CA, USA; Aalto University, Espoo, Finland

Helmut Veith Technische Universität Wien, Vienna, Austria

Igor Walukiewicz CNRS, University of Bordeaux, Bordeaux, France

James Worrell University of Oxford, Oxford, UK